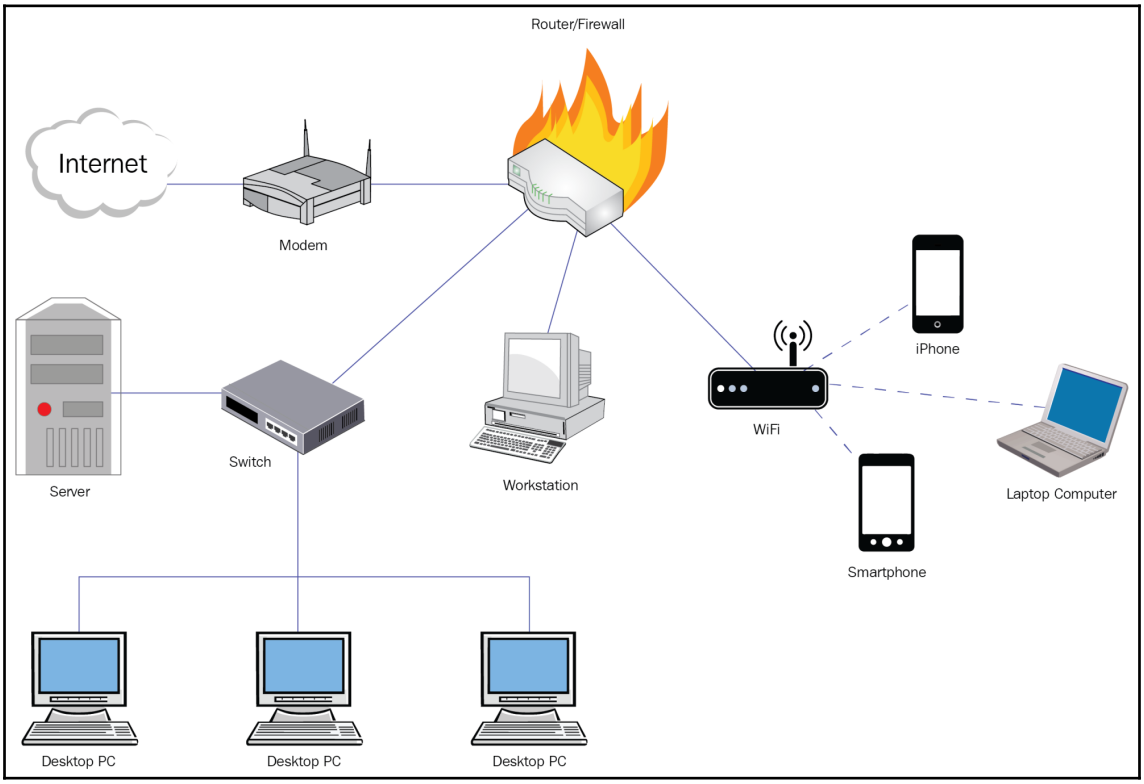
Chapter 1: Introduction to Network Vulnerability Scanning




```
C:\Users\admin>nmap -Pn 192.168.100.142
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-11 14:04 Arabian Standard Time
Nmap scan report for 192.168.100.142
Host is up (0.00064s latency).
All 1000 scanned ports on 192.168.100.142 are closed
MAC Address: 00:0C:29:DF:F9:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 28.07 seconds
```

```
C:\Users\admin>nmap -sS -Pn -p80 192.168.100.143
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-11 14:29 Arabian Standard Time
Nmap scan report for 192.168.100.143
Host is up (0.00s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:DF:F9:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 27.77 seconds
```

1 - 10 of 26

Vulnerability	Severity	QoD	Host	Location	Created
HTTP Server type and version	0.0 (Log)	80%	192.168.1.107	5357/tcp	Mon Jun 11 22:42:12 2018
SMB NativeLanMan	0.0 (Log)	95%	192.168.1.107	445/tcp	Mon Jun 11 22:37:31 2018
DIRB (NASL wrapper)	0.0 (Log)	80%	192.168.1.107	5357/tcp	Mon Jun 11 22:49:45 2018
DIRB (NASL wrapper)	0.0 (Log)	80%	192.168.1.107	2869/tcp	Mon Jun 11 22:49:45 2018
DIRB (NASL wrapper)	0.0 (Log)	80%	192.168.1.107	443/tcp	Mon Jun 11 22:49:48 2018
DIRB (NASL wrapper)	0.0 (Log)	80%	192.168.1.107	443/tcp	Mon Jun 11 22:49:48 2018
SSL/TLS: Certificate - Self-Signed Certificate Detection	0.0 (Log)	98%	192.168.1.107	443/tcp	Mon Jun 11 22:47:07 2018

Log Method

Details: Check for SMB accessible registry (OID: 1.3.6.1.4.1.25623.1.0.10400)

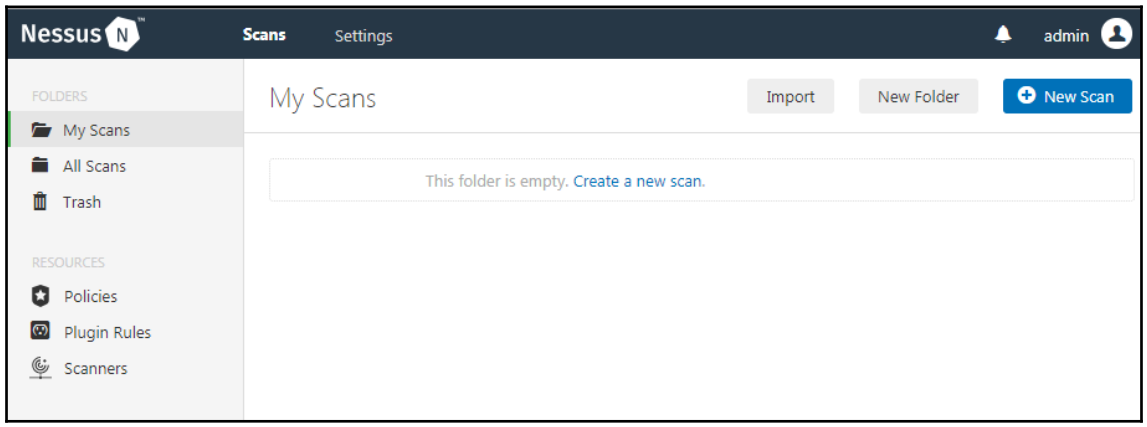
Version used: $Revision: 7186 $

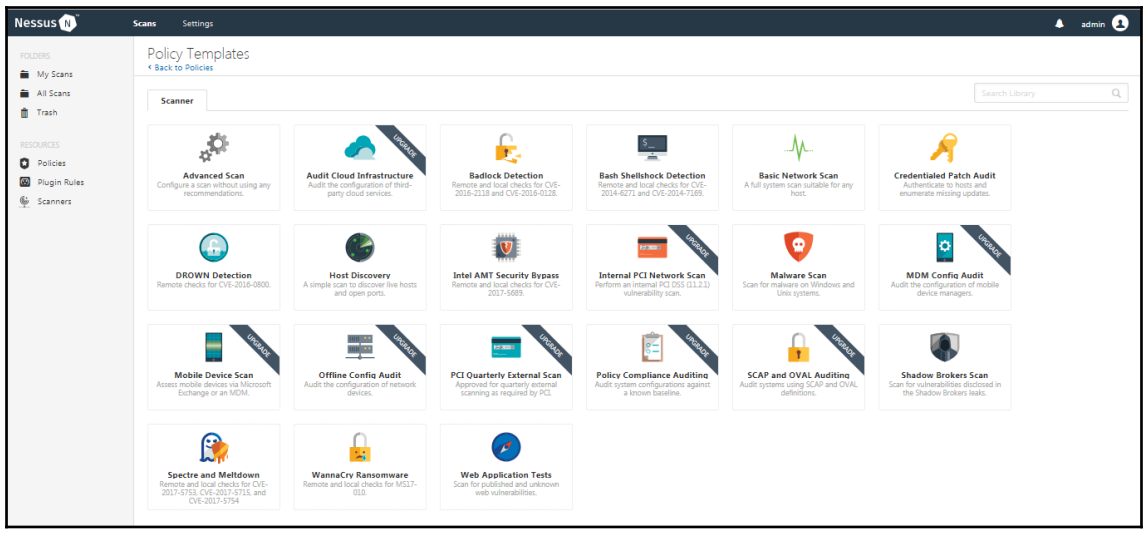
References

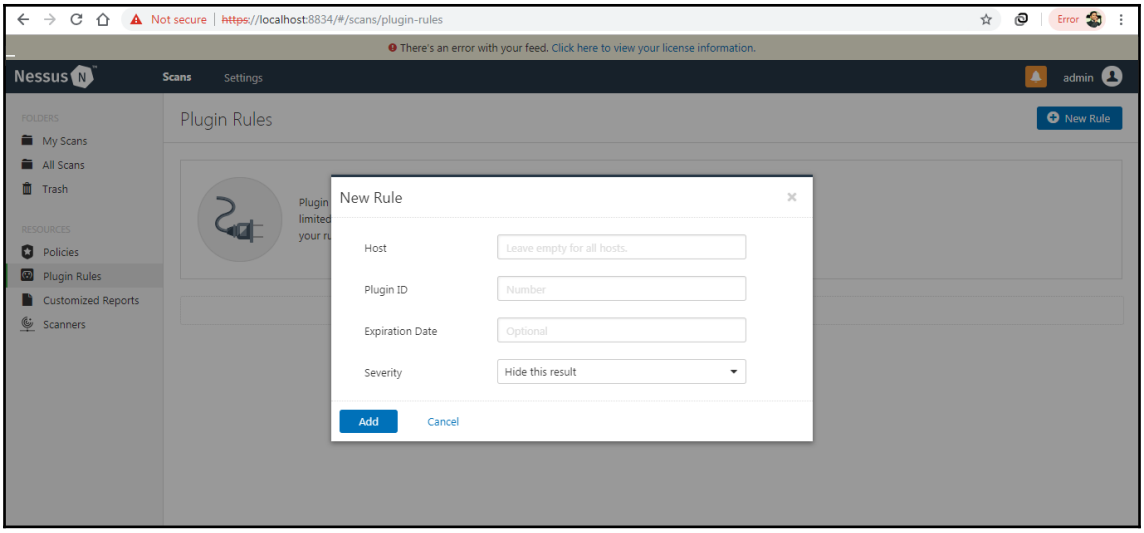
Other: http://docs.greenbone.net/GSM-Manual/gos-3.1/en/scanning.html#requirements-on-target-systems-with-windows

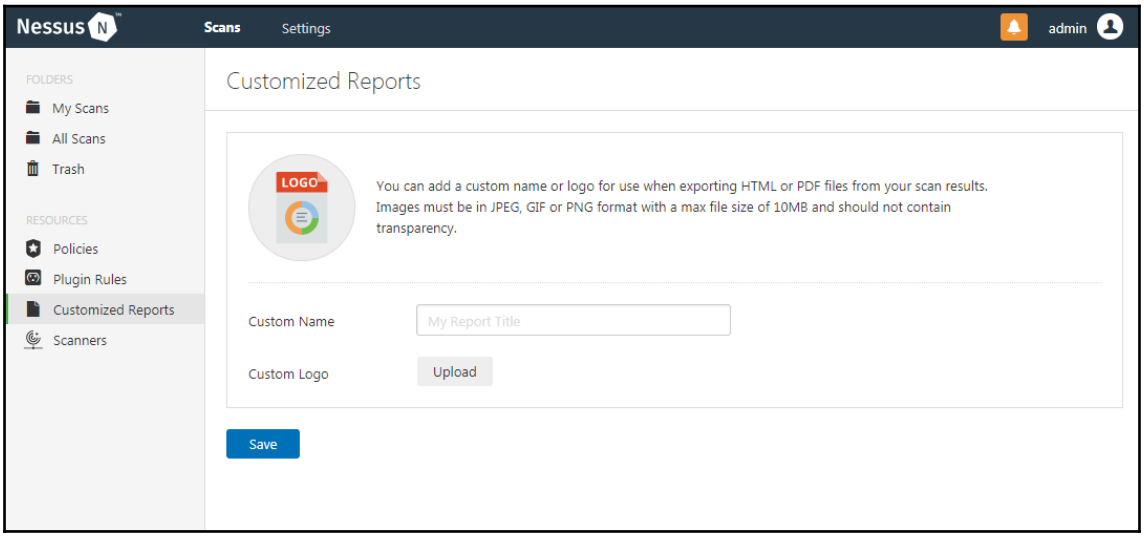
http://docs.greenbone.net/GSM-Manual/gos-4/en/vulnerabilitymanagement.html#requirements-on-target-systems-with-windows

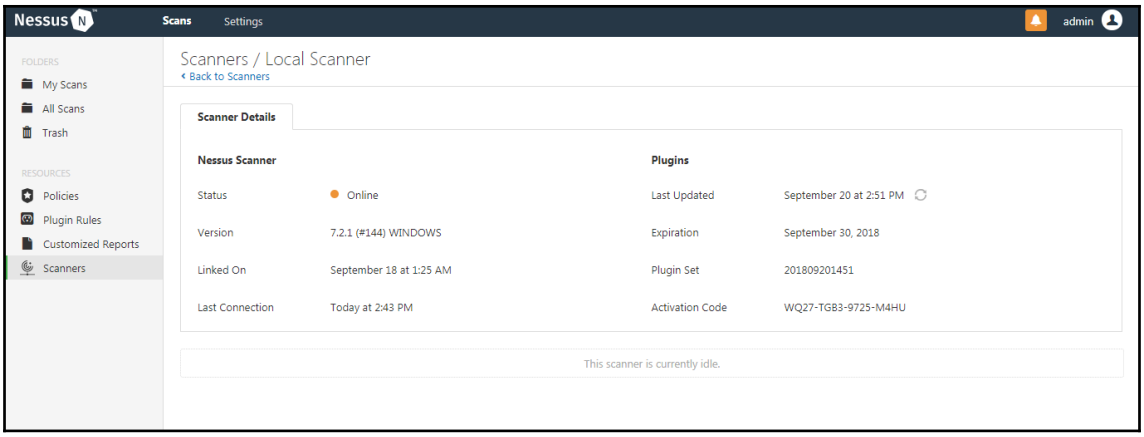
Chapter 2: Understanding Network Scanning Tools

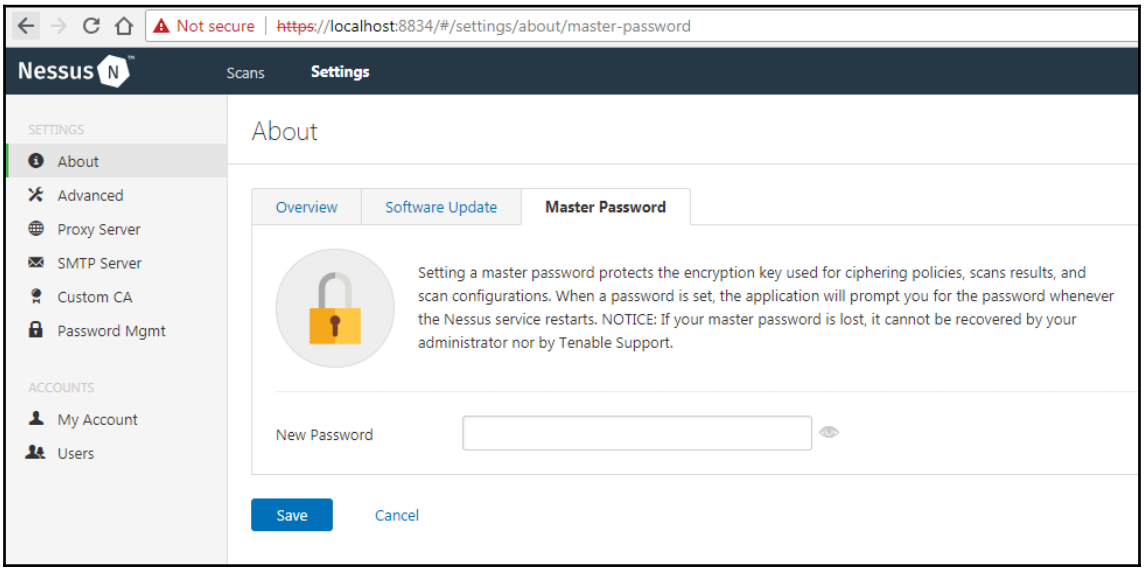


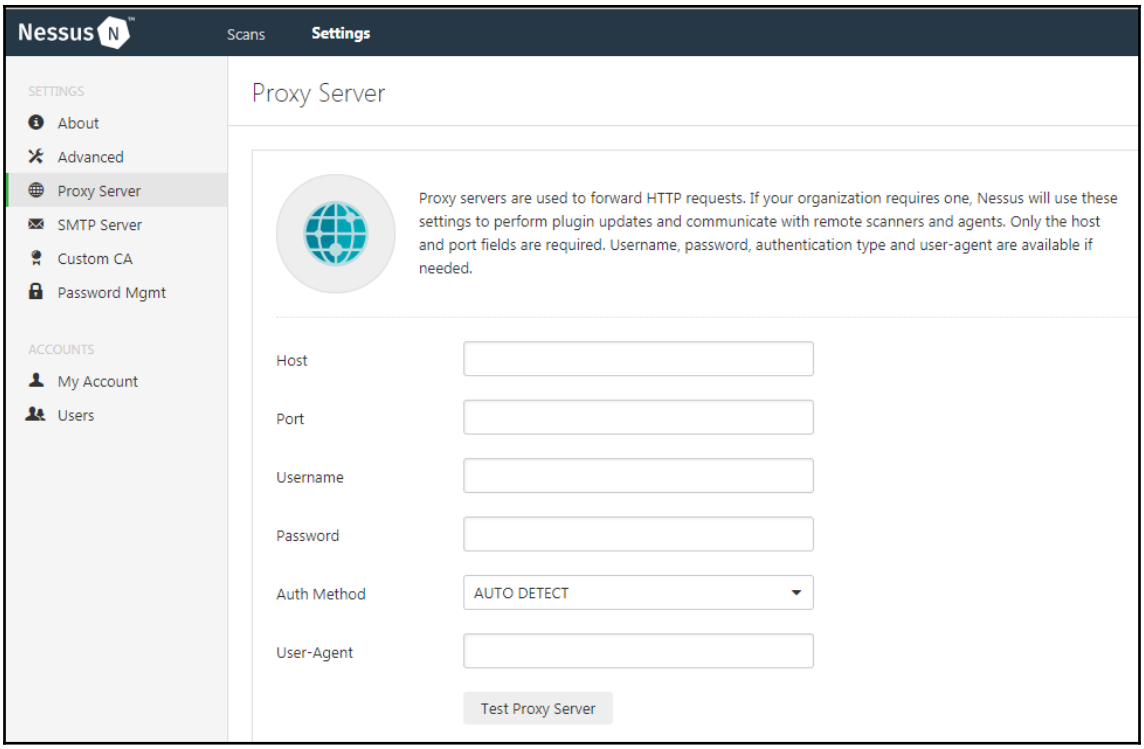


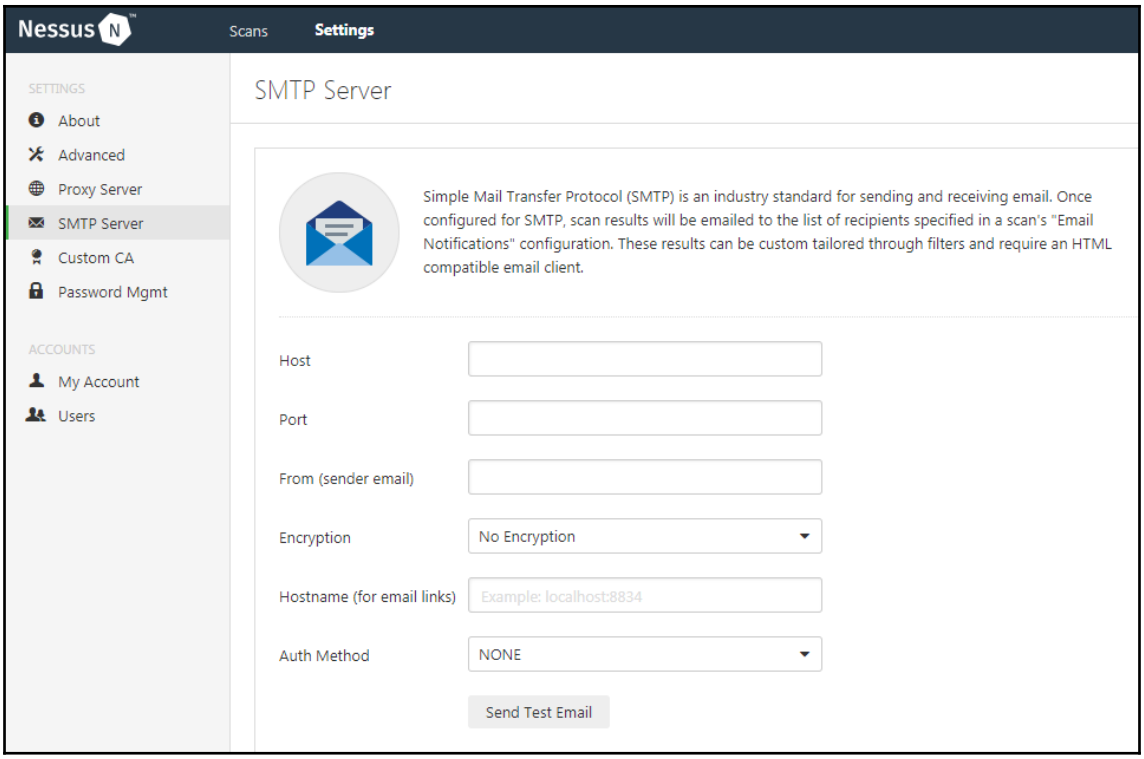

Not secure | https://localhost:8834/#/scans/plugin-rules
There's an error with your feed. Click here to view your license information.
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Plugin Rules
New Rule
New Rule
Host
Leave empty for all hosts.
Plugin ID
Number
Expiration Date
Optional
Severity
Hide this result
Add
Cancel

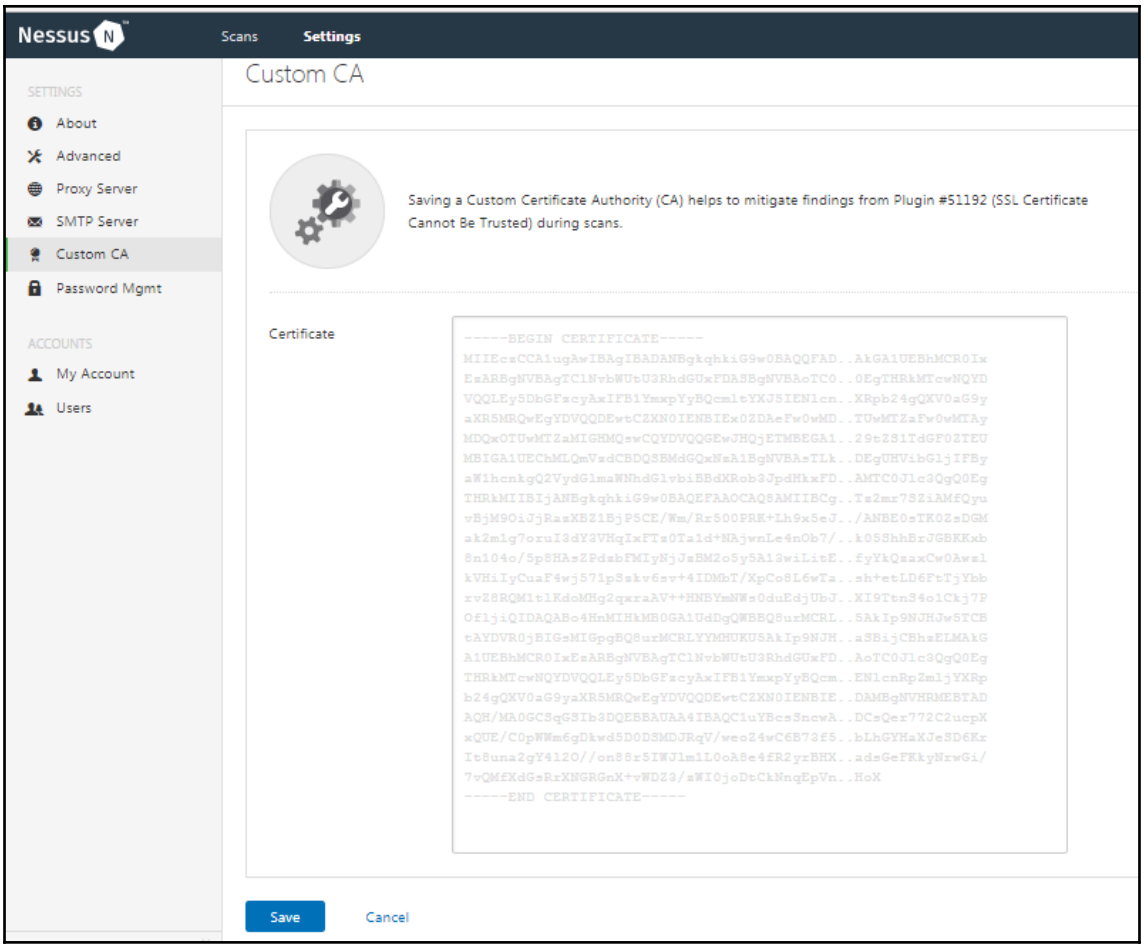

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Customized Reports
LOGO
You can add a custom name or logo for use when exporting HTML or PDF files from your scan results. Images must be in JPEG, GIF or PNG format with a max file size of 10MB and should not contain transparency.
Custom Name
My Report Title
Custom Logo
Upload
Save

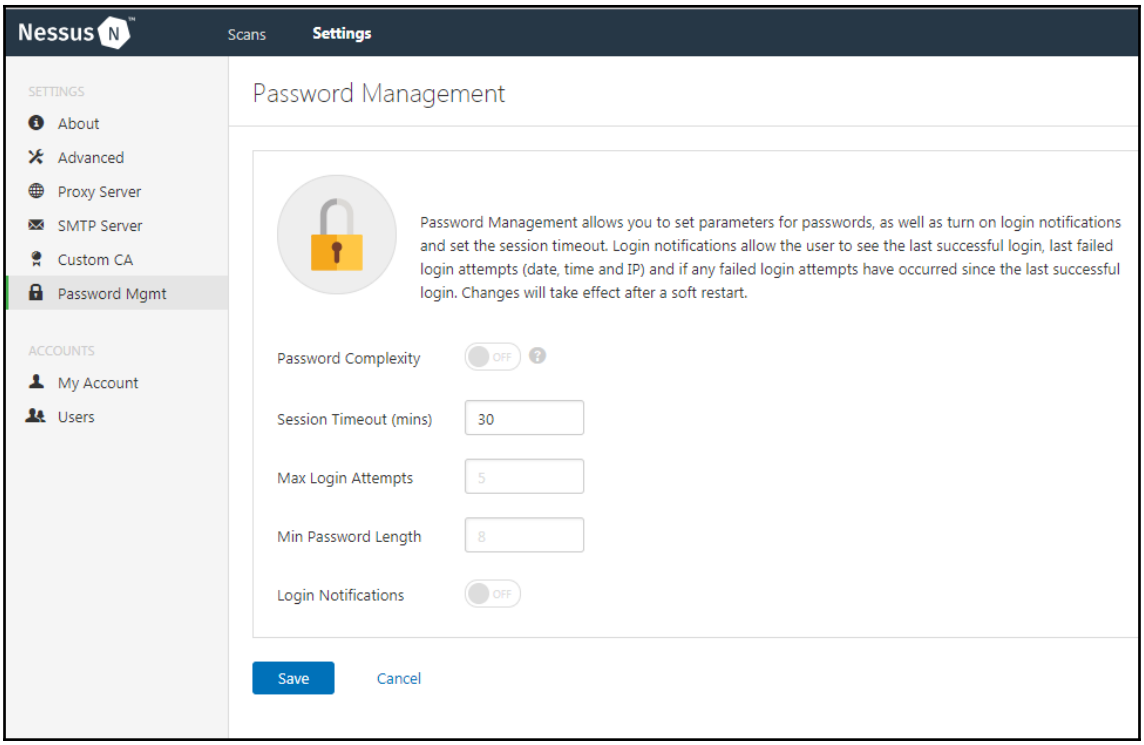

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scanners / Local Scanner
Back to Scanners
Scanner Details
Nessus Scanner
Status
Online
Version
7.2.1 (#144) WINDOWS
Linked On
September 18 at 1:25 AM
Last Connection
Today at 2:43 PM
Plugins
Last Updated
September 20 at 2:51 PM
Expiration
September 30, 2018
Plugin Set
201809201451
Activation Code
WQ27-TGB3-9725-M4HU
This scanner is currently idle.

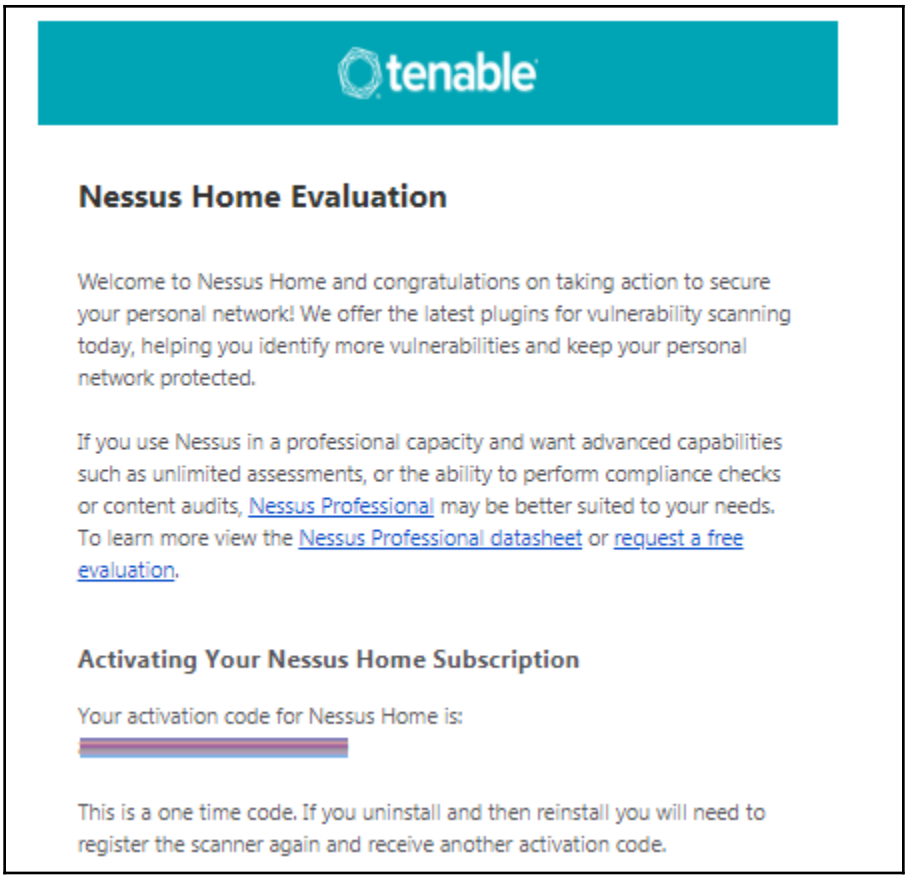

Not secure
https://localhost:8834/#/settings/about/master-password
Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
About
Overview
Software Update
Master Password
Setting a master password protects the encryption key used for ciphering policies, scans results, and scan configurations. When a password is set, the application will prompt you for the password whenever the Nessus service restarts. NOTICE: If your master password is lost, it cannot be recovered by your administrator nor by Tenable Support.
New Password
Save
Cancel


Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Proxy Server
Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus will use these settings to perform plugin updates and communicate with remote scanners and agents. Only the host and port fields are required. Username, password, authentication type and user-agent are available if needed.
Host
Port
Username
Password
Auth Method
AUTO DETECT
User-Agent
Test Proxy Server


Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
SMTP Server
Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, scan results will be emailed to the list of recipients specified in a scan's "Email Notifications" configuration. These results can be custom tailored through filters and require an HTML compatible email client.
Host
Port
From (sender email)
Encryption
No Encryption
Hostname (for email links)
Example: localhost:8834
Auth Method
NONE
Send Test Email


Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Custom CA
Saving a Custom Certificate Authority (CA) helps to mitigate findings from Plugin #51192 (SSL Certificate Cannot Be Trusted) during scans.
Certificate
-----BEGIN CERTIFICATE-----
MIIEcxCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD..AkGA1UEBhMCR0Ix
EzARBgNVBAgTClNvbWUtU3RhdGUxFDASBgNVBAoTC0..0EgTHRkMTcwNQYD
VQQLEy5DbGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcn..XRpb24gQXV0aG9y
aXR5MRQwEgYDVQQDEwtCZXN0IENBIEx0ZDAeFw0wMD..TUwMTZaFw0wMTAy
MDQwOTUwMTZaMIGHMQswCQYDVQQGEwJHQjETMBEGA1..29tZS1TdGF0ZTEU
MBIGA1UEChMLQmVzdCBDQSBMdGQxNzA1BgNVBAsTLk..DEgUHVibGljIFBy
aW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFD..AMTC0J1c3QgQ0Eg
THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg..Tz2mr7SZiAMfQyu
vBjM9OiJjRaxXBZ1BjPSCE/Wm/Rr500PRK+Lh9x5eJ../ANBE0sTK0ZsDGM
ak2m1g7oruI3dY3VHqIwFTs0Ta1d+NAjwnLe4nOb7/..k05ShhBrJGBKKxb
8n104o/5p8HAsZPdxbfMIyNjJsBM2o5y5A13wiLitE..fyYkQxaxCw0Awxl
kVHiIyCuaF4wj571pSskv6sv+4IDMbT/XpCo8L6wTa..sh+etLD6FtTjYbb
rvZ8RQM1tlKdoMHg2qxrAV++HNBYmNWs0duEdjUbJ..XI9Ttn34o1Ckj7P
Of1jiQIDAQABo4HnMIHkMB0GA1UdDgQWBBQ8urMCRL..5AkIp9NJHJw5TCB
tAYDVR0jBIGsMIGpgBQ8urMCRLYYMHUKU5AkIp9NJH..aSBijCBhzELMAkG
A1UEBhMCR0IxEzARBgNVBAgTC1NvbWUtU3RhdGUxFD..AoTC0J1c3QgQ0Eg
THRkMTcwNQYDVQQLEy5DbGFzcyAxIFB1YmxpYyBQcm..ENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MRQwEgYDVQQDEwtCZXN0IENBIE..DAMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBBAUAA4IBAQC1uYBcsSncwA..DCsQer772C2ucpX
xQUE/C0pWWm6gDkwd5D0DSMDJRqV/weo24wC6B73f5..bLhGYHaXJeSD6Kr
It8una2gY4l2O//on88r5IWJlm1L0oA8e4fR2yrBHX..adsGeFKkyNrwGi/
7vQMfXdGsRrXNGRGnX+vWDZ3/sWI0joDtCkNnqEpVn..HoX
-----END CERTIFICATE-----
Save
Cancel


Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Password Management
Password Management allows you to set parameters for passwords, as well as turn on login notifications and set the session timeout. Login notifications allow the user to see the last successful login, last failed login attempts (date, time and IP) and if any failed login attempts have occurred since the last successful login. Changes will take effect after a soft restart.
Password Complexity
OFF
Session Timeout (mins)
30
Max Login Attempts
5
Min Password Length
8
Login Notifications
OFF
Save
Cancel



tenable

Nessus Home Evaluation

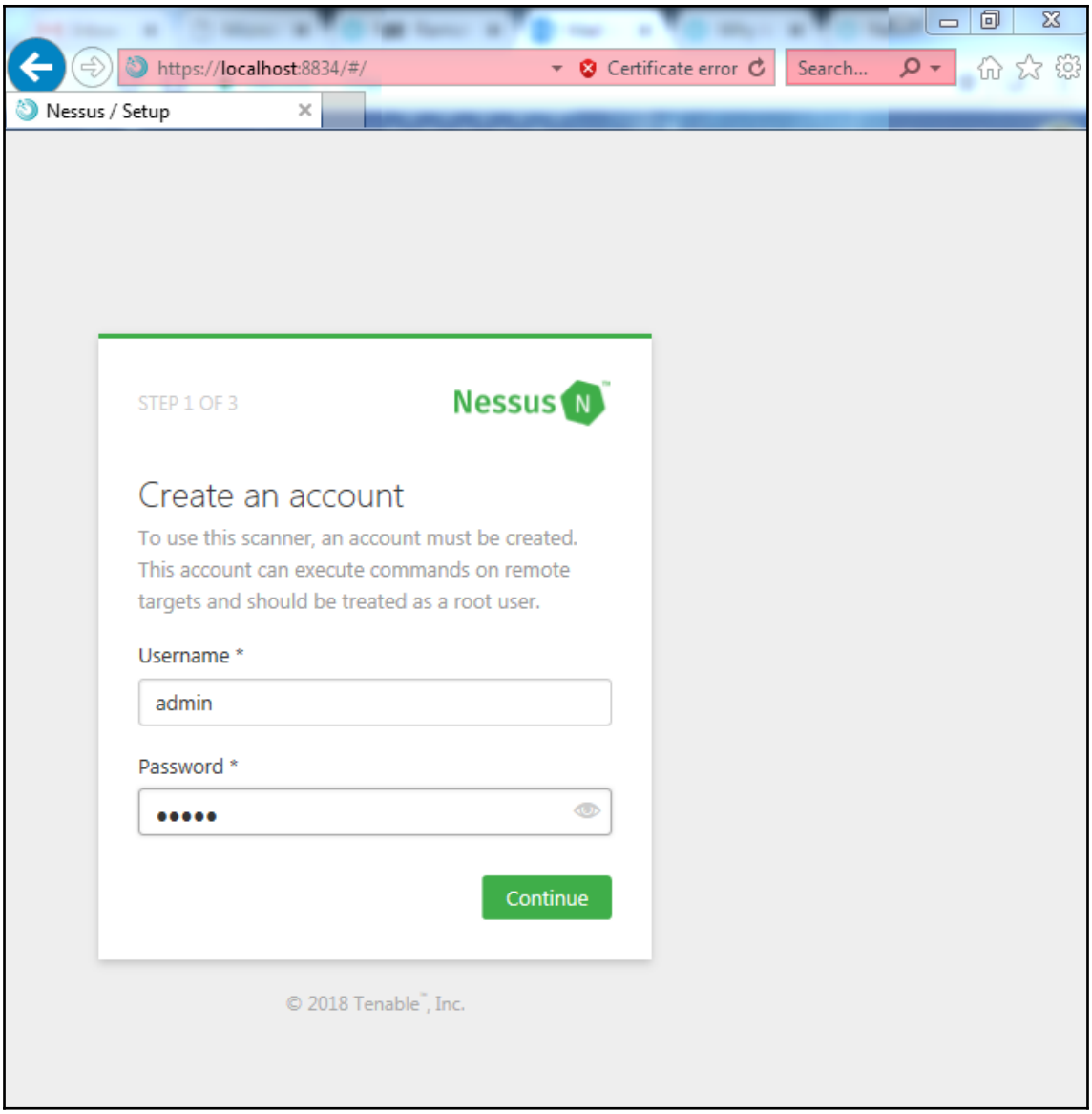
Welcome to Nessus Home and congratulations on taking action to secure your personal network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your personal network protected.

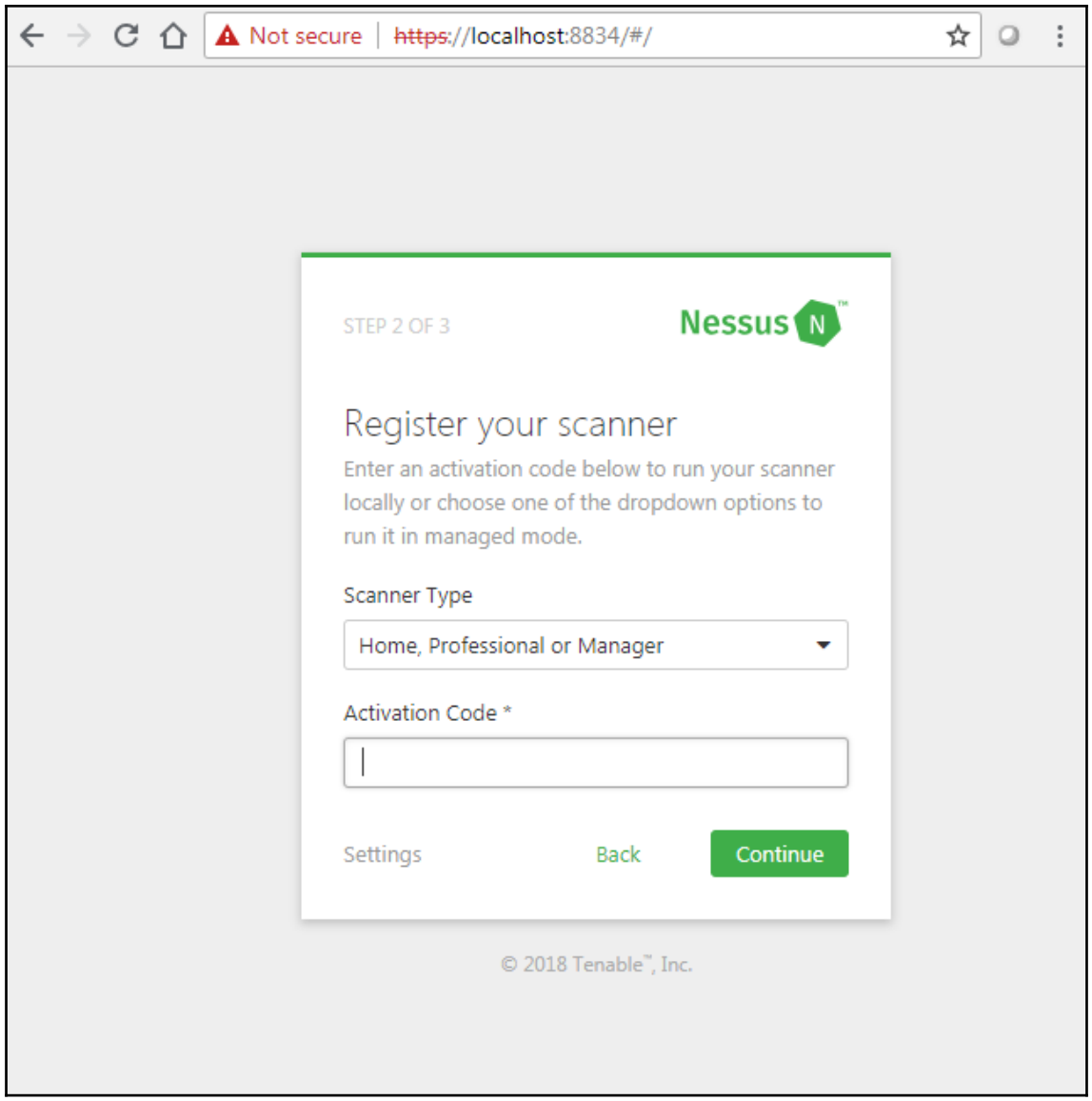
If you use Nessus in a professional capacity and want advanced capabilities such as unlimited assessments, or the ability to perform compliance checks or content audits, Nessus Professional may be better suited to your needs. To learn more view the Nessus Professional datasheet or request a free evaluation.

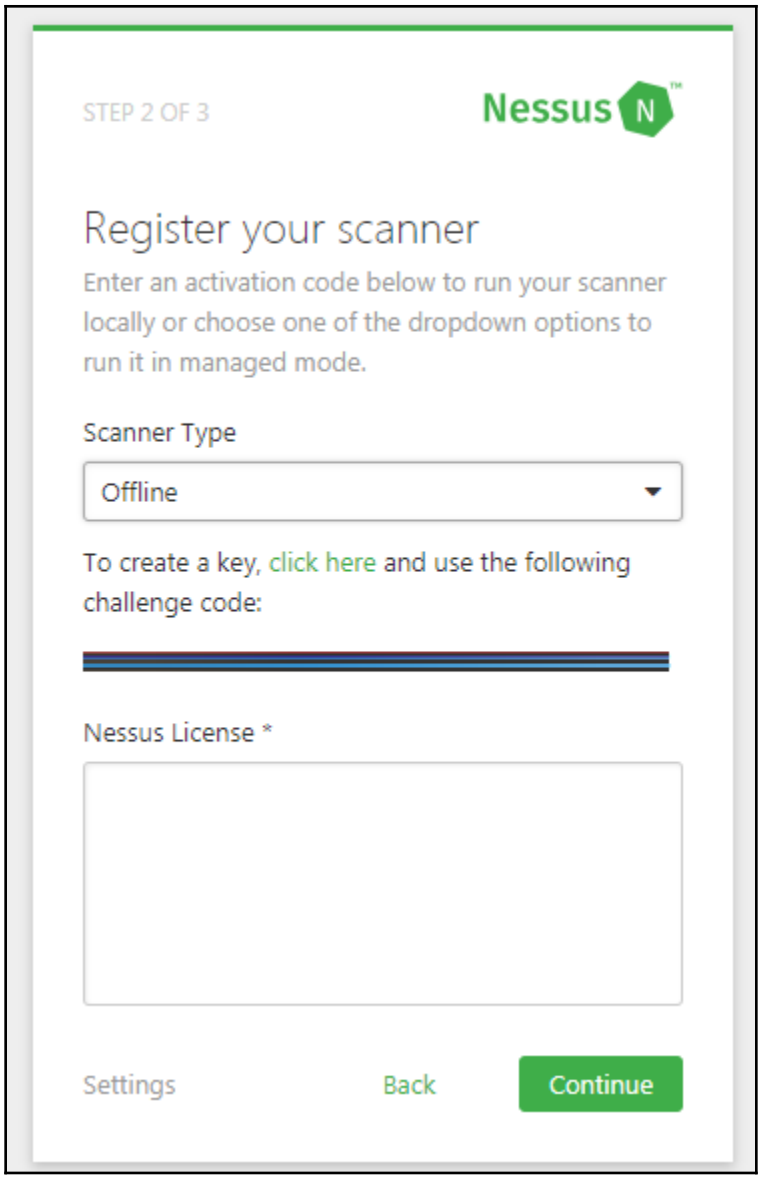
Activating Your Nessus Home Subscription

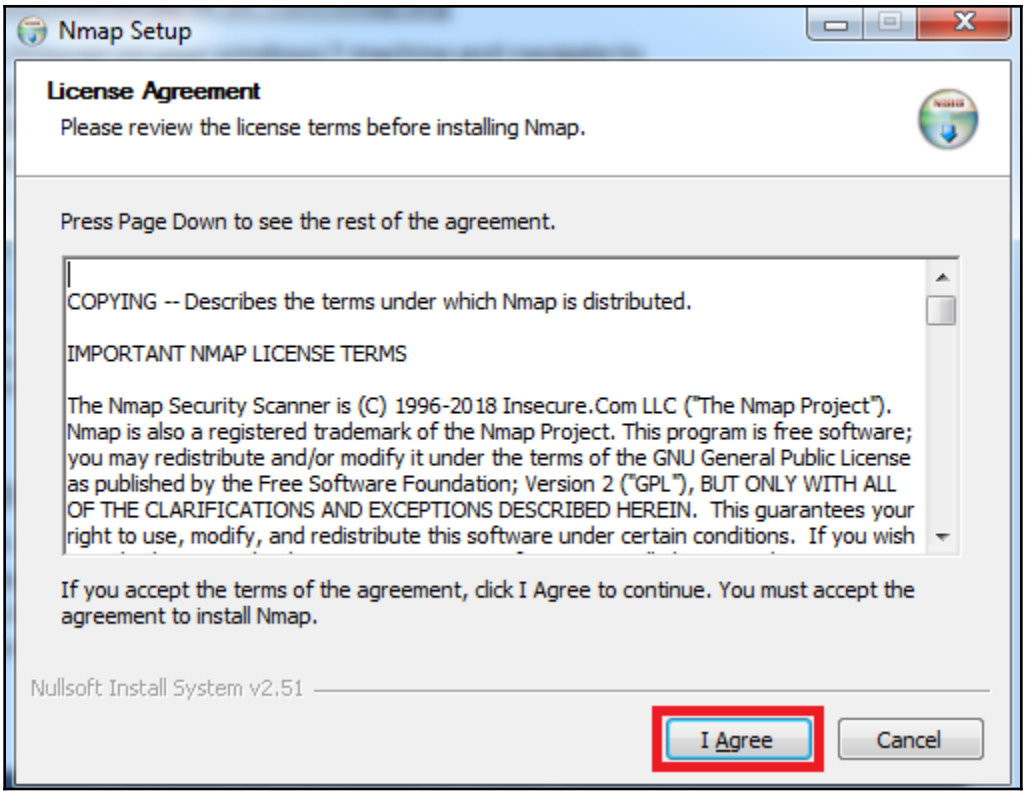
Your activation code for Nessus Home is:

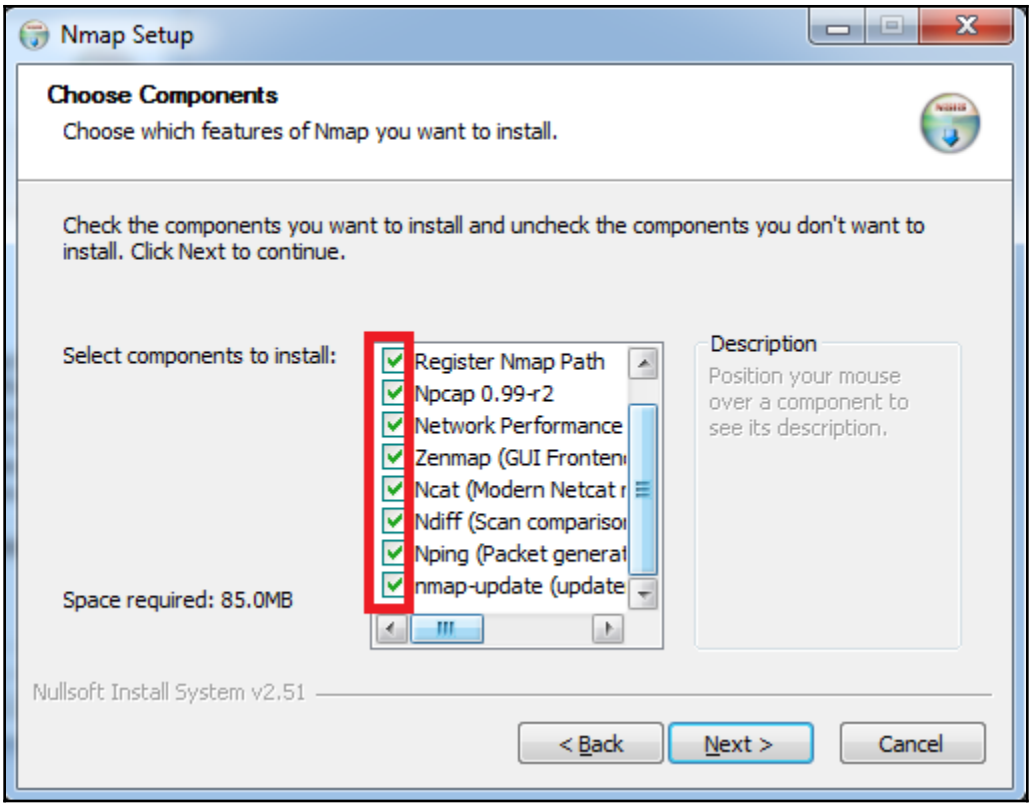
This is a one time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.


https://localhost:8834/#/
Certificate error
Search...
Nessus / Setup
STEP 1 OF 3
Nessus
Create an account
To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.
Username *
admin
Password *
Continue
© 2018 Tenable™, Inc.

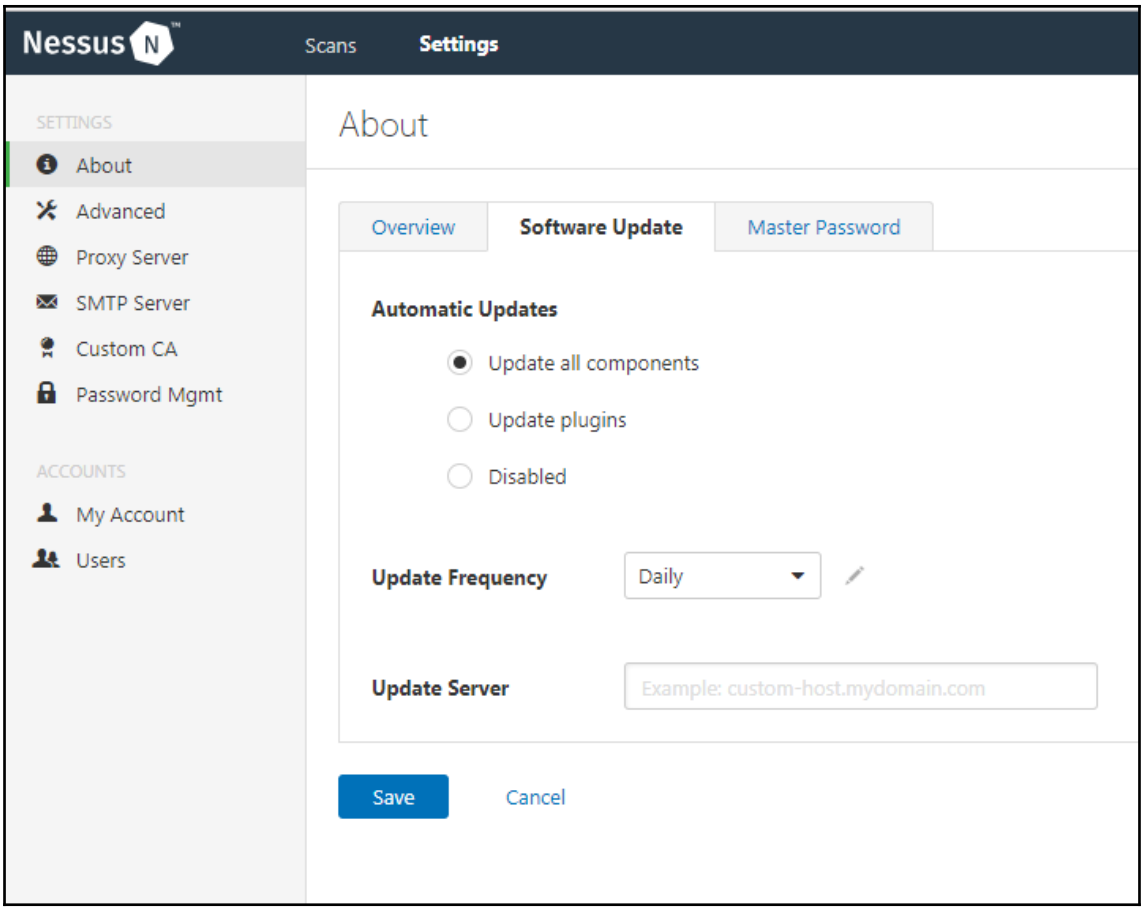

Not secure
https://localhost:8834/#/
STEP 2 OF 3
Nessus
Register your scanner
Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.
Scanner Type
Home, Professional or Manager
Activation Code *
Settings
Back
Continue
© 2018 Tenable™, Inc.

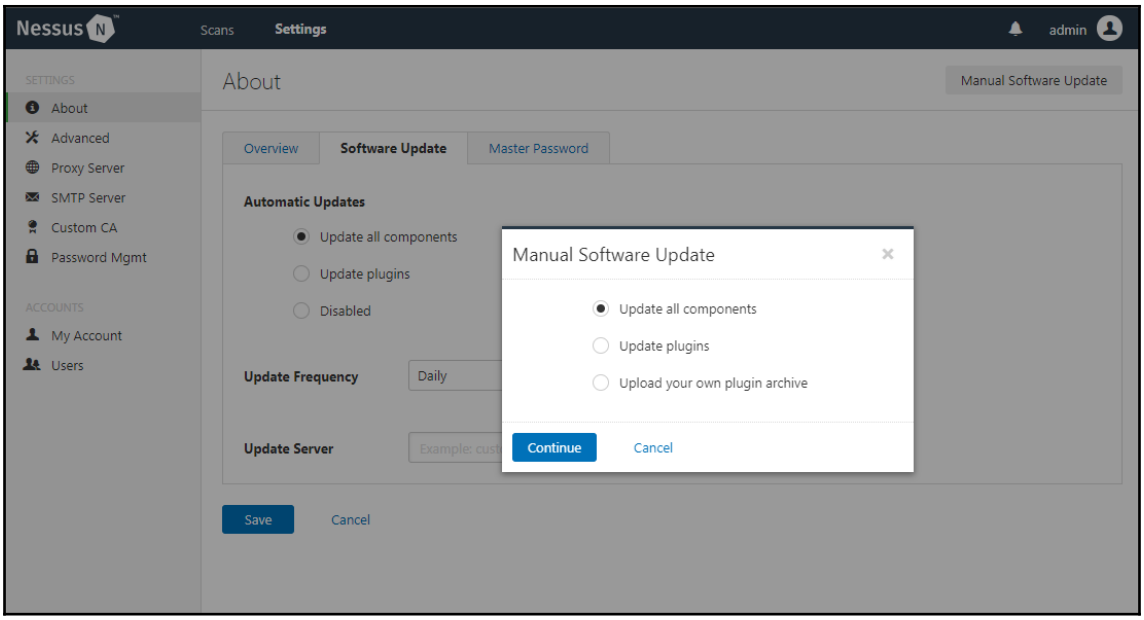

STEP 2 OF 3
Nessus
Register your scanner
Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.
Scanner Type
Offline
To create a key, click here and use the following challenge code:
Nessus License *
Settings
Back
Continue

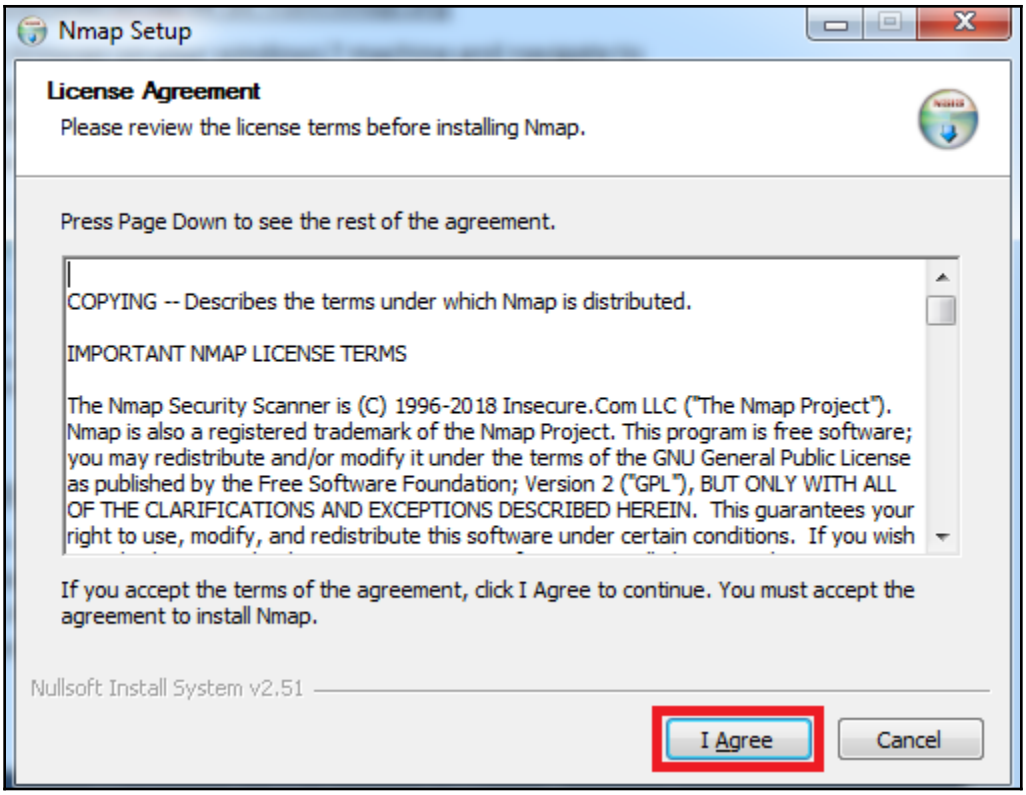

Nmap Setup
License Agreement
Please review the license terms before installing Nmap.
Press Page Down to see the rest of the agreement.
COPYING -- Describes the terms under which Nmap is distributed.
IMPORTANT NMAP LICENSE TERMS
The Nmap Security Scanner is (C) 1996-2018 Insecure.Com LLC ("The Nmap Project").
Nmap is also a registered trademark of the Nmap Project. This program is free software;
you may redistribute and/or modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; Version 2 ("GPL"), BUT ONLY WITH ALL
OF THE CLARIFICATIONS AND EXCEPTIONS DESCRIBED HEREIN. This guarantees your
right to use, modify, and redistribute this software under certain conditions. If you wish
If you accept the terms of the agreement, click I Agree to continue. You must accept the
agreement to install Nmap.
Nullsoft Install System v2.51
I Agree
Cancel

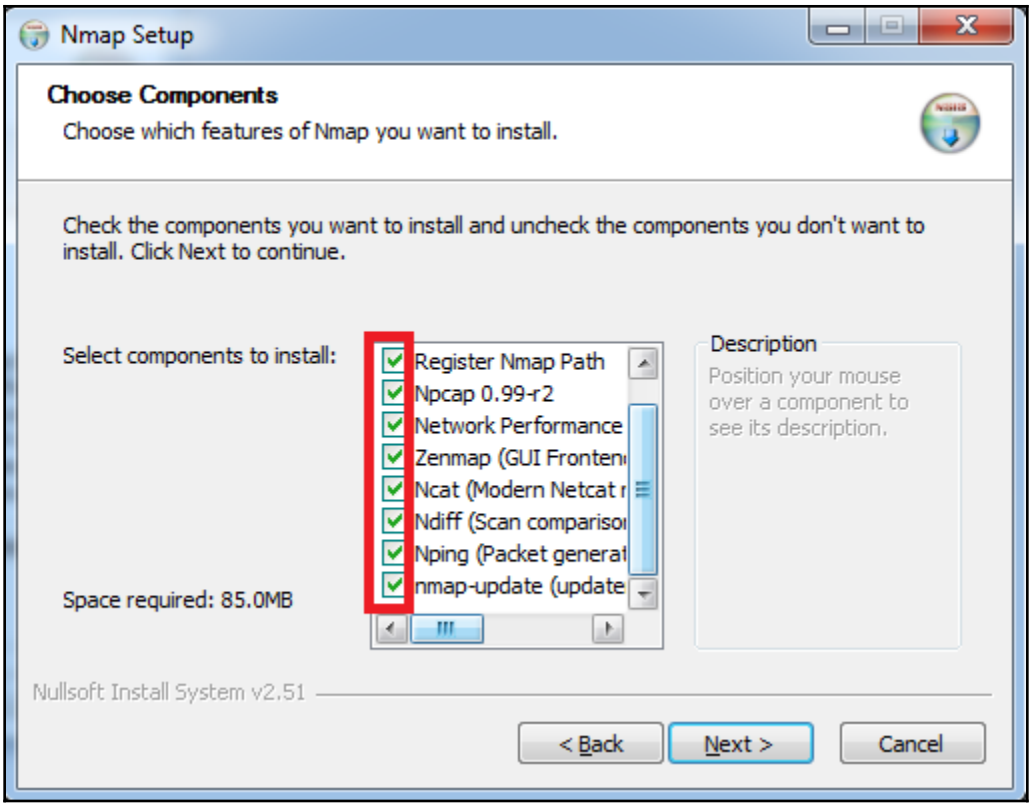



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

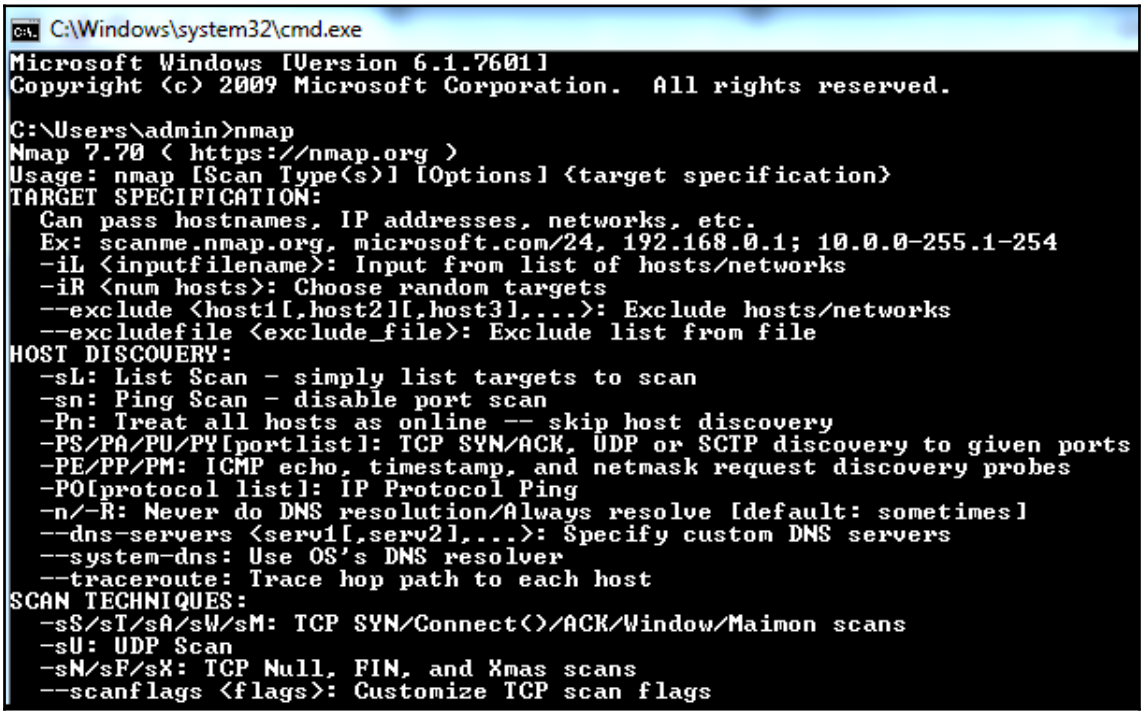

Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
About
Overview
Software Update
Master Password
Automatic Updates
Update all components
Update plugins
Disabled
Update Frequency
Daily
Update Server
Example: custom-host.mydomain.com
Save
Cancel

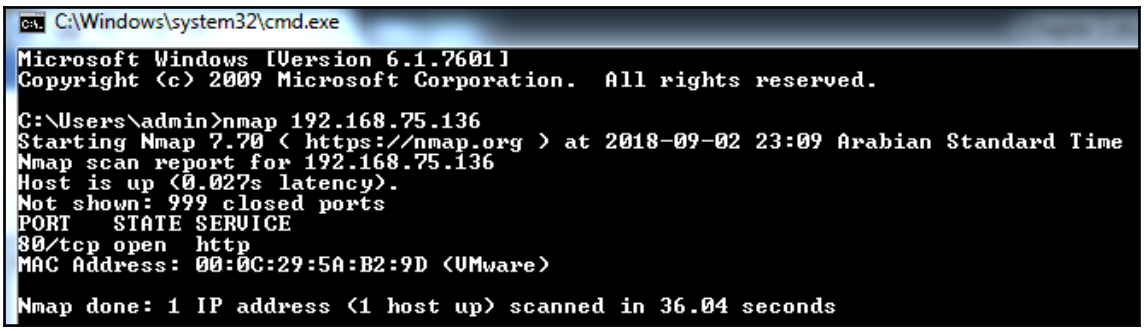

Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
About
Manual Software Update
Overview
Software Update
Master Password
Automatic Updates
Update all components
Update plugins
Disabled
Update Frequency
Daily
Update Server
Save
Cancel
Manual Software Update
Update all components
Update plugins
Upload your own plugin archive
Continue
Cancel

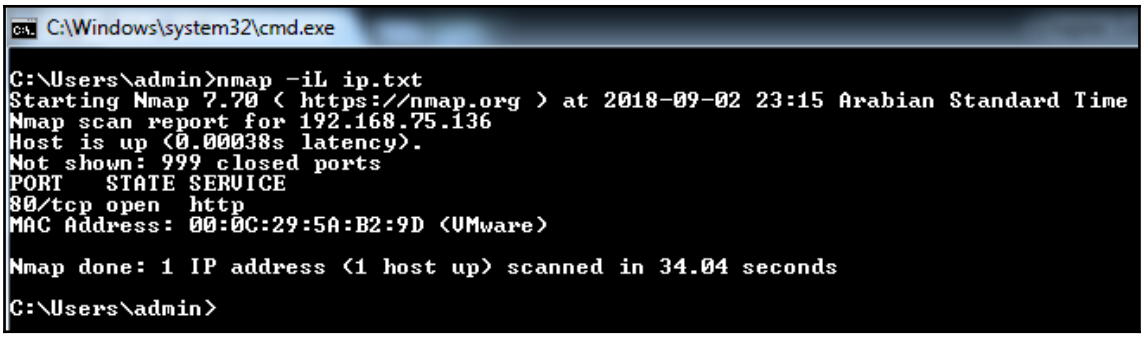

Nmap Setup
License Agreement
Please review the license terms before installing Nmap.
Press Page Down to see the rest of the agreement.
COPYING -- Describes the terms under which Nmap is distributed.
IMPORTANT NMAP LICENSE TERMS
The Nmap Security Scanner is (C) 1996-2018 Insecure.Com LLC ("The Nmap Project").
Nmap is also a registered trademark of the Nmap Project. This program is free software;
you may redistribute and/or modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; Version 2 ("GPL"), BUT ONLY WITH ALL
OF THE CLARIFICATIONS AND EXCEPTIONS DESCRIBED HEREIN. This guarantees your
right to use, modify, and redistribute this software under certain conditions. If you wish
If you accept the terms of the agreement, click I Agree to continue. You must accept the
agreement to install Nmap.
Nullsoft Install System v2.51
I Agree
Cancel

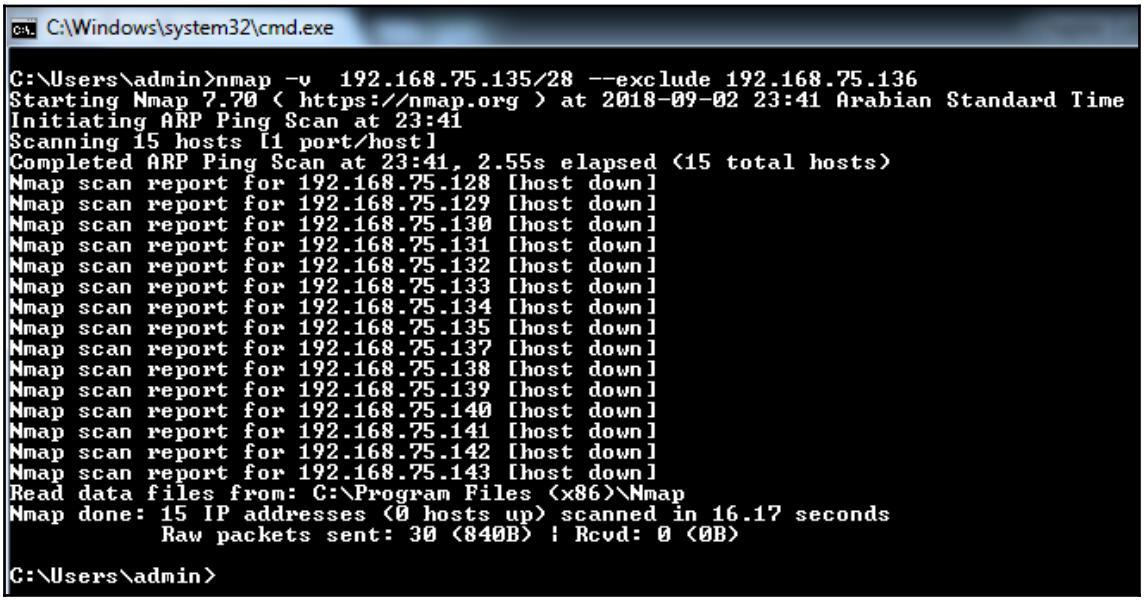

Nmap Setup
Choose Components
Choose which features of Nmap you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Register Nmap Path
Npcap 0.99-r2
Network Performance
Zenmap (GUI Fronten
Ncat (Modern Netcat
Ndiff (Scan comparis
Nping (Packet generat
nmap-update (update
Description
Position your mouse over a component to see its description.
Space required: 85.0MB
Nullsoft Install System v2.51
< Back
Next >
Cancel

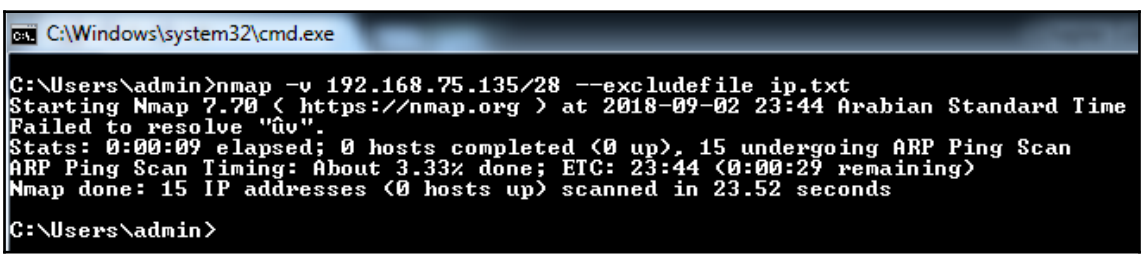
Chapter 3: Port Scanning

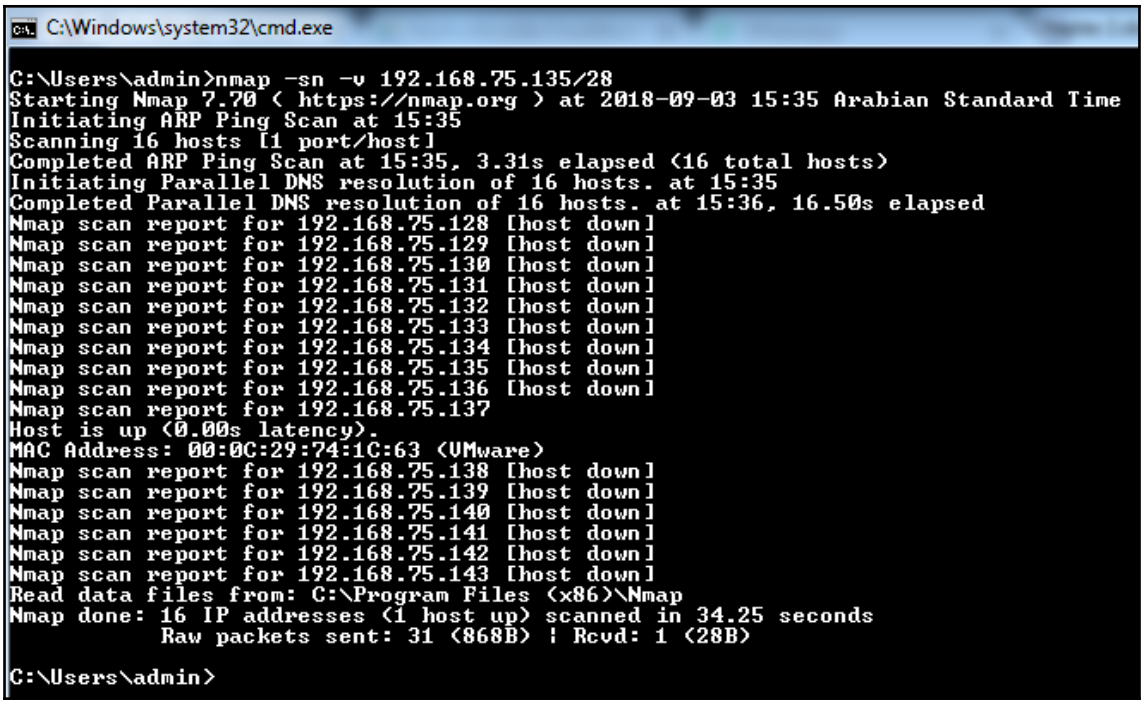


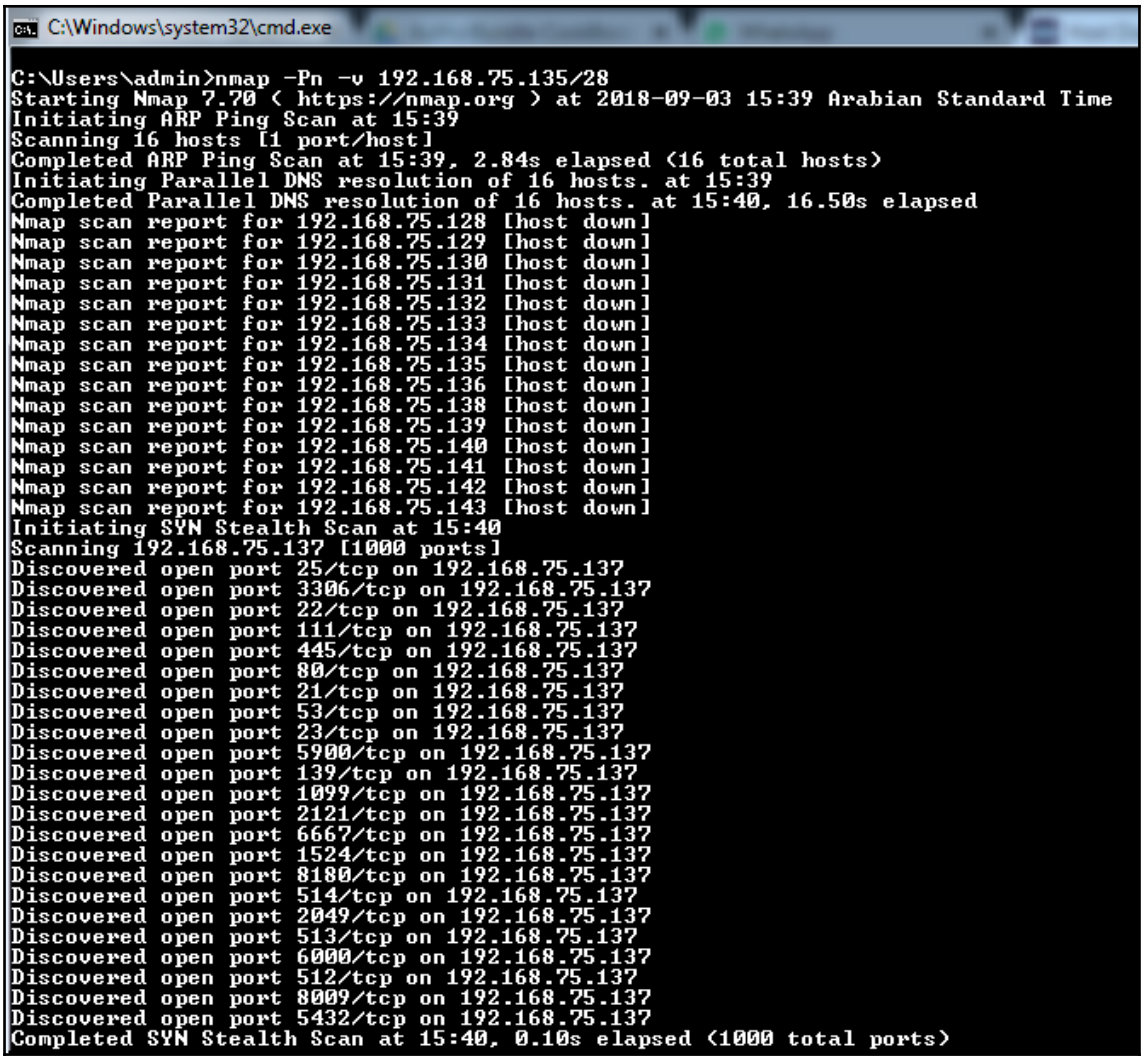


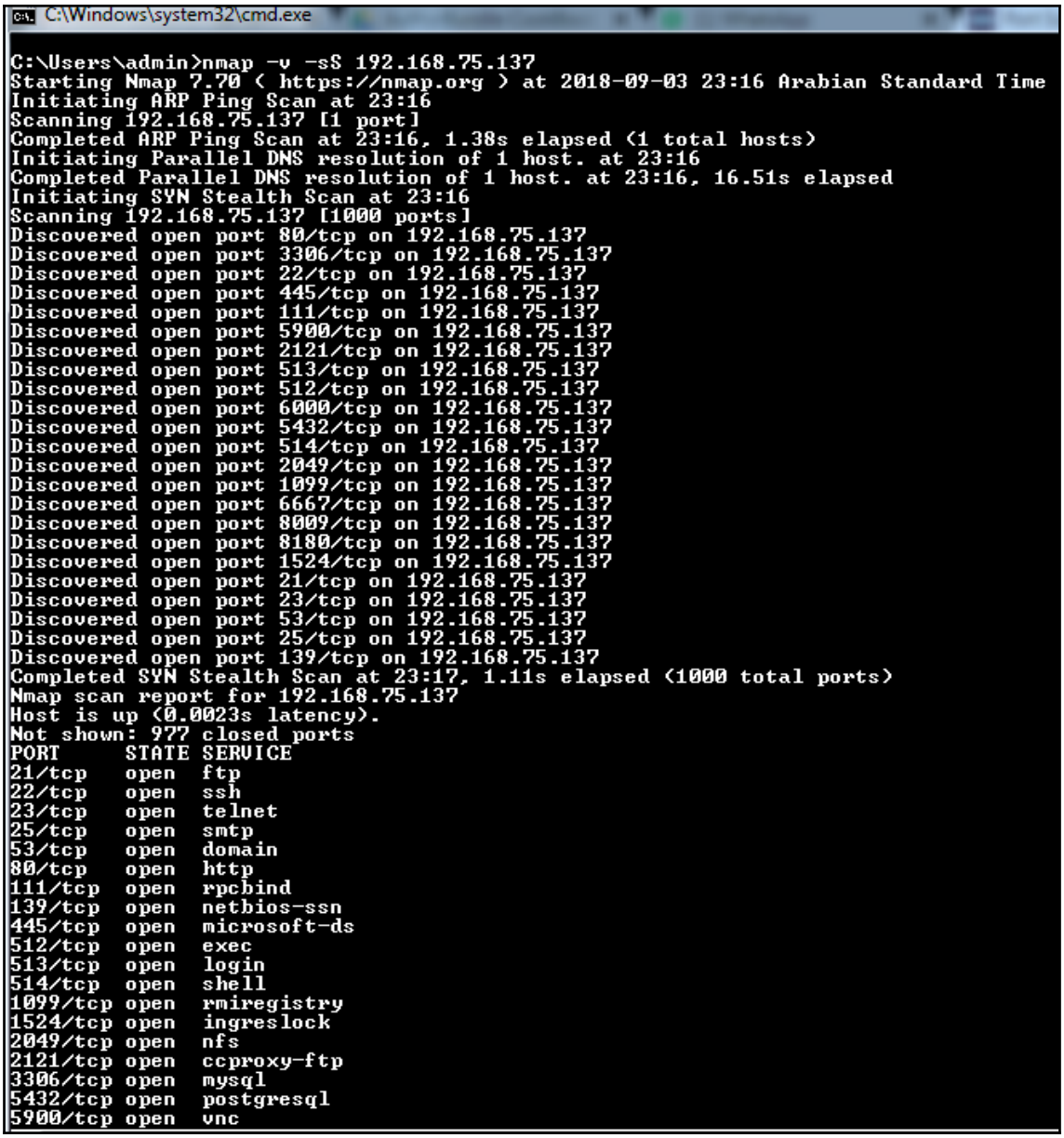

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -iL ip.txt
Starting Nmap 7.70 (https://nmap.org) at 2018-09-02 23:15 Arabian Standard Time
Nmap scan report for 192.168.75.136
Host is up (0.00038s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open http
MAC Address: 00:0C:29:5A:B2:9D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 34.04 seconds
C:\Users\admin>

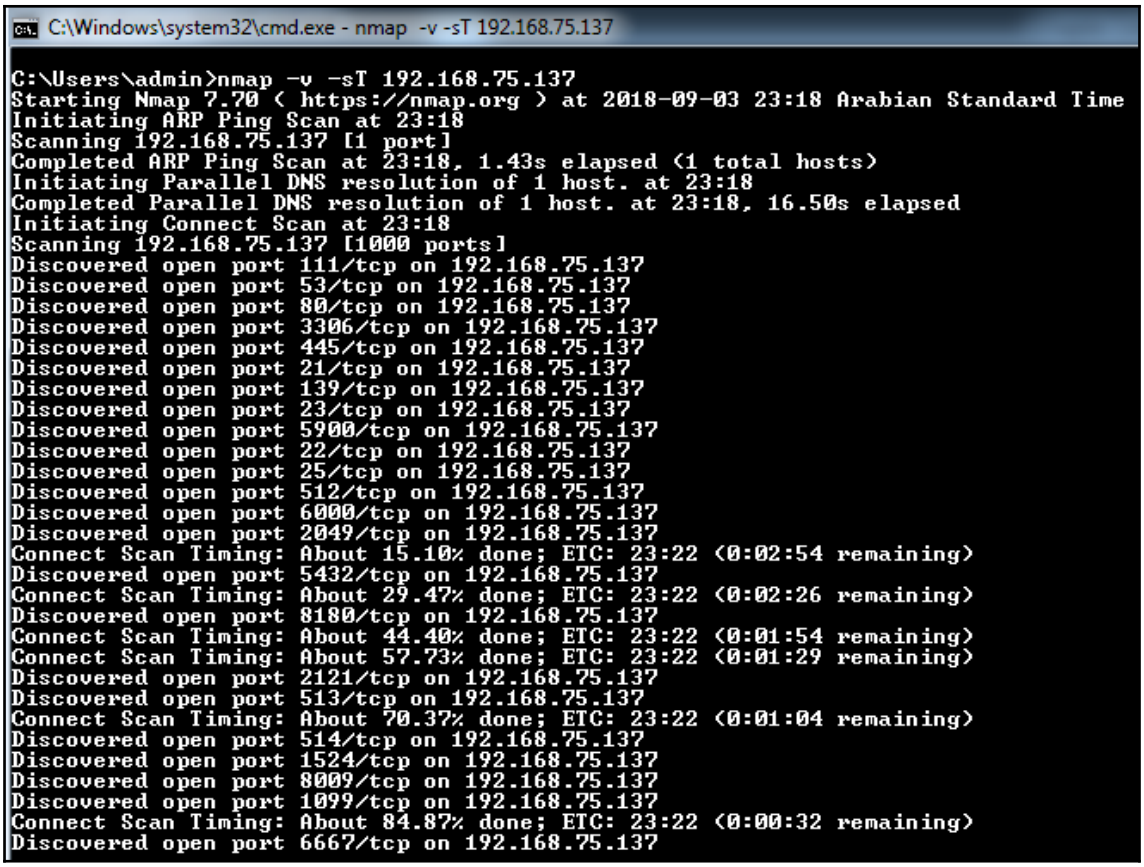

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -v 192.168.75.135/28 --exclude 192.168.75.136
Starting Nmap 7.70 (https://nmap.org) at 2018-09-02 23:41 Arabian Standard Time
Initiating ARP Ping Scan at 23:41
Scanning 15 hosts [1 port/host]
Completed ARP Ping Scan at 23:41, 2.55s elapsed (15 total hosts)
Nmap scan report for 192.168.75.128 [host down]
Nmap scan report for 192.168.75.129 [host down]
Nmap scan report for 192.168.75.130 [host down]
Nmap scan report for 192.168.75.131 [host down]
Nmap scan report for 192.168.75.132 [host down]
Nmap scan report for 192.168.75.133 [host down]
Nmap scan report for 192.168.75.134 [host down]
Nmap scan report for 192.168.75.135 [host down]
Nmap scan report for 192.168.75.137 [host down]
Nmap scan report for 192.168.75.138 [host down]
Nmap scan report for 192.168.75.139 [host down]
Nmap scan report for 192.168.75.140 [host down]
Nmap scan report for 192.168.75.141 [host down]
Nmap scan report for 192.168.75.142 [host down]
Nmap scan report for 192.168.75.143 [host down]
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 15 IP addresses (0 hosts up) scanned in 16.17 seconds
           Raw packets sent: 30 (840B) | Rcvd: 0 (0B)
C:\Users\admin>

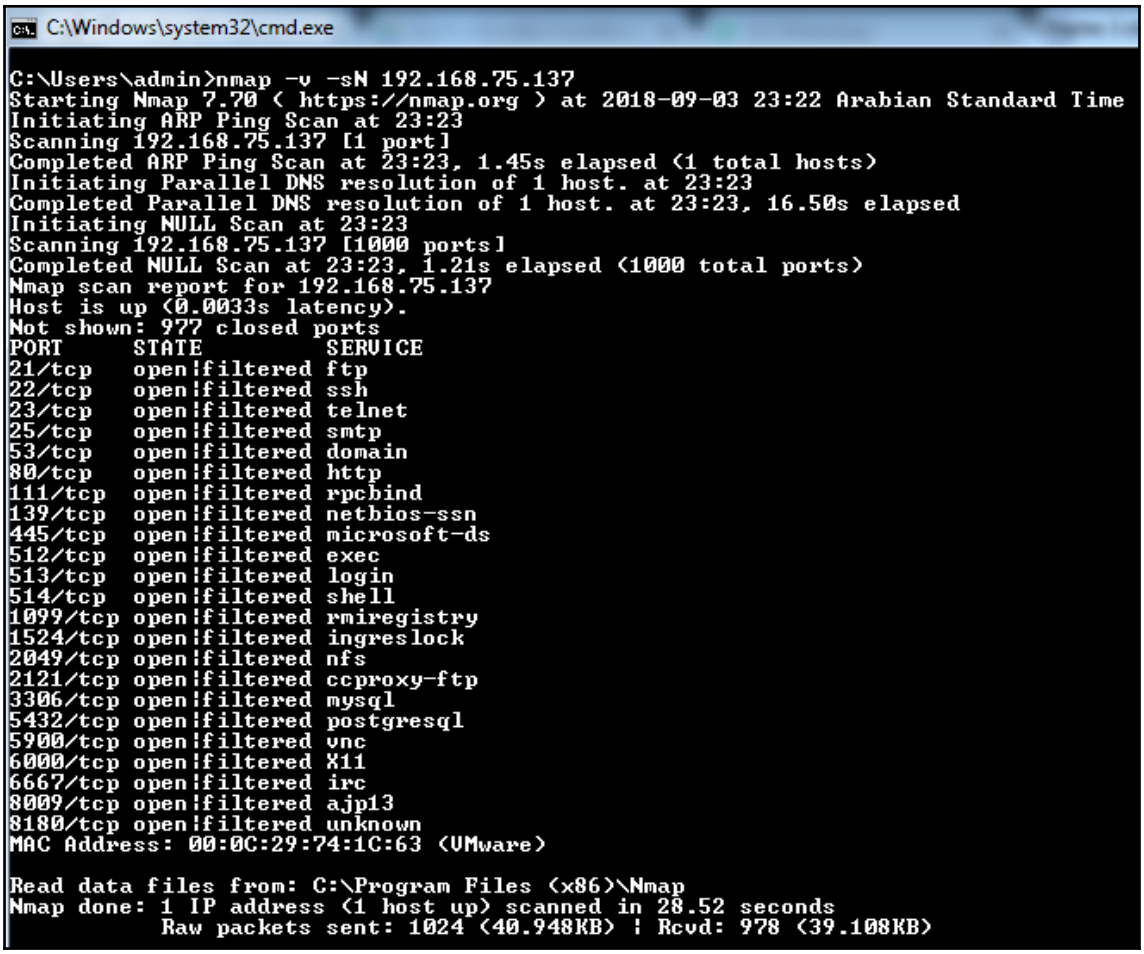

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -v 192.168.75.135/28 --excludefile ip.txt
Starting Nmap 7.70 (https://nmap.org) at 2018-09-02 23:44 Arabian Standard Time
Failed to resolve "ûv".
Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 15 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 3.33% done; ETC: 23:44 (0:00:29 remaining)
Nmap done: 15 IP addresses (0 hosts up) scanned in 23.52 seconds
C:\Users\admin>

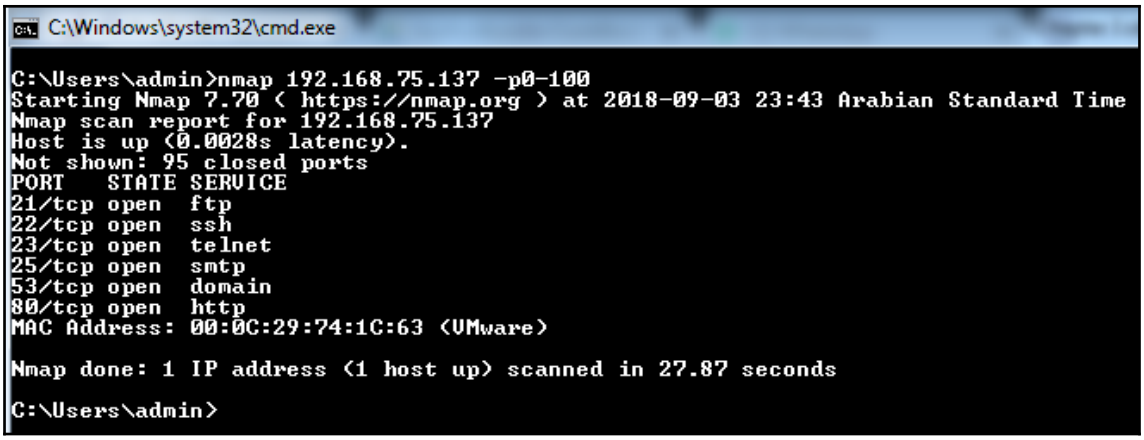

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -sn -v 192.168.75.135/28
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 15:35 Arabian Standard Time
Initiating ARP Ping Scan at 15:35
Scanning 16 hosts [1 port/host]
Completed ARP Ping Scan at 15:35, 3.31s elapsed (16 total hosts)
Initiating Parallel DNS resolution of 16 hosts. at 15:35
Completed Parallel DNS resolution of 16 hosts. at 15:36, 16.50s elapsed
Nmap scan report for 192.168.75.128 [host down]
Nmap scan report for 192.168.75.129 [host down]
Nmap scan report for 192.168.75.130 [host down]
Nmap scan report for 192.168.75.131 [host down]
Nmap scan report for 192.168.75.132 [host down]
Nmap scan report for 192.168.75.133 [host down]
Nmap scan report for 192.168.75.134 [host down]
Nmap scan report for 192.168.75.135 [host down]
Nmap scan report for 192.168.75.136 [host down]
Nmap scan report for 192.168.75.137
Host is up (0.00s latency).
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap scan report for 192.168.75.138 [host down]
Nmap scan report for 192.168.75.139 [host down]
Nmap scan report for 192.168.75.140 [host down]
Nmap scan report for 192.168.75.141 [host down]
Nmap scan report for 192.168.75.142 [host down]
Nmap scan report for 192.168.75.143 [host down]
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 16 IP addresses (1 host up) scanned in 34.25 seconds
Raw packets sent: 31 (868B) | Rcvd: 1 (28B)
C:\Users\admin>

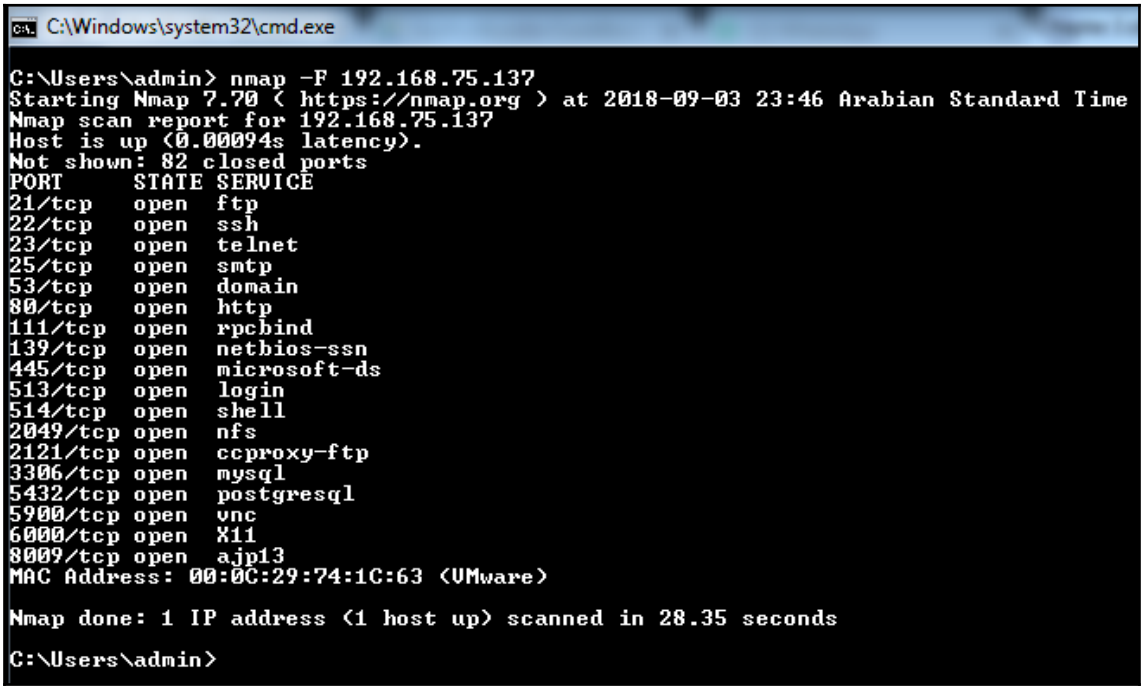

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -Pn -v 192.168.75.135/28
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 15:39 Arabian Standard Time
Initiating ARP Ping Scan at 15:39
Scanning 16 hosts [1 port/host]
Completed ARP Ping Scan at 15:39, 2.84s elapsed (16 total hosts)
Initiating Parallel DNS resolution of 16 hosts. at 15:39
Completed Parallel DNS resolution of 16 hosts. at 15:40, 16.50s elapsed
Nmap scan report for 192.168.75.128 [host down]
Nmap scan report for 192.168.75.129 [host down]
Nmap scan report for 192.168.75.130 [host down]
Nmap scan report for 192.168.75.131 [host down]
Nmap scan report for 192.168.75.132 [host down]
Nmap scan report for 192.168.75.133 [host down]
Nmap scan report for 192.168.75.134 [host down]
Nmap scan report for 192.168.75.135 [host down]
Nmap scan report for 192.168.75.136 [host down]
Nmap scan report for 192.168.75.138 [host down]
Nmap scan report for 192.168.75.139 [host down]
Nmap scan report for 192.168.75.140 [host down]
Nmap scan report for 192.168.75.141 [host down]
Nmap scan report for 192.168.75.142 [host down]
Nmap scan report for 192.168.75.143 [host down]
Initiating SYN Stealth Scan at 15:40
Scanning 192.168.75.137 [1000 ports]
Discovered open port 25/tcp on 192.168.75.137
Discovered open port 3306/tcp on 192.168.75.137
Discovered open port 22/tcp on 192.168.75.137
Discovered open port 111/tcp on 192.168.75.137
Discovered open port 445/tcp on 192.168.75.137
Discovered open port 80/tcp on 192.168.75.137
Discovered open port 21/tcp on 192.168.75.137
Discovered open port 53/tcp on 192.168.75.137
Discovered open port 23/tcp on 192.168.75.137
Discovered open port 5900/tcp on 192.168.75.137
Discovered open port 139/tcp on 192.168.75.137
Discovered open port 1099/tcp on 192.168.75.137
Discovered open port 2121/tcp on 192.168.75.137
Discovered open port 6667/tcp on 192.168.75.137
Discovered open port 1524/tcp on 192.168.75.137
Discovered open port 8180/tcp on 192.168.75.137
Discovered open port 514/tcp on 192.168.75.137
Discovered open port 2049/tcp on 192.168.75.137
Discovered open port 513/tcp on 192.168.75.137
Discovered open port 6000/tcp on 192.168.75.137
Discovered open port 512/tcp on 192.168.75.137
Discovered open port 8009/tcp on 192.168.75.137
Discovered open port 5432/tcp on 192.168.75.137
Completed SYN Stealth Scan at 15:40, 0.10s elapsed (1000 total ports)

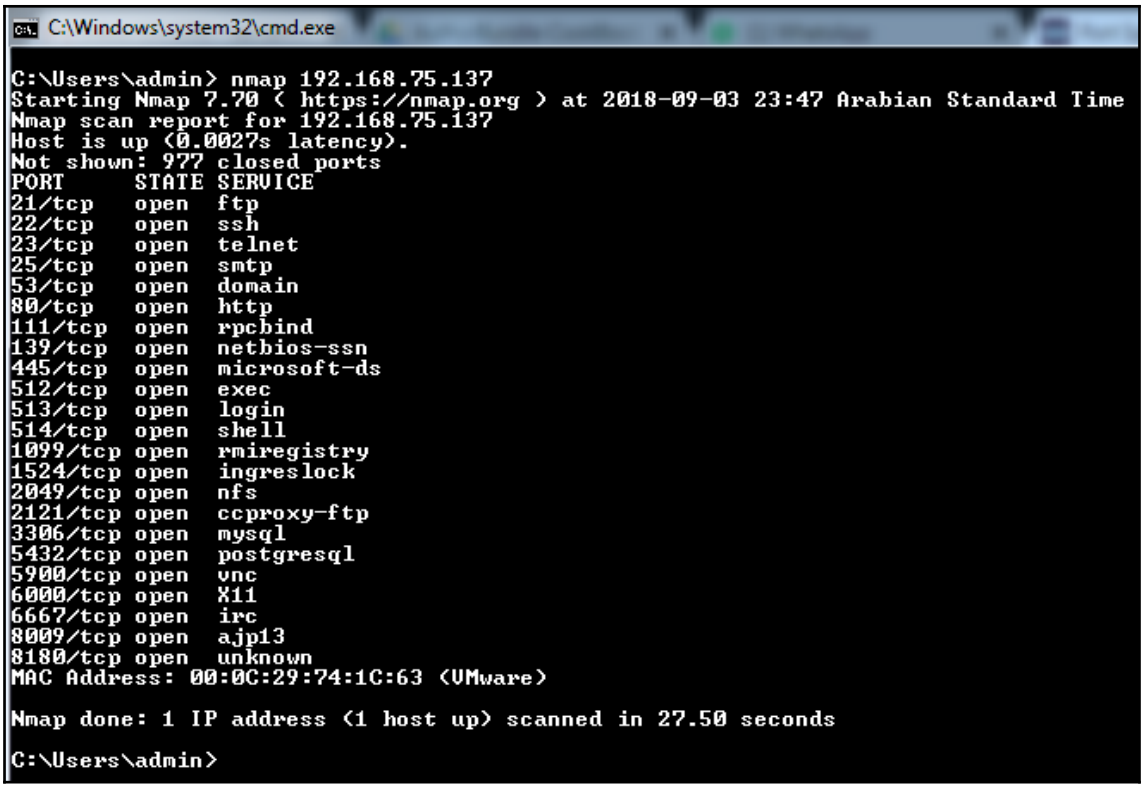

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -v -sS 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 23:16 Arabian Standard Time
Initiating ARP Ping Scan at 23:16
Scanning 192.168.75.137 [1 port]
Completed ARP Ping Scan at 23:16, 1.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:16
Completed Parallel DNS resolution of 1 host. at 23:16, 16.51s elapsed
Initiating SYN Stealth Scan at 23:16
Scanning 192.168.75.137 [1000 ports]
Discovered open port 80/tcp on 192.168.75.137
Discovered open port 3306/tcp on 192.168.75.137
Discovered open port 22/tcp on 192.168.75.137
Discovered open port 445/tcp on 192.168.75.137
Discovered open port 111/tcp on 192.168.75.137
Discovered open port 5900/tcp on 192.168.75.137
Discovered open port 2121/tcp on 192.168.75.137
Discovered open port 513/tcp on 192.168.75.137
Discovered open port 512/tcp on 192.168.75.137
Discovered open port 6000/tcp on 192.168.75.137
Discovered open port 5432/tcp on 192.168.75.137
Discovered open port 514/tcp on 192.168.75.137
Discovered open port 2049/tcp on 192.168.75.137
Discovered open port 1099/tcp on 192.168.75.137
Discovered open port 6667/tcp on 192.168.75.137
Discovered open port 8009/tcp on 192.168.75.137
Discovered open port 8180/tcp on 192.168.75.137
Discovered open port 1524/tcp on 192.168.75.137
Discovered open port 21/tcp on 192.168.75.137
Discovered open port 23/tcp on 192.168.75.137
Discovered open port 53/tcp on 192.168.75.137
Discovered open port 25/tcp on 192.168.75.137
Discovered open port 139/tcp on 192.168.75.137
Completed SYN Stealth Scan at 23:17, 1.11s elapsed (1000 total ports)
Nmap scan report for 192.168.75.137
Host is up (0.0023s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc

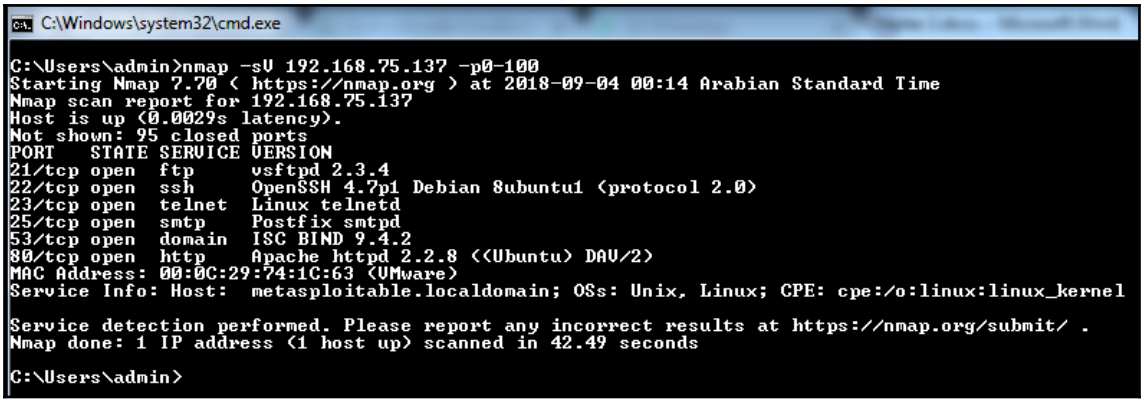

C:\Windows\system32\cmd.exe - nmap -v -sT 192.168.75.137
C:\Users\admin>nmap -v -sT 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 23:18 Arabian Standard Time
Initiating ARP Ping Scan at 23:18
Scanning 192.168.75.137 [1 port]
Completed ARP Ping Scan at 23:18, 1.43s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:18
Completed Parallel DNS resolution of 1 host. at 23:18, 16.50s elapsed
Initiating Connect Scan at 23:18
Scanning 192.168.75.137 [1000 ports]
Discovered open port 111/tcp on 192.168.75.137
Discovered open port 53/tcp on 192.168.75.137
Discovered open port 80/tcp on 192.168.75.137
Discovered open port 3306/tcp on 192.168.75.137
Discovered open port 445/tcp on 192.168.75.137
Discovered open port 21/tcp on 192.168.75.137
Discovered open port 139/tcp on 192.168.75.137
Discovered open port 23/tcp on 192.168.75.137
Discovered open port 5900/tcp on 192.168.75.137
Discovered open port 22/tcp on 192.168.75.137
Discovered open port 25/tcp on 192.168.75.137
Discovered open port 512/tcp on 192.168.75.137
Discovered open port 6000/tcp on 192.168.75.137
Discovered open port 2049/tcp on 192.168.75.137
Connect Scan Timing: About 15.10% done; ETC: 23:22 (0:02:54 remaining)
Discovered open port 5432/tcp on 192.168.75.137
Connect Scan Timing: About 29.47% done; ETC: 23:22 (0:02:26 remaining)
Discovered open port 8180/tcp on 192.168.75.137
Connect Scan Timing: About 44.40% done; ETC: 23:22 (0:01:54 remaining)
Connect Scan Timing: About 57.73% done; ETC: 23:22 (0:01:29 remaining)
Discovered open port 2121/tcp on 192.168.75.137
Discovered open port 513/tcp on 192.168.75.137
Connect Scan Timing: About 70.37% done; ETC: 23:22 (0:01:04 remaining)
Discovered open port 514/tcp on 192.168.75.137
Discovered open port 1524/tcp on 192.168.75.137
Discovered open port 8009/tcp on 192.168.75.137
Discovered open port 1099/tcp on 192.168.75.137
Connect Scan Timing: About 84.87% done; ETC: 23:22 (0:00:32 remaining)
Discovered open port 6667/tcp on 192.168.75.137

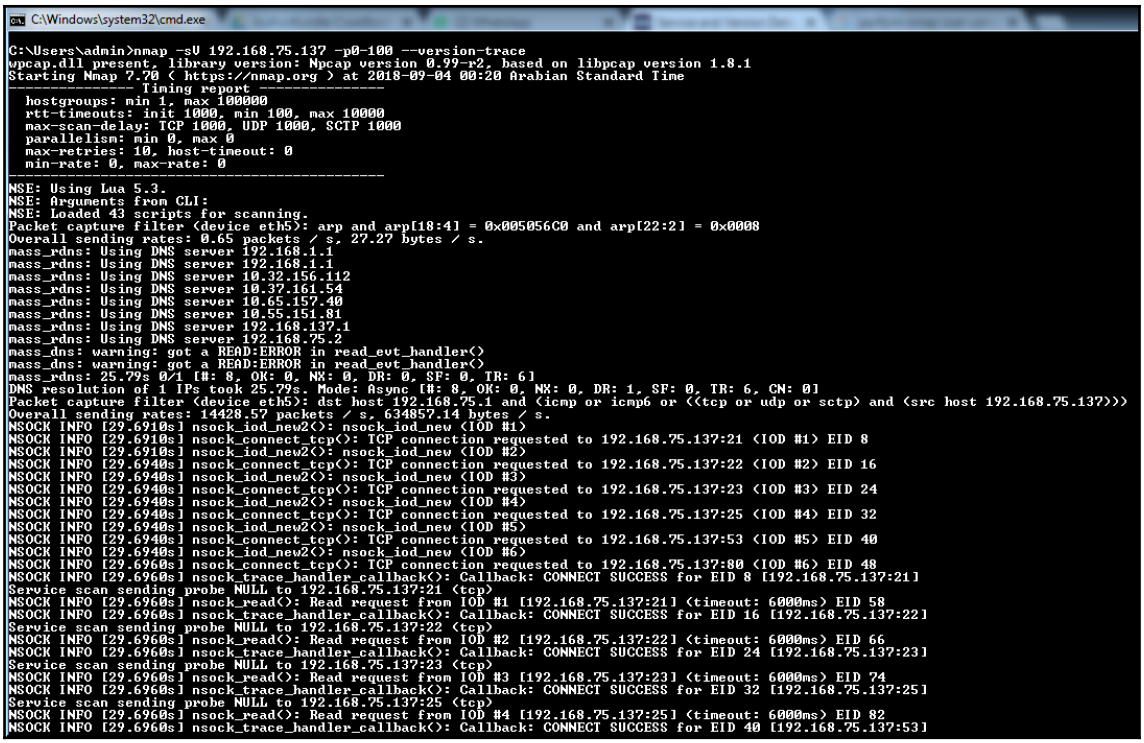

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -v -sN 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 23:22 Arabian Standard Time
Initiating ARP Ping Scan at 23:23
Scanning 192.168.75.137 [1 port]
Completed ARP Ping Scan at 23:23, 1.45s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:23
Completed Parallel DNS resolution of 1 host. at 23:23, 16.50s elapsed
Initiating NULL Scan at 23:23
Scanning 192.168.75.137 [1000 ports]
Completed NULL Scan at 23:23, 1.21s elapsed (1000 total ports)
Nmap scan report for 192.168.75.137
Host is up (0.0033s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open|filtered ftp
22/tcp open|filtered ssh
23/tcp open|filtered telnet
25/tcp open|filtered smtp
53/tcp open|filtered domain
80/tcp open|filtered http
111/tcp open|filtered rpcbind
139/tcp open|filtered netbios-ssn
445/tcp open|filtered microsoft-ds
512/tcp open|filtered exec
513/tcp open|filtered login
514/tcp open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:74:1C:63 (VMware)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 28.52 seconds
Raw packets sent: 1024 (40.948KB) | Rcvd: 978 (39.108KB)

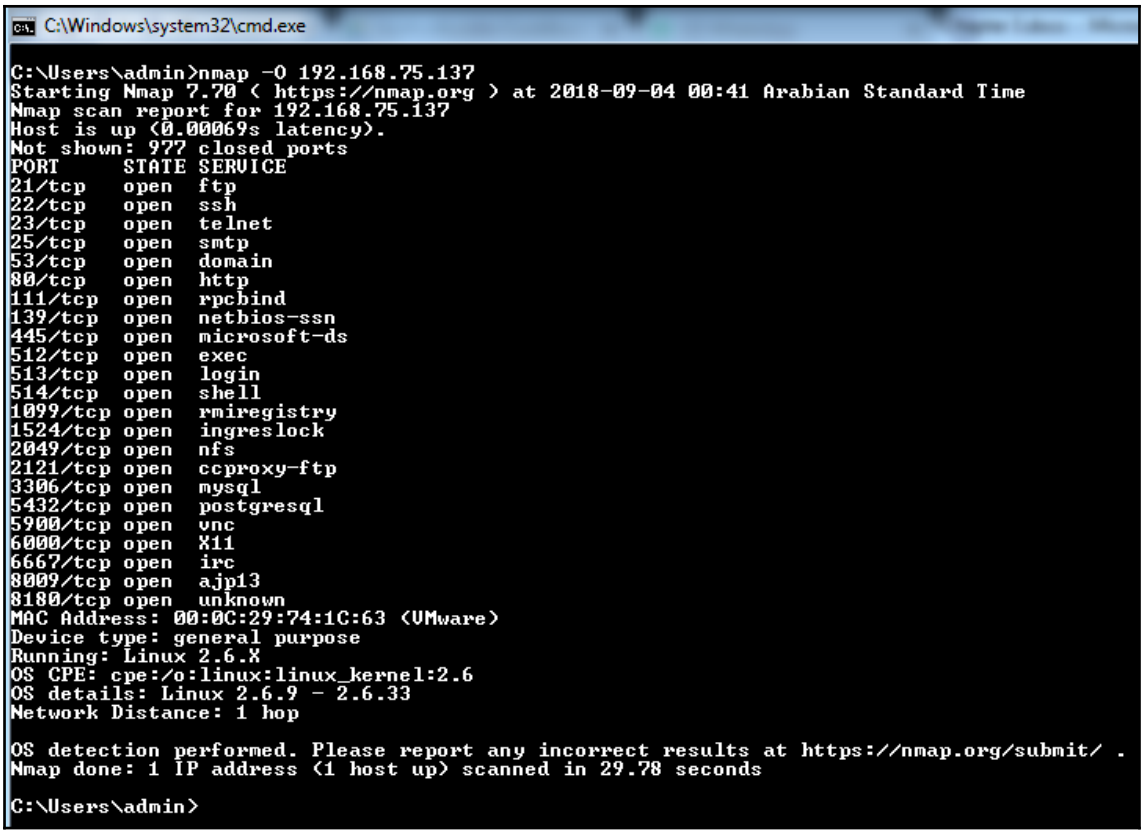

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap 192.168.75.137 -p0-100
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 23:43 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0028s latency).
Not shown: 95 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 27.87 seconds
C:\Users\admin>

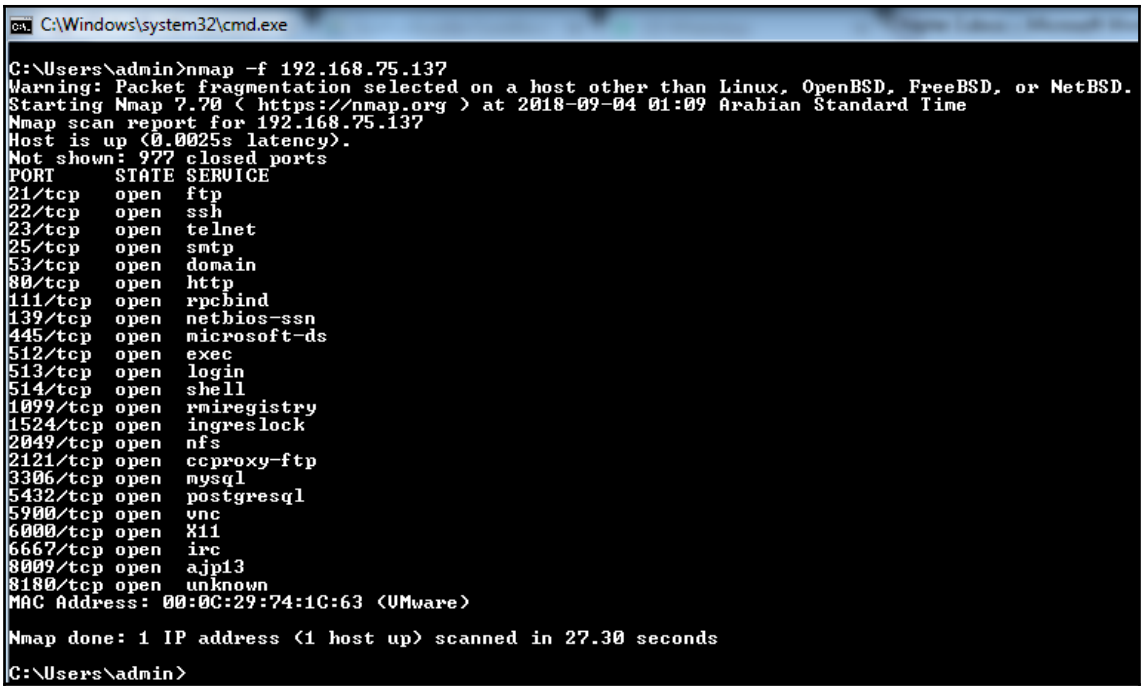

C:\Windows\system32\cmd.exe
C:\Users\admin> nmap -F 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 23:46 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.00094s latency).
Not shown: 82 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
513/tcp open login
514/tcp open shell
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
8009/tcp open ajp13
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 28.35 seconds
C:\Users\admin>

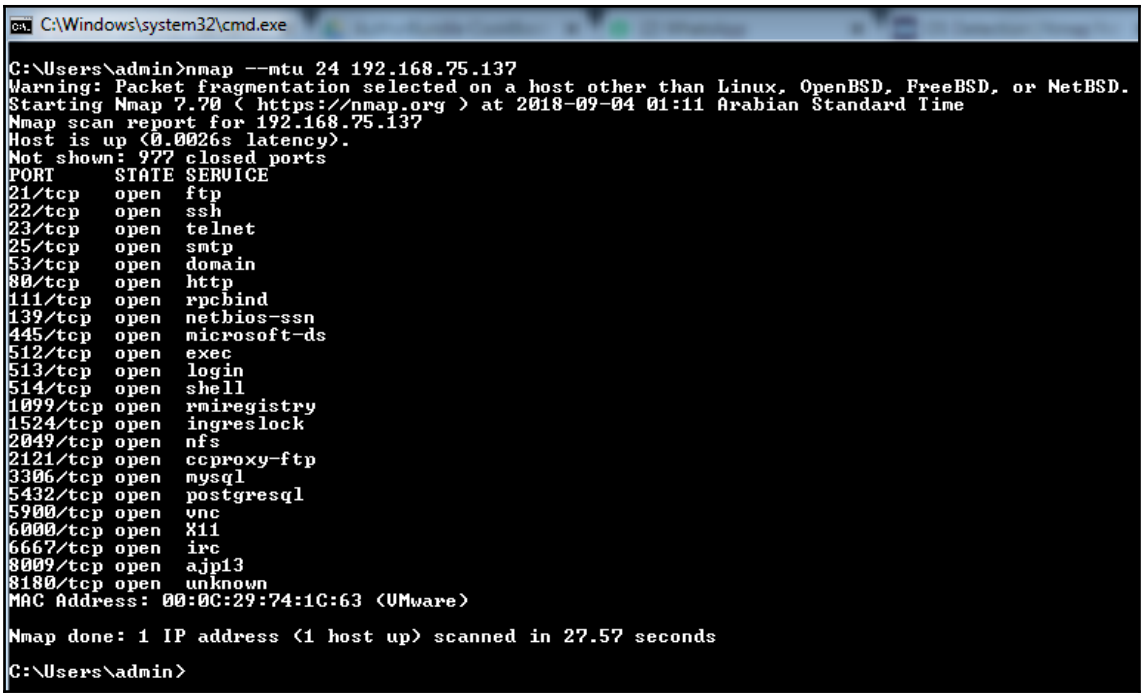

C:\Windows\system32\cmd.exe
C:\Users\admin> nmap 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-03 23:47 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 27.50 seconds
C:\Users\admin>

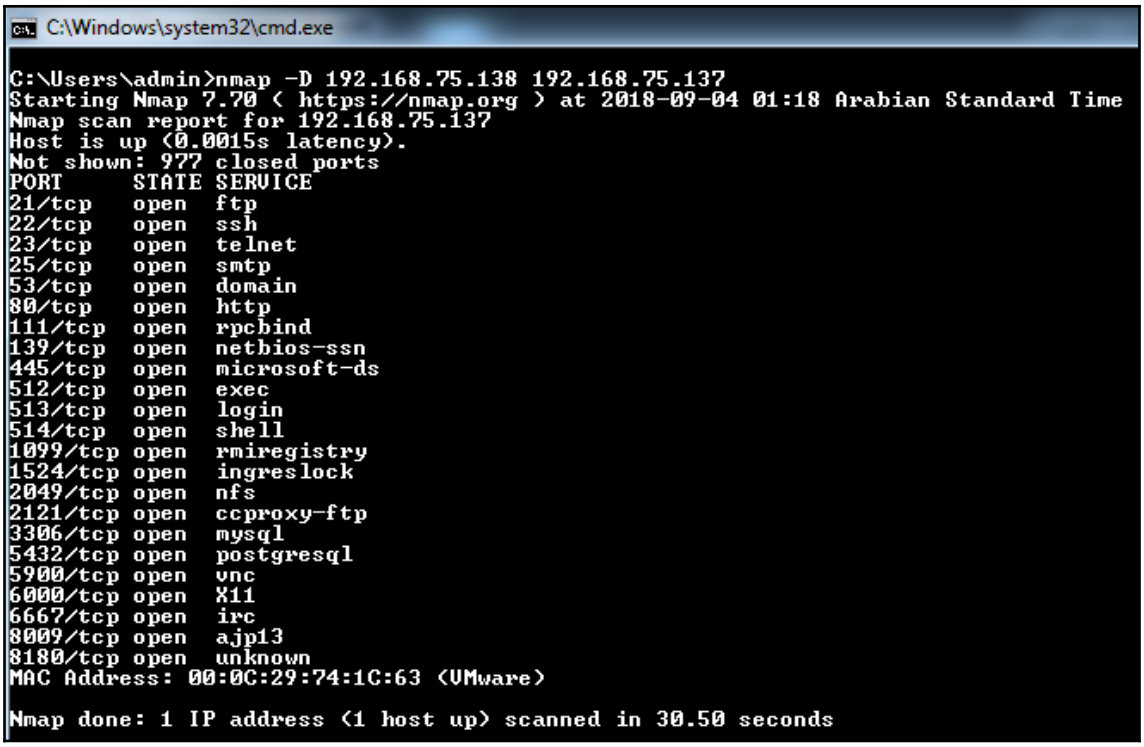

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -sV 192.168.75.137 -p0-100
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 00:14 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0029s latency).
Not shown: 95 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:74:1C:63 (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.49 seconds
C:\Users\admin>

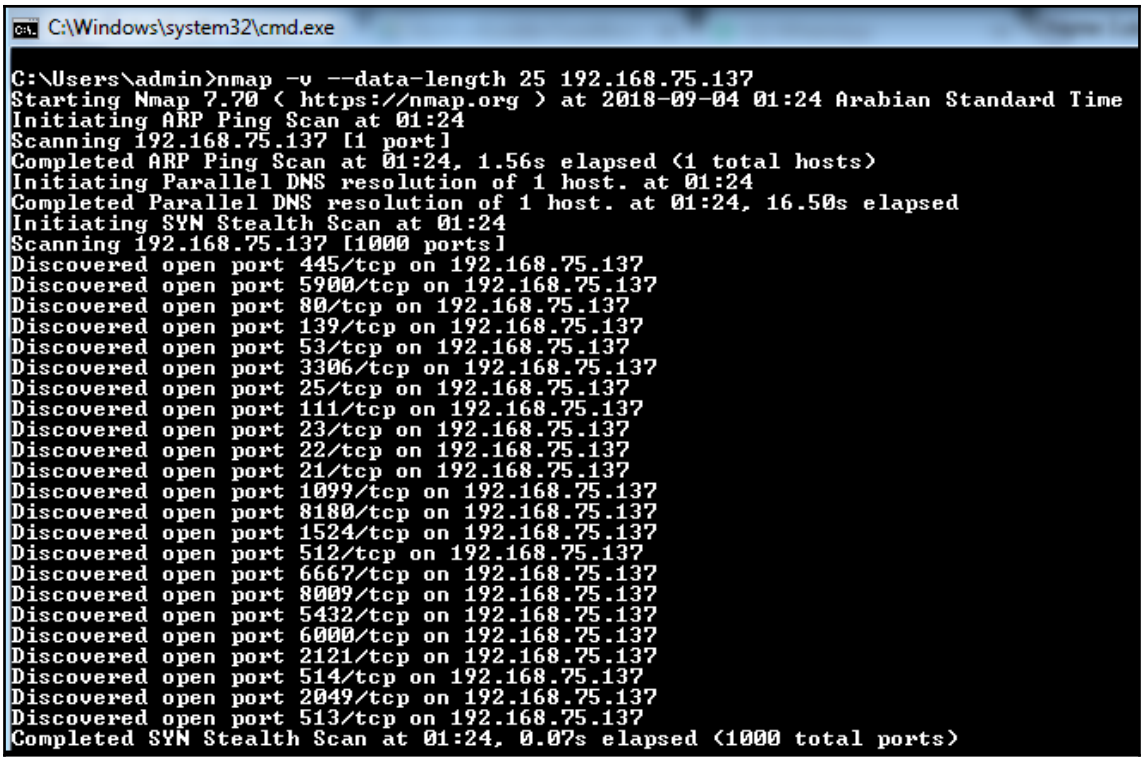

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -sV 192.168.75.137 -p0-100 --version-trace
wpcap.dll present, library version: Npcap version 0.99-r2, based on libpcap version 1.8.1
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 00:20 Arabian Standard Time
-------------- Timing report --------------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 43 scripts for scanning.
Packet capture filter (device eth5): arp and arp[18:4] = 0x005056C0 and arp[22:2] = 0x0008
Overall sending rates: 0.65 packets / s, 27.27 bytes / s.
mass_rdns: Using DNS server 192.168.1.1
mass_rdns: Using DNS server 192.168.1.1
mass_rdns: Using DNS server 10.32.156.112
mass_rdns: Using DNS server 10.37.161.54
mass_rdns: Using DNS server 10.65.157.40
mass_rdns: Using DNS server 10.55.151.81
mass_rdns: Using DNS server 192.168.137.1
mass_rdns: Using DNS server 192.168.75.2
mass_dns: warning: got a READ:ERROR in read_evt_handler()
mass_dns: warning: got a READ:ERROR in read_evt_handler()
mass_rdns: 25.79s 0/1 [#: 8, OK: 0, NX: 0, DR: 0, SF: 0, TR: 6]
DNS resolution of 1 IPs took 25.79s. Mode: Async [#: 8, OK: 0, NX: 0, DR: 1, SF: 0, TR: 6, CN: 0]
Packet capture filter (device eth5): dst host 192.168.75.1 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.75.137)))
Overall sending rates: 14428.57 packets / s, 634857.14 bytes / s.
NSOCK INFO [29.6910s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [29.6910s] nsock_connect_tcp(): TCP connection requested to 192.168.75.137:21 (IOD #1) EID 8
NSOCK INFO [29.6910s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [29.6940s] nsock_connect_tcp(): TCP connection requested to 192.168.75.137:22 (IOD #2) EID 16
NSOCK INFO [29.6940s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [29.6940s] nsock_connect_tcp(): TCP connection requested to 192.168.75.137:23 (IOD #3) EID 24
NSOCK INFO [29.6940s] nsock_iod_new2(): nsock_iod_new (IOD #4)
NSOCK INFO [29.6940s] nsock_connect_tcp(): TCP connection requested to 192.168.75.137:25 (IOD #4) EID 32
NSOCK INFO [29.6940s] nsock_iod_new2(): nsock_iod_new (IOD #5)
NSOCK INFO [29.6940s] nsock_connect_tcp(): TCP connection requested to 192.168.75.137:53 (IOD #5) EID 40
NSOCK INFO [29.6940s] nsock_iod_new2(): nsock_iod_new (IOD #6)
NSOCK INFO [29.6960s] nsock_connect_tcp(): TCP connection requested to 192.168.75.137:80 (IOD #6) EID 48
NSOCK INFO [29.6960s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.75.137:21]
Service scan sending probe NULL to 192.168.75.137:21 (tcp)
NSOCK INFO [29.6960s] nsock_read(): Read request from IOD #1 [192.168.75.137:21] (timeout: 6000ms) EID 58
NSOCK INFO [29.6960s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 16 [192.168.75.137:22]
Service scan sending probe NULL to 192.168.75.137:22 (tcp)
NSOCK INFO [29.6960s] nsock_read(): Read request from IOD #2 [192.168.75.137:22] (timeout: 6000ms) EID 66
NSOCK INFO [29.6960s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [192.168.75.137:23]
Service scan sending probe NULL to 192.168.75.137:23 (tcp)
NSOCK INFO [29.6960s] nsock_read(): Read request from IOD #3 [192.168.75.137:23] (timeout: 6000ms) EID 74
NSOCK INFO [29.6960s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 32 [192.168.75.137:25]
Service scan sending probe NULL to 192.168.75.137:25 (tcp)
NSOCK INFO [29.6960s] nsock_read(): Read request from IOD #4 [192.168.75.137:25] (timeout: 6000ms) EID 82
NSOCK INFO [29.6960s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [192.168.75.137:53]

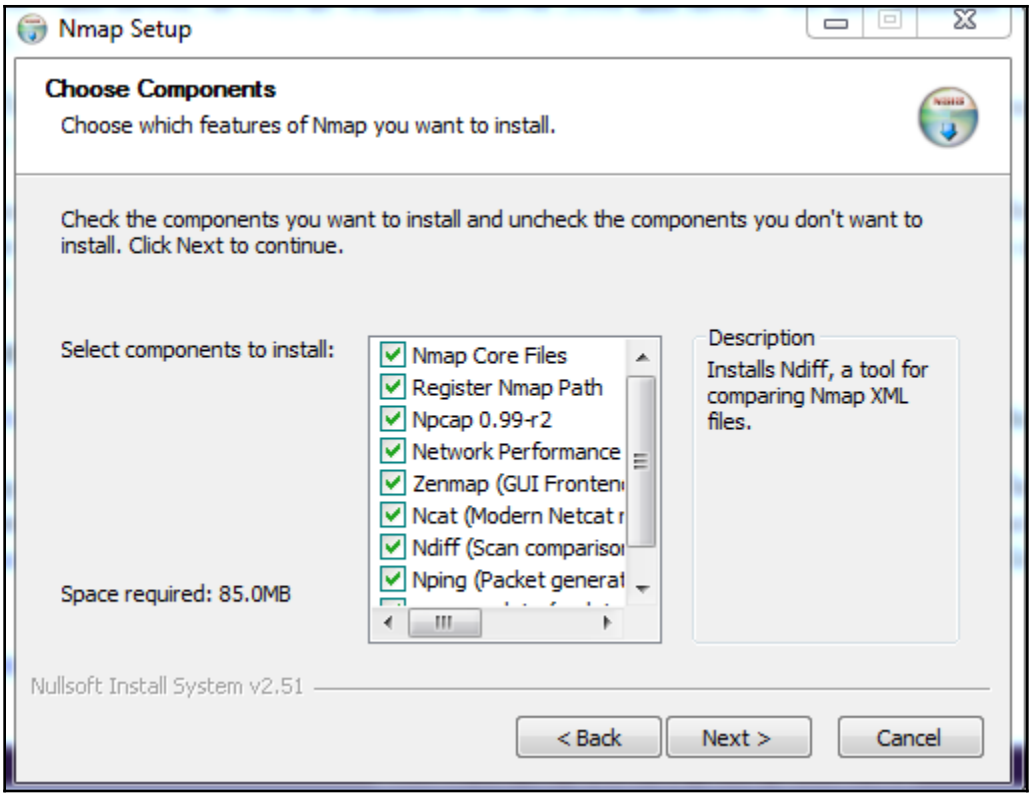

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -O 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 00:41 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.00069s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:74:1C:63 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.78 seconds
C:\Users\admin>

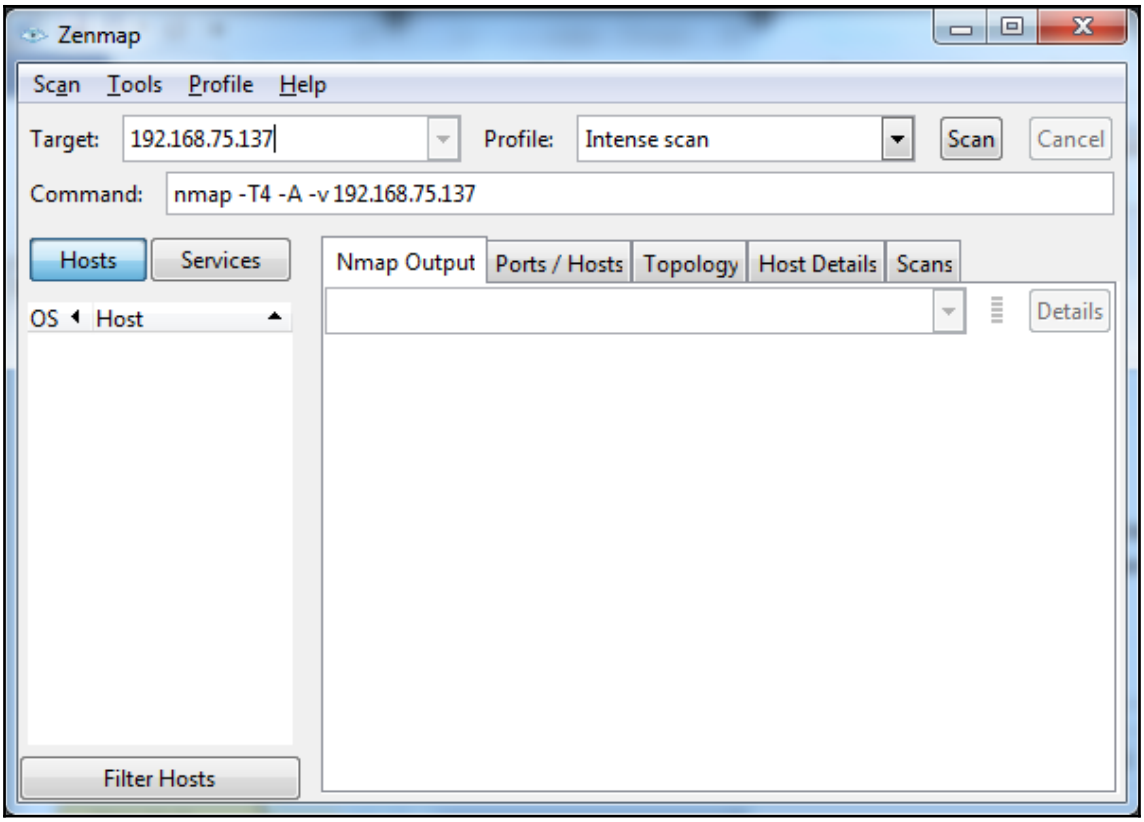

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -f 192.168.75.137
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD.
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 01:09 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 27.30 seconds
C:\Users\admin>

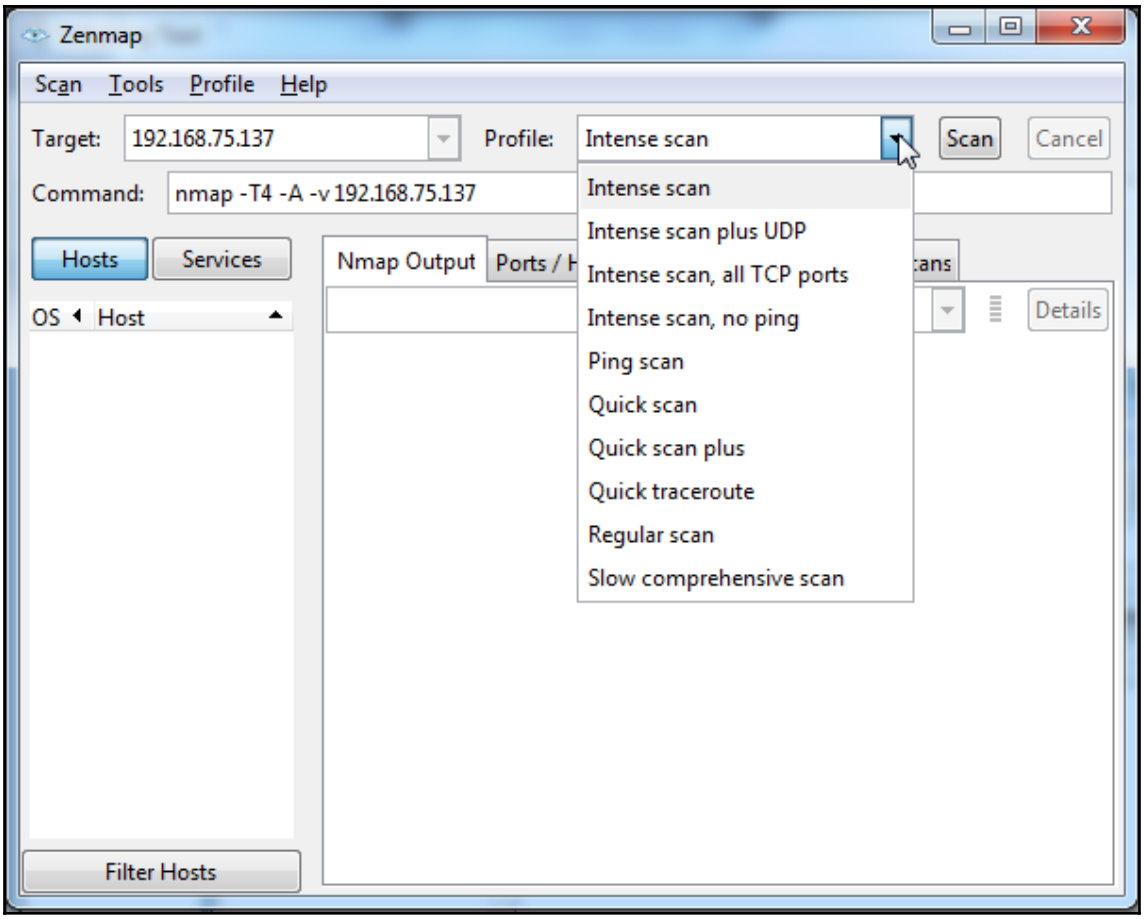

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap --mtu 24 192.168.75.137
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD.
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 01:11 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0026s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 27.57 seconds
C:\Users\admin>

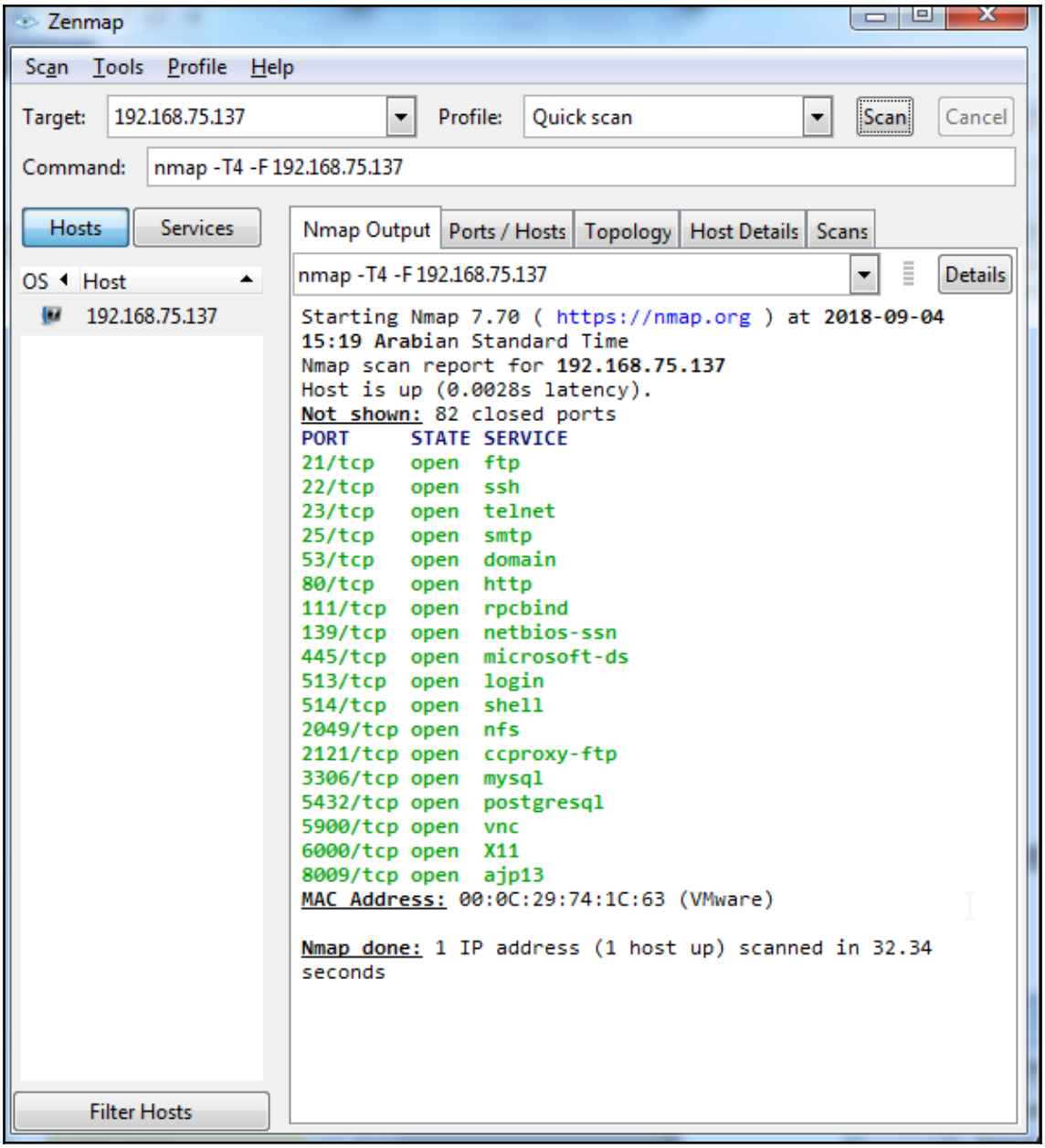

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -D 192.168.75.138 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 01:18 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0015s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 30.50 seconds

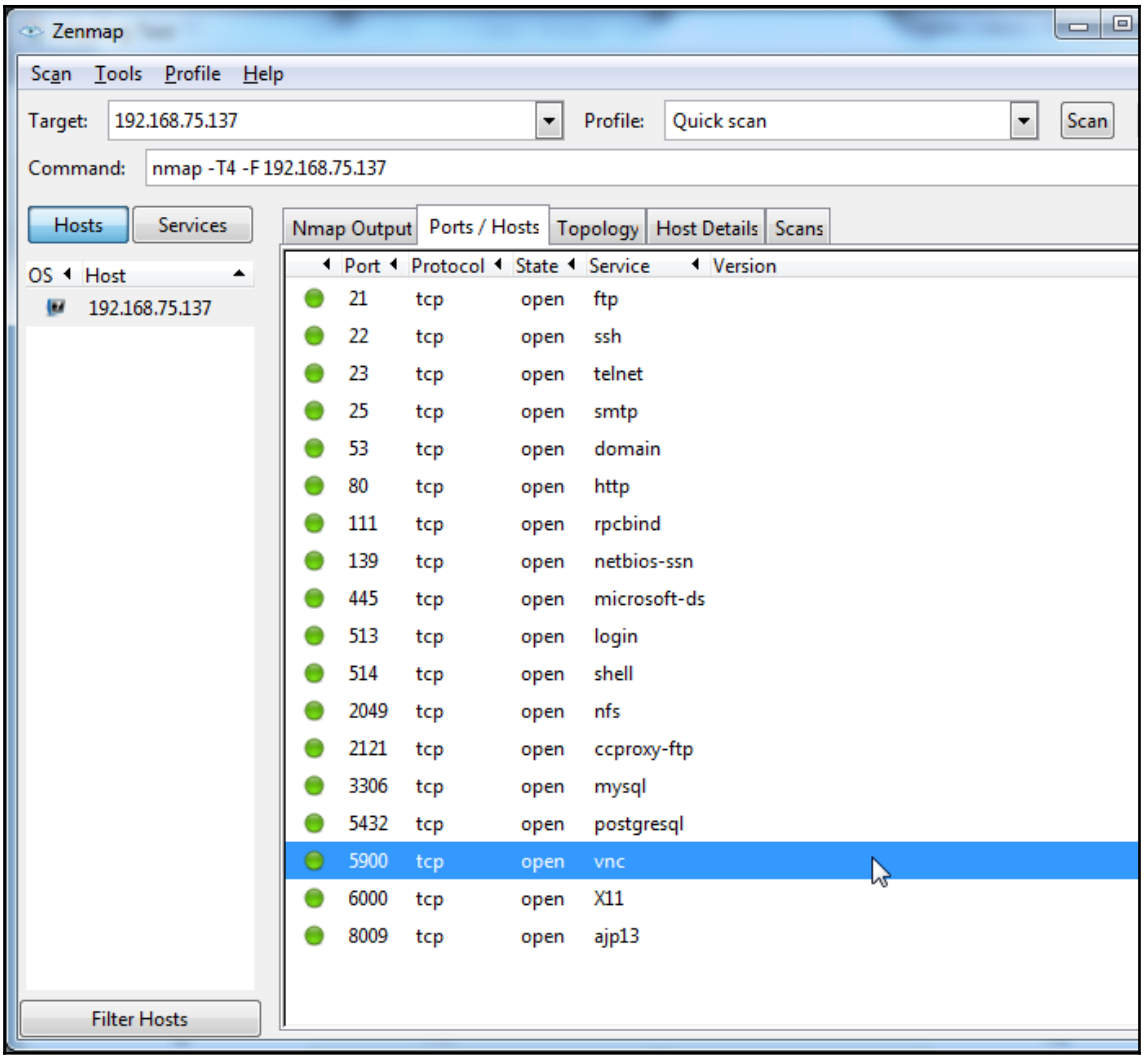

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -v --data-length 25 192.168.75.137
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 01:24 Arabian Standard Time
Initiating ARP Ping Scan at 01:24
Scanning 192.168.75.137 [1 port]
Completed ARP Ping Scan at 01:24, 1.56s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:24
Completed Parallel DNS resolution of 1 host. at 01:24, 16.50s elapsed
Initiating SYN Stealth Scan at 01:24
Scanning 192.168.75.137 [1000 ports]
Discovered open port 445/tcp on 192.168.75.137
Discovered open port 5900/tcp on 192.168.75.137
Discovered open port 80/tcp on 192.168.75.137
Discovered open port 139/tcp on 192.168.75.137
Discovered open port 53/tcp on 192.168.75.137
Discovered open port 3306/tcp on 192.168.75.137
Discovered open port 25/tcp on 192.168.75.137
Discovered open port 111/tcp on 192.168.75.137
Discovered open port 23/tcp on 192.168.75.137
Discovered open port 22/tcp on 192.168.75.137
Discovered open port 21/tcp on 192.168.75.137
Discovered open port 1099/tcp on 192.168.75.137
Discovered open port 8180/tcp on 192.168.75.137
Discovered open port 1524/tcp on 192.168.75.137
Discovered open port 512/tcp on 192.168.75.137
Discovered open port 6667/tcp on 192.168.75.137
Discovered open port 8009/tcp on 192.168.75.137
Discovered open port 5432/tcp on 192.168.75.137
Discovered open port 6000/tcp on 192.168.75.137
Discovered open port 2121/tcp on 192.168.75.137
Discovered open port 514/tcp on 192.168.75.137
Discovered open port 2049/tcp on 192.168.75.137
Discovered open port 513/tcp on 192.168.75.137
Completed SYN Stealth Scan at 01:24, 0.07s elapsed (1000 total ports)

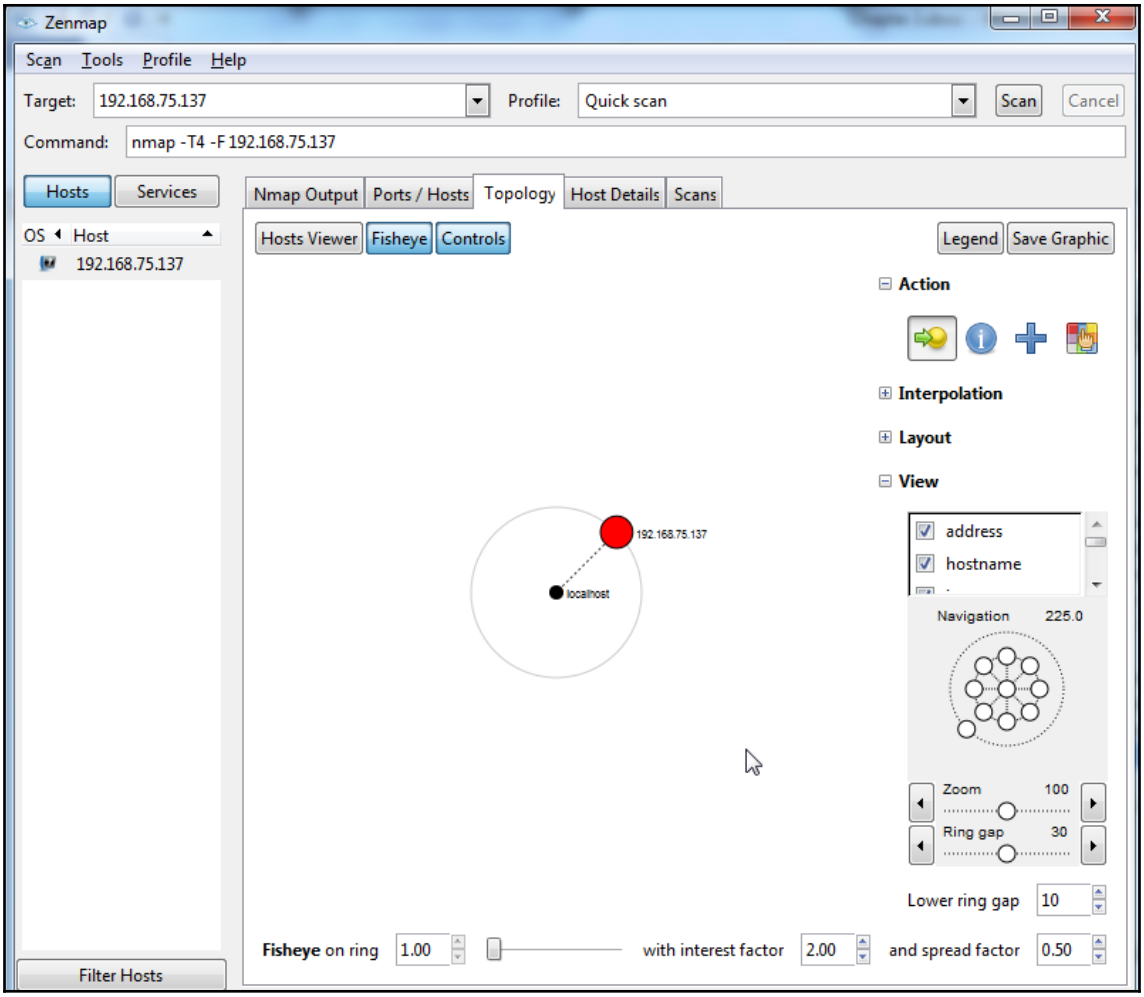

Nmap Setup
Choose Components
Choose which features of Nmap you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Nmap Core Files
Register Nmap Path
Npcap 0.99-r2
Network Performance
Zenmap (GUI Fronten
Ncat (Modern Netcat
Ndiff (Scan comparis
Nping (Packet generat
Description
Installs Ndiff, a tool for comparing Nmap XML files.
Space required: 85.0MB
Nullsoft Install System v2.51
< Back
Next >
Cancel

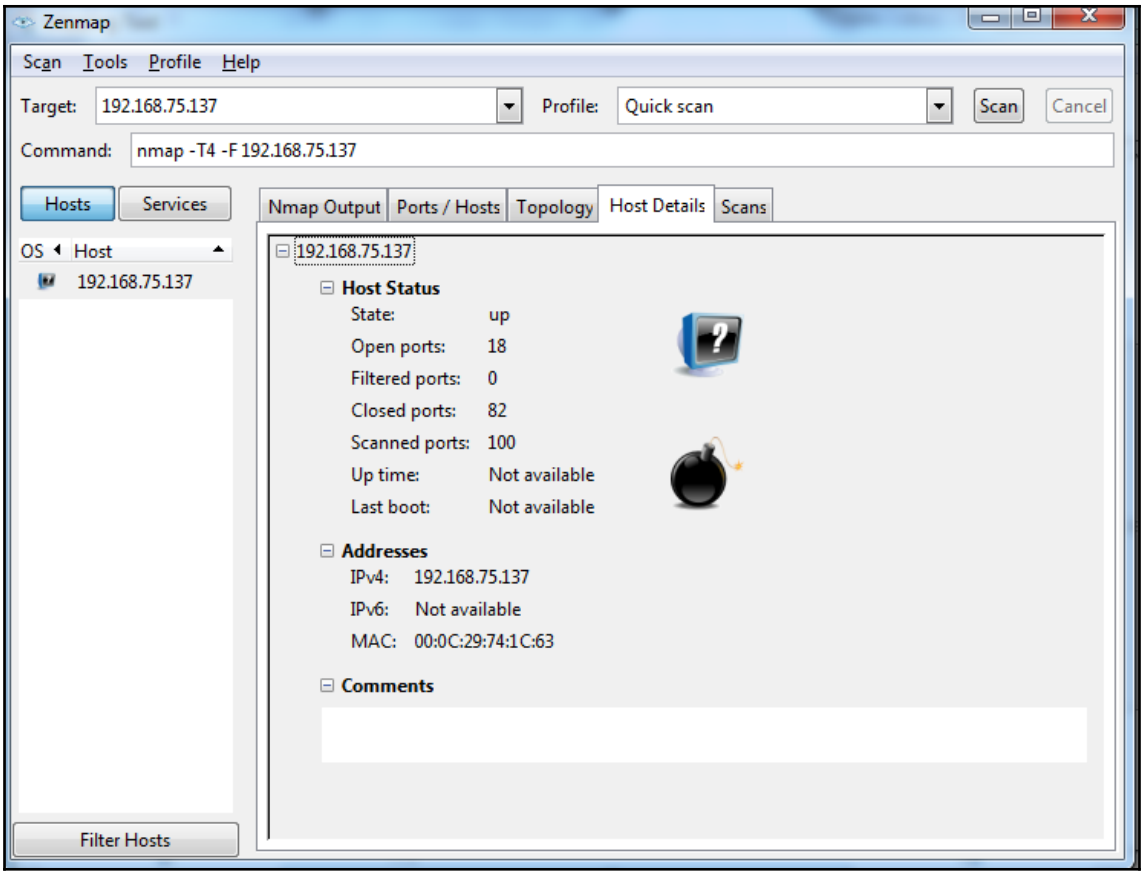

Zenmap
Scan Tools Profile Help
Target: 192.168.75.137
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.75.137
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts

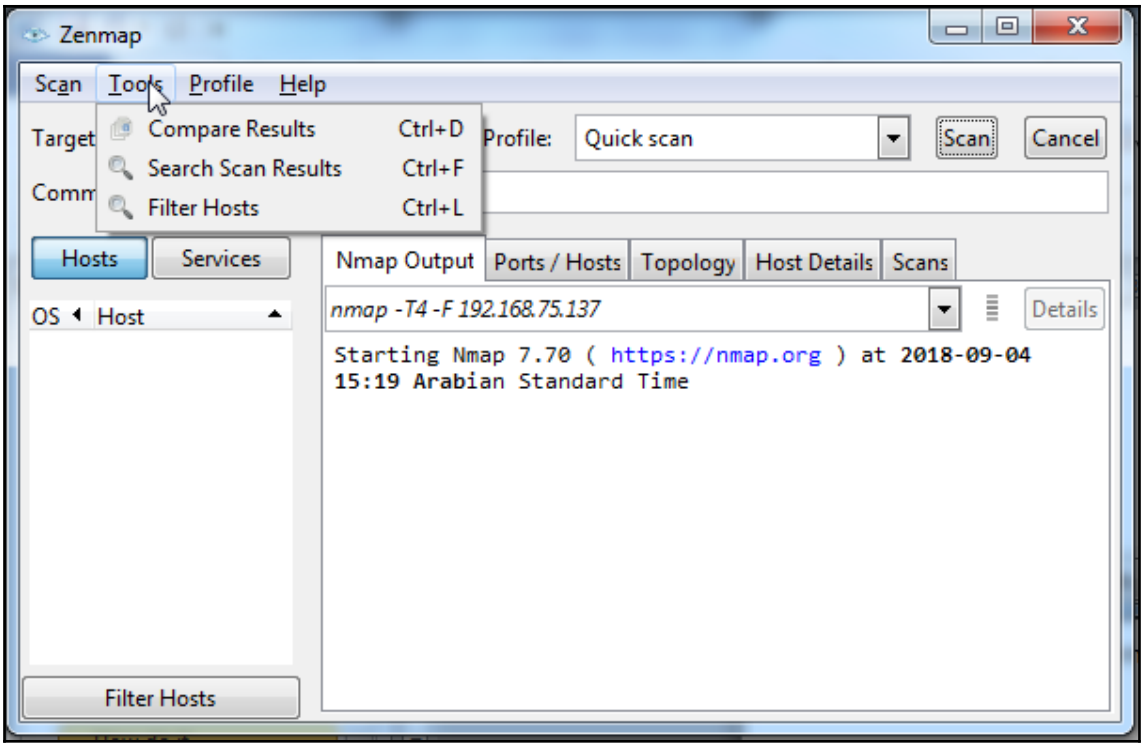

Zenmap
Scan Tools Profile Help
Target: 192.168.75.137
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.75.137
Hosts
Services
Nmap Output
Ports / H
OS
Host
Details
Filter Hosts
Intense scan
Intense scan plus UDP
Intense scan, all TCP ports
Intense scan, no ping
Ping scan
Quick scan
Quick scan plus
Quick traceroute
Regular scan
Slow comprehensive scan


Zenmap
Scan Tools Profile Help
Target: 192.168.75.137
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 192.168.75.137
Hosts
Services
OS Host
192.168.75.137
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F 192.168.75.137
Details
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04 15:19 Arabian Standard Time
Nmap scan report for 192.168.75.137
Host is up (0.0028s latency).
Not shown: 82 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
513/tcp open login
514/tcp open shell
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
8009/tcp open ajp13
MAC Address: 00:0C:29:74:1C:63 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 32.34 seconds

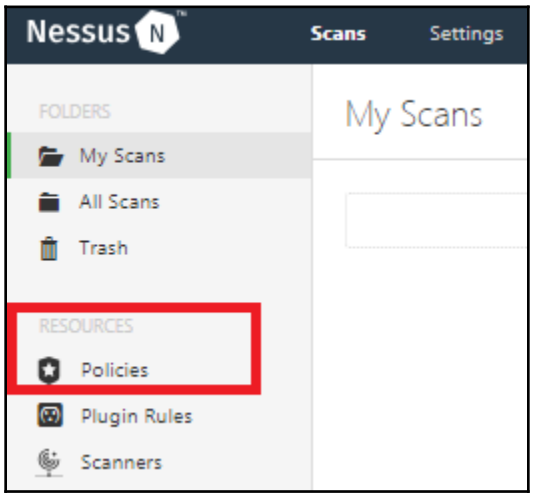

Zenmap
Scan Tools Profile Help
Target: 192.168.75.137
Profile: Quick scan
Scan
Command: nmap -T4 -F 192.168.75.137
Hosts
Services
OS Host
192.168.75.137
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port Protocol State Service Version
21 tcp open ftp
22 tcp open ssh
23 tcp open telnet
25 tcp open smtp
53 tcp open domain
80 tcp open http
111 tcp open rpcbind
139 tcp open netbios-ssn
445 tcp open microsoft-ds
513 tcp open login
514 tcp open shell
2049 tcp open nfs
2121 tcp open ccproxy-ftp
3306 tcp open mysql
5432 tcp open postgresql
5900 tcp open vnc
6000 tcp open X11
8009 tcp open ajp13

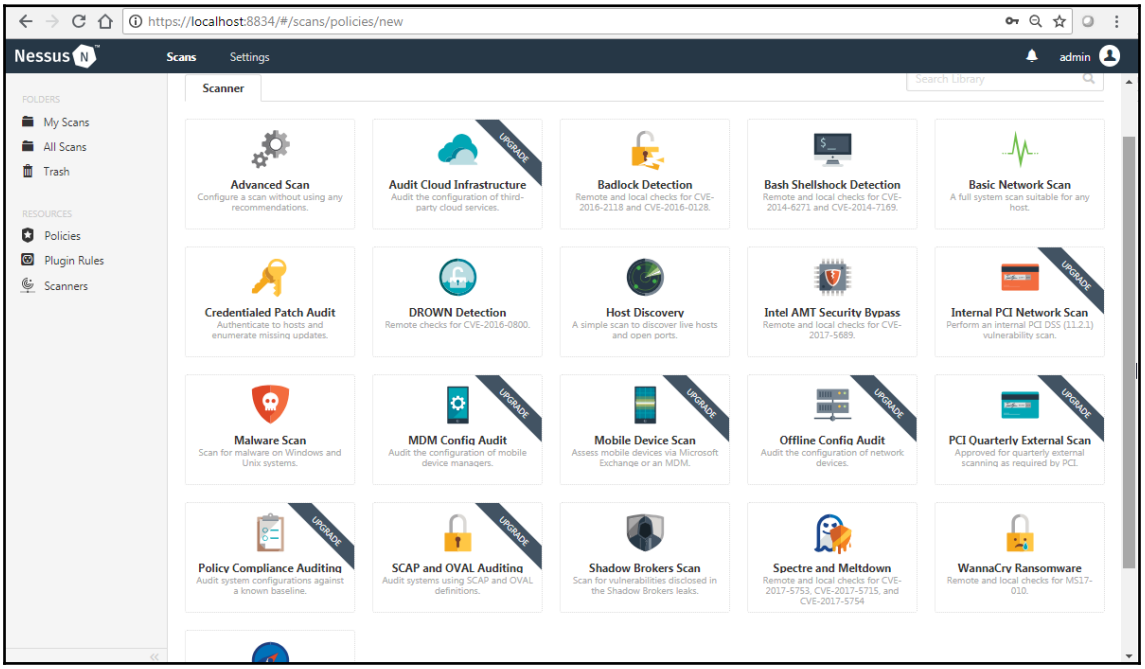

Zenmap
Scan Tools Profile Help
Target: 192.168.75.137
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 192.168.75.137
Hosts
Services
OS Host
192.168.75.137
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
Action
Interpolation
Layout
View
address
hostname
192.168.75.137
localhost
Navigation
225.0
Zoom
100
Ring gap
30
Lower ring gap
10
Fisheye on ring
1.00
with interest factor
2.00
and spread factor
0.50

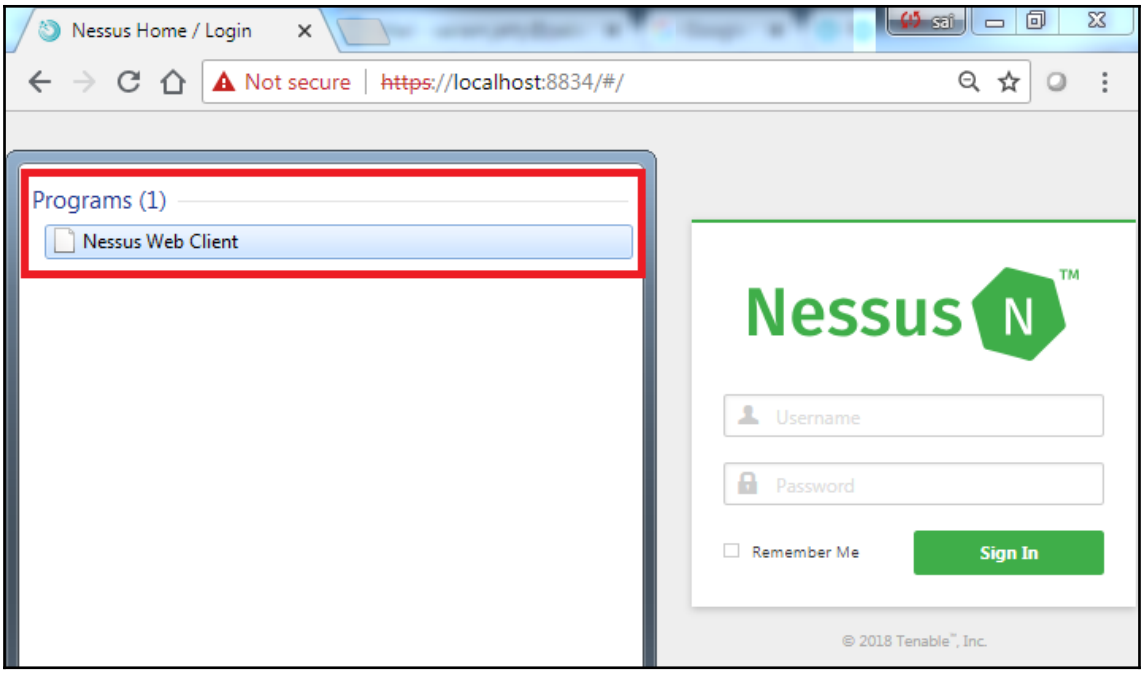

Zenmap
Scan Tools Profile Help
Target: 192.168.75.137
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 192.168.75.137
Hosts
Services
OS Host
192.168.75.137
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
192.168.75.137
Host Status
State: up
Open ports: 18
Filtered ports: 0
Closed ports: 82
Scanned ports: 100
Up time: Not available
Last boot: Not available
Addresses
IPv4: 192.168.75.137
IPv6: Not available
MAC: 00:0C:29:74:1C:63
Comments

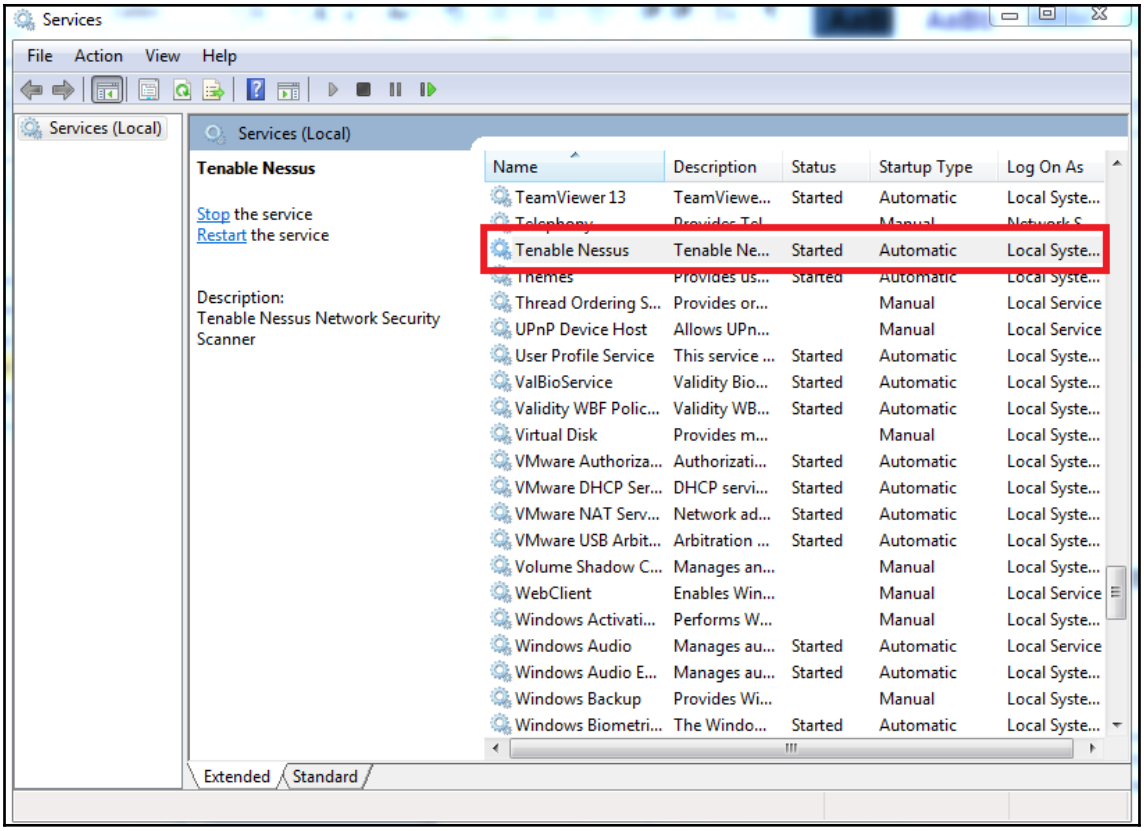

Zenmap
Scan
Tools
Profile
Help
Compare Results Ctrl+D
Search Scan Results Ctrl+F
Filter Hosts Ctrl+L
Target
Comm
Profile:
Quick scan
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
nmap -T4 -F 192.168.75.137
Details
Starting Nmap 7.70 (https://nmap.org) at 2018-09-04
15:19 Arabian Standard Time
Filter Hosts

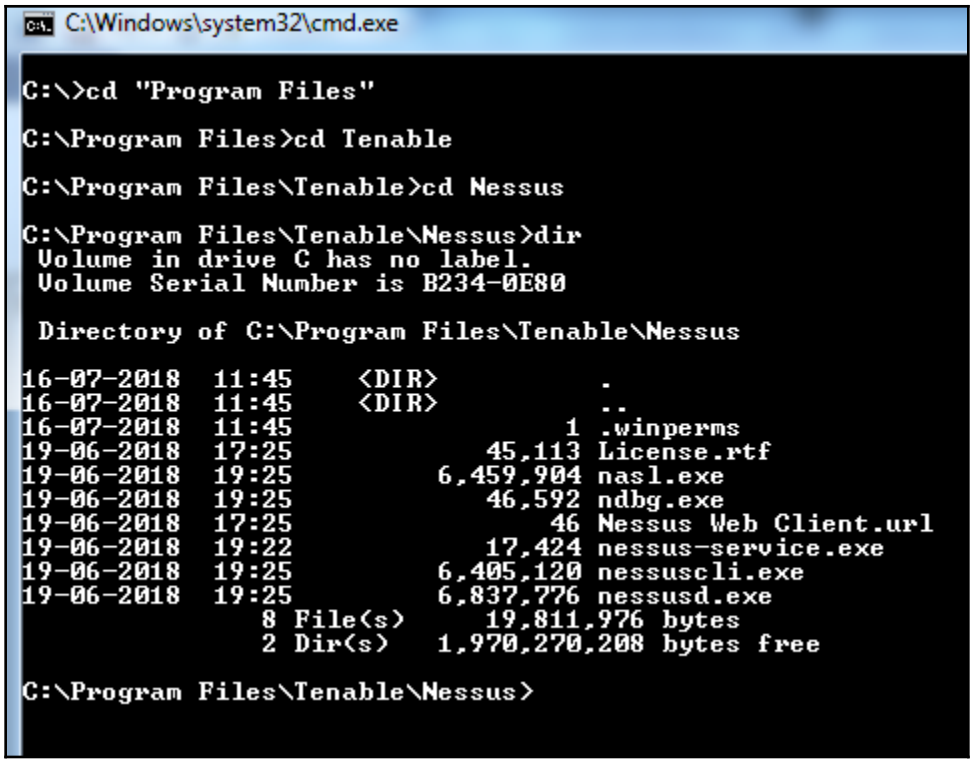
Chapter 4: Vulnerability Scanning

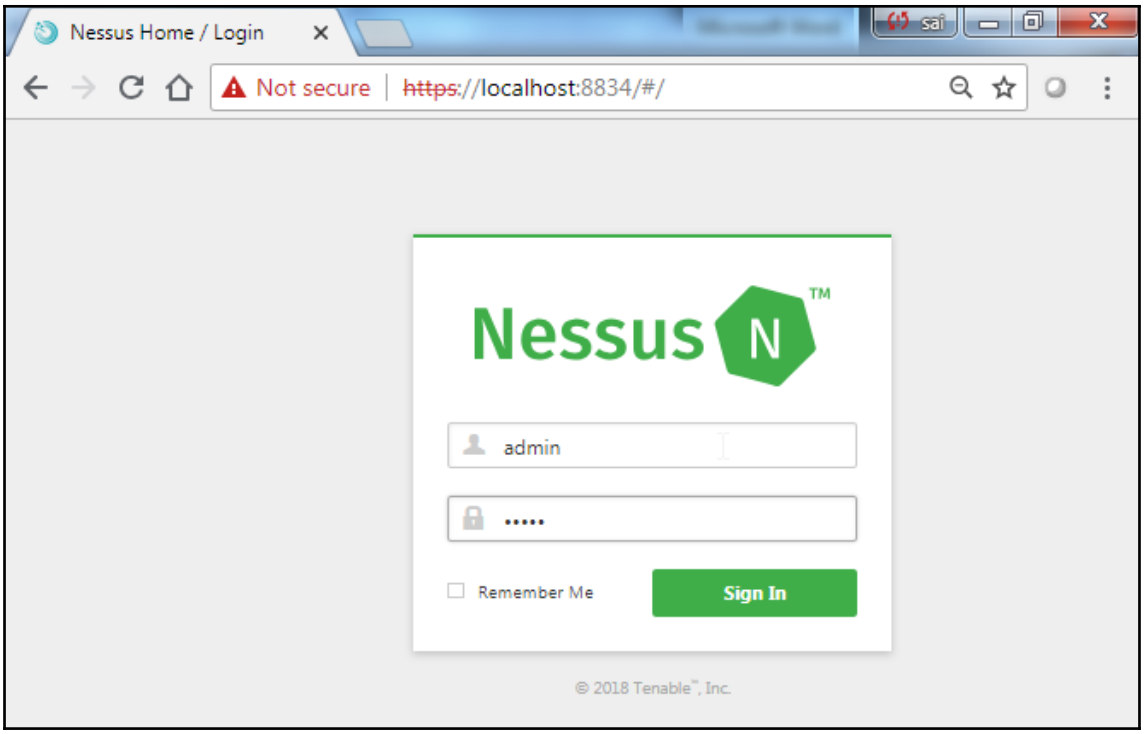


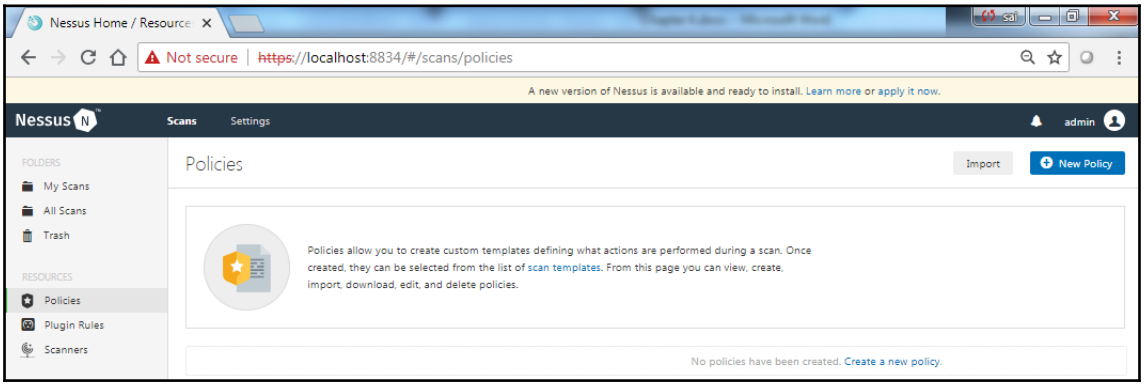


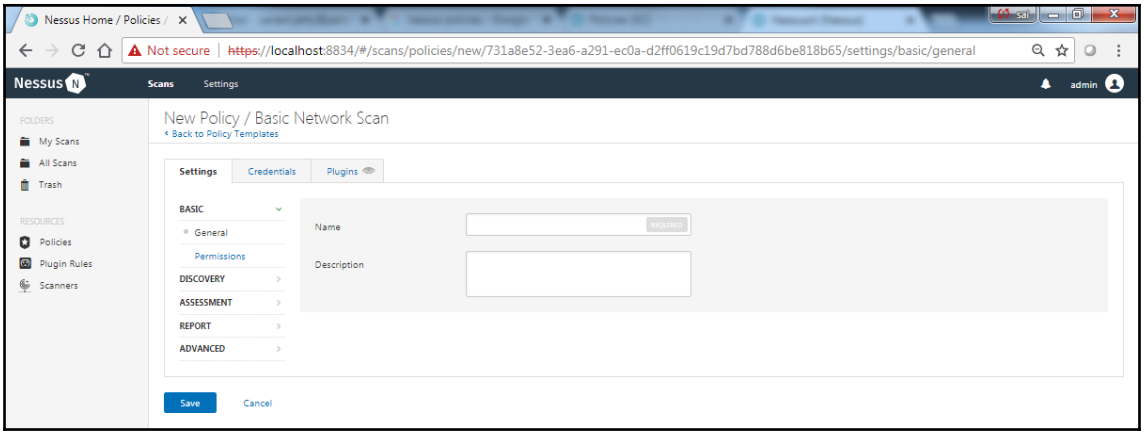

Nessus Home / Login
Not secure
https://localhost:8834/#/
Programs (1)
Nessus Web Client
Nessus
Username
Password
Remember Me
Sign In
© 2018 Tenable™, Inc.

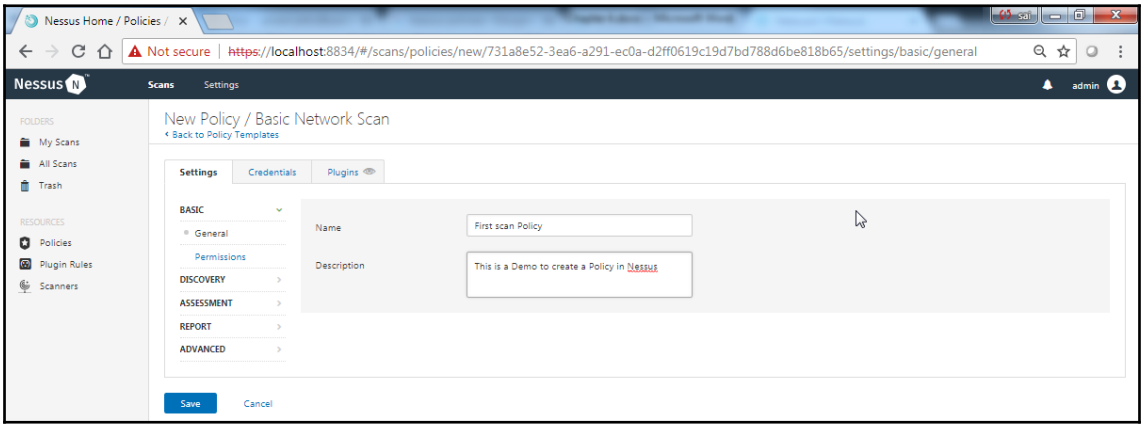

Services
File Action View Help
Services (Local)
Services (Local)
Tenable Nessus
Stop the service
Restart the service
Description:
Tenable Nessus Network Security Scanner
Name
Description
Status
Startup Type
Log On As
TeamViewer 13
TeamViewe...
Started
Automatic
Local Syste...
Tenable Nessus
Tenable Ne...
Started
Automatic
Local Syste...
Thread Ordering S...
Provides or...
Manual
Local Service
UPnP Device Host
Allows UPn...
Manual
Local Service
User Profile Service
This service ...
Started
Automatic
Local Syste...
ValBioService
Validity Bio...
Started
Automatic
Local Syste...
Validity WBF Polic...
Validity WB...
Started
Automatic
Local Syste...
Virtual Disk
Provides m...
Manual
Local Syste...
VMware Authoriza...
Authorizati...
Started
Automatic
Local Syste...
VMware DHCP Ser...
DHCP servi...
Started
Automatic
Local Syste...
VMware NAT Serv...
Network ad...
Started
Automatic
Local Syste...
VMware USB Arbit...
Arbitration ...
Started
Automatic
Local Syste...
Volume Shadow C...
Manages an...
Manual
Local Syste...
WebClient
Enables Win...
Manual
Local Service
Windows Activati...
Performs W...
Manual
Local Syste...
Windows Audio
Manages au...
Started
Automatic
Local Service
Windows Audio E...
Manages au...
Started
Automatic
Local Syste...
Windows Backup
Provides Wi...
Manual
Local Syste...
Windows Biometri...
The Windo...
Started
Automatic
Local Syste...
Extended
Standard

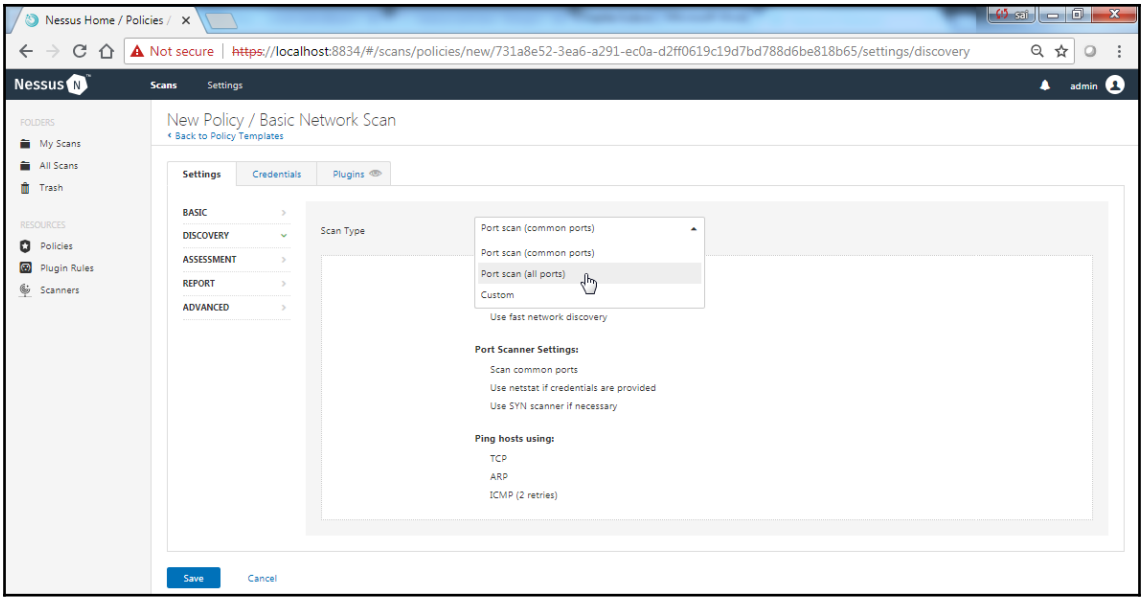

C:\Windows\system32\cmd.exe
C:\>cd "Program Files"
C:\Program Files>cd Tenable
C:\Program Files\Tenable>cd Nessus
C:\Program Files\Tenable\Nessus>dir
Volume in drive C has no label.
Volume Serial Number is B234-0E80
Directory of C:\Program Files\Tenable\Nessus
16-07-2018 11:45 <DIR> .
16-07-2018 11:45 <DIR> ..
16-07-2018 11:45 1 .winperms
19-06-2018 17:25 45,113 License.rtf
19-06-2018 19:25 6,459,904 nasl.exe
19-06-2018 19:25 46,592 ndbg.exe
19-06-2018 17:25 46 Nessus Web Client.url
19-06-2018 19:22 17,424 nessus-service.exe
19-06-2018 19:25 6,405,120 nessuscli.exe
19-06-2018 19:25 6,837,776 nessusd.exe
8 File(s) 19,811,976 bytes
2 Dir(s) 1,970,270,208 bytes free
C:\Program Files\Tenable\Nessus>

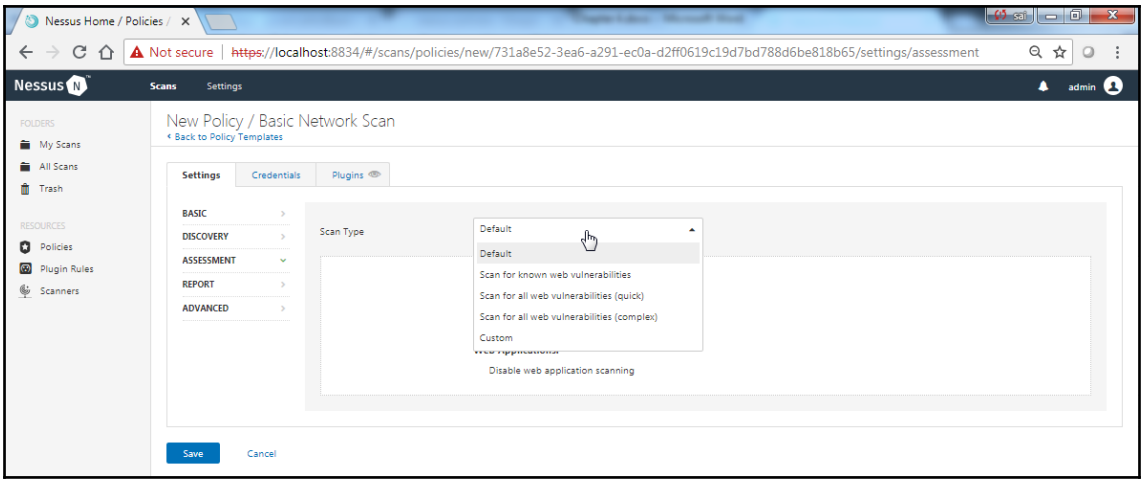

Nessus Home / Login
Not secure
https://localhost:8834/#/
Nessus
admin
Remember Me
Sign In
© 2018 Tenable™, Inc.

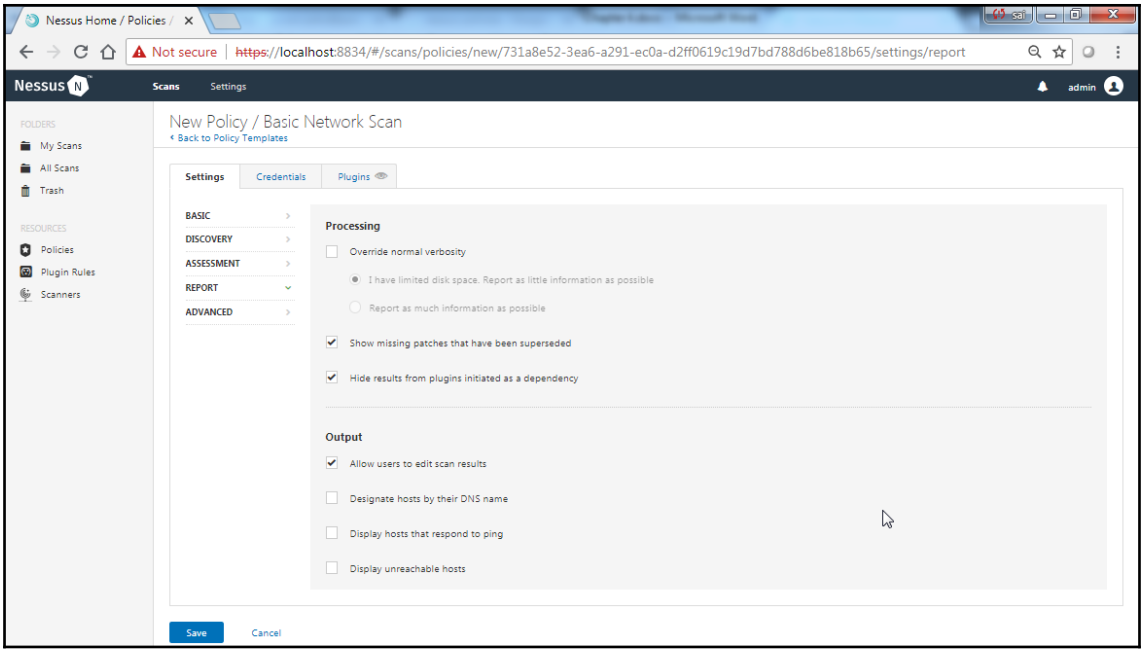

Nessus Home / Resource
Not secure
https://localhost:8834/#/scans/policies
A new version of Nessus is available and ready to install. Learn more or apply it now.
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Policies
Import
New Policy
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
No policies have been created. Create a new policy.

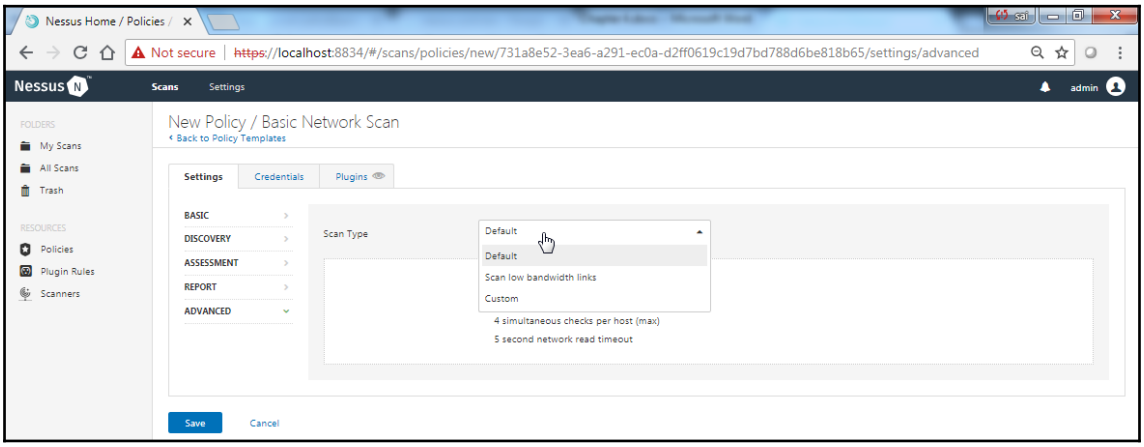

Nessus Home / Policies
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
General
Permissions
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
REQUIRED
Description
Save
Cancel

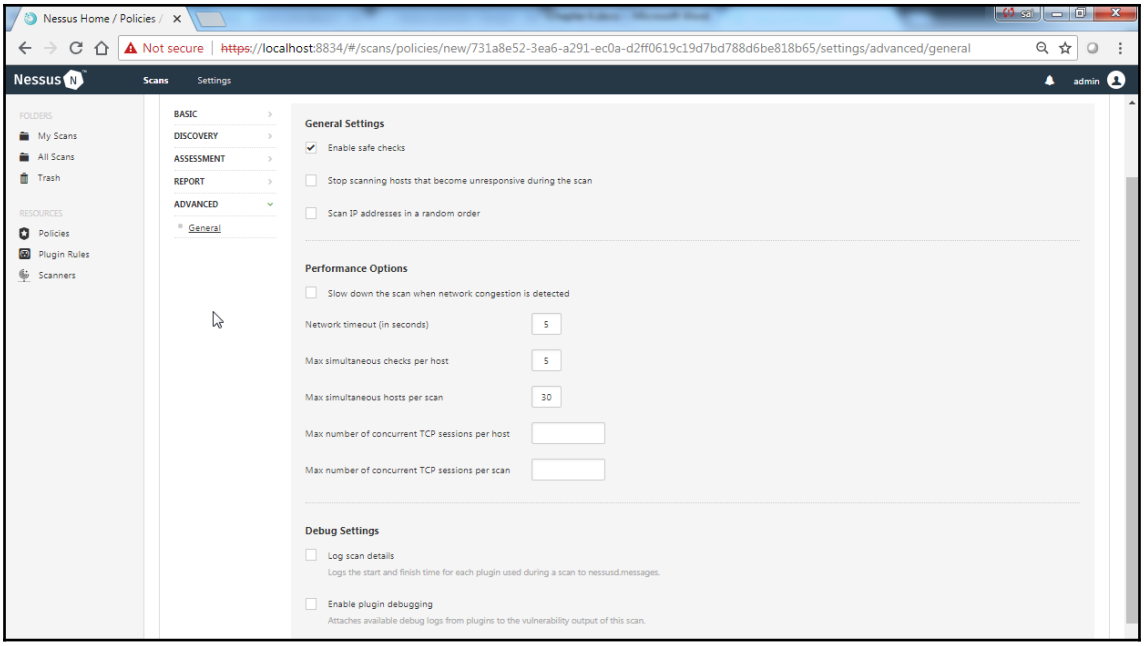

Nessus Home / Policies
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
General
Permissions
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
First scan Policy
Description
This is a Demo to create a Policy in Nessus
Save
Cancel

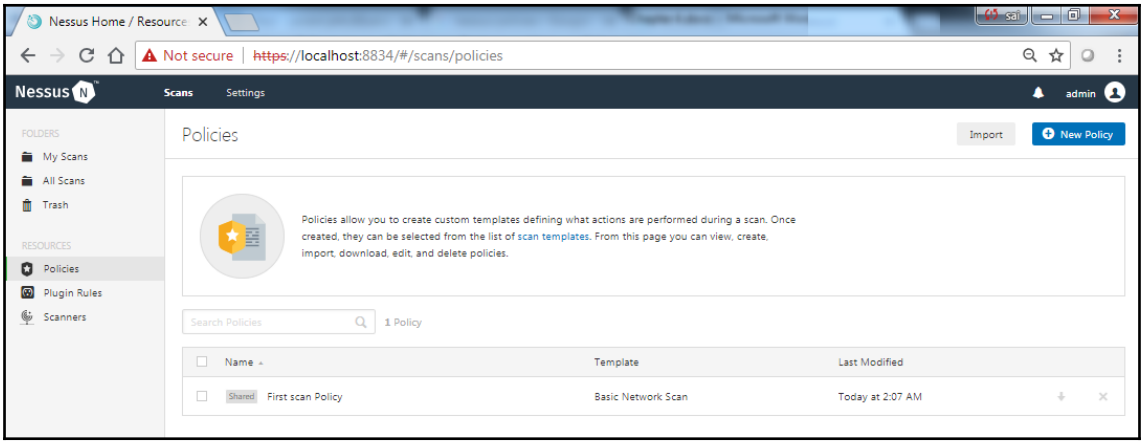

Nessus Home / Policies
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/discovery
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (common ports)
Port scan (common ports)
Port scan (all ports)
Custom
Use fast network discovery
Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)
Save
Cancel

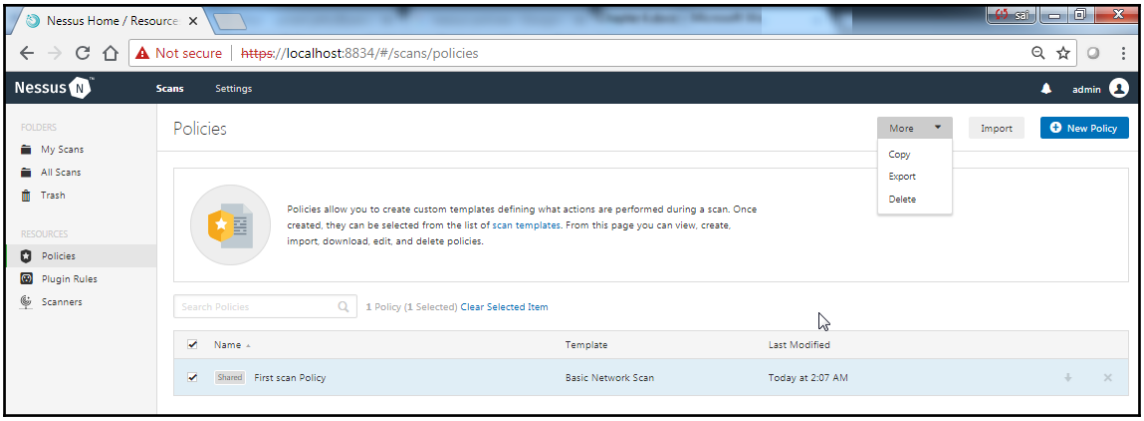

Nessus Home / Policies
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/assessment
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Default
Default
Scan for known web vulnerabilities
Scan for all web vulnerabilities (quick)
Scan for all web vulnerabilities (complex)
Custom
Disable web application scanning
Save
Cancel

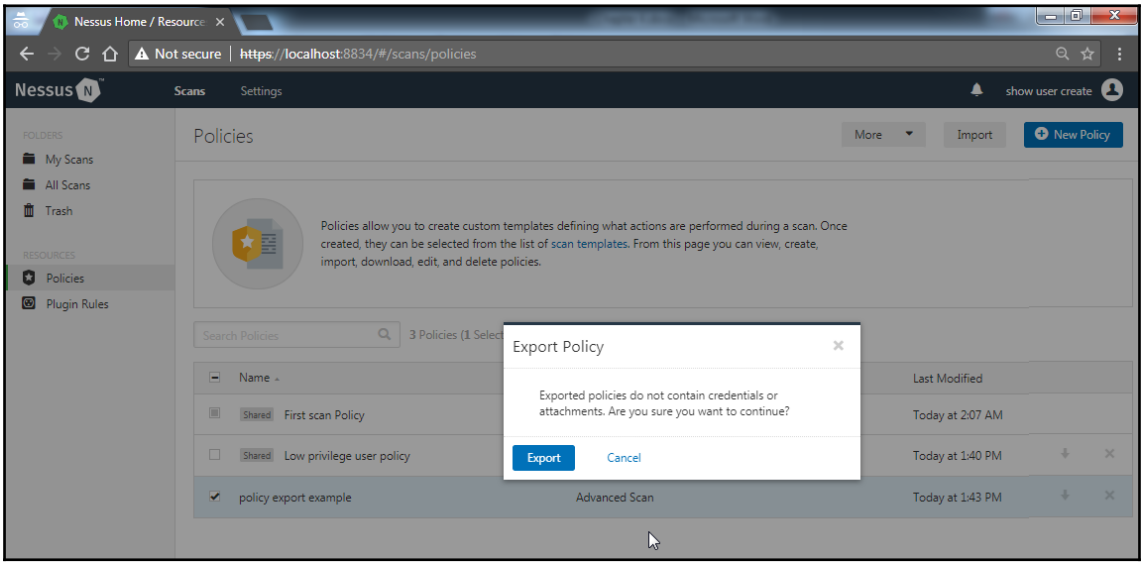

Nessus Home / Policies /
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/report
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Processing
Override normal verbosity
I have limited disk space. Report as little information as possible
Report as much information as possible
Show missing patches that have been superseded
Hide results from plugins initiated as a dependency
Output
Allow users to edit scan results
Designate hosts by their DNS name
Display hosts that respond to ping
Display unreachable hosts
Save
Cancel

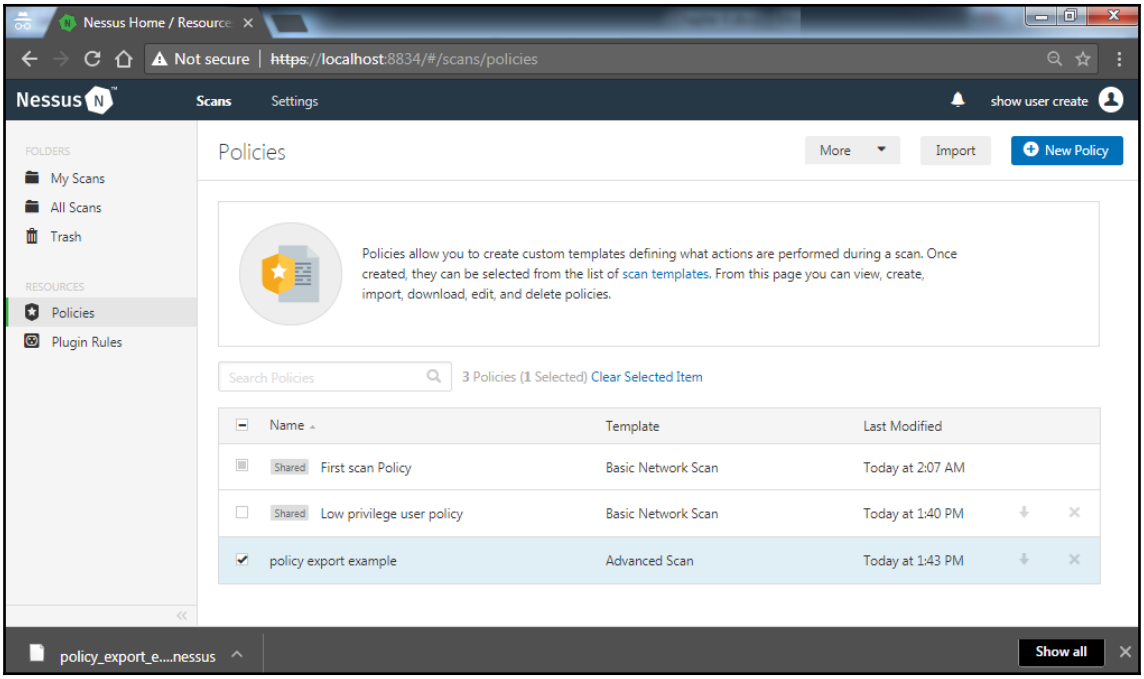

Nessus Home / Policies /
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/advanced
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Default
Default
Scan low bandwidth links
Custom
4 simultaneous checks per host (max)
5 second network read timeout
Save
Cancel

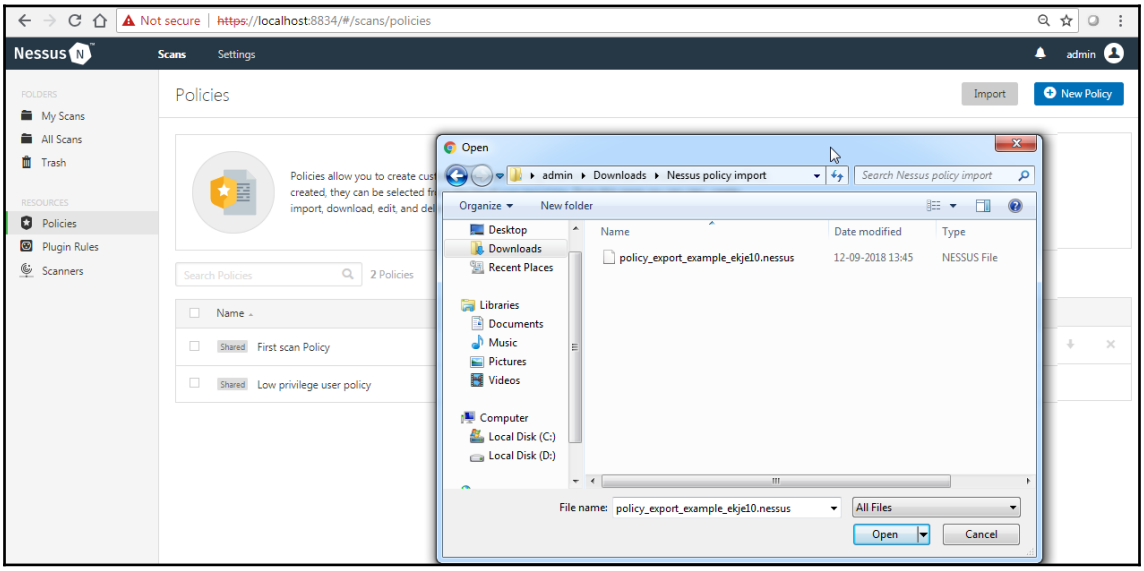

Nessus Home / Policies
Not secure
https://localhost:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/advanced/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
General
General Settings
Enable safe checks
Stop scanning hosts that become unresponsive during the scan
Scan IP addresses in a random order
Performance Options
Slow down the scan when network congestion is detected
Network timeout (in seconds)
5
Max simultaneous checks per host
5
Max simultaneous hosts per scan
30
Max number of concurrent TCP sessions per host
Max number of concurrent TCP sessions per scan
Debug Settings
Log scan details
Logs the start and finish time for each plugin used during a scan to nessusd.messages.
Enable plugin debugging
Attaches available debug logs from plugins to the vulnerability output of this scan.

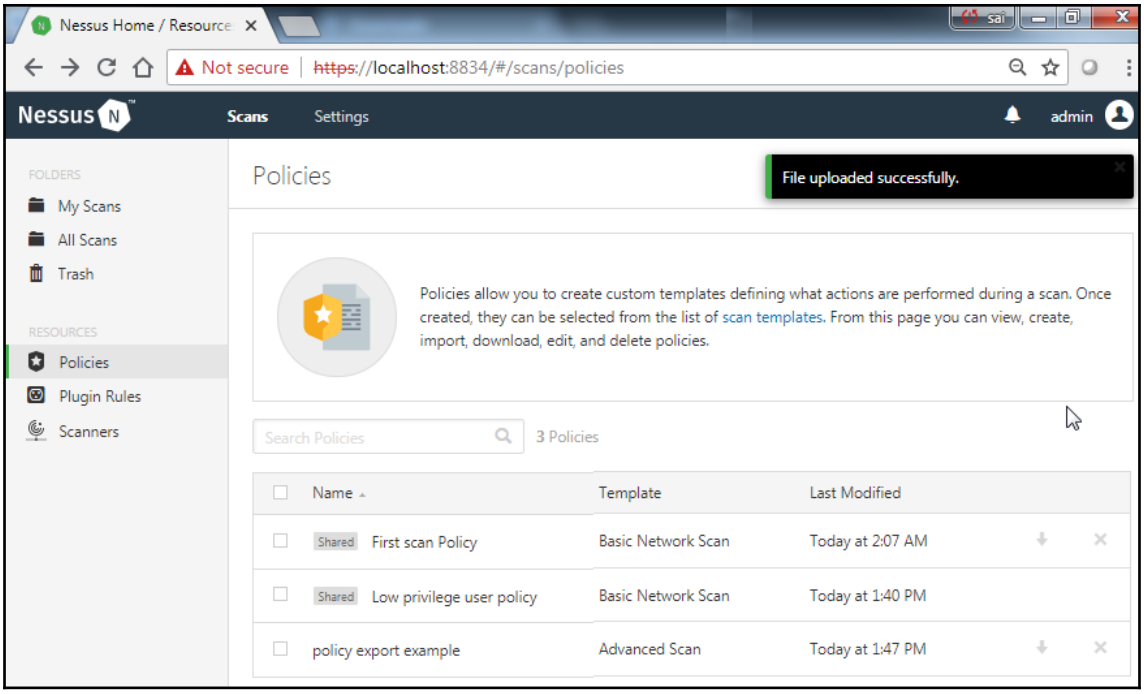

Nessus Home / Resource
Not secure
https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Policies
Import
New Policy
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
1 Policy
Name
Template
Last Modified
Shared
First scan Policy
Basic Network Scan
Today at 2:07 AM

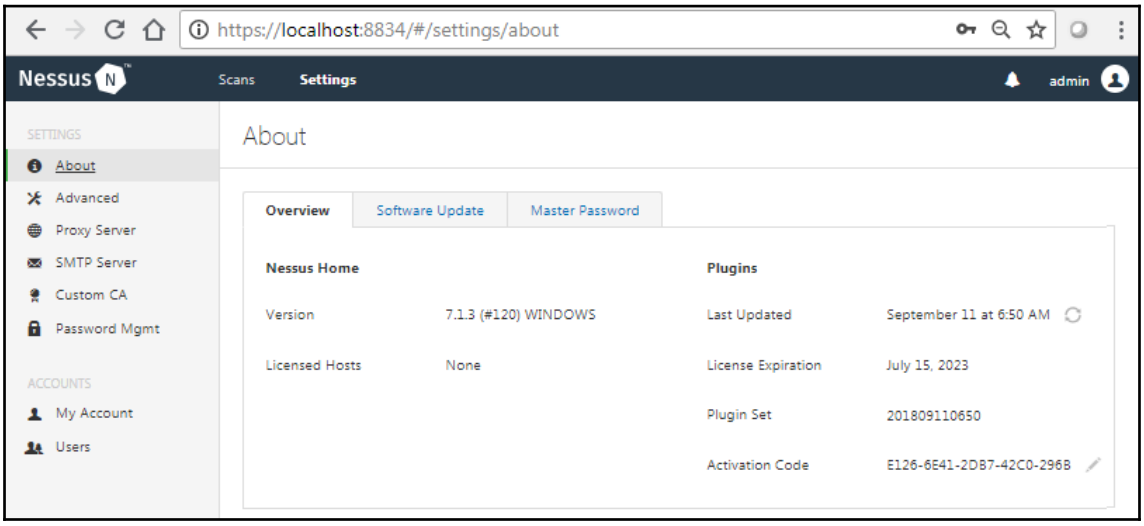

Nessus Home / Resource
Not secure
https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Policies
More
Import
New Policy
Copy
Export
Delete
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
1 Policy (1 Selected) Clear Selected Item
Name
Template
Last Modified
Shared
First scan Policy
Basic Network Scan
Today at 2:07 AM

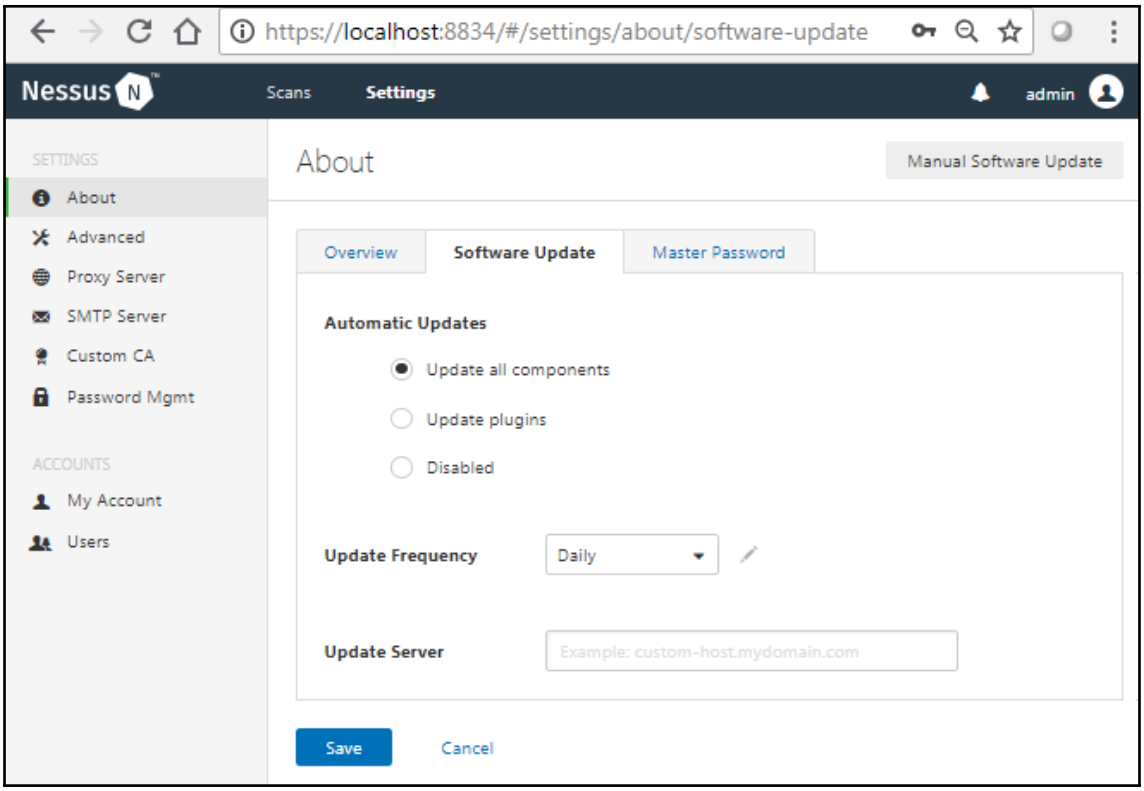

Nessus Home / Resource
Not secure
https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
show user create
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Policies
More
Import
New Policy
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
Export Policy
Exported policies do not contain credentials or attachments. Are you sure you want to continue?
Export
Cancel
Name
Last Modified
Shared
First scan Policy
Today at 2:07 AM
Shared
Low privilege user policy
Today at 1:40 PM
policy export example
Advanced Scan
Today at 1:43 PM

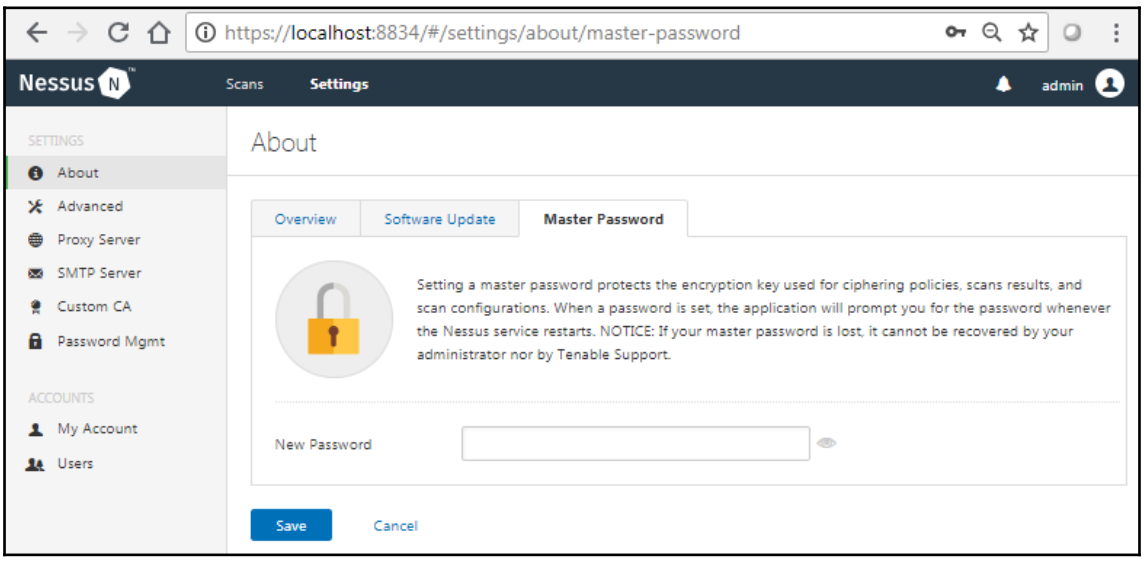

Nessus Home / Resource
Not secure | https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
show user create
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Policies
More
Import
New Policy
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
3 Policies (1 Selected) Clear Selected Item
Name
Template
Last Modified
Shared
First scan Policy
Basic Network Scan
Today at 2:07 AM
Shared
Low privilege user policy
Basic Network Scan
Today at 1:40 PM
policy export example
Advanced Scan
Today at 1:43 PM
policy_export_e....nessus
Show all

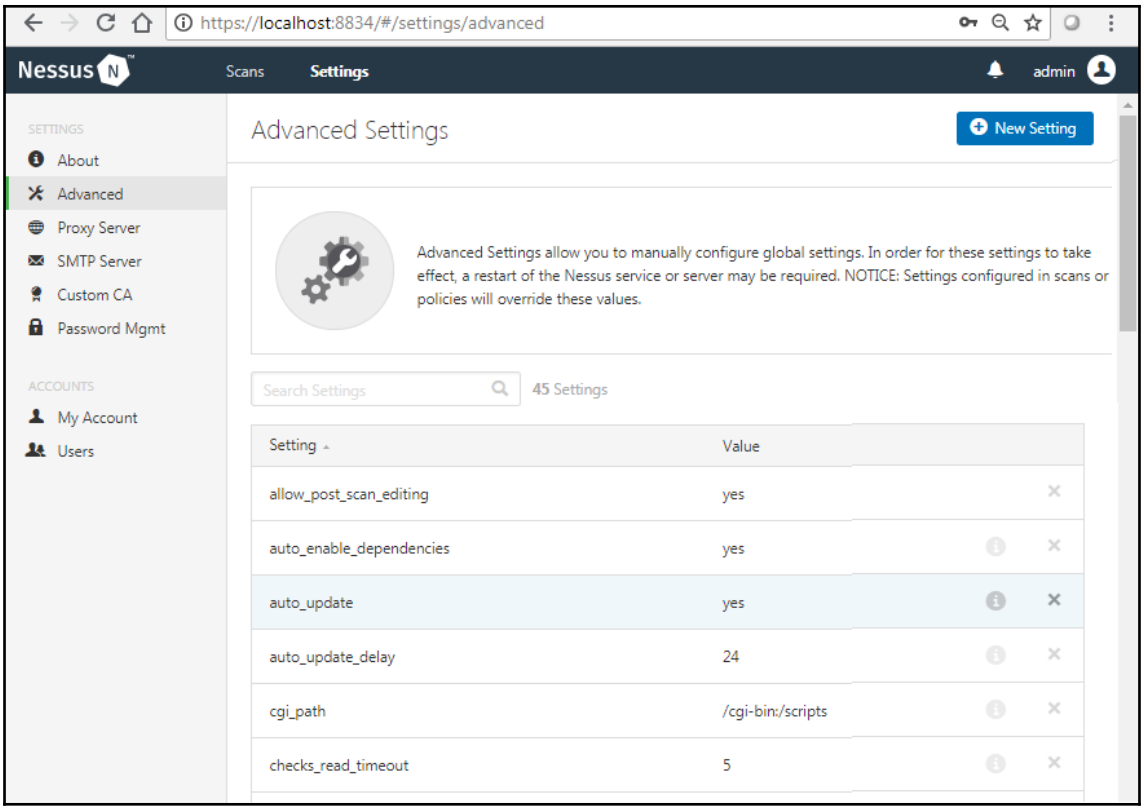

Not secure | https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
admin
Policies
Import
New Policy
Open
admin ▸ Downloads ▸ Nessus policy import
Search Nessus policy import
Organize
New folder
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Name
Date modified
Type
policy_export_example_ekje10.nessus
12-09-2018 13:45
NESSUS File
File name: policy_export_example_ekje10.nessus
All Files
Open
Cancel

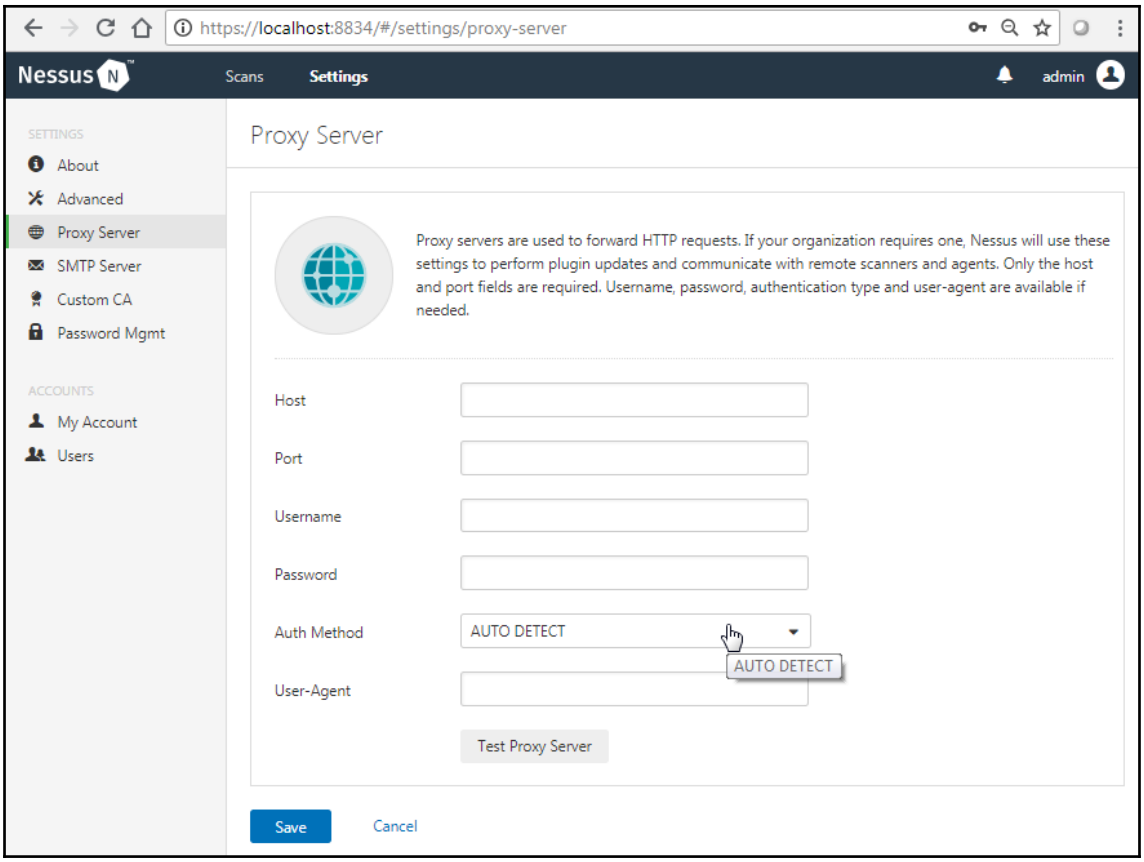

Nessus Home / Resource
Not secure
https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Policies
File uploaded successfully.
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
3 Policies
Name
Template
Last Modified
Shared
First scan Policy
Basic Network Scan
Today at 2:07 AM
Shared
Low privilege user policy
Basic Network Scan
Today at 1:40 PM
policy export example
Advanced Scan
Today at 1:47 PM

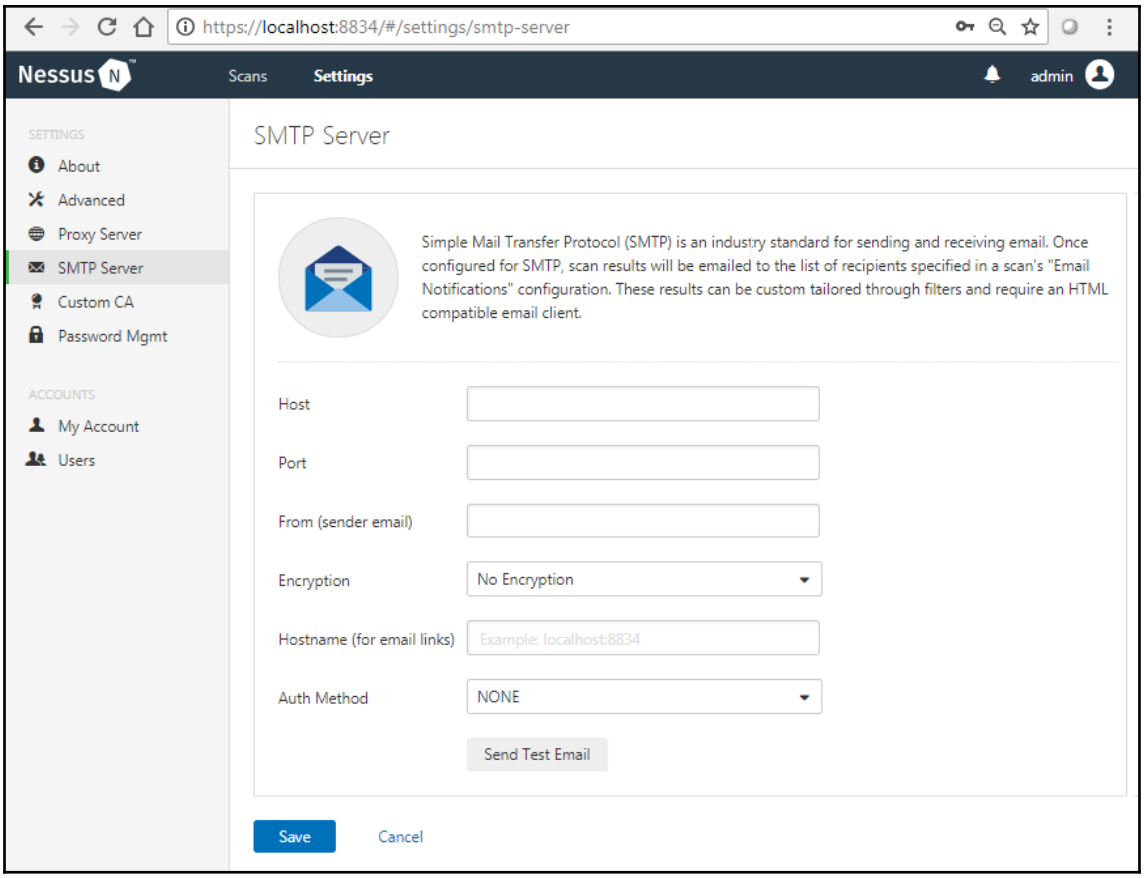

https://localhost:8834/#/settings/about
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
About
Overview
Software Update
Master Password
Nessus Home
Version
7.1.3 (#120) WINDOWS
Licensed Hosts
None
Plugins
Last Updated
September 11 at 6:50 AM
License Expiration
July 15, 2023
Plugin Set
201809110650
Activation Code
E126-6E41-2D87-42C0-296B

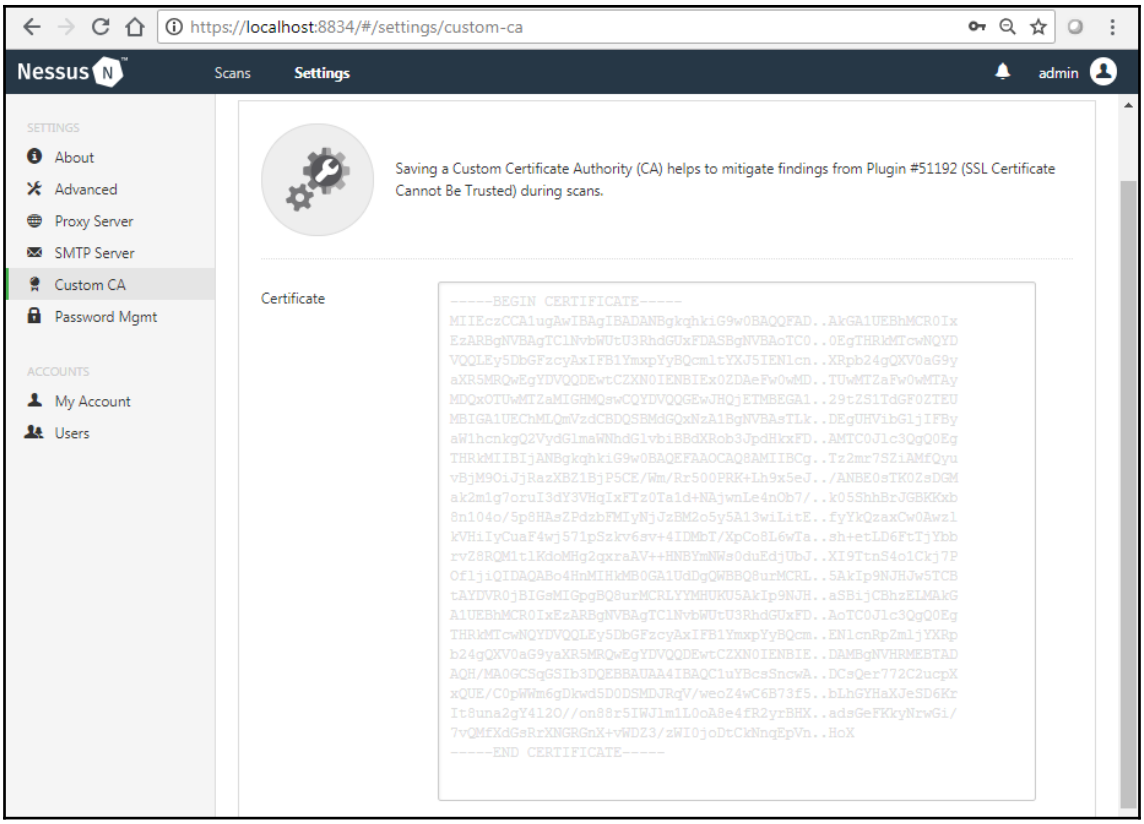

https://localhost:8834/#/settings/about/software-update
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
About
Manual Software Update
Overview
Software Update
Master Password
Automatic Updates
Update all components
Update plugins
Disabled
Update Frequency
Daily
Update Server
Example: custom-host.mydomain.com
Save
Cancel

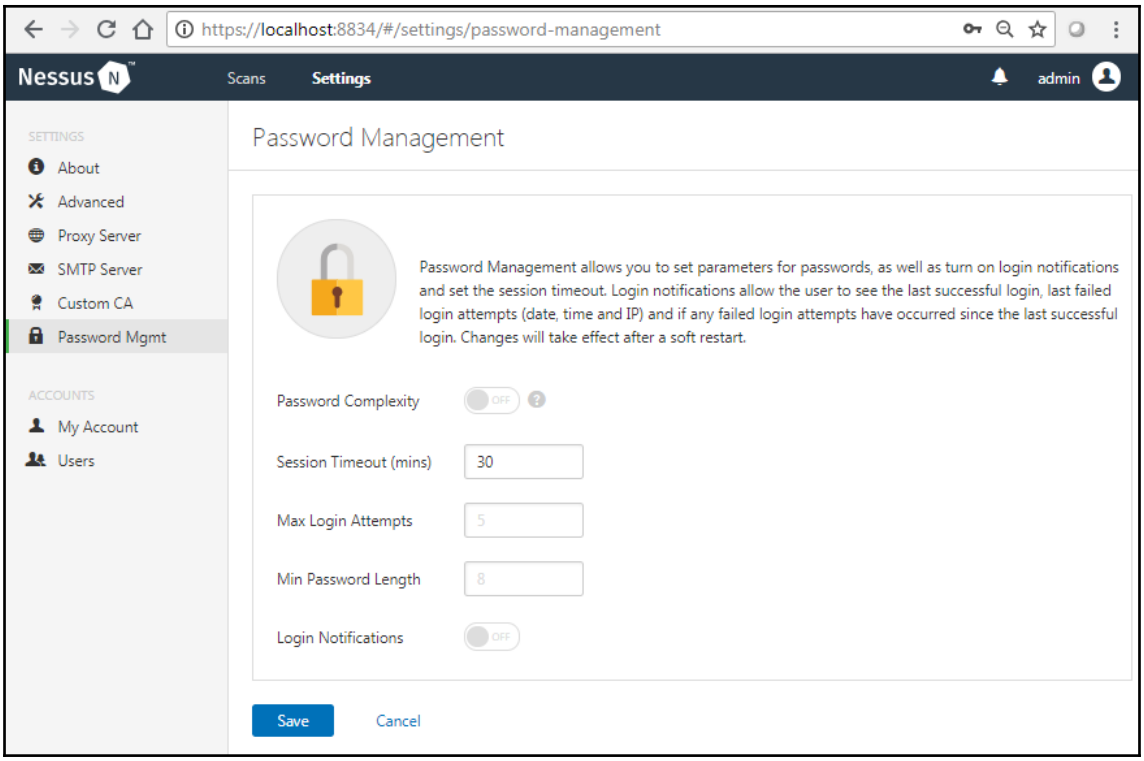

https://localhost:8834/#/settings/about/master-password
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
About
Overview
Software Update
Master Password
Setting a master password protects the encryption key used for ciphering policies, scans results, and scan configurations. When a password is set, the application will prompt you for the password whenever the Nessus service restarts. NOTICE: If your master password is lost, it cannot be recovered by your administrator nor by Tenable Support.
New Password
Save
Cancel

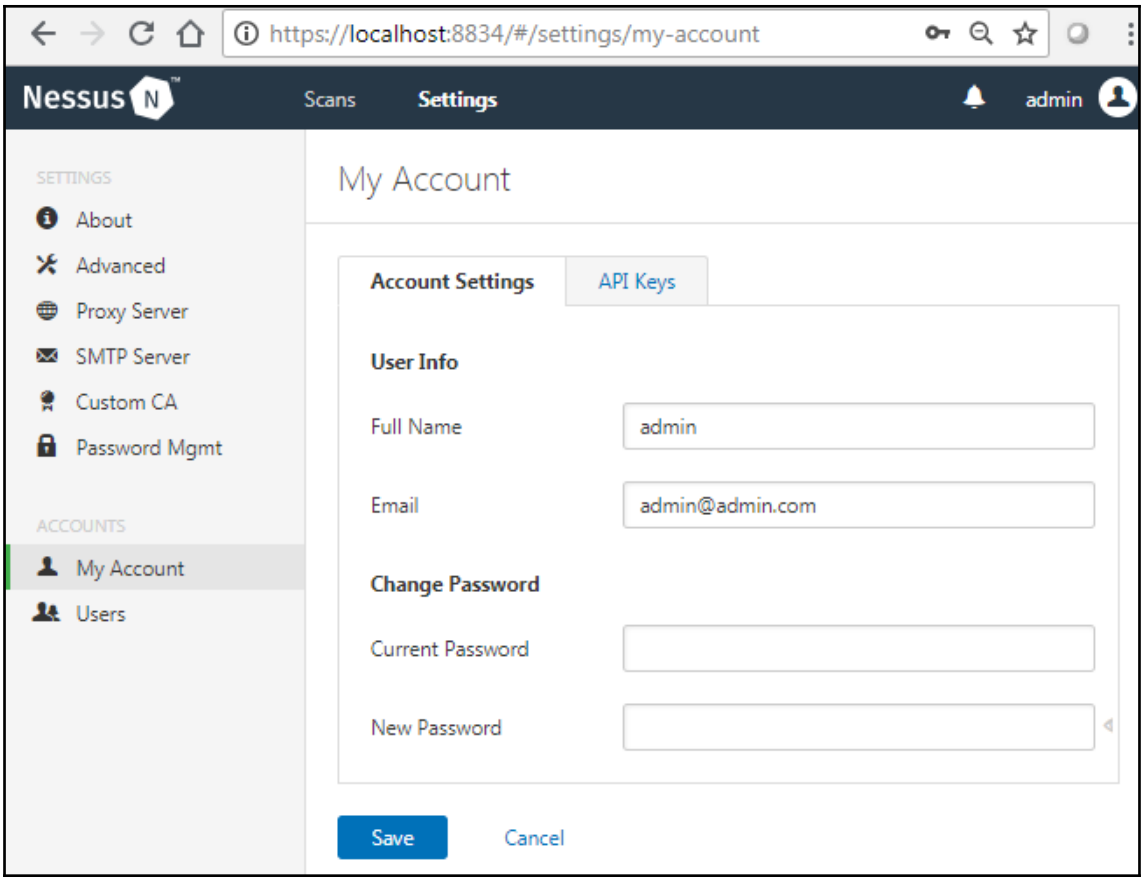

https://localhost:8834/#/settings/advanced
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Advanced Settings
New Setting
Advanced Settings allow you to manually configure global settings. In order for these settings to take effect, a restart of the Nessus service or server may be required. NOTICE: Settings configured in scans or policies will override these values.
Search Settings
45 Settings
Setting
Value
allow_post_scan_editing
yes
auto_enable_dependencies
yes
auto_update
yes
auto_update_delay
24
cgi_path
/cgi-bin:/scripts
checks_read_timeout
5

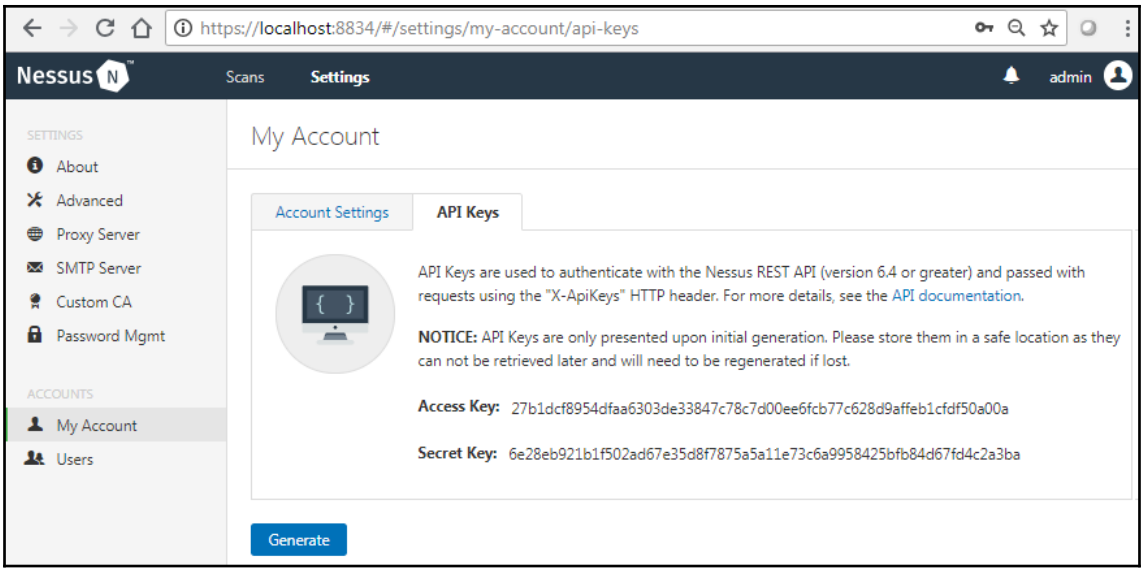

https://localhost:8834/#/settings/proxy-server
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Proxy Server
Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus will use these settings to perform plugin updates and communicate with remote scanners and agents. Only the host and port fields are required. Username, password, authentication type and user-agent are available if needed.
Host
Port
Username
Password
Auth Method
AUTO DETECT
AUTO DETECT
User-Agent
Test Proxy Server
Save
Cancel

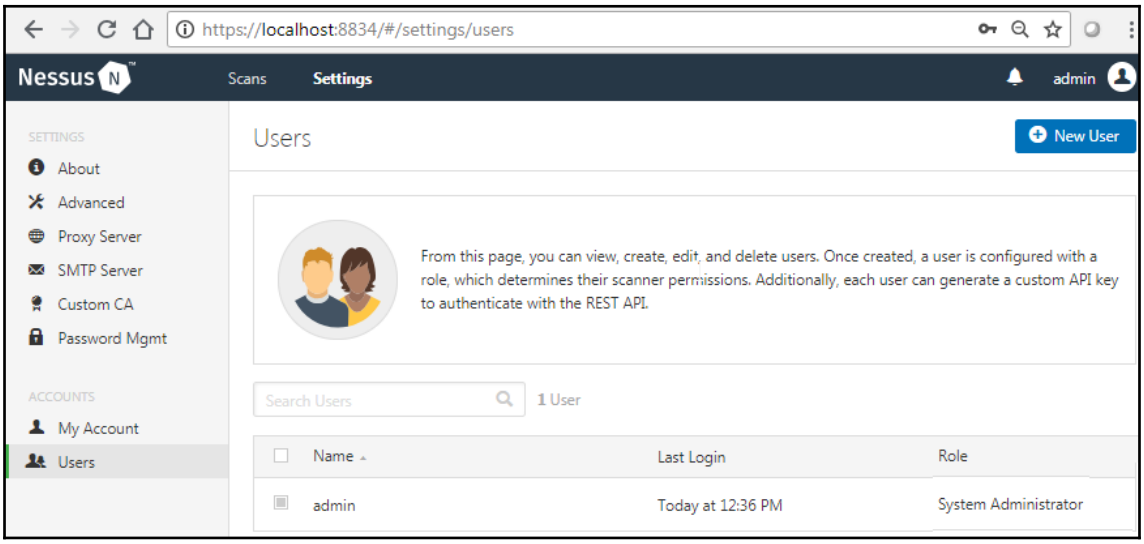

https://localhost:8834/#/settings/smtp-server
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
SMTP Server
Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, scan results will be emailed to the list of recipients specified in a scan's "Email Notifications" configuration. These results can be custom tailored through filters and require an HTML compatible email client.
Host
Port
From (sender email)
Encryption
No Encryption
Hostname (for email links)
Example: localhost:8834
Auth Method
NONE
Send Test Email
Save
Cancel

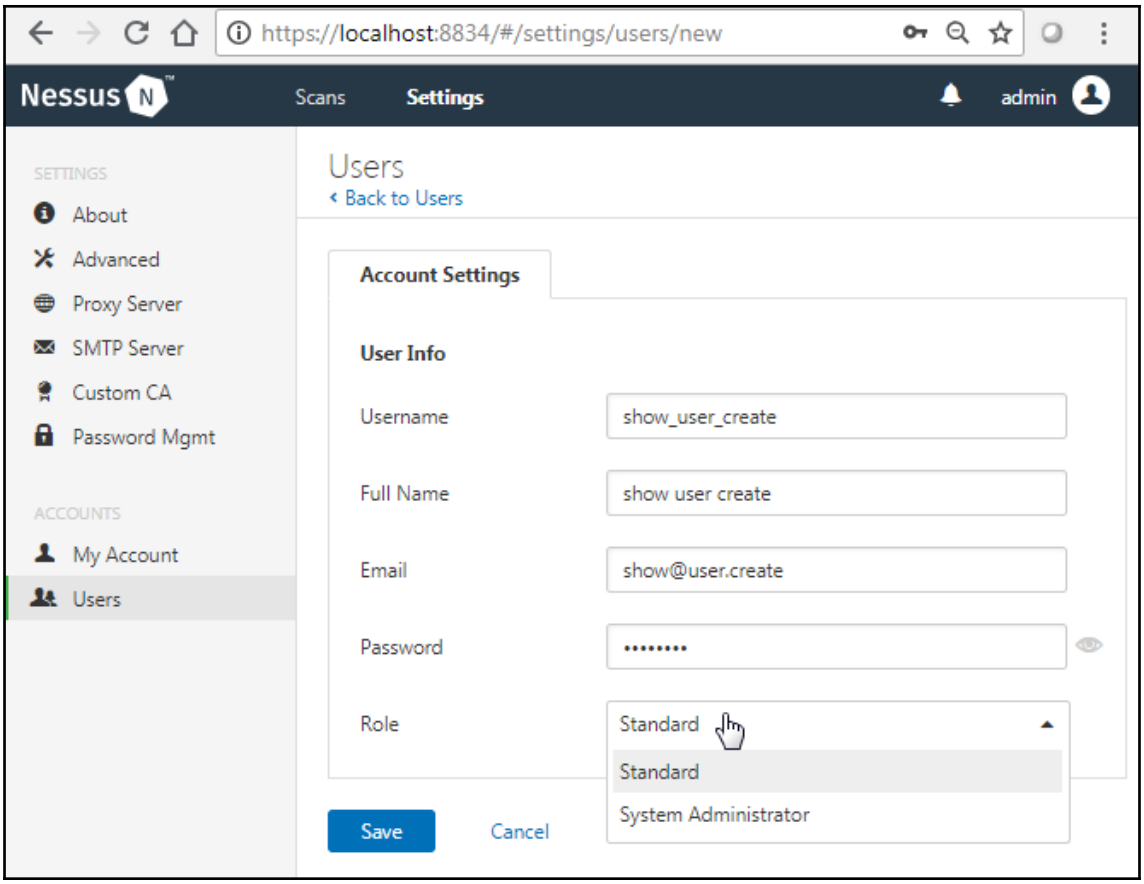

https://localhost:8834/#/settings/custom-ca
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Saving a Custom Certificate Authority (CA) helps to mitigate findings from Plugin #51192 (SSL Certificate Cannot Be Trusted) during scans.
Certificate
-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD..AkGA1UEBhMCR0Ix
EzARBgNVBAgTClNvbWUtU3RhdGUxFDASBgNVBAoTC0..0EgTHRkMTcwNQYD
VQQLEy5DbGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcn..XRpb24gQXV0aG9y
aXR5MRQwEgYDVQQDEwtCZXN0IENBIEx0ZDAeFw0wMD..TUwMTZaFw0wMTAy
MDQxOTUwMTZaMIGHMQswCQYDVQQGEwJHQjETMBEGA1..29tZS1TdGF0ZTEU
MBIGA1UEChMLQmVzdCBDQSBMdGQxNzA1BgNVBAsTLk..DEgUHVibGljIFBy
aWlhcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFD..AMTC0J1c3QgQ0Eg
THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg..Tz2mr7SZiAMfQyu
vBjM9OiJjRazXBZ1BjP5CE/Wm/Rr500PRK+Lh9x5eJ../ANBE0sTK0ZsDGM
ak2m1g7oruI3dY3VHqIxFTz0Ta1d+NAjwnLe4nOb7/..k05ShhBrJGBKKxb
8n104o/5p8HAsZPdzbFMIyNjJzBM2o5y5A13wiLitE..fyYkQzaxCw0Awzl
kVHiIyCuaF4wj571pSzkv6sv+4IDMbT/XpCo8L6wTa..sh+etLD6FtTjYbb
rvZ8RQM1tlKdoMHg2qxraAV++HNBYmNWs0duEdjUbJ..XI9TtnS4o1Ckj7P
OfljiQIDAQABo4HnMIHkMB0GA1UdDgQWBBQ8urMCRL..5AkIp9NJHJw5TCB
tAYDVR0jBIGsMIGpgBQ8urMCRLYYMHUKU5AkIp9NJH..aSBijCBhzELMAkG
A1UEBhMCR0IxEzARBgNVBAgTClNvbWUtU3RhdGUxFD..AoTC0J1c3QgQ0Eg
THRkMTcwNQYDVQQLEy5DbGFzcyAxIFB1YmxpYyBQcm..ENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MRQwEgYDVQQDEwtCZXN0IENBIE..DAMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBBAUAA4IBAQC1uYBcsSncwA..DCsQer772C2ucpX
xQUE/C0pWWm6gDkwd5D0DSMDJRqV/weoZ4wC6B73f5..bLhGYHaXJeSD6Kr
It8una2gY4120//on88r5IWJlm1L0oA8e4fR2yrBHX..adsGeFKkyNrwGi/
7vQMfXdGsRrXNGRGnX+vWDZ3/zWI0joDtCkNnqEpVn..HoX
-----END CERTIFICATE-----

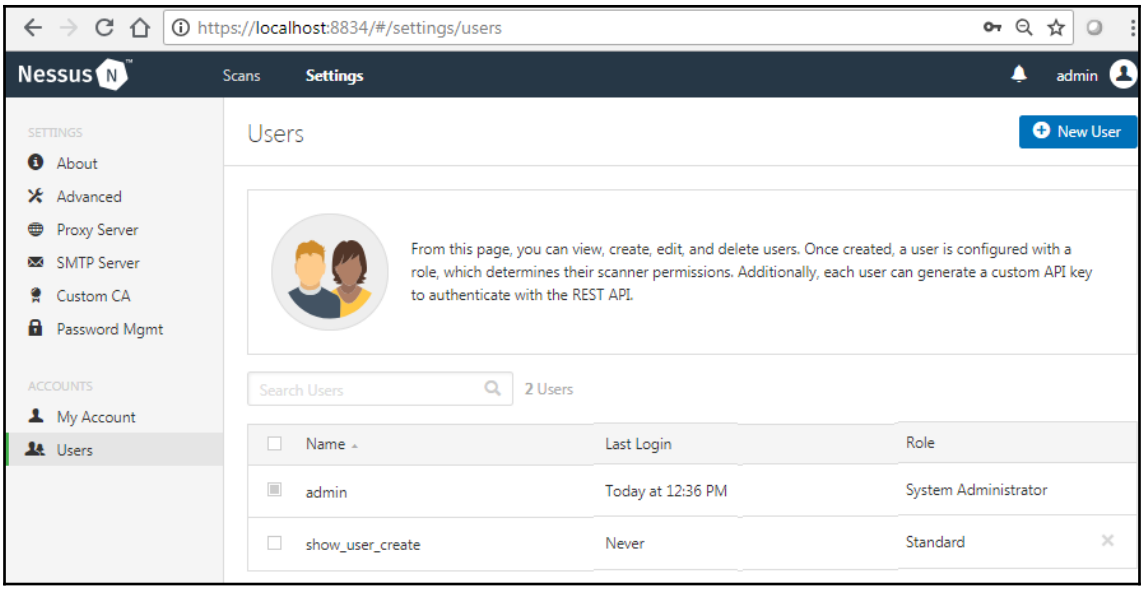

https://localhost:8834/#/settings/password-management
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Password Management
Password Management allows you to set parameters for passwords, as well as turn on login notifications and set the session timeout. Login notifications allow the user to see the last successful login, last failed login attempts (date, time and IP) and if any failed login attempts have occurred since the last successful login. Changes will take effect after a soft restart.
Password Complexity
OFF
Session Timeout (mins)
30
Max Login Attempts
5
Min Password Length
8
Login Notifications
OFF
Save
Cancel

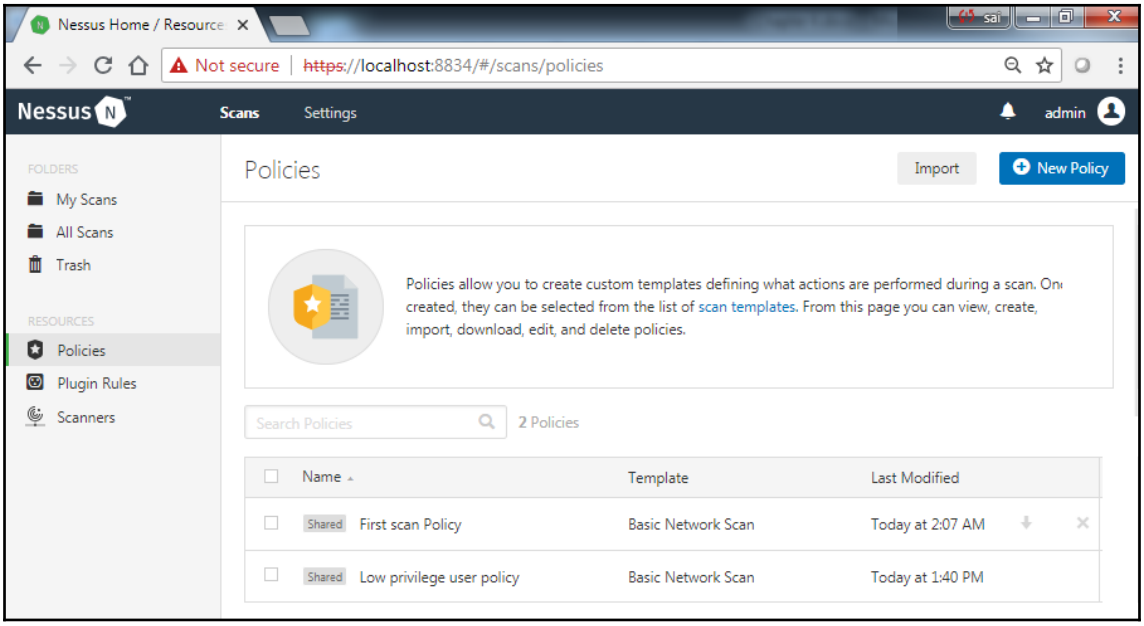

https://localhost:8834/#/settings/my-account
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
My Account
Account Settings
API Keys
User Info
Full Name
admin
Email
admin@admin.com
Change Password
Current Password
New Password
Save
Cancel

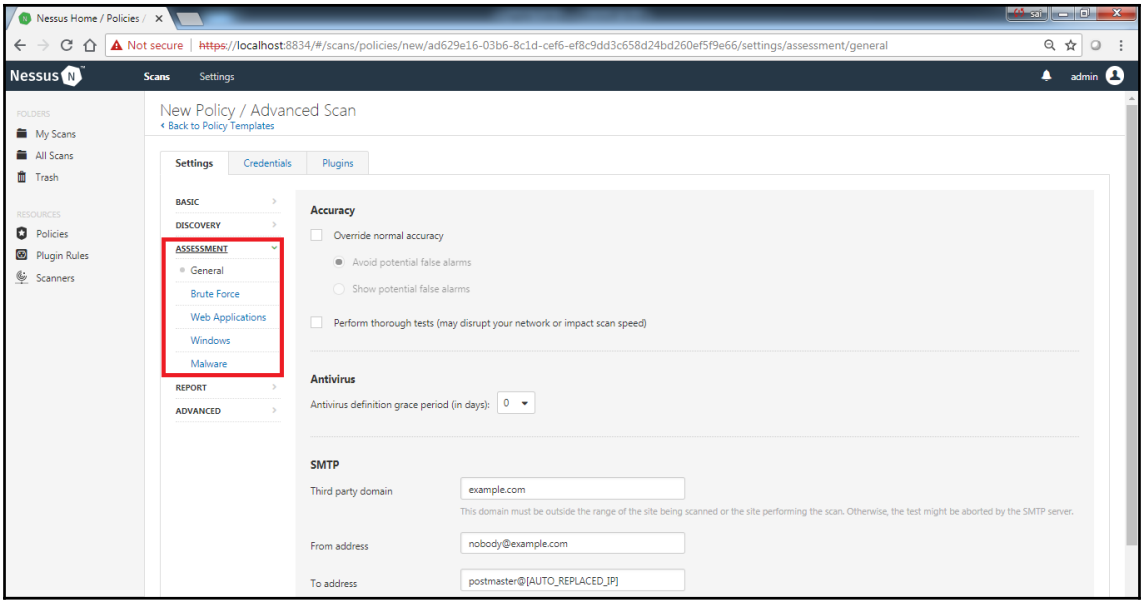

https://localhost:8834/#/settings/my-account/api-keys
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
My Account
Account Settings
API Keys
API Keys are used to authenticate with the Nessus REST API (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header. For more details, see the API documentation.
NOTICE: API Keys are only presented upon initial generation. Please store them in a safe location as they can not be retrieved later and will need to be regenerated if lost.
Access Key: 27b1dcf8954dfaa6303de33847c78c7d00ee6fcb77c628d9affeb1cfdf50a00a
Secret Key: 6e28eb921b1f502ad67e35d8f7875a5a11e73c6a9958425bfb84d67fd4c2a3ba
Generate

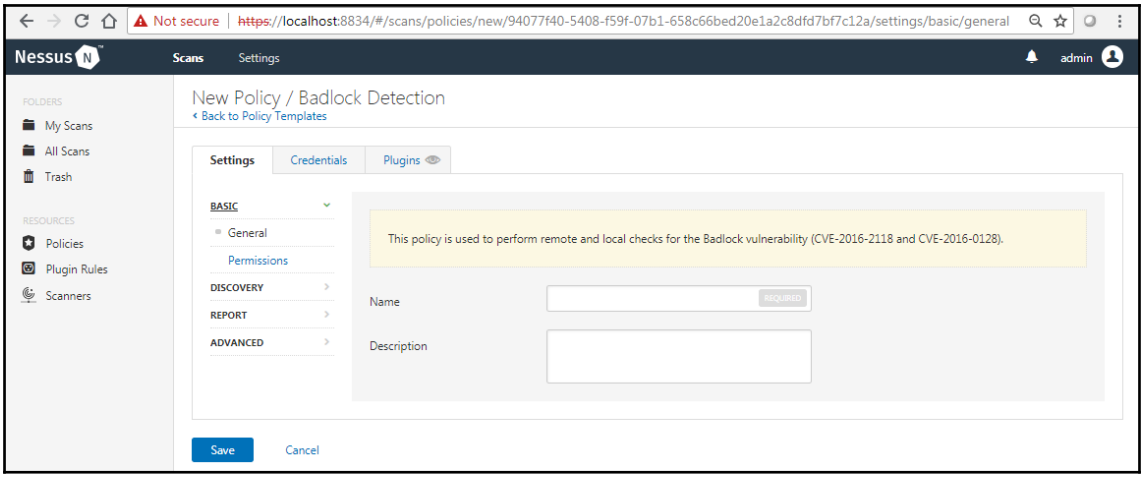

https://localhost:8834/#/settings/users
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Users
New User
From this page, you can view, create, edit, and delete users. Once created, a user is configured with a role, which determines their scanner permissions. Additionally, each user can generate a custom API key to authenticate with the REST API.
Search Users
1 User
Name
Last Login
Role
admin
Today at 12:36 PM
System Administrator

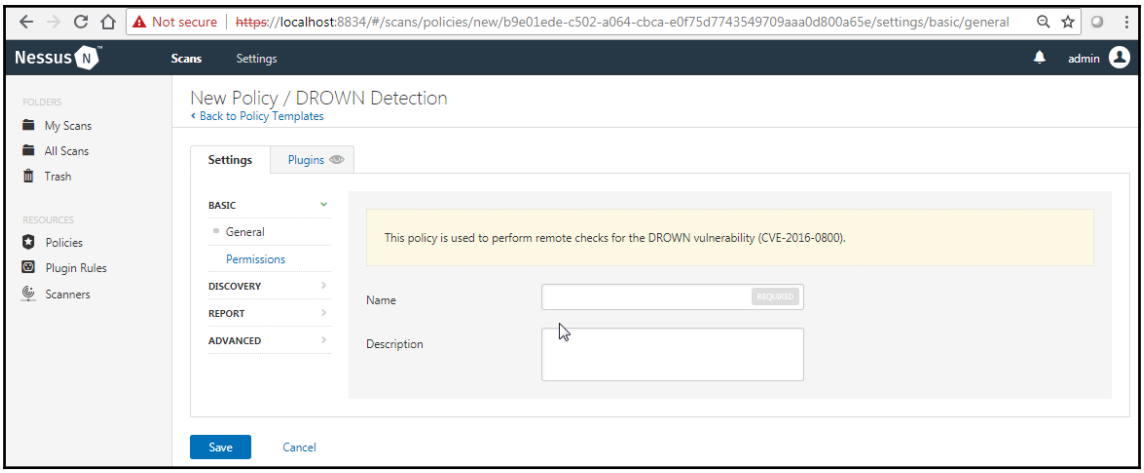

https://localhost:8834/#/settings/users/new
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Users
Back to Users
Account Settings
User Info
Username
show_user_create
Full Name
show user create
Email
show@user.create
Password
Role
Standard
Standard
System Administrator
Save
Cancel

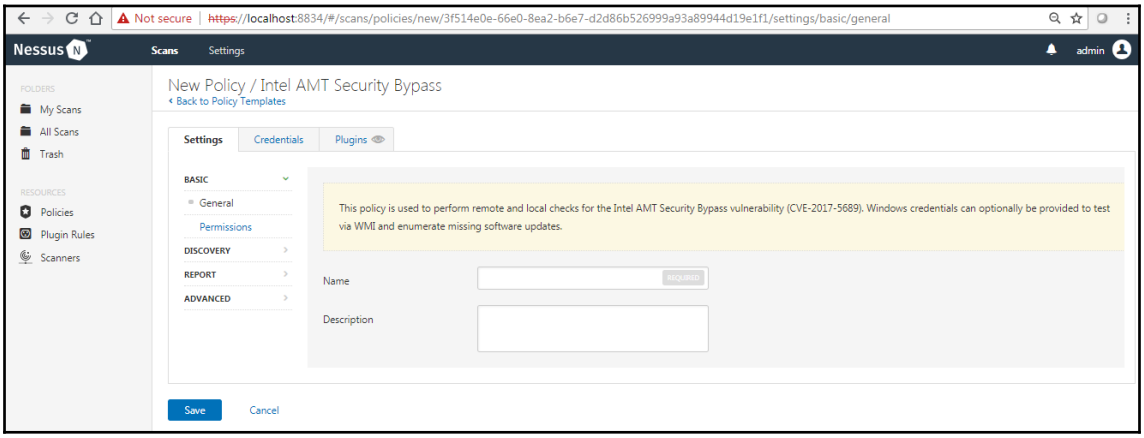

https://localhost:8834/#/settings/users
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
ACCOUNTS
My Account
Users
Users
New User
From this page, you can view, create, edit, and delete users. Once created, a user is configured with a role, which determines their scanner permissions. Additionally, each user can generate a custom API key to authenticate with the REST API.
Search Users
2 Users
Name
Last Login
Role
admin
Today at 12:36 PM
System Administrator
show_user_create
Never
Standard

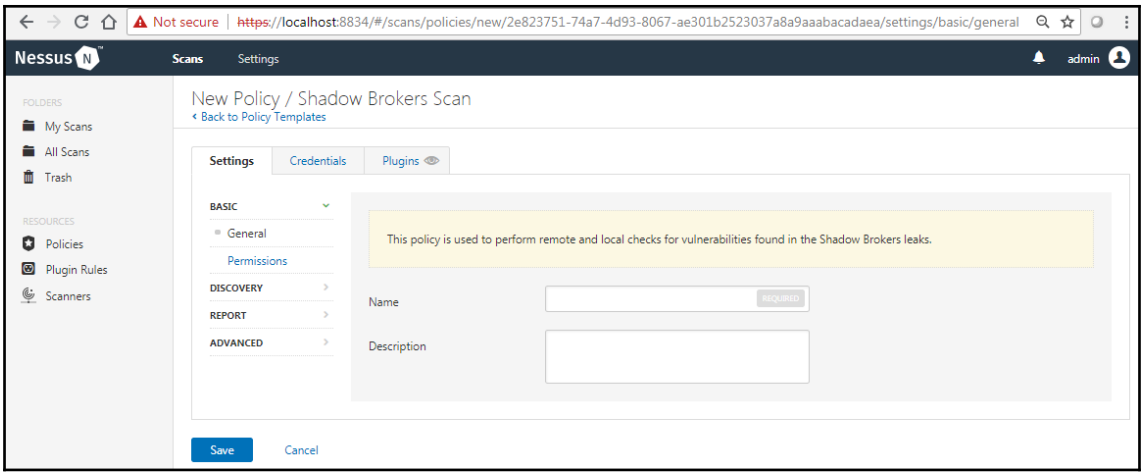

Nessus Home / Resource
Not secure
https://localhost:8834/#/scans/policies
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Policies
Import
New Policy
Policies allow you to create custom templates defining what actions are performed during a scan. On
created, they can be selected from the list of scan templates. From this page you can view, create,
import, download, edit, and delete policies.
Search Policies
2 Policies
Name
Template
Last Modified
Shared
First scan Policy
Basic Network Scan
Today at 2:07 AM
Shared
Low privilege user policy
Basic Network Scan
Today at 1:40 PM

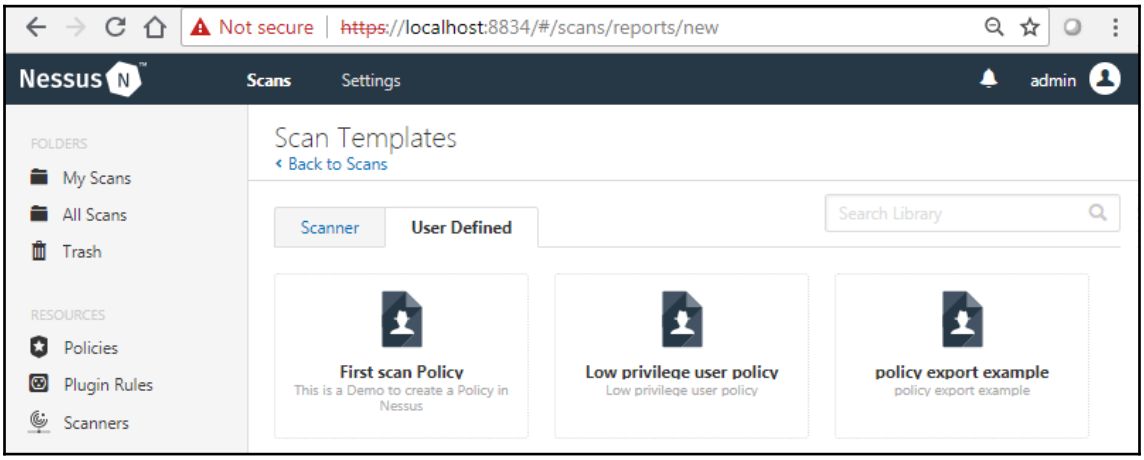

Nessus Home / Policies
Not secure https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/assessment/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
General
Brute Force
Web Applications
Windows
Malware
REPORT
ADVANCED
Accuracy
Override normal accuracy
Avoid potential false alarms
Show potential false alarms
Perform thorough tests (may disrupt your network or impact scan speed)
Antivirus
Antivirus definition grace period (in days):
0
SMTP
Third party domain
example.com
This domain must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be aborted by the SMTP server.
From address
nobody@example.com
To address
postmaster@[AUTO_REPLACED_IP]

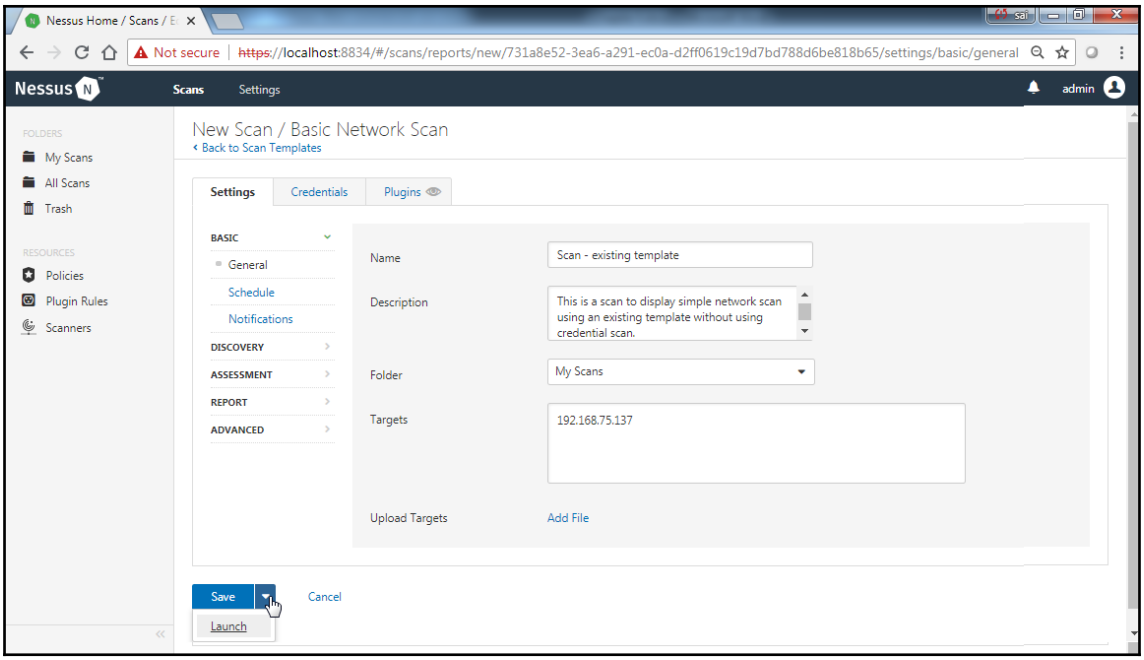

Not secure https://localhost:8834/#/scans/policies/new/94077f40-5408-f59f-07b1-658c66bed20e1a2c8dfd7bf7c12a/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Badlock Detection
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
General
Permissions
DISCOVERY
REPORT
ADVANCED
This policy is used to perform remote and local checks for the Badlock vulnerability (CVE-2016-2118 and CVE-2016-0128).
Name
REQUIRED
Description
Save
Cancel

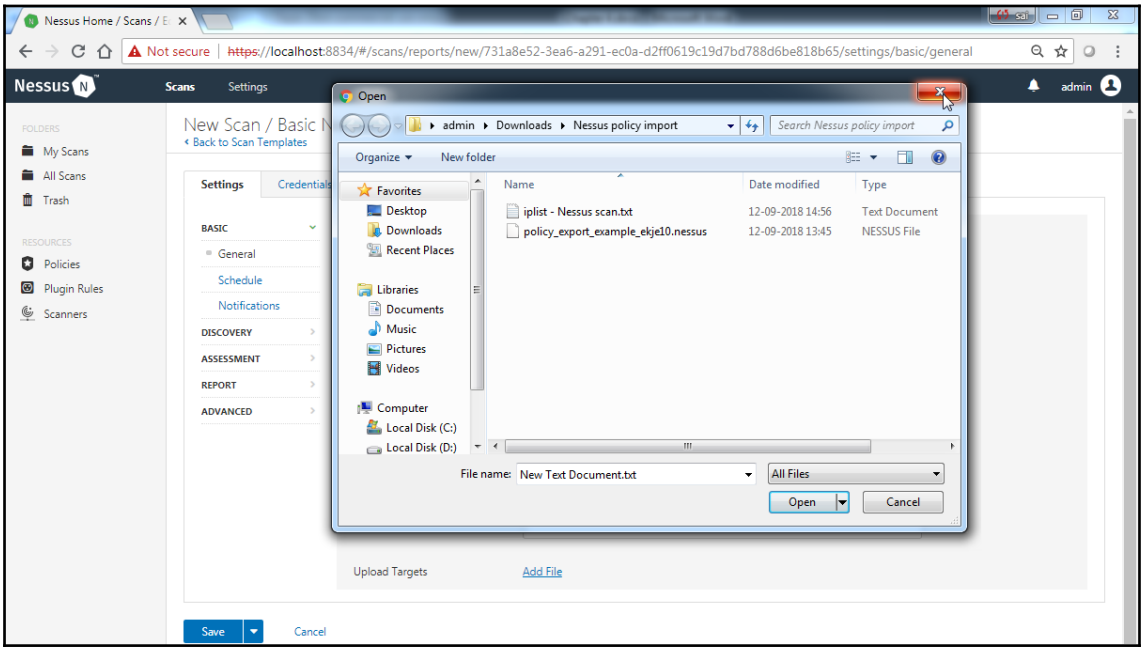

Not secure | https://localhost:8834/#/scans/policies/new/b9e01ede-c502-a064-cbca-e0f75d7743549709aaa0d800a65e/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / DROWN Detection
Back to Policy Templates
Settings
Plugins
BASIC
General
Permissions
DISCOVERY
REPORT
ADVANCED
This policy is used to perform remote checks for the DROWN vulnerability (CVE-2016-0800).
Name
REQUIRED
Description
Save
Cancel

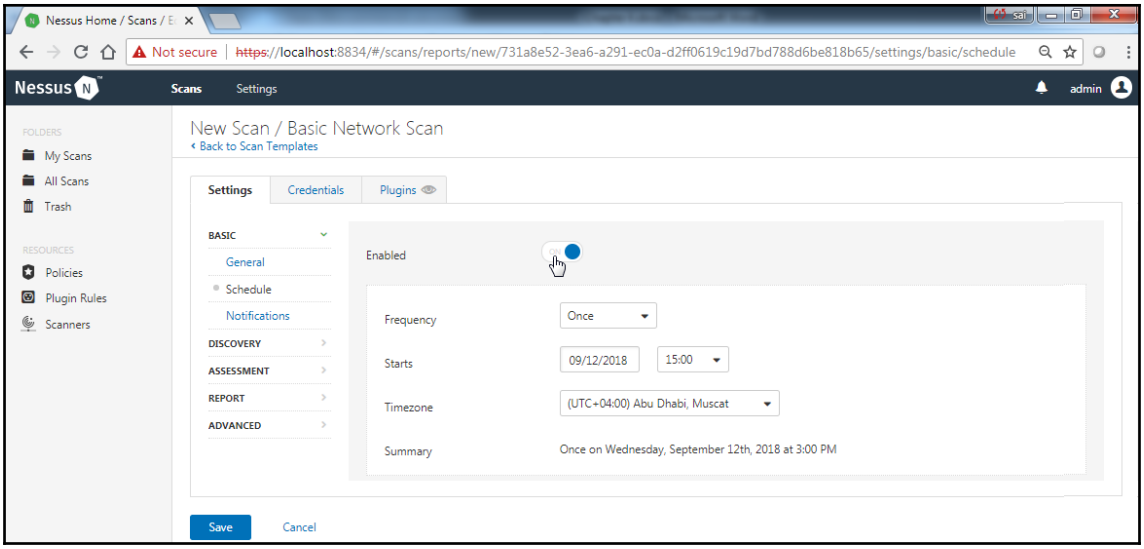

Not secure | https://localhost:8834/#/scans/policies/new/3f514e0e-66e0-8ea2-b6e7-d2d86b526999a93a89944d19e1f1/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Intel AMT Security Bypass
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
General
Permissions
DISCOVERY
REPORT
ADVANCED
This policy is used to perform remote and local checks for the Intel AMT Security Bypass vulnerability (CVE-2017-5689). Windows credentials can optionally be provided to test via WMI and enumerate missing software updates.
Name
REQUIRED
Description
Save
Cancel

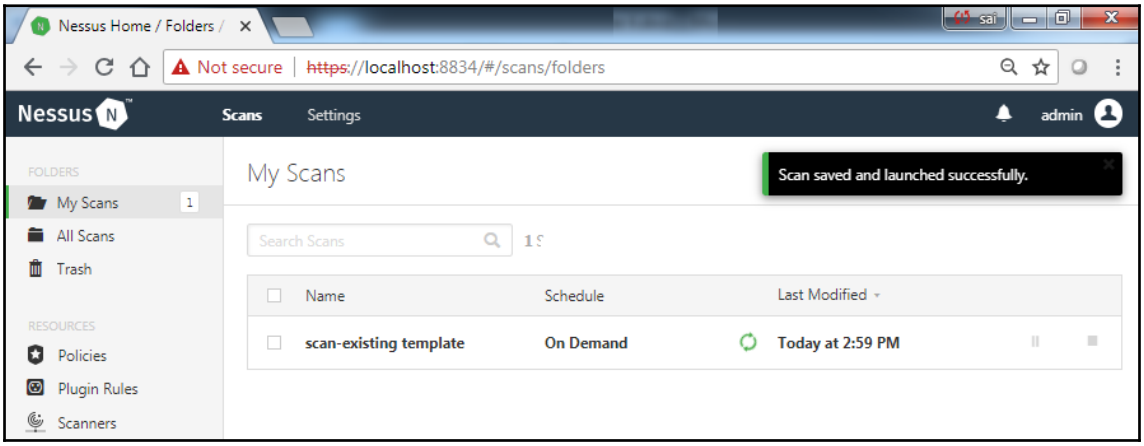

Not secure | https://localhost:8834/#/scans/policies/new/2e823751-74a7-4d93-8067-ae301b2523037a8a9aaabacadaea/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Policy / Shadow Brokers Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
General
Permissions
DISCOVERY
REPORT
ADVANCED
This policy is used to perform remote and local checks for vulnerabilities found in the Shadow Brokers leaks.
Name
REQUIRED
Description
Save
Cancel

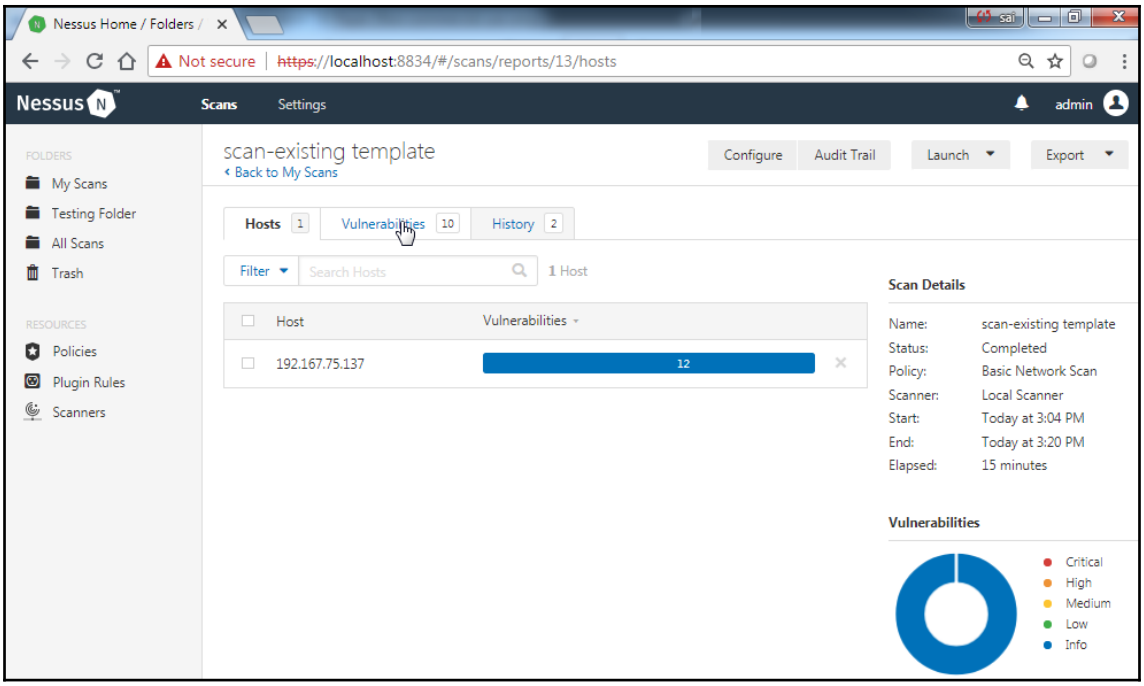

Not secure | https://localhost:8834/#/scans/reports/new
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
First scan Policy
This is a Demo to create a Policy in Nessus
Low privileqe user policy
Low privileqe user policy
policy export example
policy export example

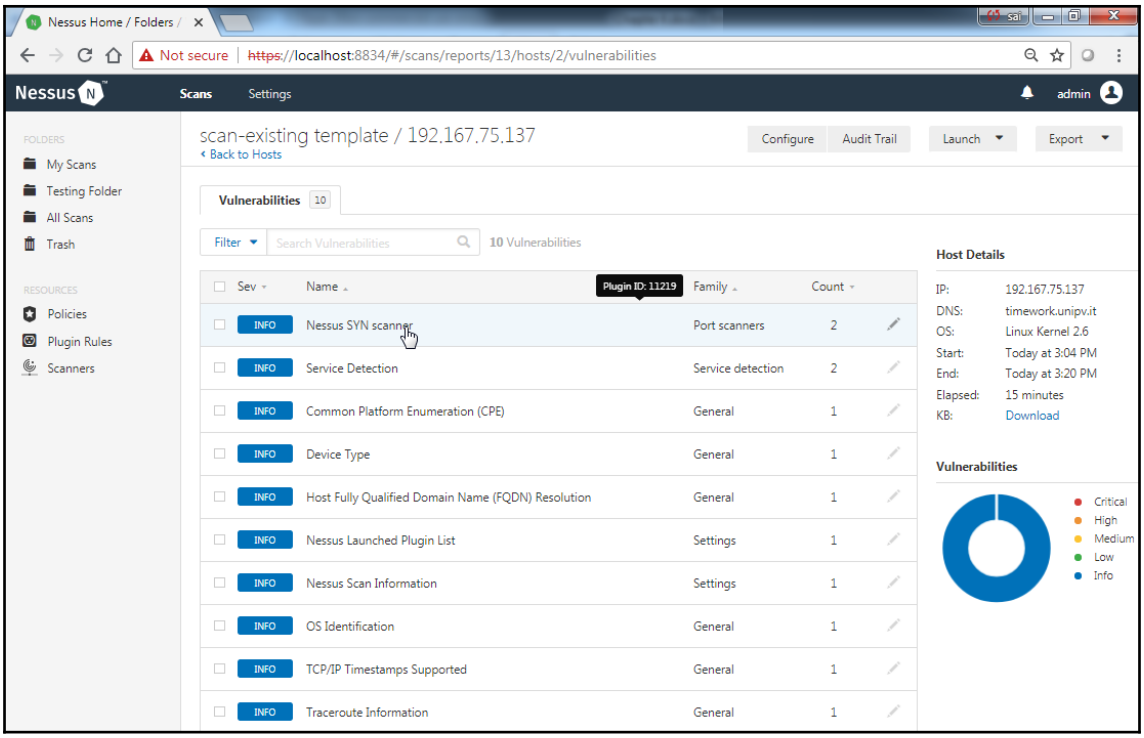

Nessus Home / Scans /
Not secure
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Scan - existing template
Description
This is a scan to display simple network scan using an existing template without using credential scan.
Folder
My Scans
Targets
192.168.75.137
Upload Targets
Add File
Save
Launch
Cancel

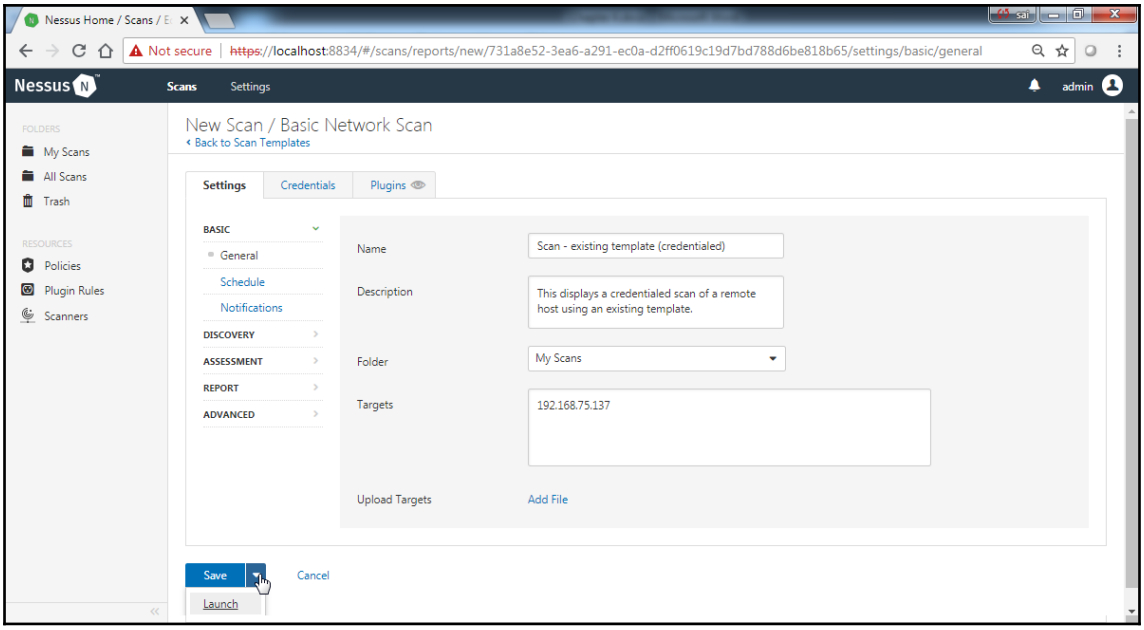

Nessus Home / Scans /
Not secure
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Nessus
Scans
Settings
admin
Open
admin
Downloads
Nessus policy import
Search Nessus policy import
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Name
Date modified
Type
iplist - Nessus scan.txt
12-09-2018 14:56
Text Document
policy_export_example_ekje10.nessus
12-09-2018 13:45
NESSUS File
File name:
New Text Document.txt
All Files
Open
Cancel
Upload Targets
Add File
Save
Cancel

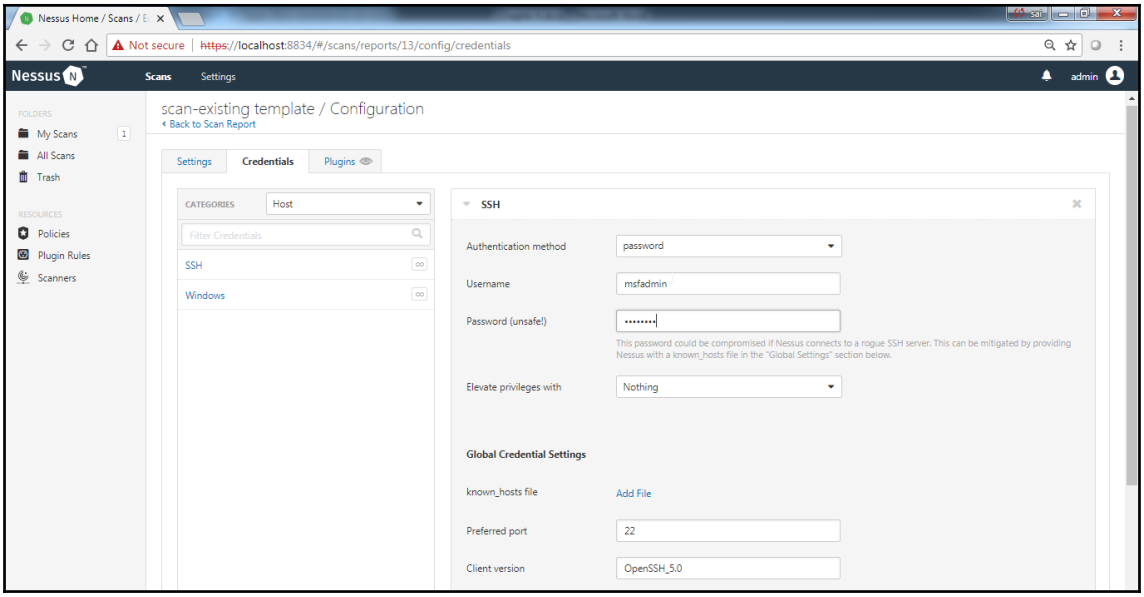

Nessus Home / Scans /
Not secure
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/schedule
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Enabled
Frequency
Once
Starts
09/12/2018
15:00
Timezone
(UTC+04:00) Abu Dhabi, Muscat
Summary
Once on Wednesday, September 12th, 2018 at 3:00 PM
Save
Cancel

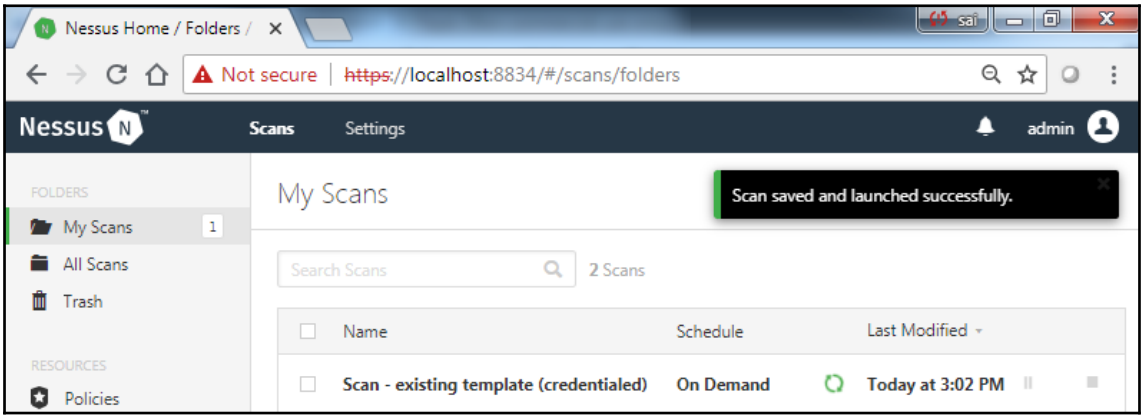

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders
Nessus
Scans
Settings
admin
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
Scan saved and launched successfully.
Search Scans
Name
Schedule
Last Modified
scan-existing template
On Demand
Today at 2:59 PM

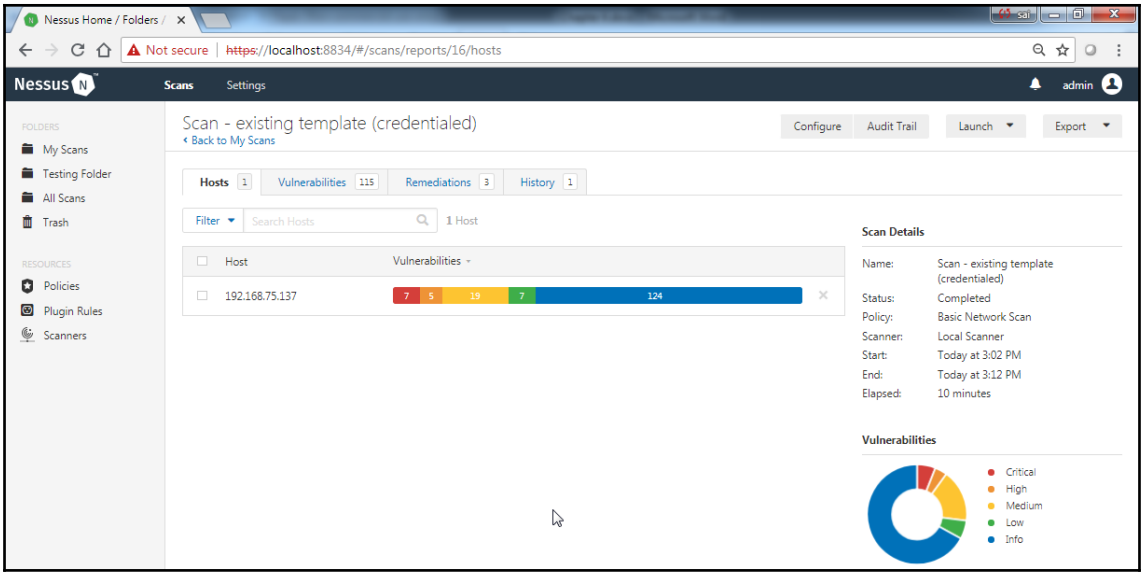

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/reports/13/hosts
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
scan-existing template
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 10
History 2
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.167.75.137
12
Scan Details
Name: scan-existing template
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 3:04 PM
End: Today at 3:20 PM
Elapsed: 15 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

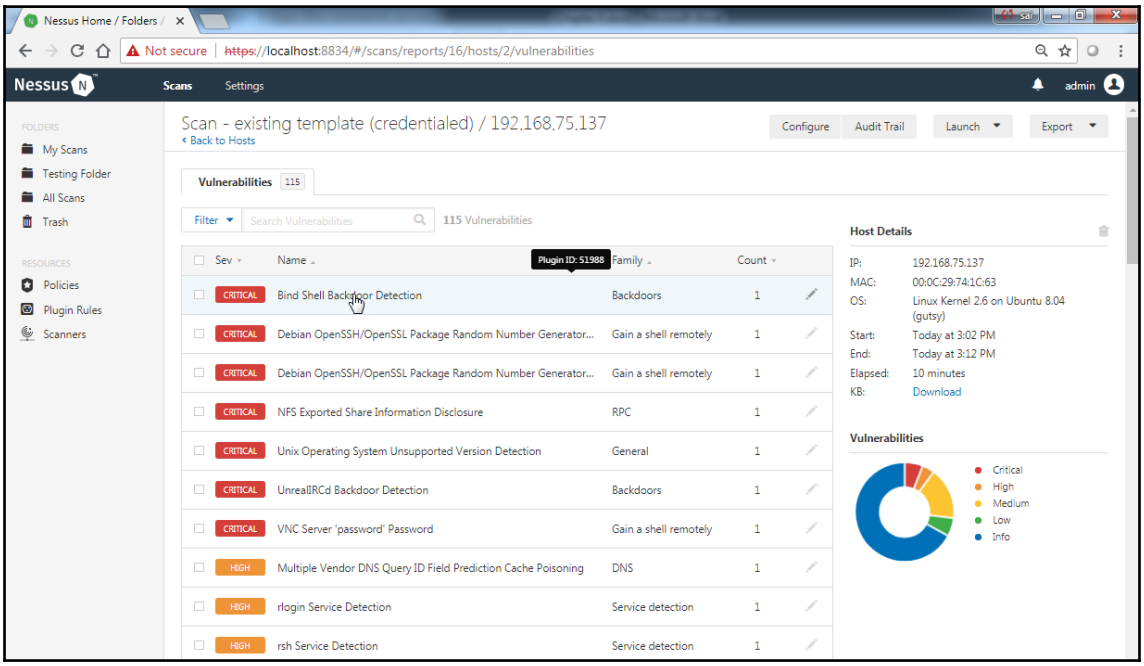

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/reports/13/hosts/2/vulnerabilities
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
scan-existing template / 192.167.75.137
Back to Hosts
Configure
Audit Trail
Launch
Export
Vulnerabilities 10
Filter
Search Vulnerabilities
10 Vulnerabilities
Sev
Name
Plugin ID: 11219
Family
Count
INFO
Nessus SYN scanner
Port scanners
2
Service Detection
Service detection
2
Common Platform Enumeration (CPE)
General
1
Device Type
General
1
Host Fully Qualified Domain Name (FQDN) Resolution
General
1
Nessus Launched Plugin List
Settings
1
Nessus Scan Information
Settings
1
OS Identification
General
1
TCP/IP Timestamps Supported
General
1
Traceroute Information
General
1
Host Details
IP: 192.167.75.137
DNS: timework.unipv.it
OS: Linux Kernel 2.6
Start: Today at 3:04 PM
End: Today at 3:20 PM
Elapsed: 15 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info

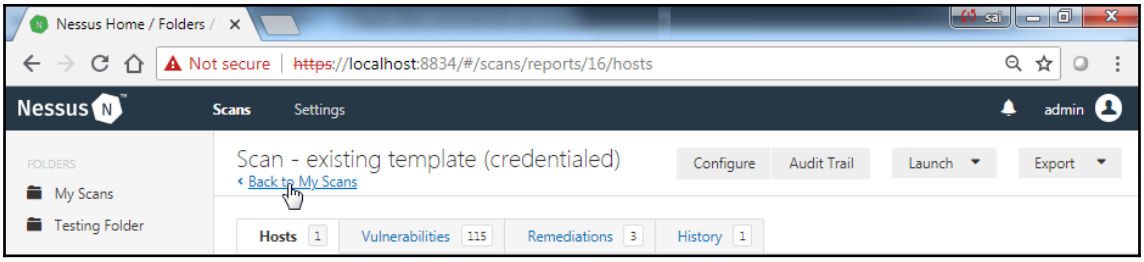

Nessus Home / Scans /
Not secure
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Scan - existing template (credentialed)
Description
This displays a credentialed scan of a remote host using an existing template.
Folder
My Scans
Targets
192.168.75.137
Upload Targets
Add File
Save
Cancel
Launch

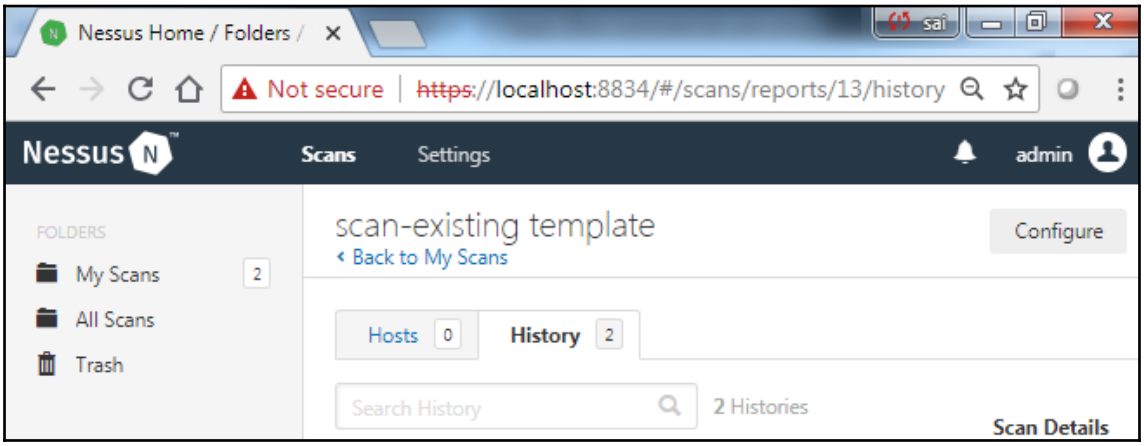

Nessus Home / Scans /
Not secure
https://localhost:8834/#/scans/reports/13/config/credentials
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
scan-existing template / Configuration
Back to Scan Report
Settings
Credentials
Plugins
CATEGORIES
Host
Filter Credentials
SSH
Windows
SSH
Authentication method
password
Username
msfadmin
Password (unsafe!)
This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.
Elevate privileges with
Nothing
Global Credential Settings
known_hosts file
Add File
Preferred port
22
Client version
OpenSSH_5.0

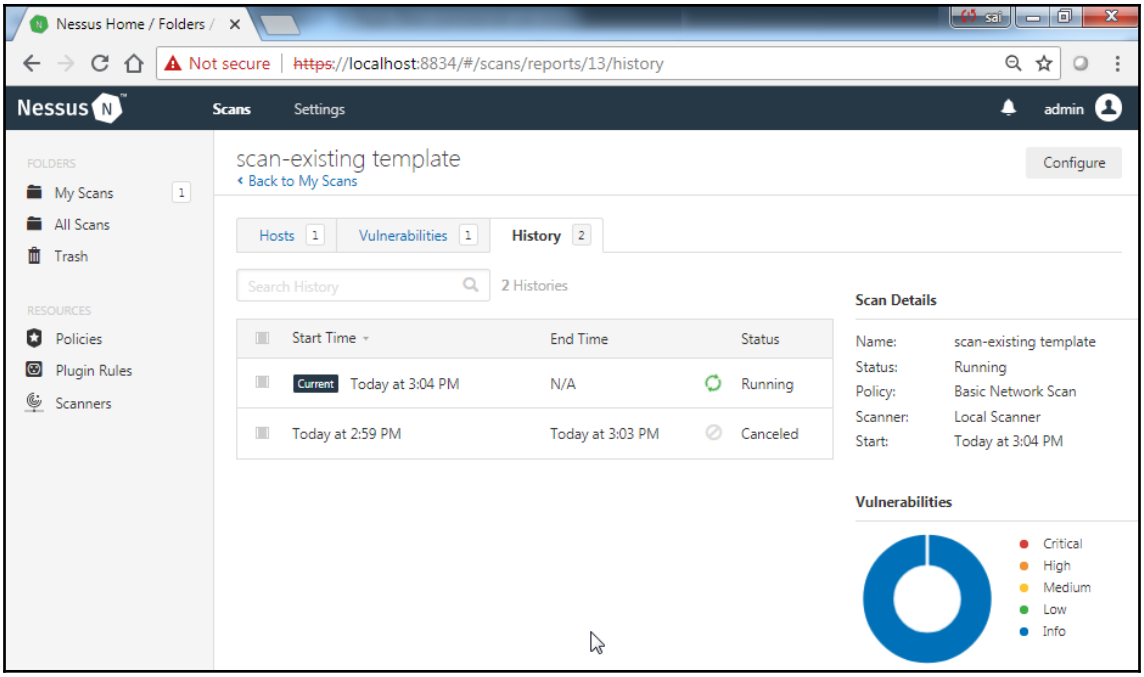

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders
Nessus
Scans
Settings
admin
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
My Scans
Scan saved and launched successfully.
Search Scans
2 Scans
Name
Schedule
Last Modified
Scan - existing template (credentialed)
On Demand
Today at 3:02 PM

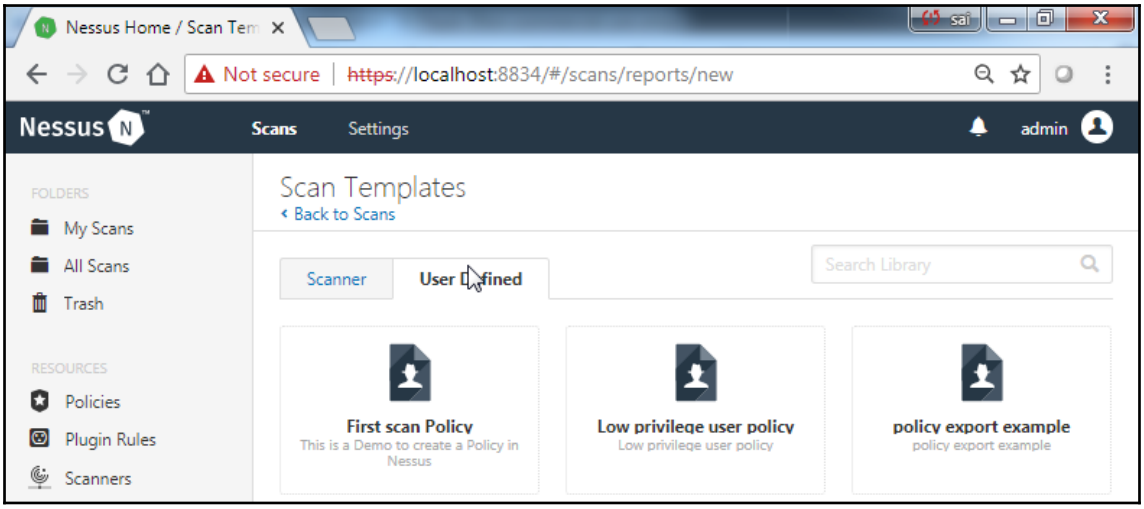

Nessus Home / Folders
Not secure
https://localhost:8834/#/scans/reports/16/hosts
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Scan - existing template (credentialed)
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 115
Remediations 3
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.75.137
7 5 19 7 124
Scan Details
Name: Scan - existing template (credentialed)
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 3:02 PM
End: Today at 3:12 PM
Elapsed: 10 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

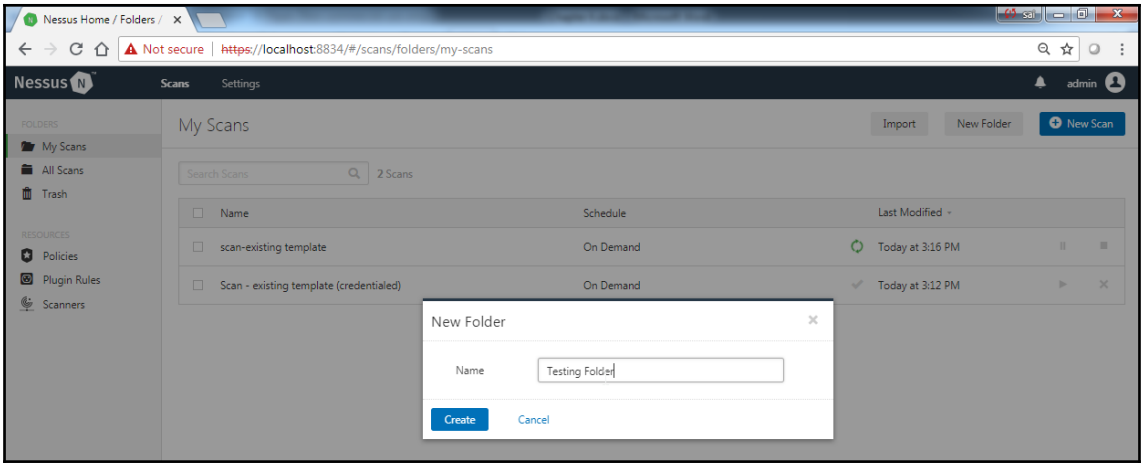

Nessus Home / Folders
Not secure
https://localhost:8834/#/scans/reports/16/hosts/2/vulnerabilities
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Scan - existing template (credentialed) / 192.168.75.137
Back to Hosts
Configure
Audit Trail
Launch
Export
Vulnerabilities 115
Filter
Search Vulnerabilities
115 Vulnerabilities
Sev
Name
Plugin ID: 51988
Family
Count
CRITICAL Bind Shell Backdoor Detection Backdoors 1
CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator... Gain a shell remotely 1
CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator... Gain a shell remotely 1
CRITICAL NFS Exported Share Information Disclosure RPC 1
CRITICAL Unix Operating System Unsupported Version Detection General 1
CRITICAL UnrealIRCd Backdoor Detection Backdoors 1
CRITICAL VNC Server 'password' Password Gain a shell remotely 1
HIGH Multiple Vendor DNS Query ID Field Prediction Cache Poisoning DNS 1
HIGH rlogin Service Detection Service detection 1
HIGH rsh Service Detection Service detection 1
Host Details
IP: 192.168.75.137
MAC: 00:0C:29:74:1C:63
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 3:02 PM
End: Today at 3:12 PM
Elapsed: 10 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info

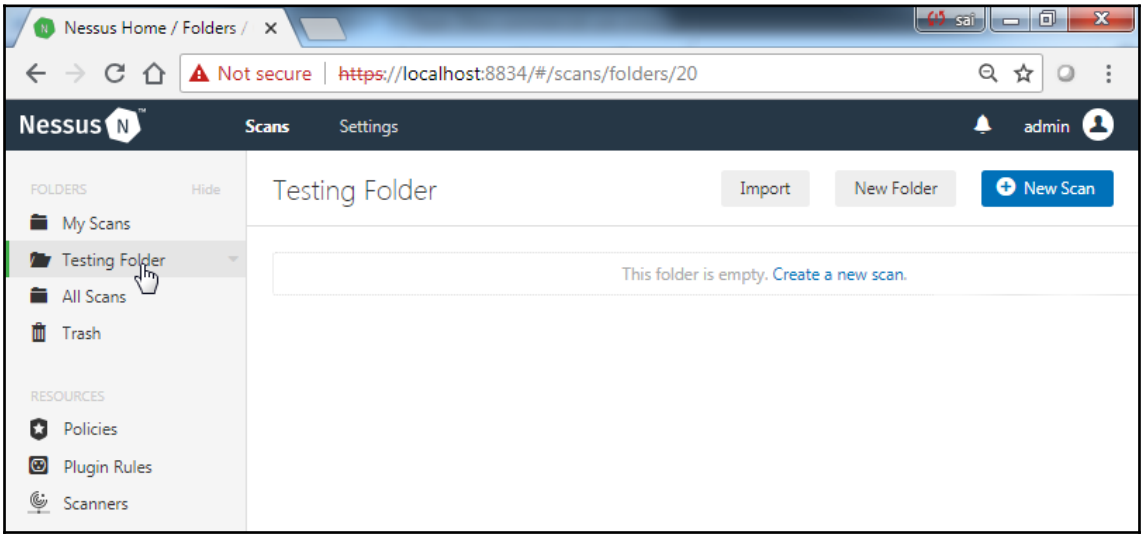

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/reports/16/hosts
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
Scan - existing template (credentialed)
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 115
Remediations 3
History 1

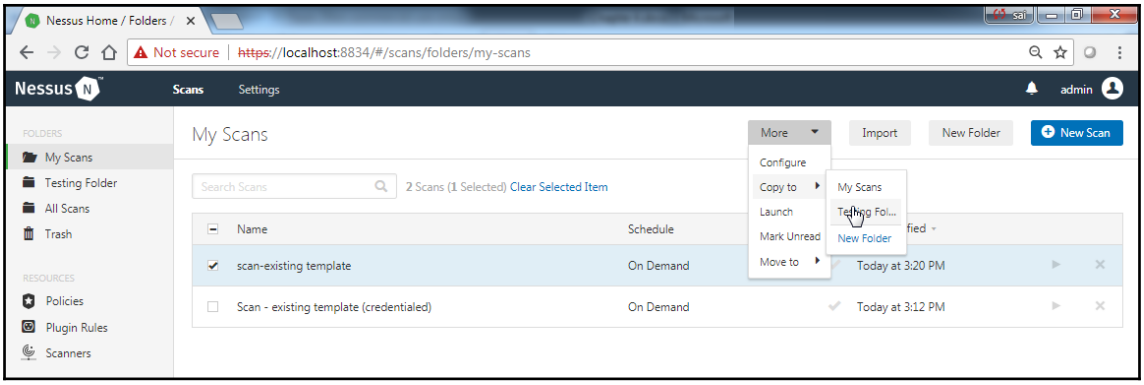

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/reports/13/history
Nessus
Scans
Settings
admin
FOLDERS
My Scans 2
All Scans
Trash
scan-existing template
Back to My Scans
Configure
Hosts 0
History 2
Search History
2 Histories
Scan Details

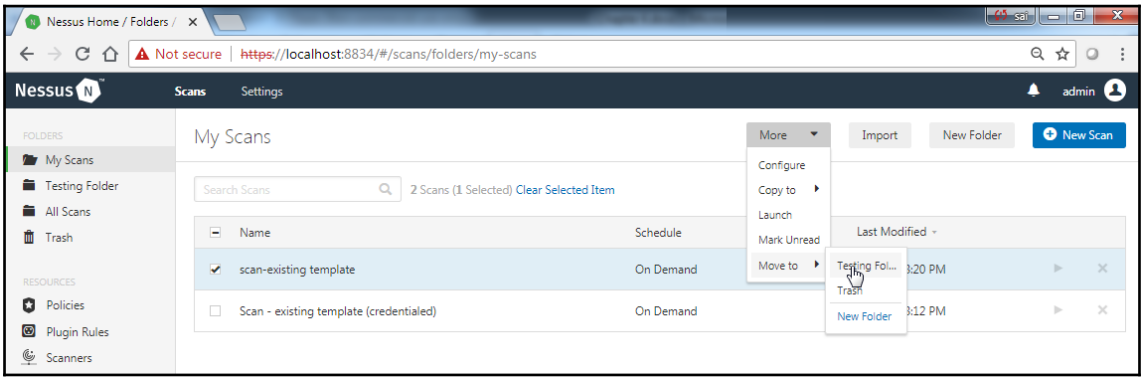

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/reports/13/history
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
scan-existing template
Back to My Scans
Configure
Hosts 1
Vulnerabilities 1
History 2
Search History
2 Histories
Start Time
End Time
Status
Current
Today at 3:04 PM
N/A
Running
Today at 2:59 PM
Today at 3:03 PM
Canceled
Scan Details
Name: scan-existing template
Status: Running
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 3:04 PM
Vulnerabilities
Critical
High
Medium
Low
Info

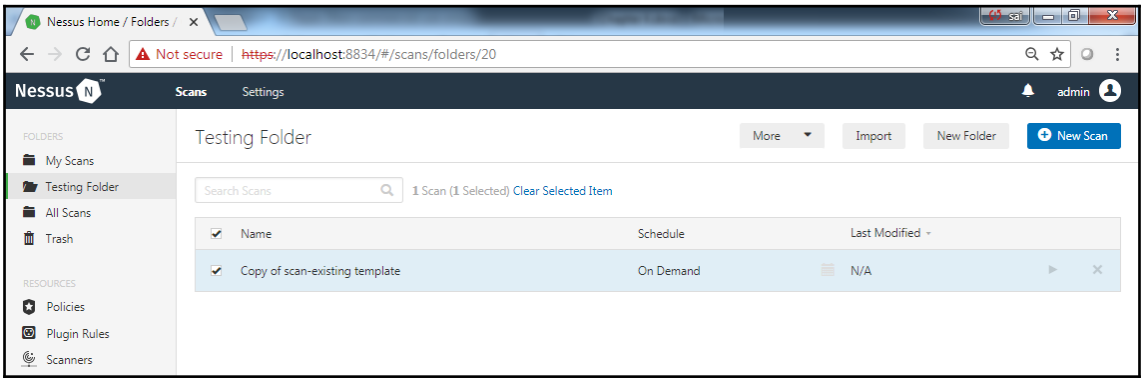

Nessus Home / Scan Tem
Not secure
https://localhost:8834/#/scans/reports/new
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
First scan Policy
This is a Demo to create a Policy in Nessus
Low privilege user policy
Low privilege user policy
policy export example
policy export example

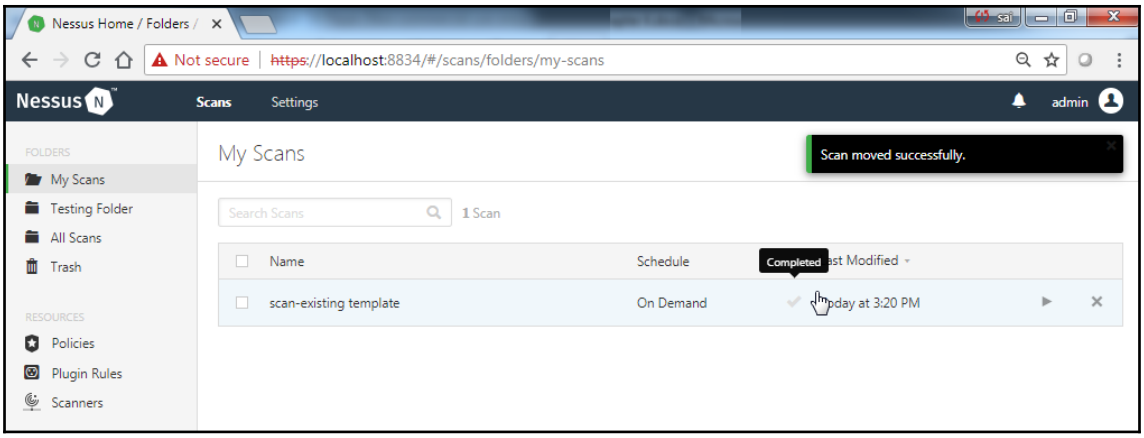

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/my-scans
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
Import
New Folder
New Scan
Search Scans
2 Scans
Name
Schedule
Last Modified
scan-existing template
On Demand
Today at 3:16 PM
Scan - existing template (credentialed)
On Demand
Today at 3:12 PM
New Folder
Name
Testing Folder
Create
Cancel

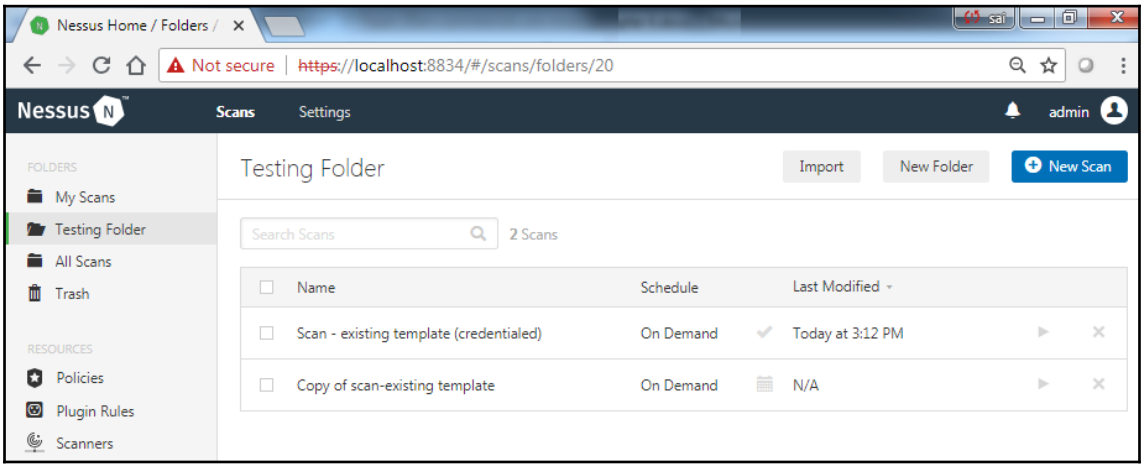

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/20
Nessus
Scans
Settings
admin
FOLDERS
Hide
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Testing Folder
Import
New Folder
New Scan
This folder is empty. Create a new scan.

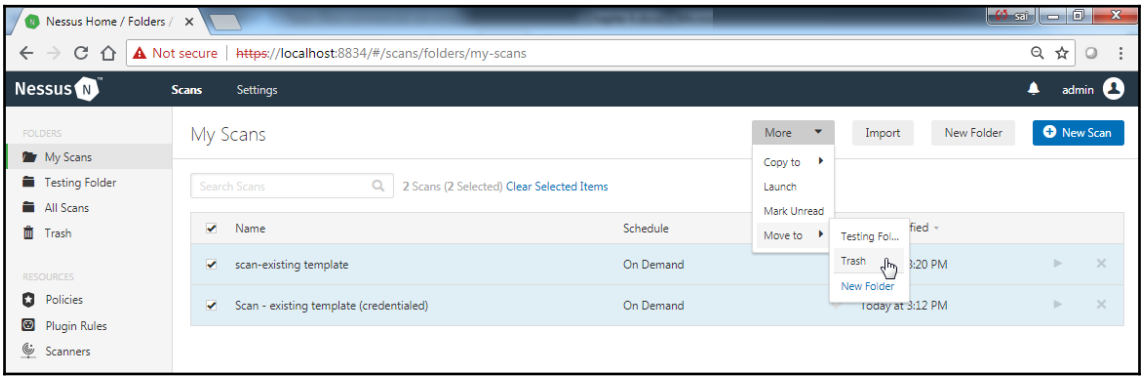

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/my-scans
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
More
Import
New Folder
New Scan
Configure
Copy to
Launch
Mark Unread
Move to
My Scans
Testing Fol...
New Folder
Search Scans
2 Scans (1 Selected) Clear Selected Item
Name
Schedule
scan-existing template
On Demand
Today at 3:20 PM
Scan - existing template (credentialed)
On Demand
Today at 3:12 PM


Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/my-scans
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
More
Import
New Folder
New Scan
Configure
Copy to
Launch
Mark Unread
Move to
Testing Fol...
Trash
New Folder
Search Scans
2 Scans (1 Selected) Clear Selected Item
Name
Schedule
Last Modified
scan-existing template
On Demand
Scan - existing template (credentialed)
On Demand

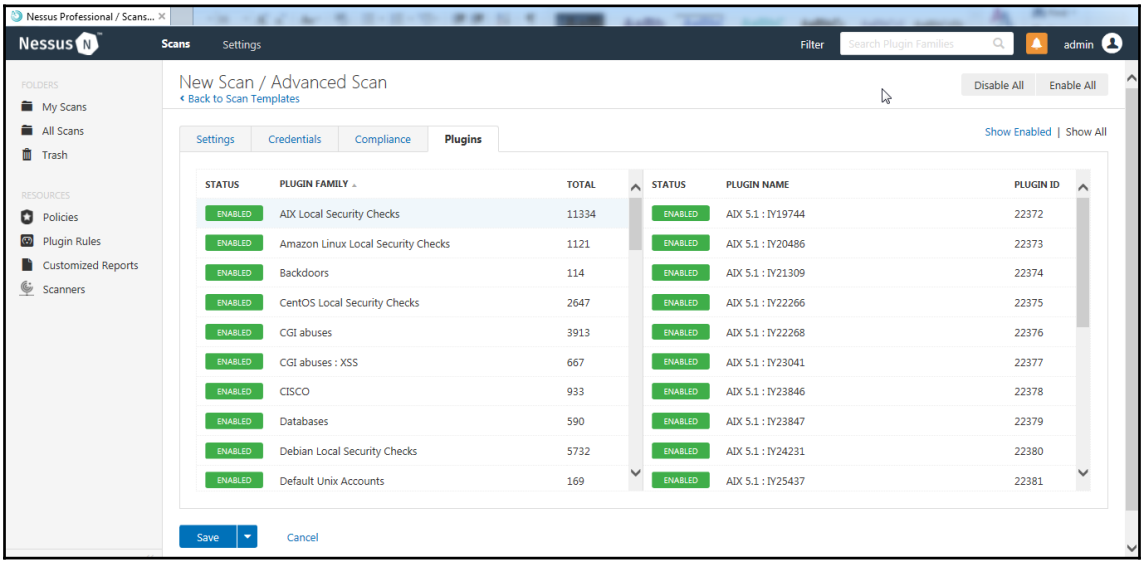

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/20
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Testing Folder
More
Import
New Folder
New Scan
Search Scans
1 Scan (1 Selected) Clear Selected Item
Name
Schedule
Last Modified
Copy of scan-existing template
On Demand
N/A

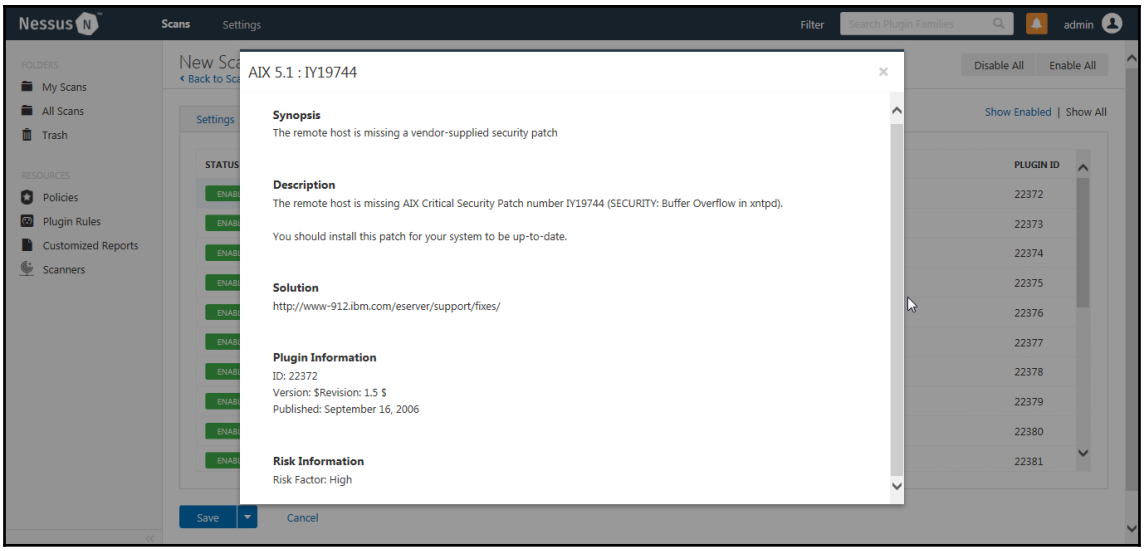

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/my-scans
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
Scan moved successfully.
Search Scans
1 Scan
Name
Schedule
Completed
Last Modified
scan-existing template
On Demand
Today at 3:20 PM

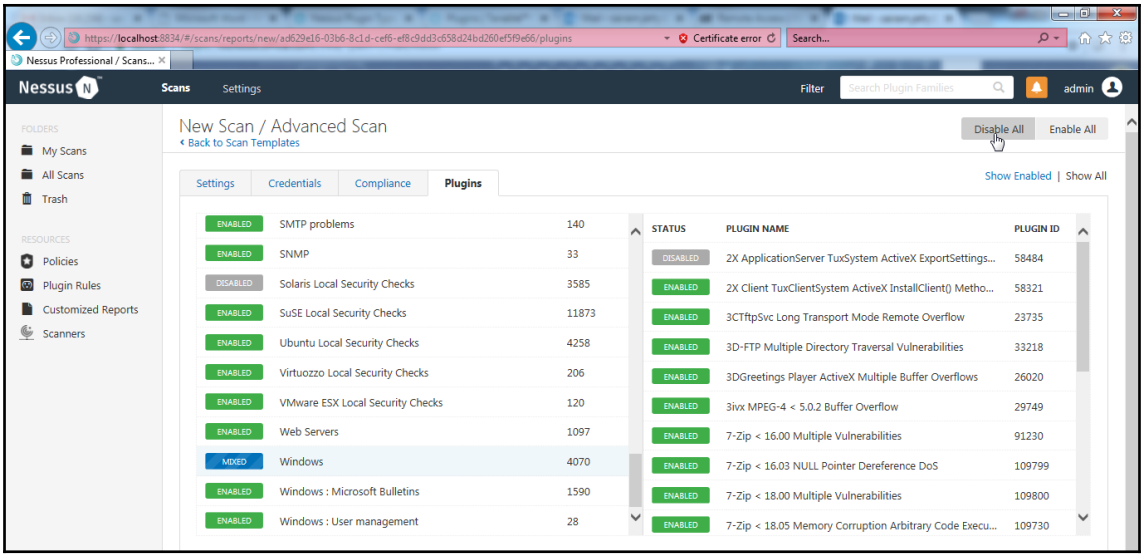

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/20
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Testing Folder
Import
New Folder
New Scan
Search Scans
2 Scans
Name
Schedule
Last Modified
Scan - existing template (credentialed)
On Demand
Today at 3:12 PM
Copy of scan-existing template
On Demand
N/A

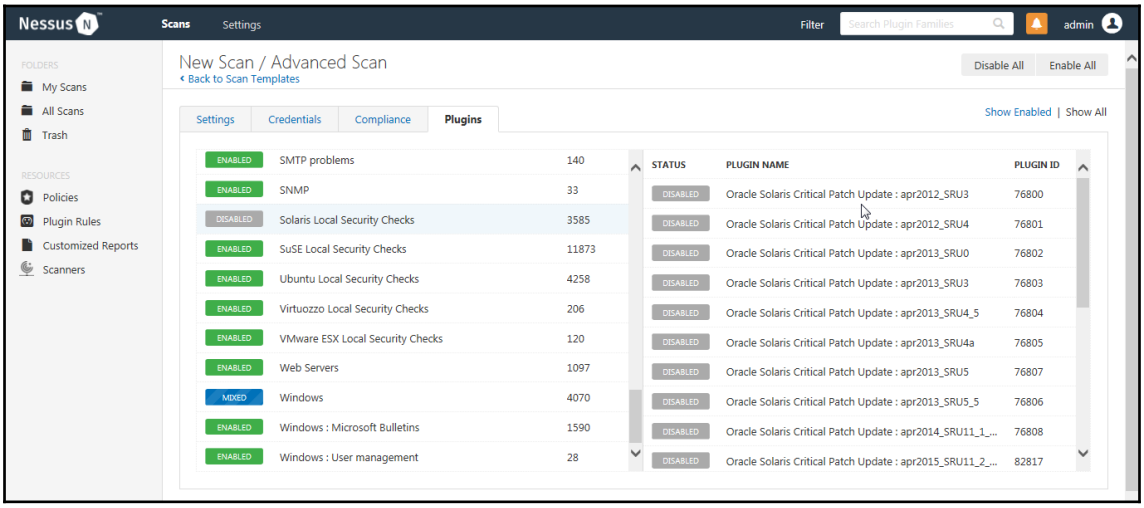

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/folders/my-scans
Nessus
Scans
Settings
admin
FOLDERS
My Scans
Testing Folder
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
More
Import
New Folder
New Scan
Copy to
Launch
Mark Unread
Move to
Testing Fol...
Trash
New Folder
Search Scans
2 Scans (2 Selected) Clear Selected Items
Name
Schedule
scan-existing template
On Demand
Scan - existing template (credentialed)
On Demand

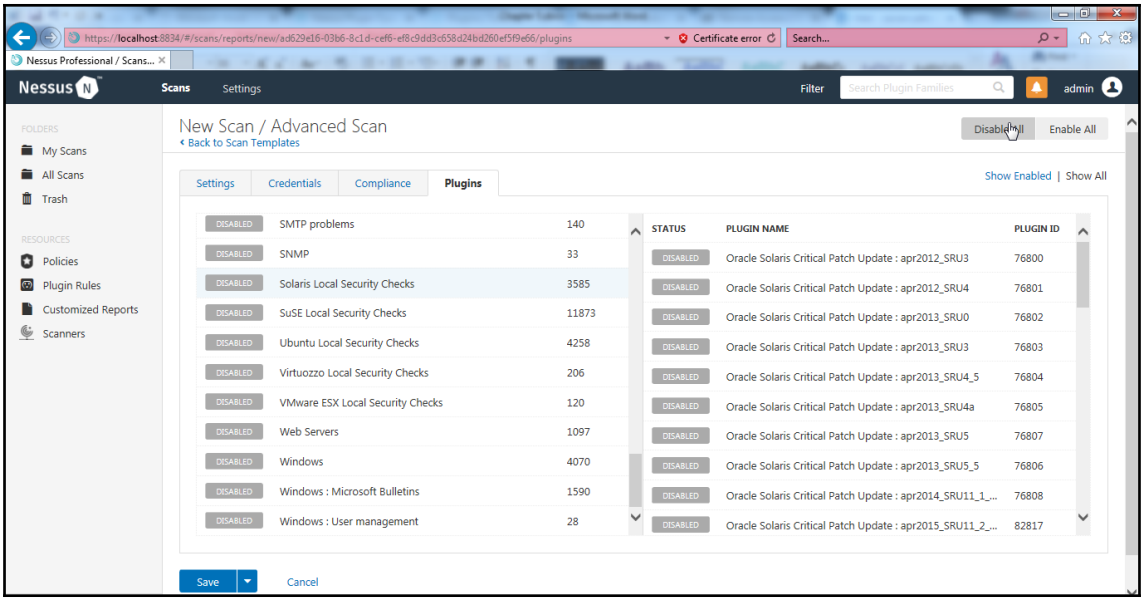
Chapter 5: Configuration Audits

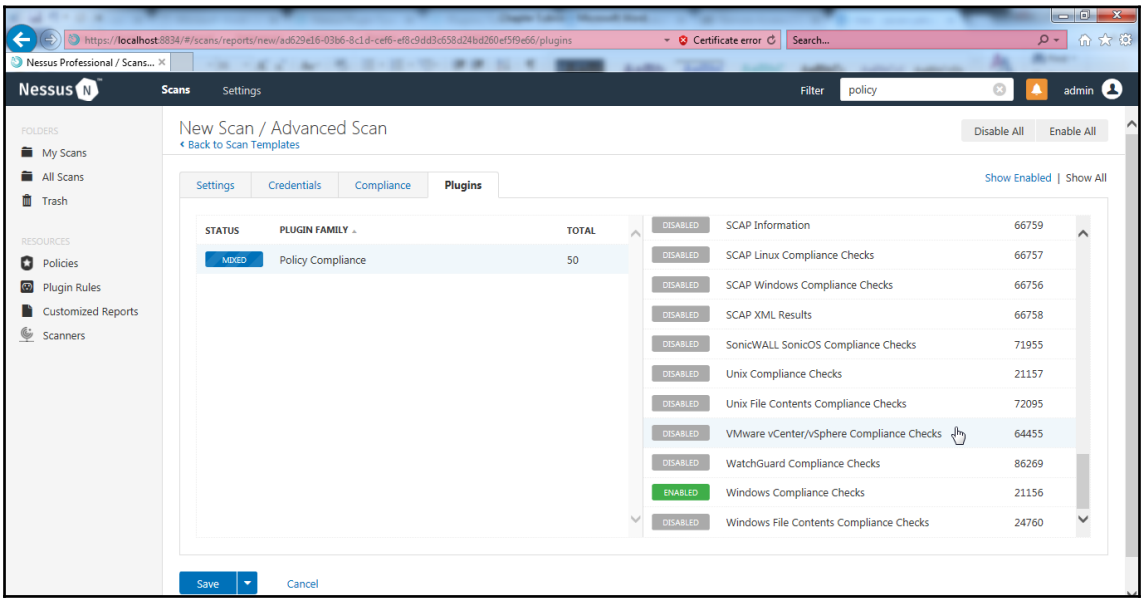


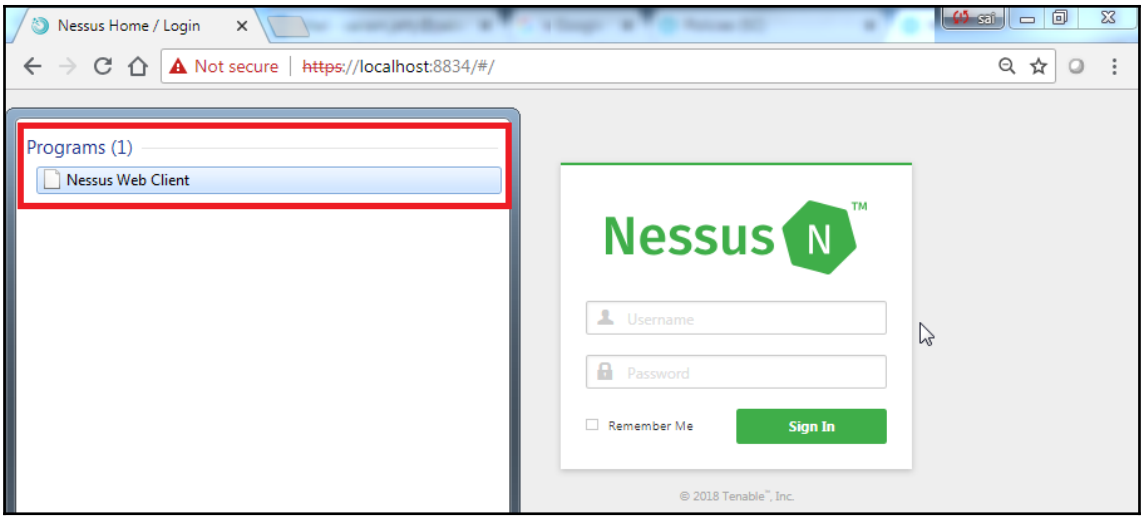


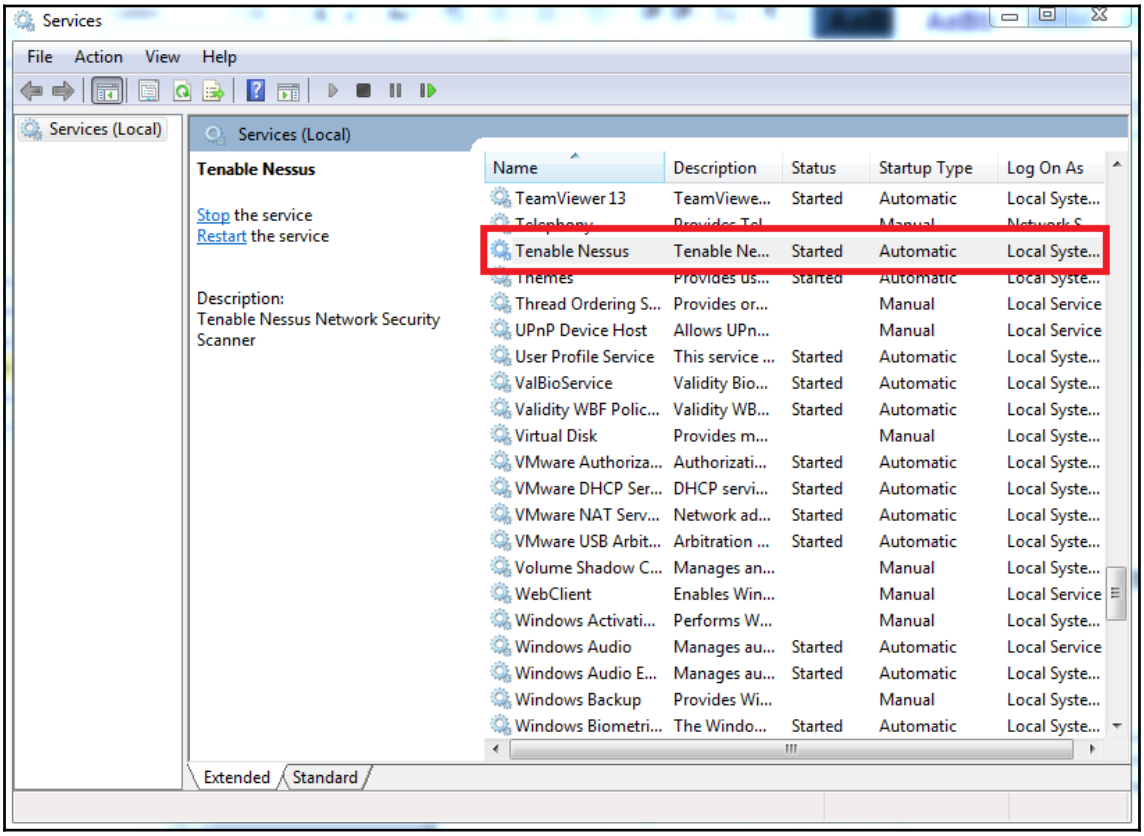

https://localhost:8834/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/plugins
Certificate error
Search...
Nessus Professional / Scans...
Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
ENABLED SMTP problems 140
ENABLED SNMP 33
DISABLED Solaris Local Security Checks 3585
ENABLED SuSE Local Security Checks 11873
ENABLED Ubuntu Local Security Checks 4258
ENABLED Virtuozzo Local Security Checks 206
ENABLED VMware ESX Local Security Checks 120
ENABLED Web Servers 1097
MIXED Windows 4070
ENABLED Windows : Microsoft Bulletins 1590
ENABLED Windows : User management 28
STATUS PLUGIN NAME PLUGIN ID
DISABLED 2X ApplicationServer TuxSystem ActiveX ExportSettings... 58484
ENABLED 2X Client TuxClientSystem ActiveX InstallClient() Metho... 58321
ENABLED 3CTftpSvc Long Transport Mode Remote Overflow 23735
ENABLED 3D-FTP Multiple Directory Traversal Vulnerabilities 33218
ENABLED 3DGreetings Player ActiveX Multiple Buffer Overflows 26020
ENABLED 3ivx MPEG-4 < 5.0.2 Buffer Overflow 29749
ENABLED 7-Zip < 16.00 Multiple Vulnerabilities 91230
ENABLED 7-Zip < 16.03 NULL Pointer Dereference DoS 109799
ENABLED 7-Zip < 18.00 Multiple Vulnerabilities 109800
ENABLED 7-Zip < 18.05 Memory Corruption Arbitrary Code Execu... 109730

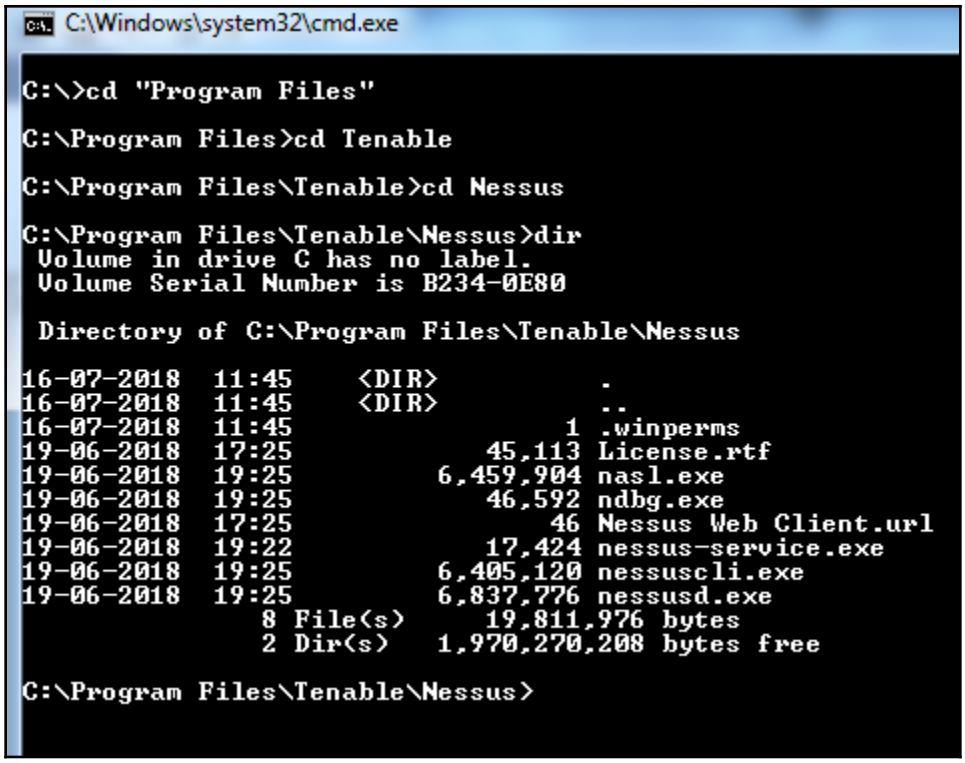

Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
ENABLED SMTP problems 140
ENABLED SNMP 33
DISABLED Solaris Local Security Checks 3585
ENABLED SuSE Local Security Checks 11873
ENABLED Ubuntu Local Security Checks 4258
ENABLED Virtuozzo Local Security Checks 206
ENABLED VMware ESX Local Security Checks 120
ENABLED Web Servers 1097
MIXED Windows 4070
ENABLED Windows : Microsoft Bulletins 1590
ENABLED Windows : User management 28
STATUS PLUGIN NAME PLUGIN ID
DISABLED Oracle Solaris Critical Patch Update : apr2012_SRU3 76800
DISABLED Oracle Solaris Critical Patch Update : apr2012_SRU4 76801
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU0 76802
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU3 76803
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU4_5 76804
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU4a 76805
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU5 76807
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU5_5 76806
DISABLED Oracle Solaris Critical Patch Update : apr2014_SRU11_1_... 76808
DISABLED Oracle Solaris Critical Patch Update : apr2015_SRU11_2_... 82817

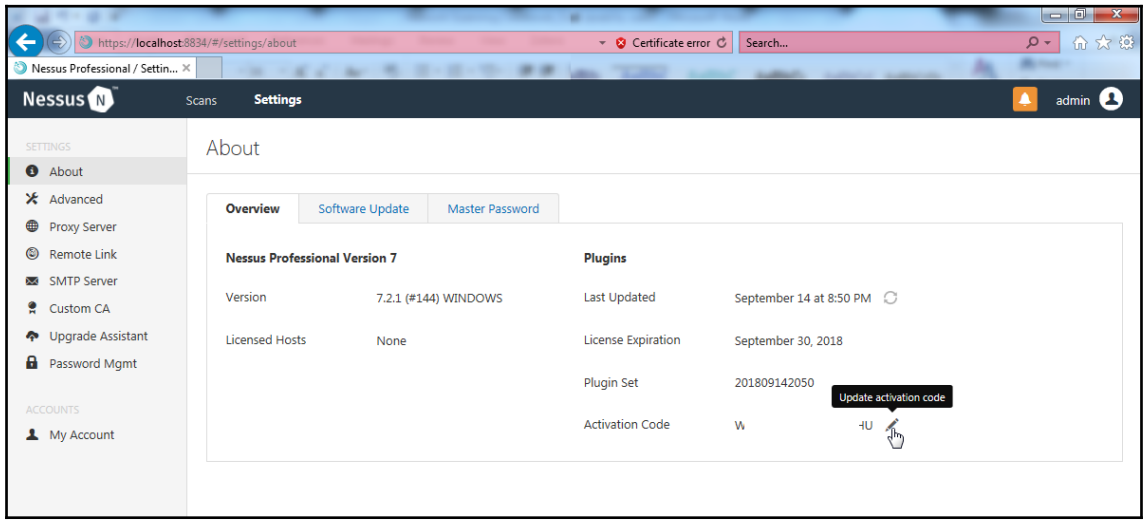

Nessus Professional / Scans...
Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
DISABLED SMTP problems 140
DISABLED SNMP 33
DISABLED Solaris Local Security Checks 3585
DISABLED SuSE Local Security Checks 11873
DISABLED Ubuntu Local Security Checks 4258
DISABLED Virtuozzo Local Security Checks 206
DISABLED VMware ESX Local Security Checks 120
DISABLED Web Servers 1097
DISABLED Windows 4070
DISABLED Windows : Microsoft Bulletins 1590
DISABLED Windows : User management 28
STATUS PLUGIN NAME PLUGIN ID
DISABLED Oracle Solaris Critical Patch Update : apr2012_SRU3 76800
DISABLED Oracle Solaris Critical Patch Update : apr2012_SRU4 76801
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU0 76802
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU3 76803
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU4_5 76804
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU4a 76805
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU5 76807
DISABLED Oracle Solaris Critical Patch Update : apr2013_SRU5_5 76806
DISABLED Oracle Solaris Critical Patch Update : apr2014_SRU11_1_... 76808
DISABLED Oracle Solaris Critical Patch Update : apr2015_SRU11_2_... 82817
Save
Cancel

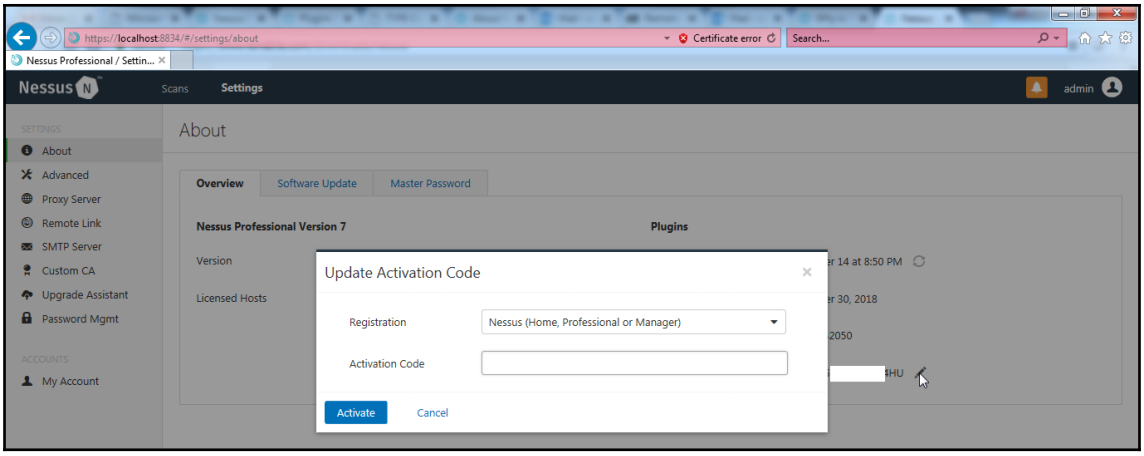

Nessus Professional / Scans...
Nessus
Scans
Settings
Filter
policy
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
STATUS PLUGIN FAMILY TOTAL
MIXED Policy Compliance 50
DISABLED SCAP Information 66759
DISABLED SCAP Linux Compliance Checks 66757
DISABLED SCAP Windows Compliance Checks 66756
DISABLED SCAP XML Results 66758
DISABLED SonicWALL SonicOS Compliance Checks 71955
DISABLED Unix Compliance Checks 21157
DISABLED Unix File Contents Compliance Checks 72095
DISABLED VMware vCenter/vSphere Compliance Checks 64455
DISABLED WatchGuard Compliance Checks 86269
ENABLED Windows Compliance Checks 21156
DISABLED Windows File Contents Compliance Checks 24760
Save
Cancel


Nessus Home / Login
Not secure
https://localhost:8834/#/
Programs (1)
Nessus Web Client
Nessus
Username
Password
Remember Me
Sign In
© 2018 Tenable™, Inc.

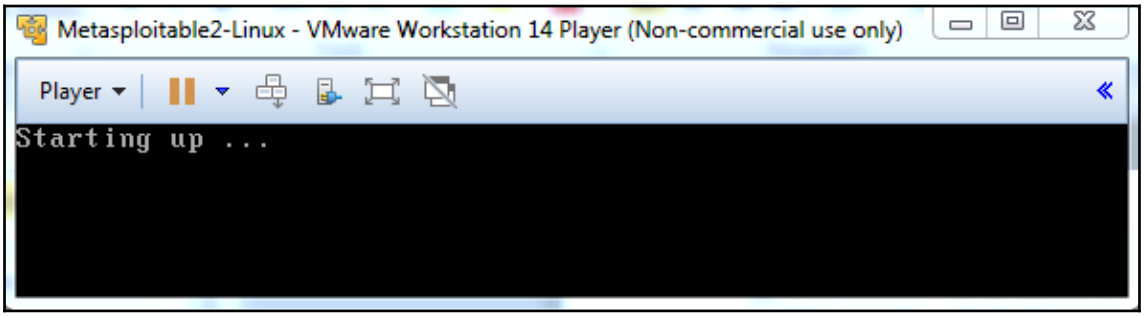

Services
File Action View Help
Services (Local)
Services (Local)
Tenable Nessus
Stop the service
Restart the service
Description:
Tenable Nessus Network Security Scanner
Name
Description
Status
Startup Type
Log On As
TeamViewer 13
TeamViewe...
Started
Automatic
Local Syste...
Tenable Nessus
Tenable Ne...
Started
Automatic
Local Syste...
Thread Ordering S...
Provides or...
Manual
Local Service
UPnP Device Host
Allows UPn...
Manual
Local Service
User Profile Service
This service ...
Started
Automatic
Local Syste...
ValBioService
Validity Bio...
Started
Automatic
Local Syste...
Validity WBF Polic...
Validity WB...
Started
Automatic
Local Syste...
Virtual Disk
Provides m...
Manual
Local Syste...
VMware Authoriza...
Authorizati...
Started
Automatic
Local Syste...
VMware DHCP Ser...
DHCP servi...
Started
Automatic
Local Syste...
VMware NAT Serv...
Network ad...
Started
Automatic
Local Syste...
VMware USB Arbit...
Arbitration ...
Started
Automatic
Local Syste...
Volume Shadow C...
Manages an...
Manual
Local Syste...
WebClient
Enables Win...
Manual
Local Service
Windows Activati...
Performs W...
Manual
Local Syste...
Windows Audio
Manages au...
Started
Automatic
Local Service
Windows Audio E...
Manages au...
Started
Automatic
Local Syste...
Windows Backup
Provides Wi...
Manual
Local Syste...
Windows Biometri...
The Windo...
Started
Automatic
Local Syste...
Extended
Standard

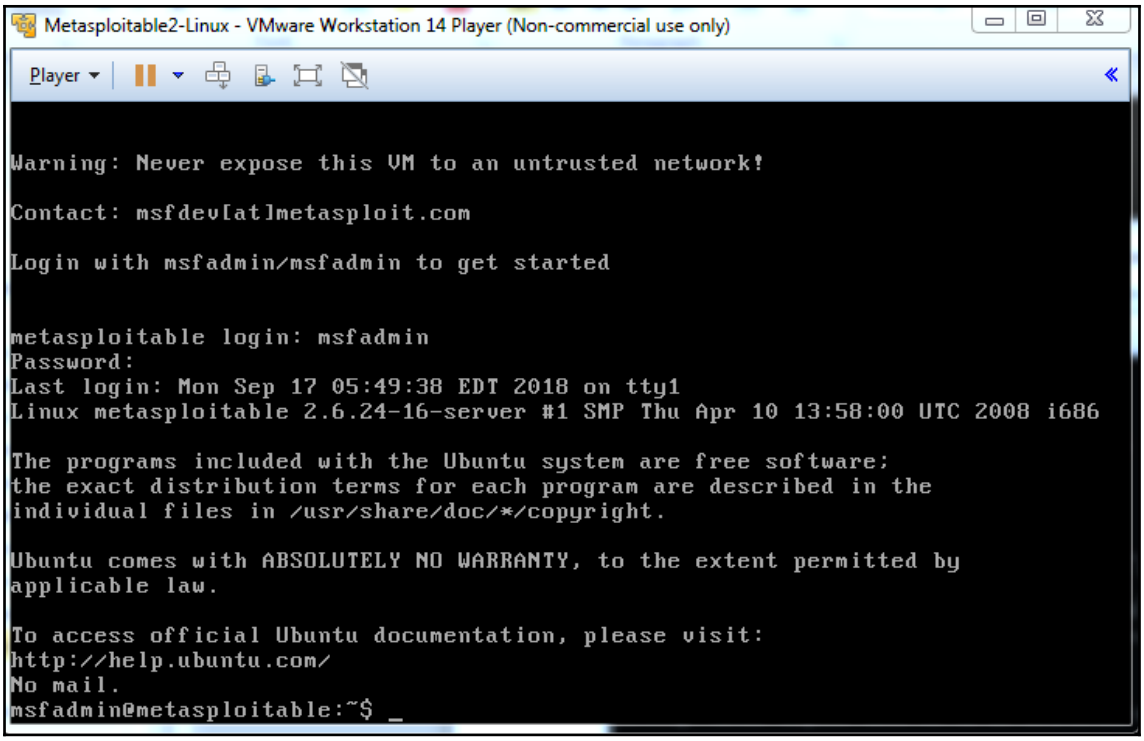

C:\Windows\system32\cmd.exe
C:\>cd "Program Files"
C:\Program Files>cd Tenable
C:\Program Files\Tenable>cd Nessus
C:\Program Files\Tenable\Nessus>dir
Volume in drive C has no label.
Volume Serial Number is B234-0E80
Directory of C:\Program Files\Tenable\Nessus
16-07-2018 11:45 <DIR> .
16-07-2018 11:45 <DIR> ..
16-07-2018 11:45 1 .winperms
19-06-2018 17:25 45,113 License.rtf
19-06-2018 19:25 6,459,904 nasl.exe
19-06-2018 19:25 46,592 ndbg.exe
19-06-2018 17:25 46 Nessus Web Client.url
19-06-2018 19:22 17,424 nessus-service.exe
19-06-2018 19:25 6,405,120 nessuscli.exe
19-06-2018 19:25 6,837,776 nessusd.exe
8 File(s) 19,811,976 bytes
2 Dir(s) 1,970,270,208 bytes free
C:\Program Files\Tenable\Nessus>

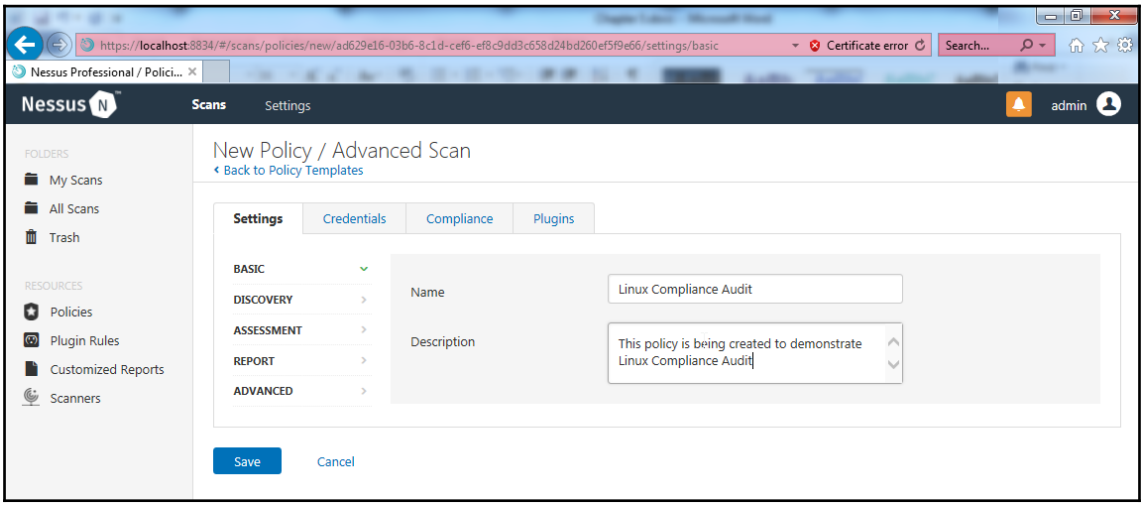

https://localhost:8834/#/settings/about
Certificate error
Search...
Nessus Professional / Settin...
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
ACCOUNTS
My Account
About
Overview
Software Update
Master Password
Nessus Professional Version 7
Version
7.2.1 (#144) WINDOWS
Licensed Hosts
None
Plugins
Last Updated
September 14 at 8:50 PM
License Expiration
September 30, 2018
Plugin Set
201809142050
Activation Code
Update activation code

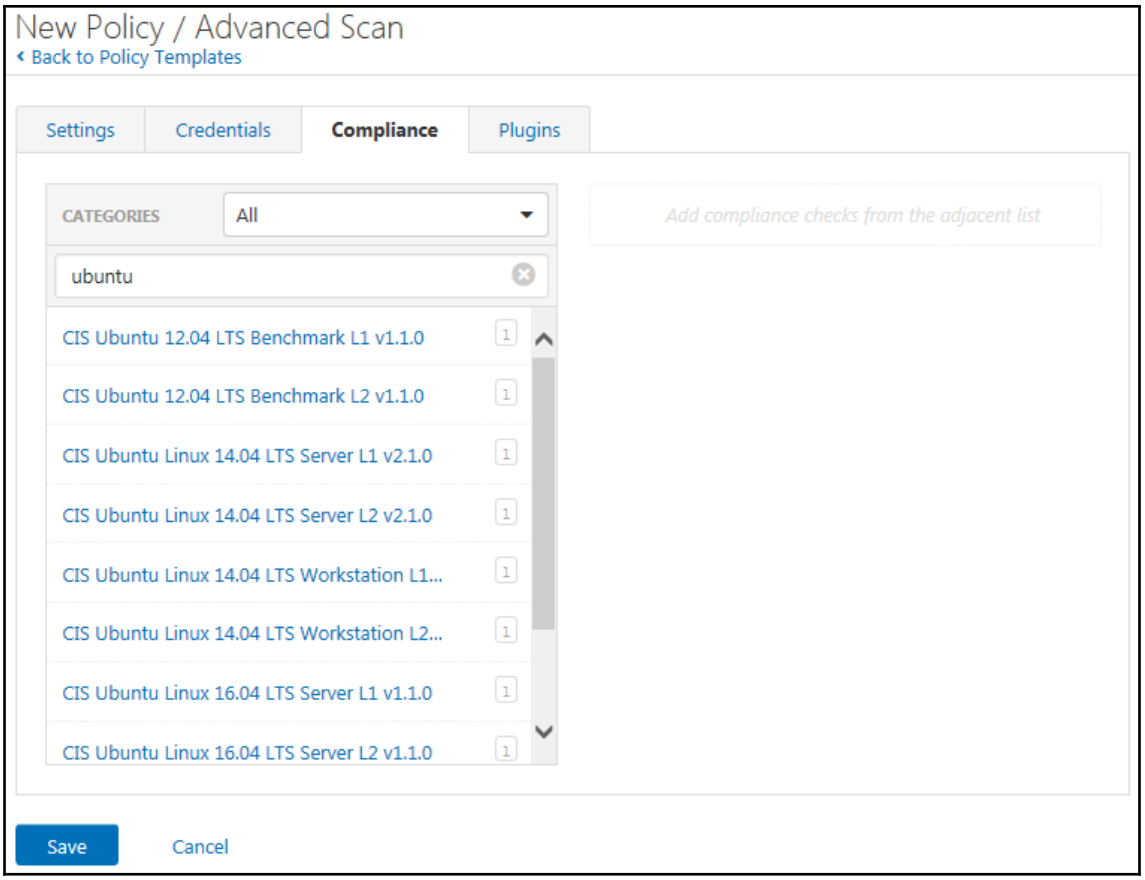


Metasploitable.nvram	04-09-2018 16:53	NVRAM File	9 KB
Metasploitable.vmdk	17-09-2018 13:48	VMware virtual dis...	18,81,024 KB
Metasploitable.vmsd	07-05-2010 14:46	VMSD File	0 KB
Metasploitable.vmx	17-09-2018 13:47	VMware virtual m...	3 KB
Metasploitable.vmxf	07-05-2010 14:46	VMXF File	1 KB

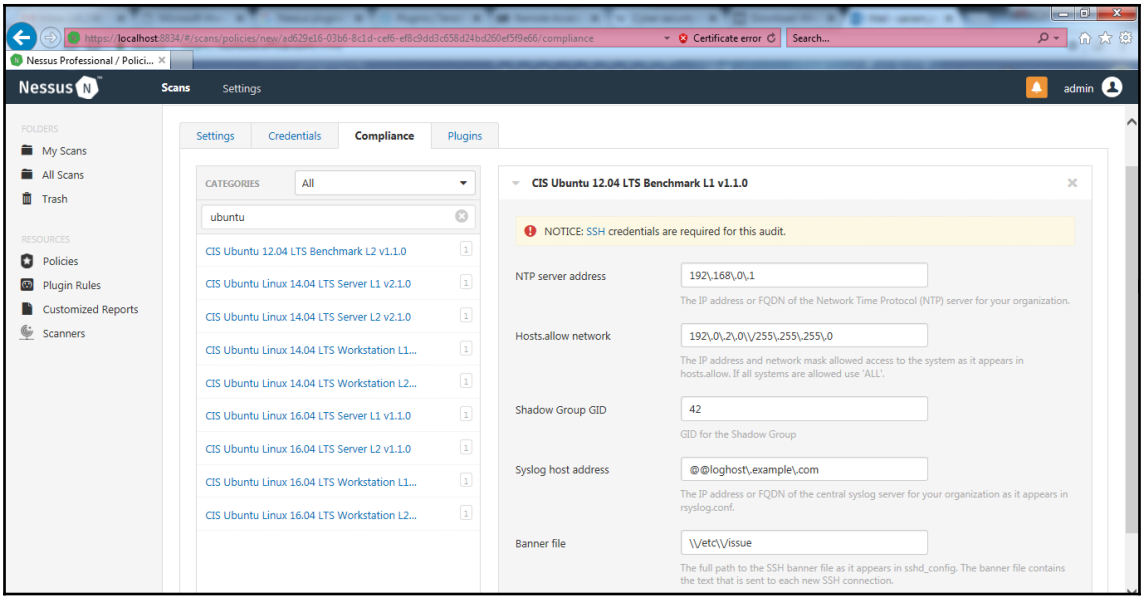


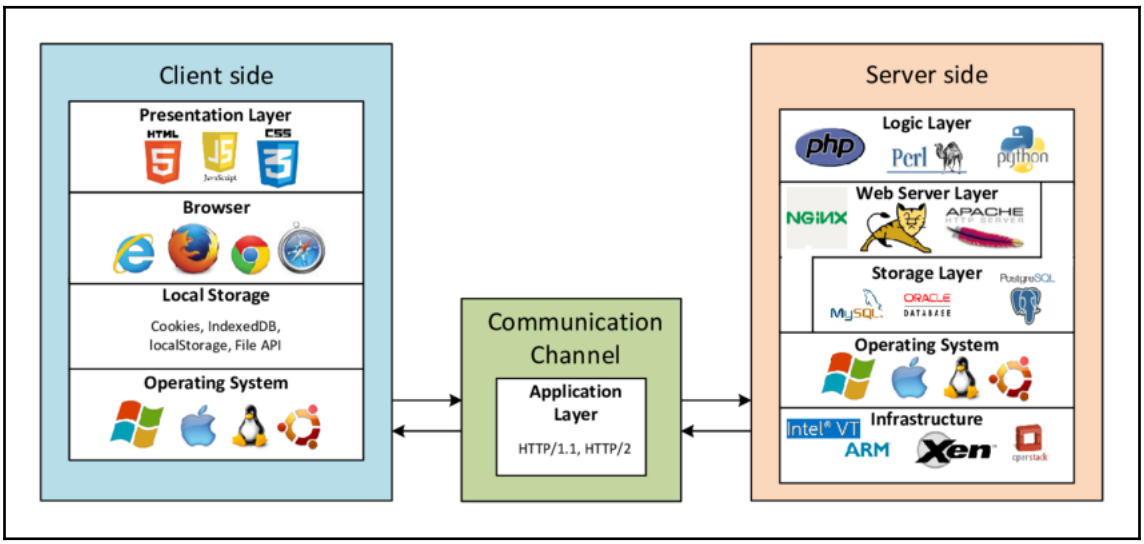

Metasploitable2-Linux - VMware Workstation 14 Player (Non-commercial use only)
Player
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Mon Sep 17 05:49:38 EDT 2018 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _

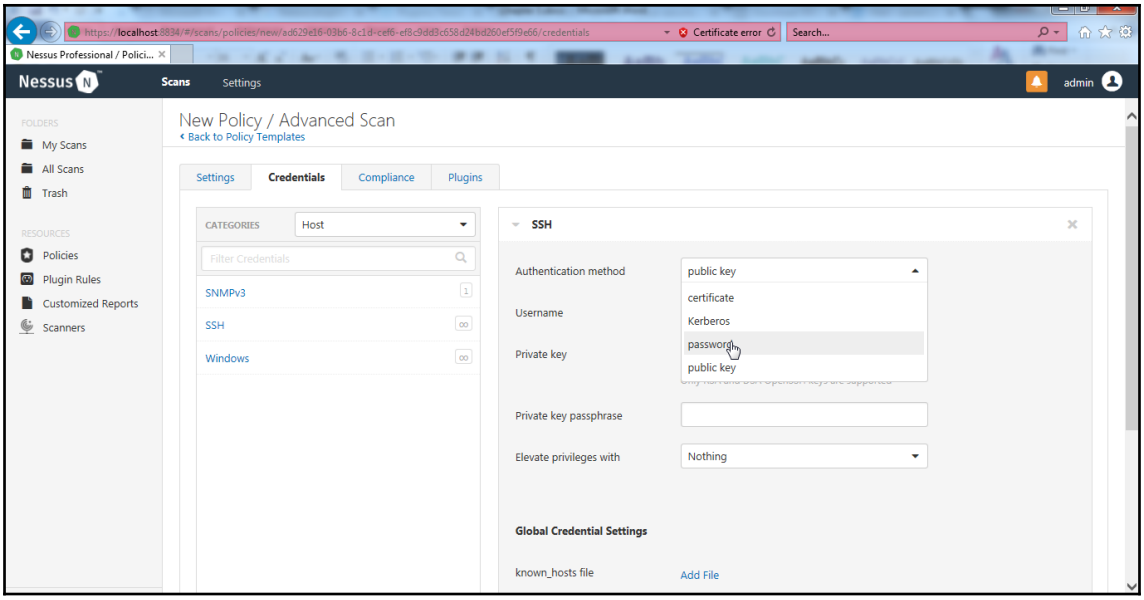

https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic
Certificate error
Search...
Nessus Professional / Polici...
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Linux Compliance Audit
Description
This policy is being created to demonstrate Linux Compliance Audit
Save
Cancel

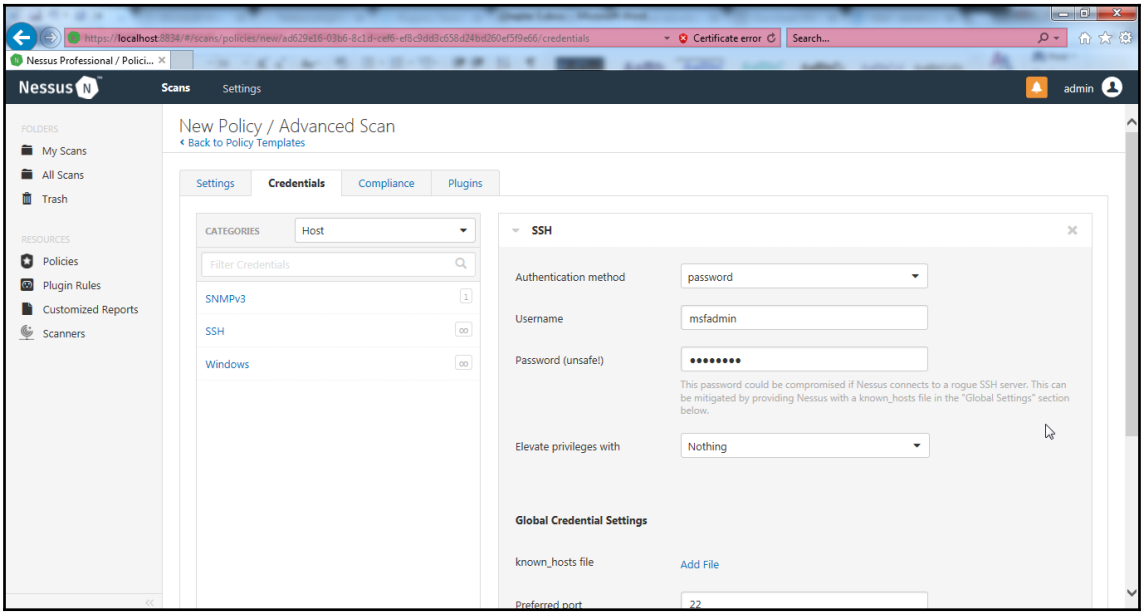


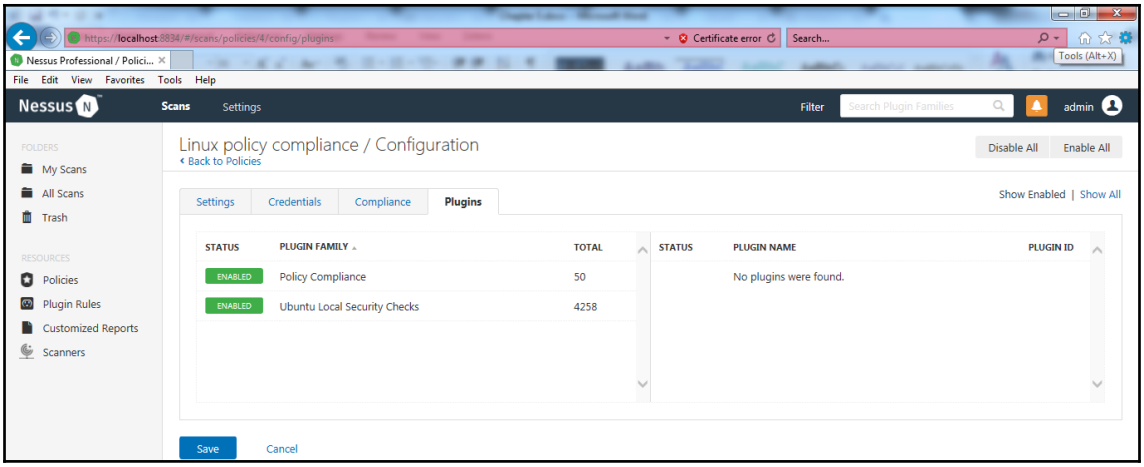

```
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

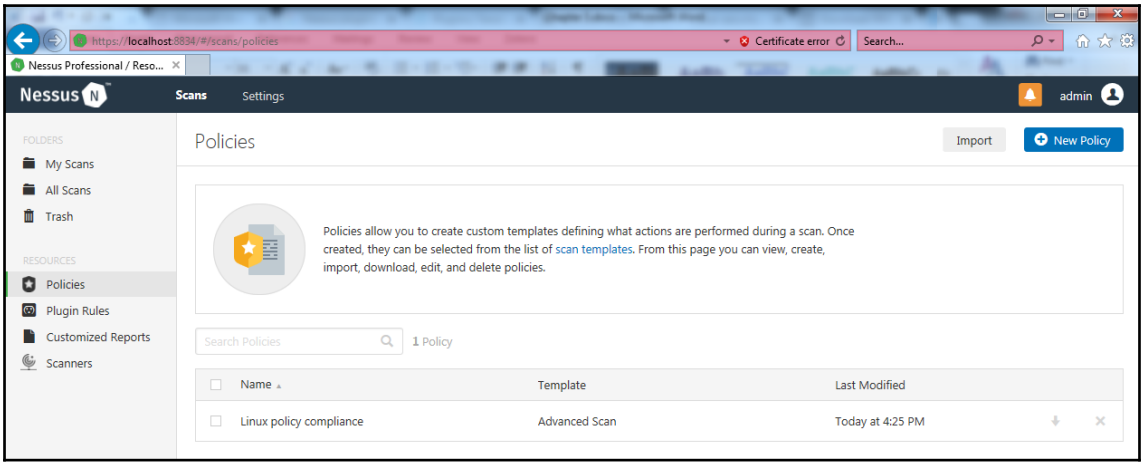

Nessus Professional / Polici...
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Settings
Credentials
Compliance
Plugins
CATEGORIES
All
ubuntu
CIS Ubuntu 12.04 LTS Benchmark L2 v1.1.0
CIS Ubuntu Linux 14.04 LTS Server L1 v2.1.0
CIS Ubuntu Linux 14.04 LTS Server L2 v2.1.0
CIS Ubuntu Linux 14.04 LTS Workstation L1...
CIS Ubuntu Linux 14.04 LTS Workstation L2...
CIS Ubuntu Linux 16.04 LTS Server L1 v1.1.0
CIS Ubuntu Linux 16.04 LTS Server L2 v1.1.0
CIS Ubuntu Linux 16.04 LTS Workstation L1...
CIS Ubuntu Linux 16.04 LTS Workstation L2...
CIS Ubuntu 12.04 LTS Benchmark L1 v1.1.0
NOTICE: SSH credentials are required for this audit.
NTP server address
192\.168\.0\.1
The IP address or FQDN of the Network Time Protocol (NTP) server for your organization.
Hosts.allow network
192\.0\.2\.0\\/255\.255\.255\.0
The IP address and network mask allowed access to the system as it appears in hosts.allow. If all systems are allowed use 'ALL'.
Shadow Group GID
42
GID for the Shadow Group
Syslog host address
@@loghost\.example\.com
The IP address or FQDN of the central syslog server for your organization as it appears in rsyslog.conf.
Banner file
\\/etc\\/issue
The full path to the SSH banner file as it appears in sshd_config. The banner file contains the text that is sent to each new SSH connection.

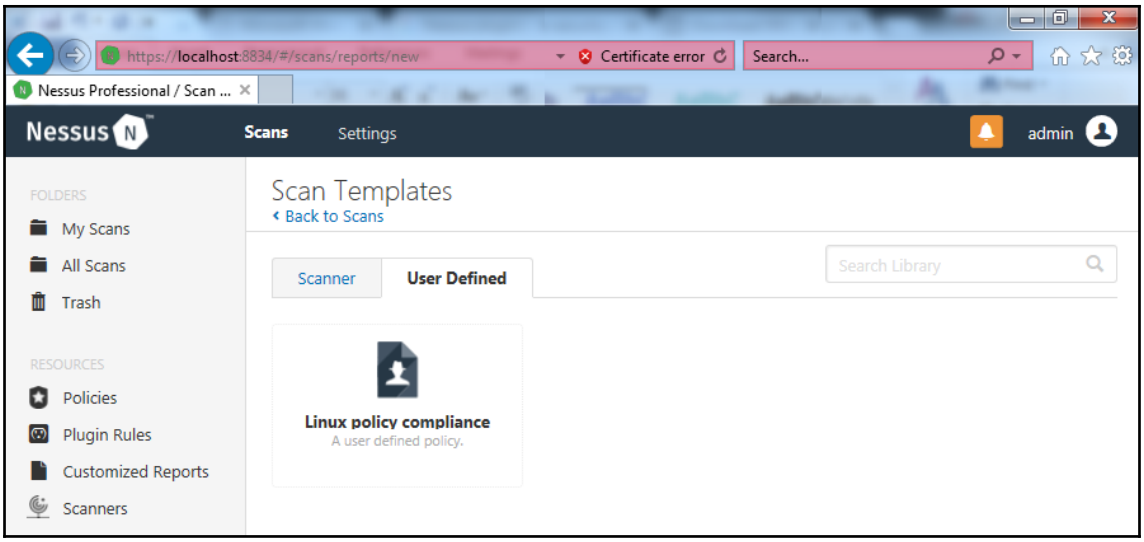

Client side
Presentation Layer
HTML
CSS
Browser
Local Storage
Cookies, IndexedDB, localStorage, File API
Operating System
Communication Channel
Application Layer
HTTP/1.1, HTTP/2
Server side
Logic Layer
php
Perl
python
Web Server Layer
NGINX
APACHE
Storage Layer
MySQL
ORACLE DATABASE
PostgreSQL
Operating System
Infrastructure
Intel® VT
ARM
Xen


Nessus Professional / Polici...
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
SSH
Authentication method
public key
Username
Private key
Private key passphrase
Elevate privileges with
Nothing
Global Credential Settings
known_hosts file
Add File
certificate
Kerberos
password
public key

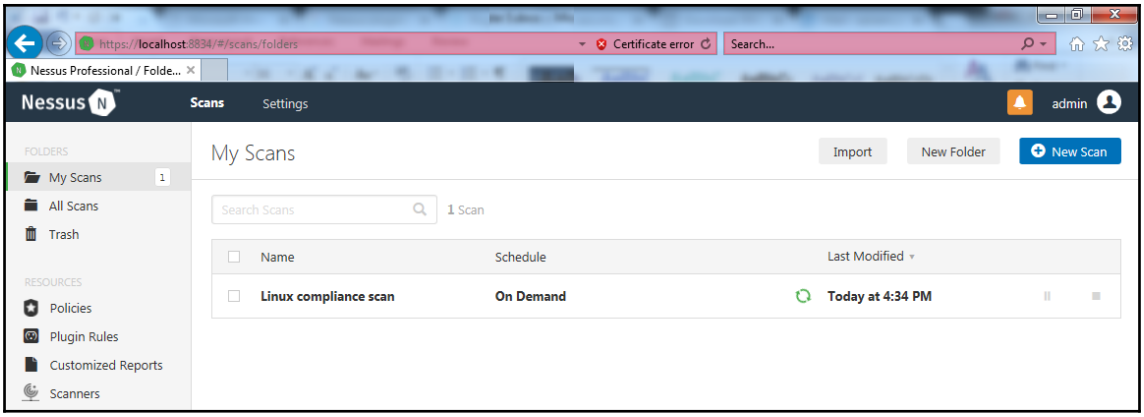

Nessus Professional / Polici...
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
SSH
Authentication method
password
Username
msfadmin
Password (unsafe!)
This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.
Elevate privileges with
Nothing
Global Credential Settings
known_hosts file
Add File
Preferred port
22

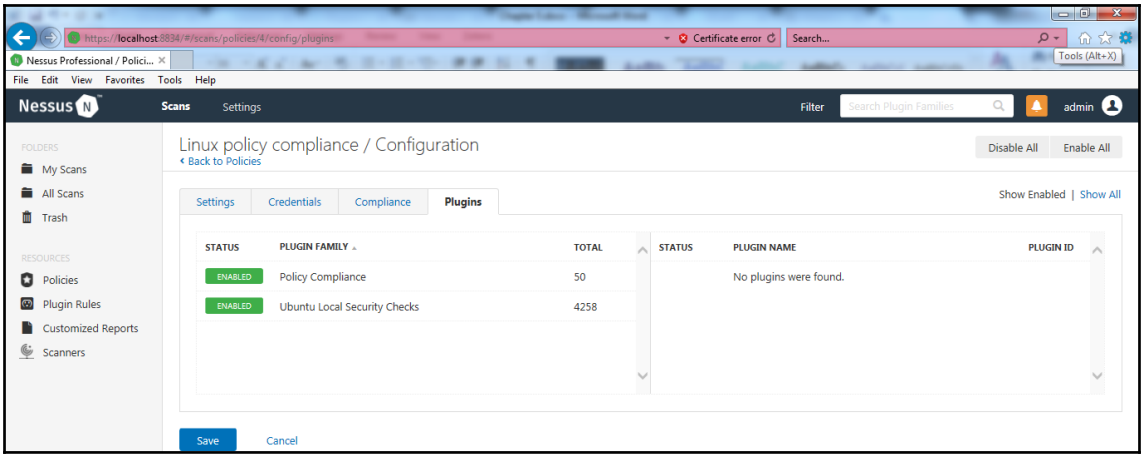

https://localhost:8834/#/scans/policies/4/config/plugins
Certificate error
Search...
Nessus Professional / Polici...
File Edit View Favorites Tools Help
Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Linux policy compliance / Configuration
Back to Policies
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
STATUS
PLUGIN FAMILY
TOTAL
STATUS
PLUGIN NAME
PLUGIN ID
ENABLED
Policy Compliance
50
ENABLED
Ubuntu Local Security Checks
4258
No plugins were found.
Save
Cancel

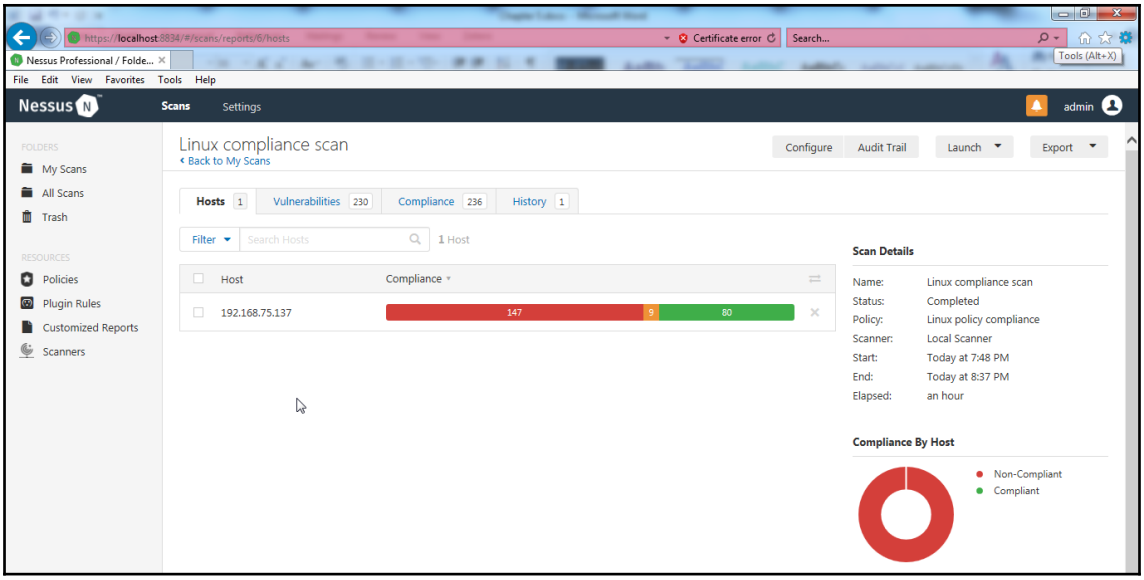

https://localhost:8834/#/scans/policies
Certificate error
Search...
Nessus Professional / Reso...
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Policies
Import
New Policy
Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.
Search Policies
1 Policy
Name
Template
Last Modified
Linux policy compliance
Advanced Scan
Today at 4:25 PM

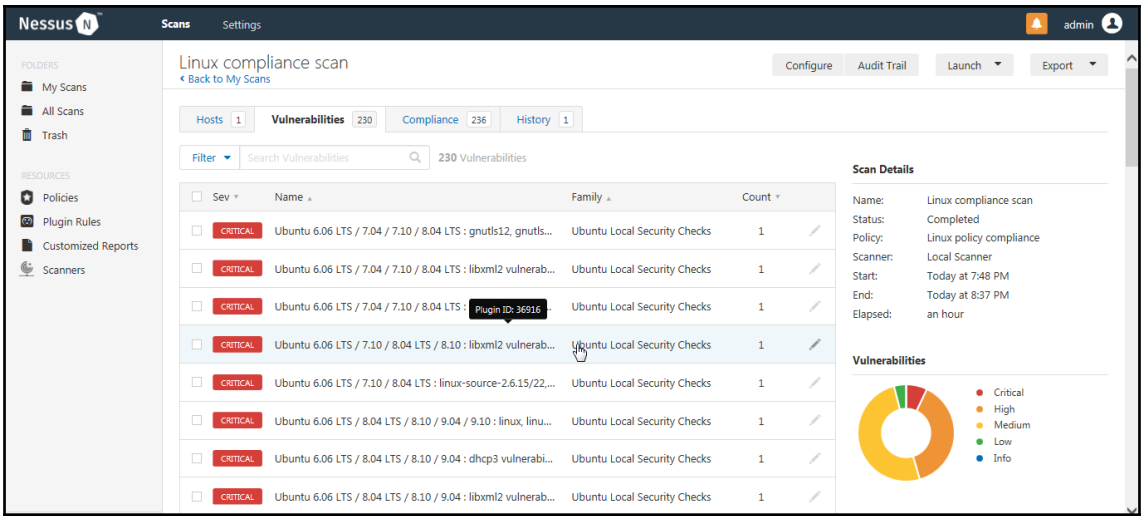


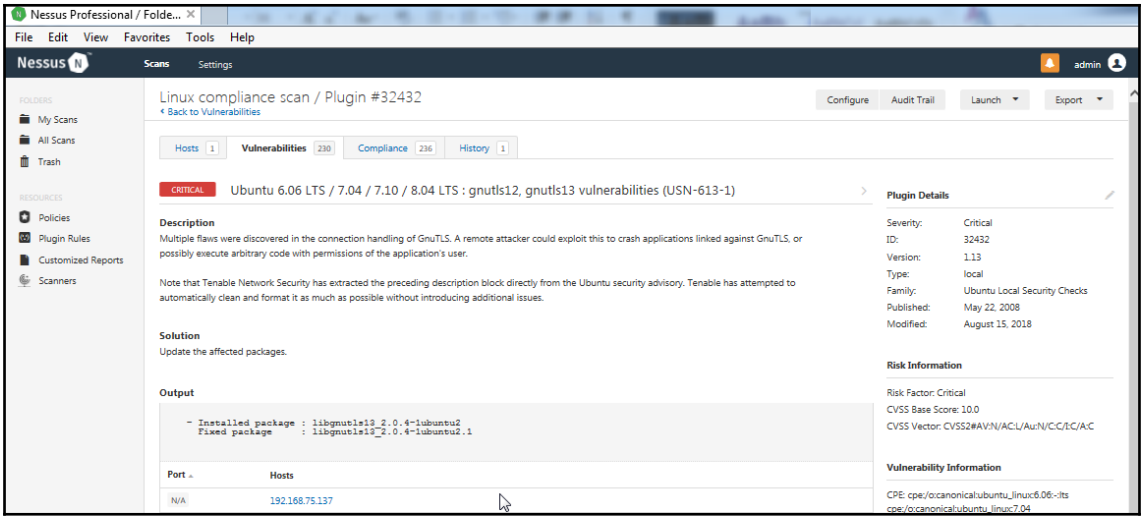

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:74:1c:63
          inet addr:192.168.75.137  Bcast:192.168.75.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe74:1c63/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2786 errors:0 dropped:0 overruns:0 frame:0
          TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:188676 (184.2 KB)  TX bytes:20942 (20.4 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:764 errors:0 dropped:0 overruns:0 frame:0
          TX packets:764 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:332277 (324.4 KB)  TX bytes:332277 (324.4 KB)
```

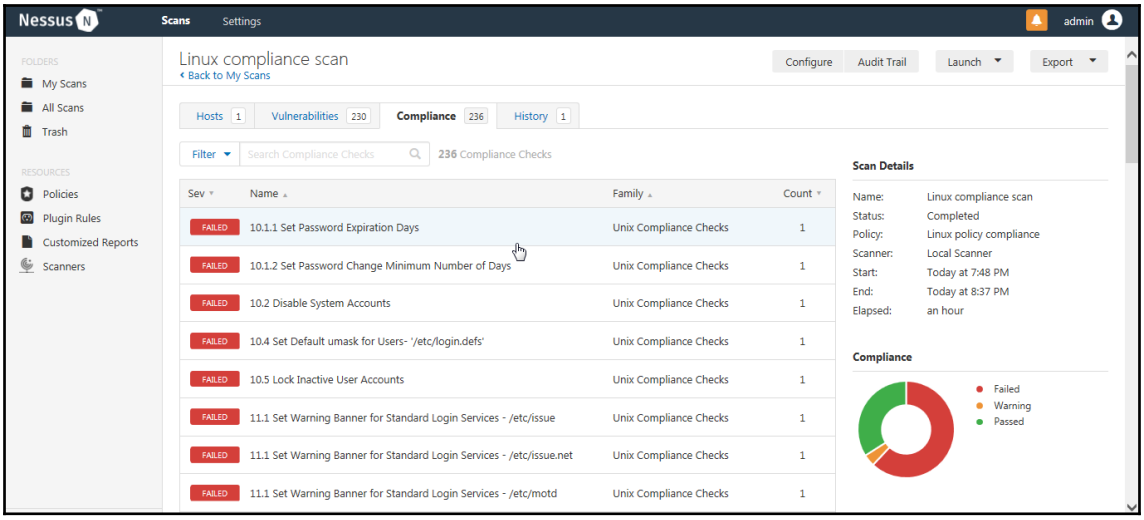

https://localhost:8834/#/scans/folders
Certificate error
Search...
Nessus Professional / Folde...
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
Linux compliance scan
On Demand
Today at 4:34 PM

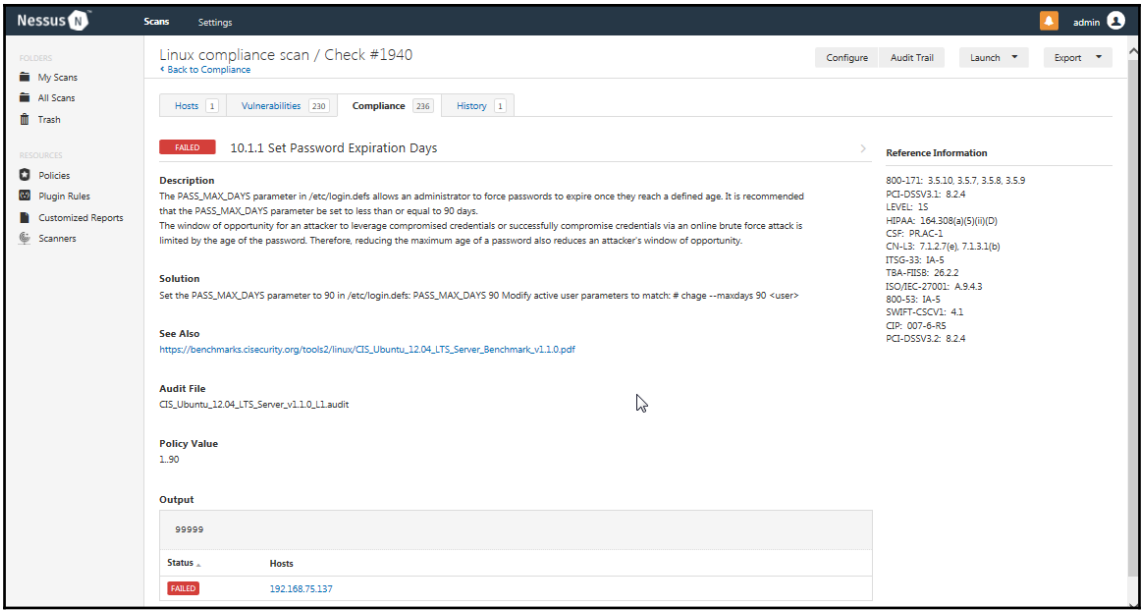

https://localhost:8834/#/scans/policies/4/config/plugins
Certificate error
Search...
Nessus Professional / Polici...
Tools (Alt+X)
File Edit View Favorites Tools Help
Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Linux policy compliance / Configuration
Back to Policies
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
STATUS
PLUGIN FAMILY
TOTAL
ENABLED
Policy Compliance
50
ENABLED
Ubuntu Local Security Checks
4258
STATUS
PLUGIN NAME
PLUGIN ID
No plugins were found.
Save
Cancel


https://localhost:8834/#/scans/reports/6/hosts
Certificate error
Search...
Nessus Professional / Folde...
File Edit View Favorites Tools Help
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Linux compliance scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 230
Compliance 236
History 1
Filter
Search Hosts
1 Host
Host
Compliance
192.168.75.137
147
9
80
Scan Details
Name: Linux compliance scan
Status: Completed
Policy: Linux policy compliance
Scanner: Local Scanner
Start: Today at 7:48 PM
End: Today at 8:37 PM
Elapsed: an hour
Compliance By Host
Non-Compliant
Compliant

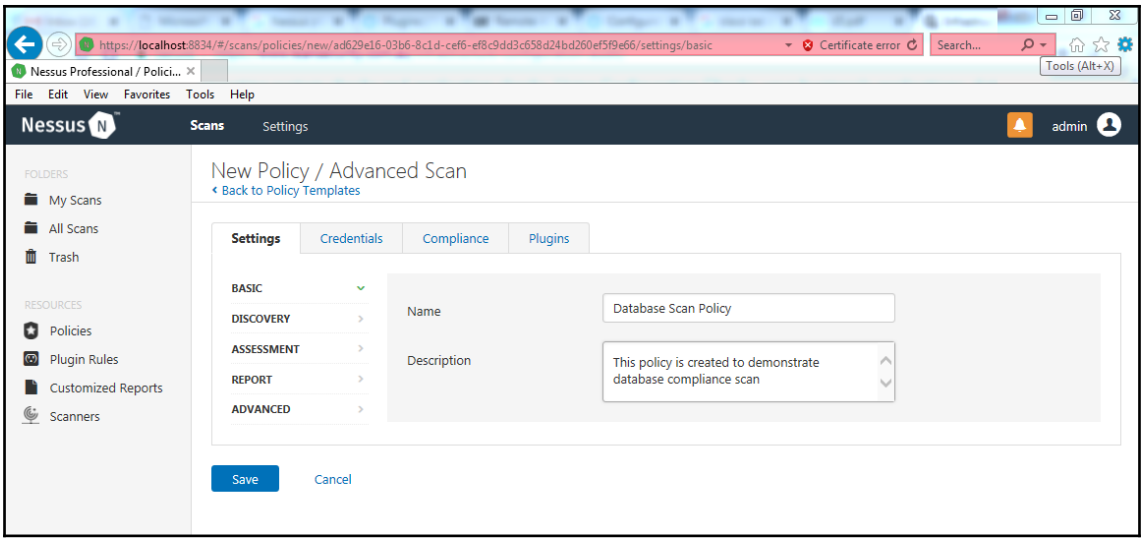

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Linux compliance scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 230
Compliance 236
History 1
Filter
Search Vulnerabilities
230 Vulnerabilities
Sev
Name
Family
Count
CRITICAL
Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls...
Ubuntu Local Security Checks
1
Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerab...
Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS :
Plugin ID: 36916
Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libxml2 vulnerab...
Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22,...
Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linu...
Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerabi...
Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libxml2 vulnerab...
Scan Details
Name: Linux compliance scan
Status: Completed
Policy: Linux policy compliance
Scanner: Local Scanner
Start: Today at 7:48 PM
End: Today at 8:37 PM
Elapsed: an hour
Vulnerabilities
Critical
High
Medium
Low
Info

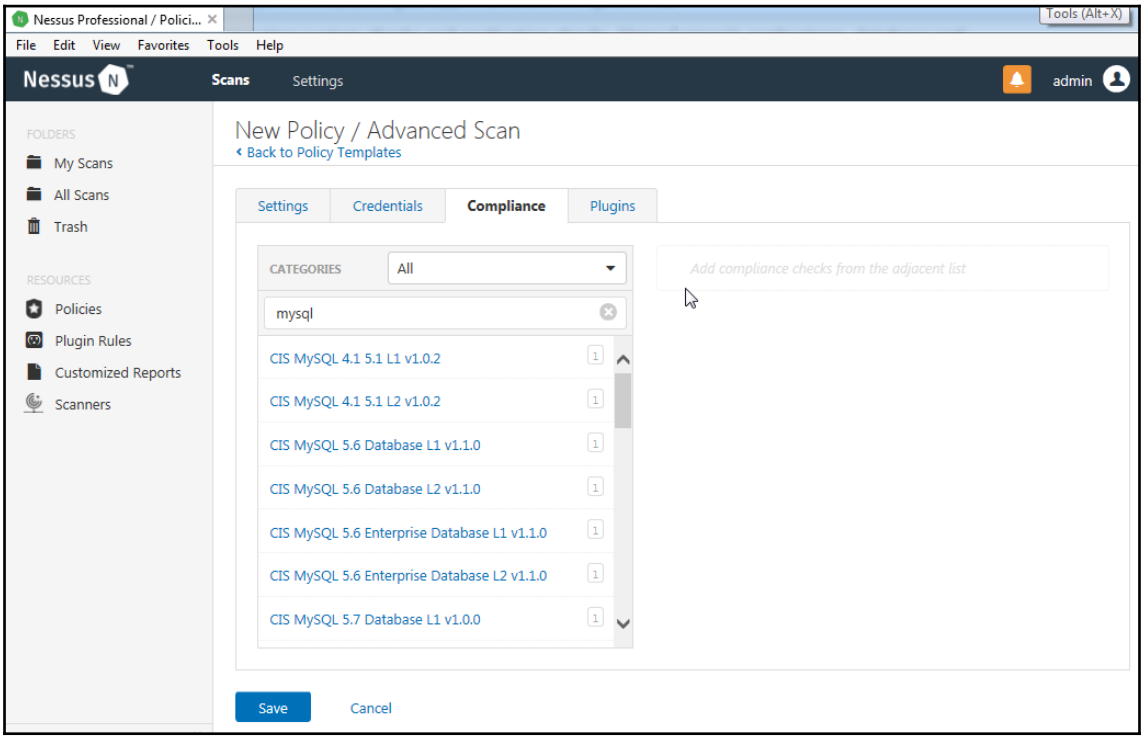

Nessus Professional / Folde...
File Edit View Favorites Tools Help
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Linux compliance scan / Plugin #32432
Back to Vulnerabilities
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 230
Compliance 236
History 1
CRITICAL
Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-613-1)
Description
Multiple flaws were discovered in the connection handling of GnuTLS. A remote attacker could exploit this to crash applications linked against GnuTLS, or possibly execute arbitrary code with permissions of the application's user.
Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.
Solution
Update the affected packages.
Output
- Installed package : libgnutls13_2.0.4-1ubuntu2
Fixed package : libgnutls13_2.0.4-1ubuntu2.1
Port
Hosts
N/A
192.168.75.137
Plugin Details
Severity: Critical
ID: 32432
Version: 1.13
Type: local
Family: Ubuntu Local Security Checks
Published: May 22, 2008
Modified: August 15, 2018
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Vulnerability Information
CPE: cpe:/o:canonical:ubuntu_linux:6.06:-:lts
cpe:/o:canonical:ubuntu_linux:7.04

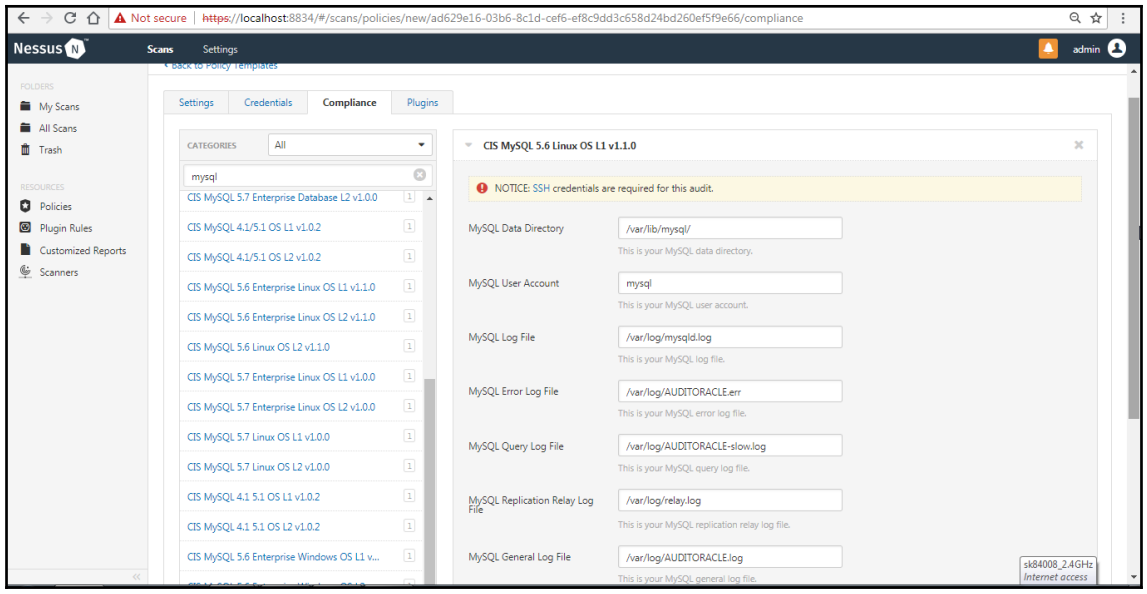

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Linux compliance scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 230
Compliance 236
History 1
Filter
Search Compliance Checks
236 Compliance Checks
Sev
Name
Family
Count
FAILED 10.1.1 Set Password Expiration Days Unix Compliance Checks 1
FAILED 10.1.2 Set Password Change Minimum Number of Days Unix Compliance Checks 1
FAILED 10.2 Disable System Accounts Unix Compliance Checks 1
FAILED 10.4 Set Default umask for Users- '/etc/login.defs' Unix Compliance Checks 1
FAILED 10.5 Lock Inactive User Accounts Unix Compliance Checks 1
FAILED 11.1 Set Warning Banner for Standard Login Services - /etc/issue Unix Compliance Checks 1
FAILED 11.1 Set Warning Banner for Standard Login Services - /etc/issue.net Unix Compliance Checks 1
FAILED 11.1 Set Warning Banner for Standard Login Services - /etc/motd Unix Compliance Checks 1
Scan Details
Name: Linux compliance scan
Status: Completed
Policy: Linux policy compliance
Scanner: Local Scanner
Start: Today at 7:48 PM
End: Today at 8:37 PM
Elapsed: an hour
Compliance
Failed
Warning
Passed

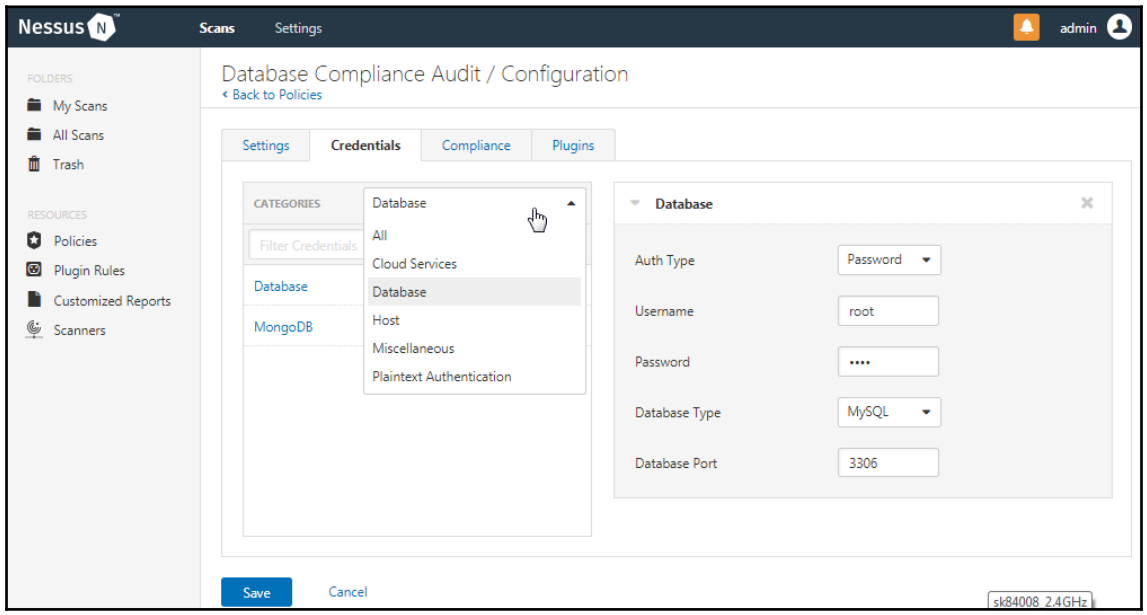


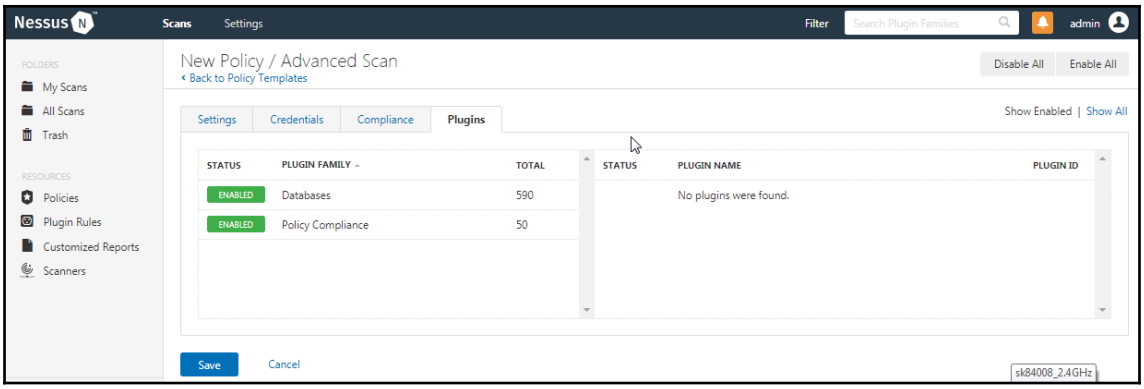

```
root@kali:~# service mysql start
root@kali:~# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.1.26-MariaDB-1 Debian buildd-unstable

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]> update user set password=PASSWORD("toor") where User='root';
Query OK, 1 row affected (0.18 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MariaDB [mysql]> Ctrl-C -- exit!
```

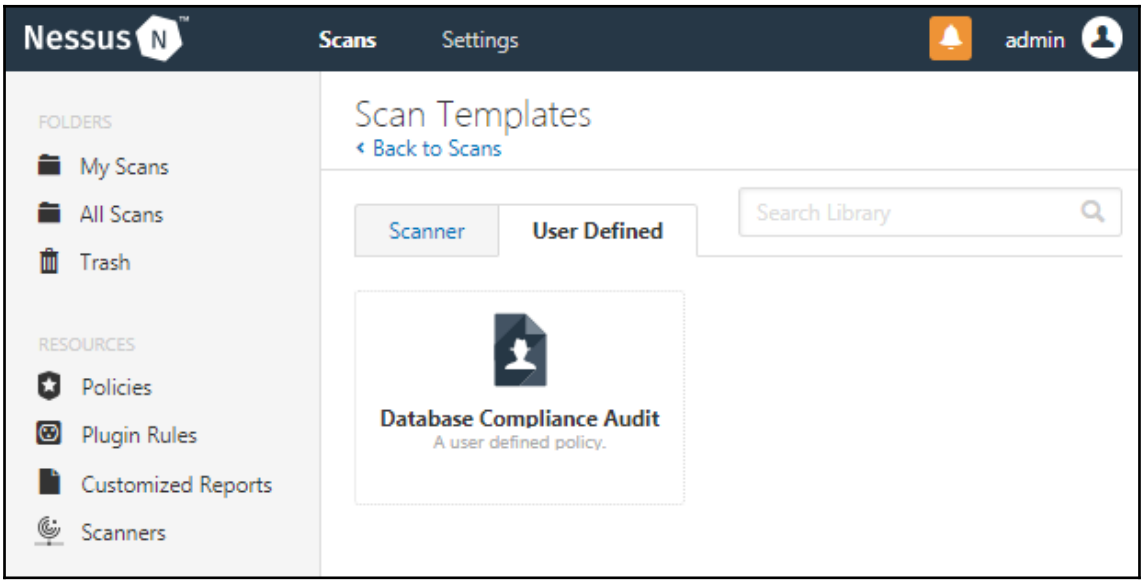

https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic
Certificate error
Search...
Nessus Professional / Polici...
Tools (Alt+X)
File Edit View Favorites Tools Help
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Database Scan Policy
Description
This policy is created to demonstrate database compliance scan
Save
Cancel


Nessus Professional / Polici...
Tools (Alt+X)
File Edit View Favorites Tools Help
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
CATEGORIES
All
mysql
Add compliance checks from the adjacent list
CIS MySQL 4.1 5.1 L1 v1.0.2
CIS MySQL 4.1 5.1 L2 v1.0.2
CIS MySQL 5.6 Database L1 v1.1.0
CIS MySQL 5.6 Database L2 v1.1.0
CIS MySQL 5.6 Enterprise Database L1 v1.1.0
CIS MySQL 5.6 Enterprise Database L2 v1.1.0
CIS MySQL 5.7 Database L1 v1.0.0
Save
Cancel

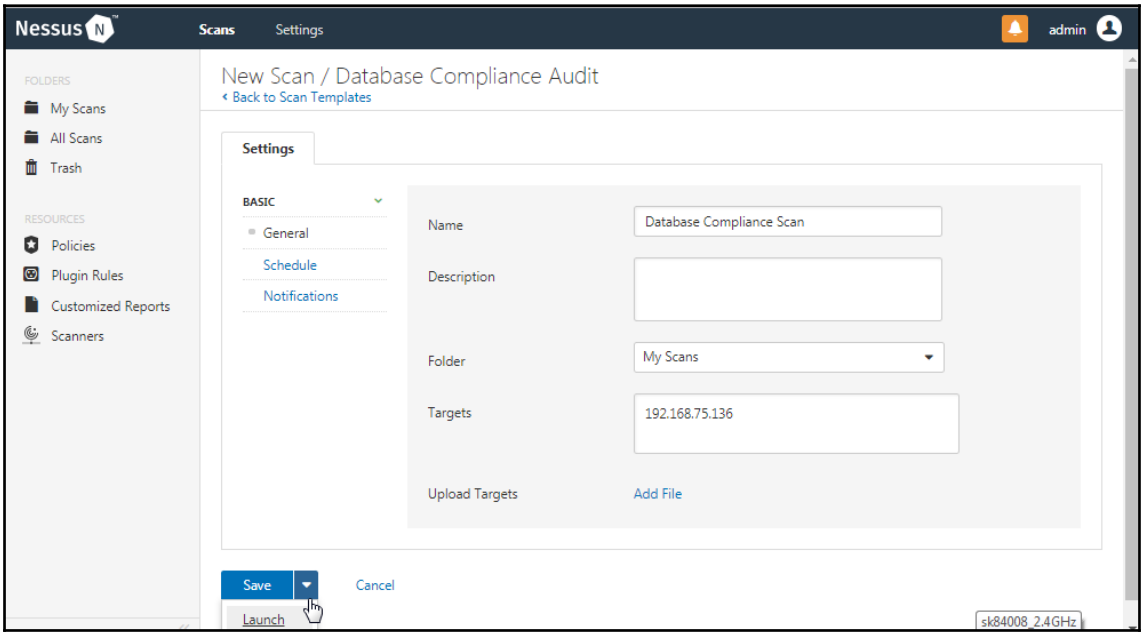

Not secure
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/compliance
Nessus
Scans
Settings
admin
Back to Policy Templates
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Settings
Credentials
Compliance
Plugins
CATEGORIES
All
mysql
CIS MySQL 5.7 Enterprise Database L2 v1.0.0
CIS MySQL 4.1/5.1 OS L1 v1.0.2
CIS MySQL 4.1/5.1 OS L2 v1.0.2
CIS MySQL 5.6 Enterprise Linux OS L1 v1.1.0
CIS MySQL 5.6 Enterprise Linux OS L2 v1.1.0
CIS MySQL 5.6 Linux OS L2 v1.1.0
CIS MySQL 5.7 Enterprise Linux OS L1 v1.0.0
CIS MySQL 5.7 Enterprise Linux OS L2 v1.0.0
CIS MySQL 5.7 Linux OS L1 v1.0.0
CIS MySQL 5.7 Linux OS L2 v1.0.0
CIS MySQL 4.1 5.1 OS L1 v1.0.2
CIS MySQL 4.1 5.1 OS L2 v1.0.2
CIS MySQL 5.6 Enterprise Windows OS L1 v...
CIS MySQL 5.6 Linux OS L1 v1.1.0
NOTICE: SSH credentials are required for this audit.
MySQL Data Directory
/var/lib/mysql/
This is your MySQL data directory.
MySQL User Account
mysql
This is your MySQL user account.
MySQL Log File
/var/log/mysqld.log
This is your MySQL log file.
MySQL Error Log File
/var/log/AUDITORACLE.err
This is your MySQL error log file.
MySQL Query Log File
/var/log/AUDITORACLE-slow.log
This is your MySQL query log file.
MySQL Replication Relay Log File
/var/log/relay.log
This is your MySQL replication relay log file.
MySQL General Log File
/var/log/AUDITORACLE.log
This is your MySQL general log file.
sk84008_2.4GHz
Internet access


Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Database Compliance Audit / Configuration
Back to Policies
Settings
Credentials
Compliance
Plugins
CATEGORIES
Database
Filter Credentials
Database
MongoDB
All
Cloud Services
Database
Host
Miscellaneous
Plaintext Authentication
Database
Auth Type
Password
Username
root
Password
Database Type
MySQL
Database Port
3306
Save
Cancel
sk84008_2.4GHz


Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Disable All
Enable All
Settings
Credentials
Compliance
Plugins
Show Enabled | Show All
STATUS
PLUGIN FAMILY
TOTAL
STATUS
PLUGIN NAME
PLUGIN ID
ENABLED
Databases
590
No plugins were found.
ENABLED
Policy Compliance
50
Save
Cancel
sk84008_2.4GHz

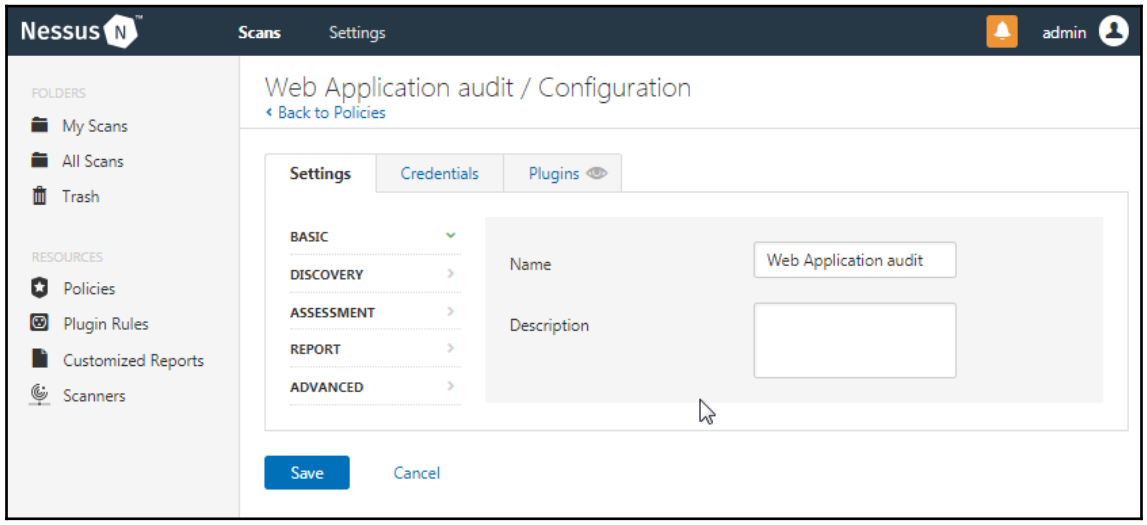

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
Database Compliance Audit
A user defined policy.

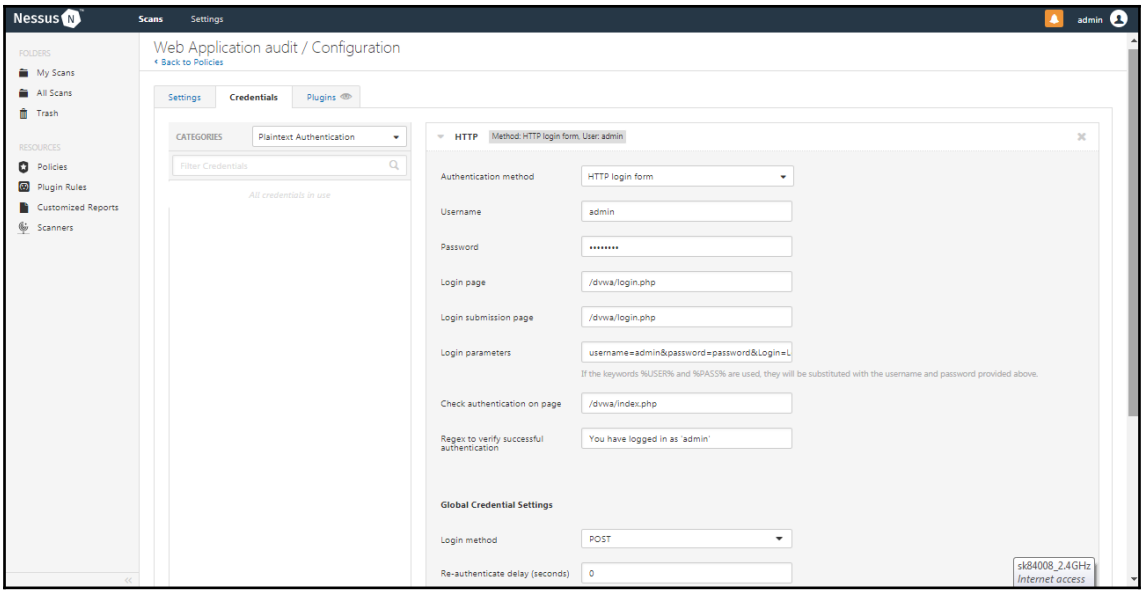
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.75.136  netmask 255.255.255.0  broadcast 192.168.75.255
        inet6 fe80::20c:29ff:fe5a:b29d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5a:b2:9d  txqueuelen 1000  (Ethernet)
        RX packets 394  bytes 29891 (29.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99  bytes 8251 (8.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1596 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1596 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

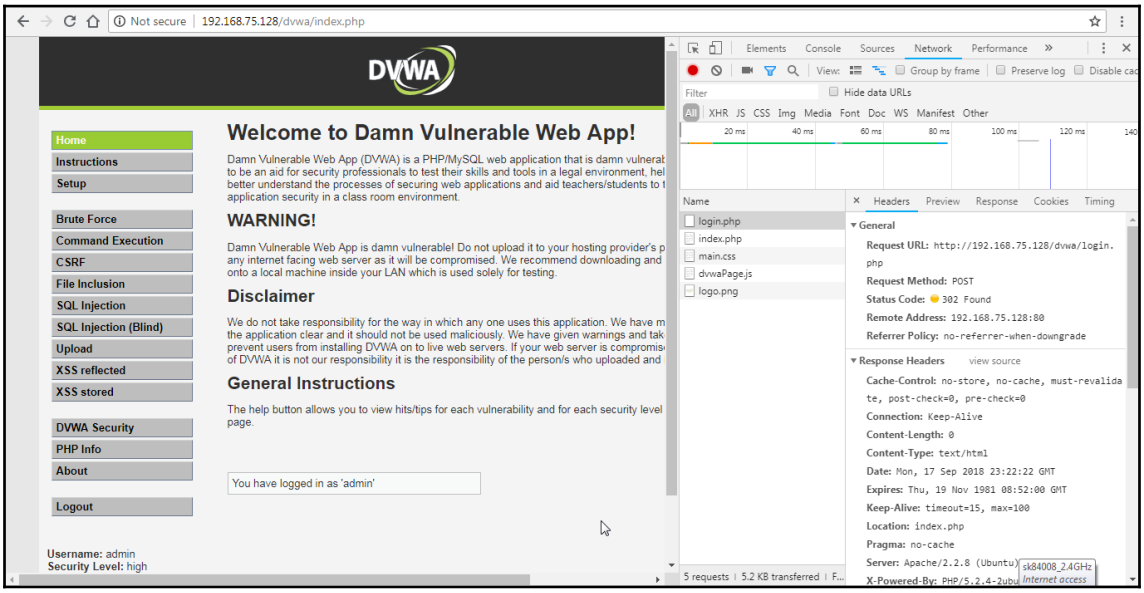


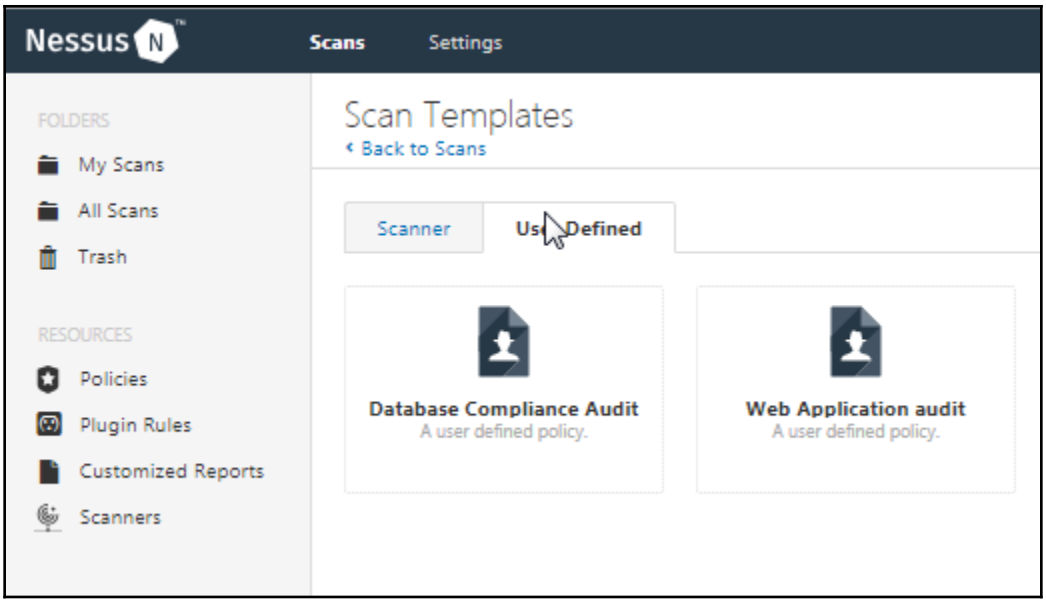

Not secure
192.168.75.128
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV

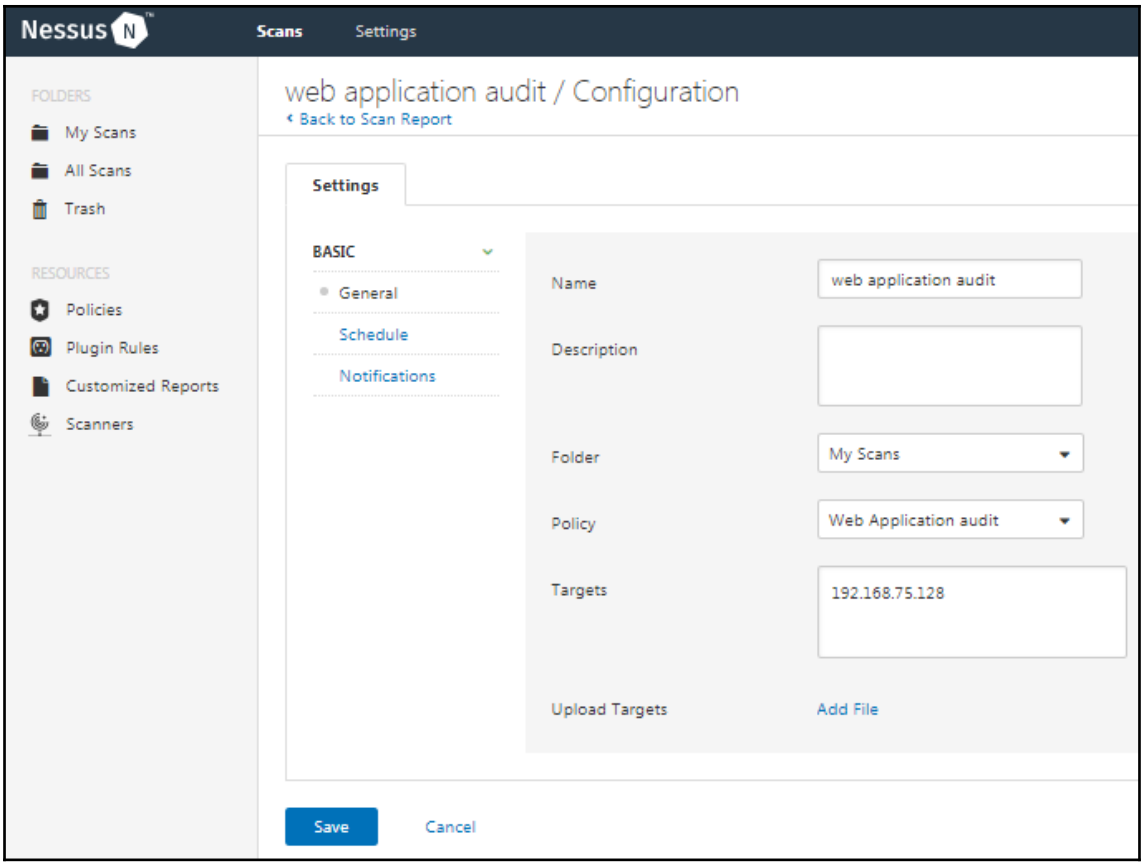

Not secure
192.168.75.128/dvwa/login.php
DVWA
Username
Password
Logi
Use password for:
admin
You have logged out

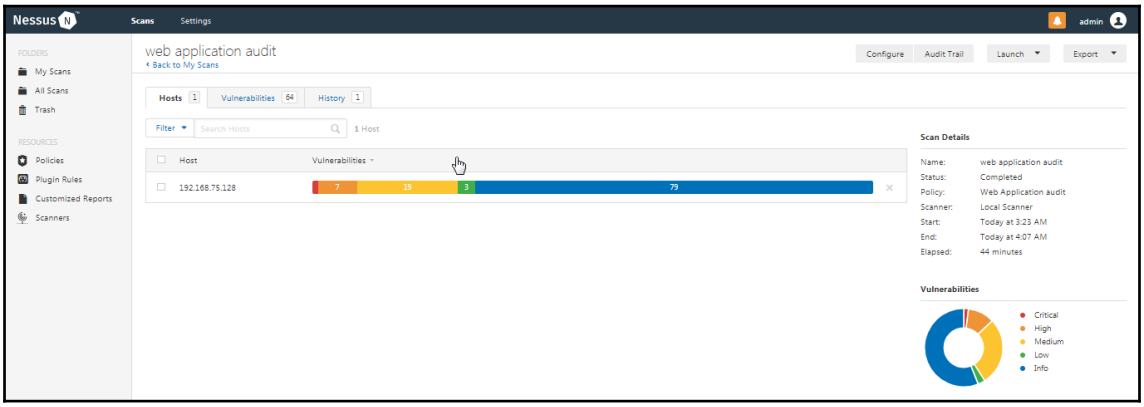

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Web Application audit / Configuration
Back to Policies
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Web Application audit
Description
Save
Cancel

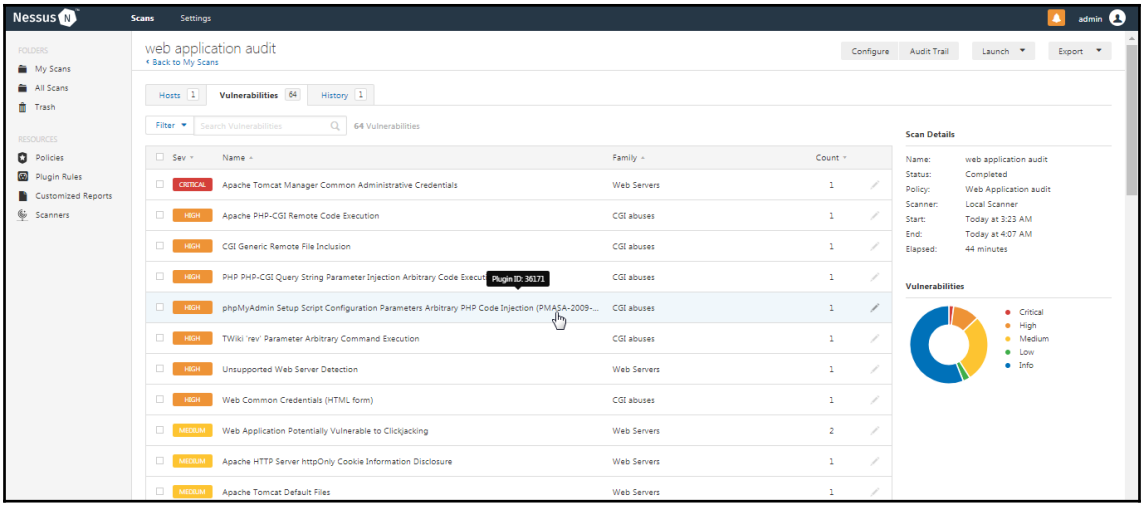

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Web Application audit / Configuration
Back to Policies
Settings
Credentials
Plugins
CATEGORIES
Plaintext Authentication
Filter Credentials
All credentials in use
HTTP
Method: HTTP login form, User: admin
Authentication method
HTTP login form
Username
admin
Password
Login page
/dvwa/login.php
Login submission page
/dvwa/login.php
Login parameters
username=admin&password=password&Login=L
If the keywords %USER% and %PASS% are used, they will be substituted with the username and password provided above.
Check authentication on page
/dvwa/index.php
Regex to verify successful authentication
You have logged in as 'admin'
Global Credential Settings
Login method
POST
Re-authenticate delay (seconds)
0
sk84008_2.4GHz
Internet access

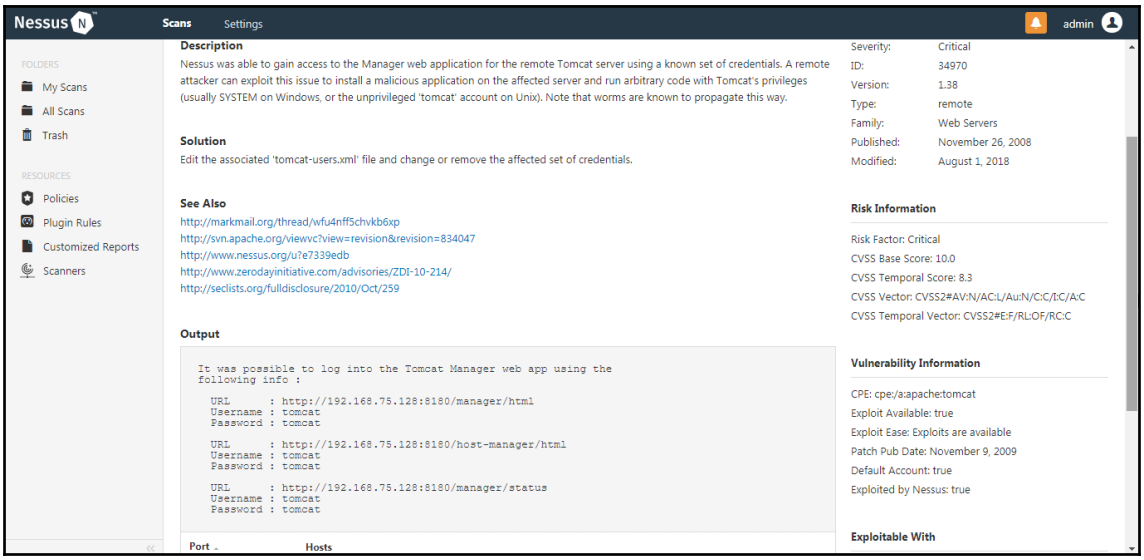

Not secure
192.168.75.128/dvwa/index.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerat
to be an aid for security professionals to test their skills and tools in a legal environment, hel
better understand the processes of securing web applications and aid teachers/students to t
application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's p
any internet facing web server as it will be compromised. We recommend downloading and
onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have m
the application clear and it should not be used maliciously. We have given warnings and tak
prevent users from installing DVWA on to live web servers. If your web server is compromis
of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level
page.
You have logged in as 'admin'
Username: admin
Security Level: high
Elements
Console
Sources
Network
Performance
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Name
login.php
index.php
main.css
dvwaPage.js
logo.png
Headers
Preview
Response
Cookies
Timing
General
Request URL: http://192.168.75.128/dvwa/login.php
Request Method: POST
Status Code: 302 Found
Remote Address: 192.168.75.128:80
Referrer Policy: no-referrer-when-downgrade
Response Headers
view source
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Length: 0
Content-Type: text/html
Date: Mon, 17 Sep 2018 23:22:22 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=15, max=100
Location: index.php
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu)
X-Powered-By: PHP/5.2.4-2ubu
5 requests
5.2 KB transferred
sk84008_2.4GHz
Internet access


Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Database Compliance Audit
A user defined policy.
Web Application audit
A user defined policy.

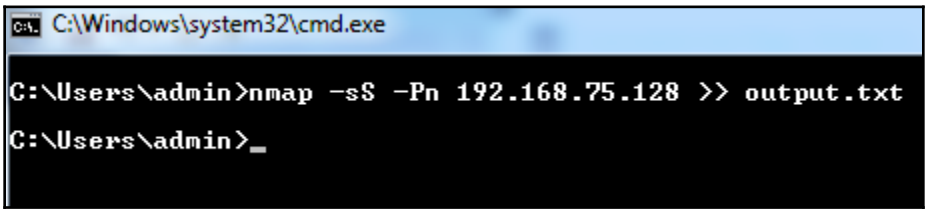

Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
web application audit / Configuration
Back to Scan Report
Settings
BASIC
General
Schedule
Notifications
Name
web application audit
Description
Folder
My Scans
Policy
Web Application audit
Targets
192.168.75.128
Upload Targets
Add File
Save
Cancel

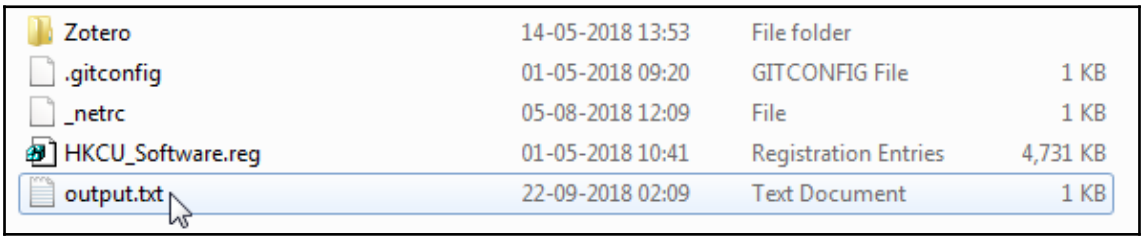

Nessus
Scans
Settings
admin
web application audit
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 64
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.75.128
7
19
3
79
Scan Details
Name: web application audit
Status: Completed
Policy: Web Application audit
Scanner: Local Scanner
Start: Today at 3:23 AM
End: Today at 4:07 AM
Elapsed: 44 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

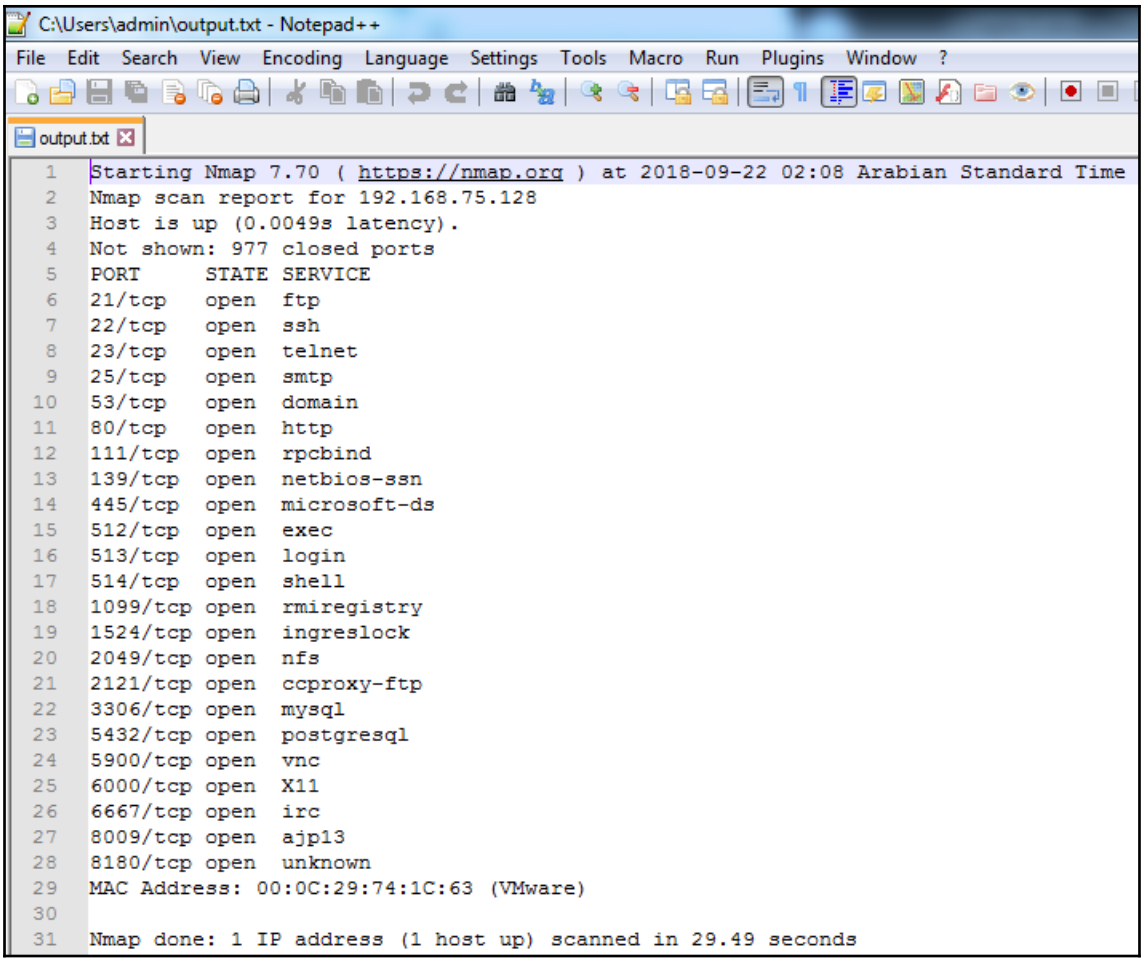

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
web application audit
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 64
History 1
Filter
Search Vulnerabilities
64 Vulnerabilities
Sev
Name
Family
Count
CRITICAL Apache Tomcat Manager Common Administrative Credentials Web Servers 1
HIGH Apache PHP-CGI Remote Code Execution CGI abuses 1
HIGH CGI Generic Remote File Inclusion CGI abuses 1
HIGH PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execut Plugin ID: 36171 CGI abuses 1
HIGH phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-... CGI abuses 1
HIGH TWiki 'rev' Parameter Arbitrary Command Execution CGI abuses 1
HIGH Unsupported Web Server Detection Web Servers 1
HIGH Web Common Credentials (HTML form) CGI abuses 1
MEDIUM Web Application Potentially Vulnerable to Clickjacking Web Servers 2
MEDIUM Apache HTTP Server httpOnly Cookie Information Disclosure Web Servers 1
MEDIUM Apache Tomcat Default Files Web Servers 1
Scan Details
Name: web application audit
Status: Completed
Policy: Web Application audit
Scanner: Local Scanner
Start: Today at 3:23 AM
End: Today at 4:07 AM
Elapsed: 44 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

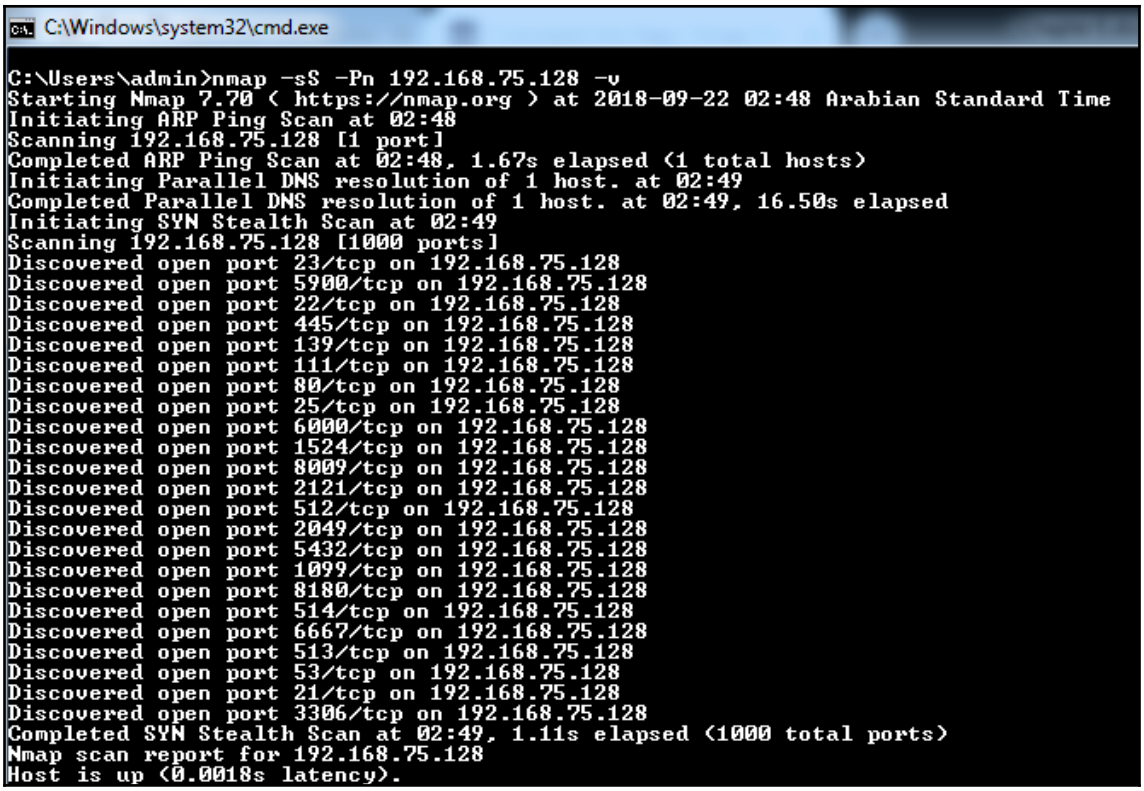

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Description
Nessus was able to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can exploit this issue to install a malicious application on the affected server and run arbitrary code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix). Note that worms are known to propagate this way.
Solution
Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.
See Also
http://markmail.org/thread/wfu4nff5chvkb6xp
http://svn.apache.org/viewvc?view=revision&revision=834047
http://www.nessus.org/u?e7339edb
http://www.zerodayinitiative.com/advisories/ZDI-10-214/
http://seclists.org/fulldisclosure/2010/Oct/259
Output
It was possible to log into the Tomcat Manager web app using the following info :
URL : http://192.168.75.128:8180/manager/html
Username : tomcat
Password : tomcat
URL : http://192.168.75.128:8180/host-manager/html
Username : tomcat
Password : tomcat
URL : http://192.168.75.128:8180/manager/status
Username : tomcat
Password : tomcat
Port
Hosts
Severity: Critical
ID: 34970
Version: 1.38
Type: remote
Family: Web Servers
Published: November 26, 2008
Modified: August 1, 2018
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: November 9, 2009
Default Account: true
Exploited by Nessus: true
Exploitable With

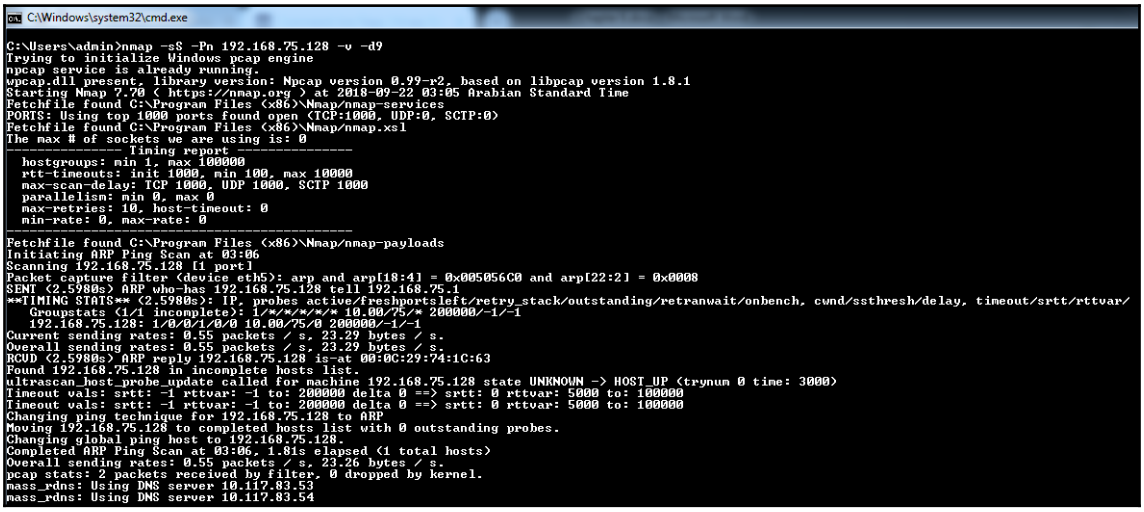
Chapter 6: Report Analysis and Confirmation



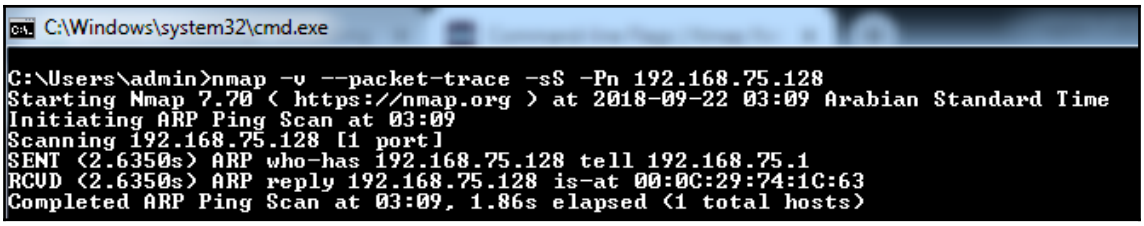


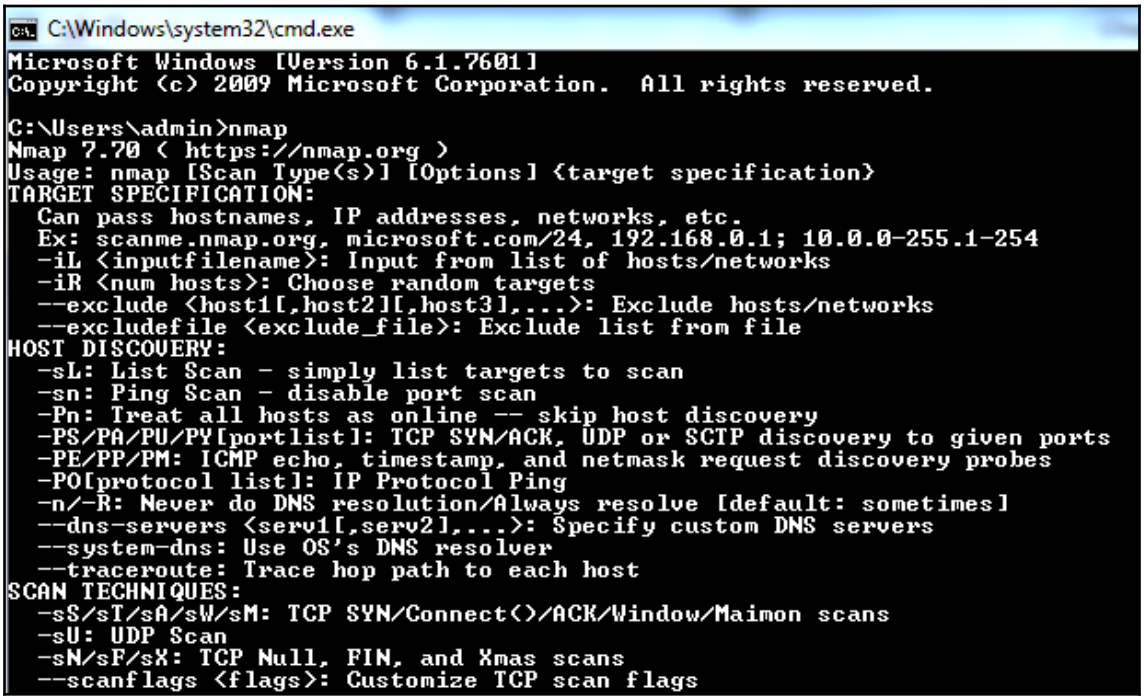

C:\Users\admin\output.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
output.txt
1 Starting Nmap 7.70 (https://nmap.org) at 2018-09-22 02:08 Arabian Standard Time
2 Nmap scan report for 192.168.75.128
3 Host is up (0.0049s latency).
4 Not shown: 977 closed ports
5 PORT STATE SERVICE
6 21/tcp open ftp
7 22/tcp open ssh
8 23/tcp open telnet
9 25/tcp open smtp
10 53/tcp open domain
11 80/tcp open http
12 111/tcp open rpcbind
13 139/tcp open netbios-ssn
14 445/tcp open microsoft-ds
15 512/tcp open exec
16 513/tcp open login
17 514/tcp open shell
18 1099/tcp open rmiregistry
19 1524/tcp open ingreslock
20 2049/tcp open nfs
21 2121/tcp open ccproxy-ftp
22 3306/tcp open mysql
23 5432/tcp open postgresql
24 5900/tcp open vnc
25 6000/tcp open X11
26 6667/tcp open irc
27 8009/tcp open ajp13
28 8180/tcp open unknown
29 MAC Address: 00:0C:29:74:1C:63 (VMware)
30
31 Nmap done: 1 IP address (1 host up) scanned in 29.49 seconds

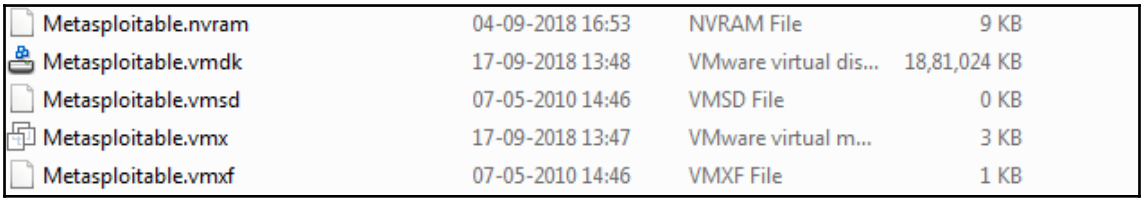

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -sS -Pn 192.168.75.128 -v
Starting Nmap 7.70 (https://nmap.org) at 2018-09-22 02:48 Arabian Standard Time
Initiating ARP Ping Scan at 02:48
Scanning 192.168.75.128 [1 port]
Completed ARP Ping Scan at 02:48, 1.67s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:49
Completed Parallel DNS resolution of 1 host. at 02:49, 16.50s elapsed
Initiating SYN Stealth Scan at 02:49
Scanning 192.168.75.128 [1000 ports]
Discovered open port 23/tcp on 192.168.75.128
Discovered open port 5900/tcp on 192.168.75.128
Discovered open port 22/tcp on 192.168.75.128
Discovered open port 445/tcp on 192.168.75.128
Discovered open port 139/tcp on 192.168.75.128
Discovered open port 111/tcp on 192.168.75.128
Discovered open port 80/tcp on 192.168.75.128
Discovered open port 25/tcp on 192.168.75.128
Discovered open port 6000/tcp on 192.168.75.128
Discovered open port 1524/tcp on 192.168.75.128
Discovered open port 8009/tcp on 192.168.75.128
Discovered open port 2121/tcp on 192.168.75.128
Discovered open port 512/tcp on 192.168.75.128
Discovered open port 2049/tcp on 192.168.75.128
Discovered open port 5432/tcp on 192.168.75.128
Discovered open port 1099/tcp on 192.168.75.128
Discovered open port 8180/tcp on 192.168.75.128
Discovered open port 514/tcp on 192.168.75.128
Discovered open port 6667/tcp on 192.168.75.128
Discovered open port 513/tcp on 192.168.75.128
Discovered open port 53/tcp on 192.168.75.128
Discovered open port 21/tcp on 192.168.75.128
Discovered open port 3306/tcp on 192.168.75.128
Completed SYN Stealth Scan at 02:49, 1.11s elapsed (1000 total ports)
Nmap scan report for 192.168.75.128
Host is up (0.0018s latency).

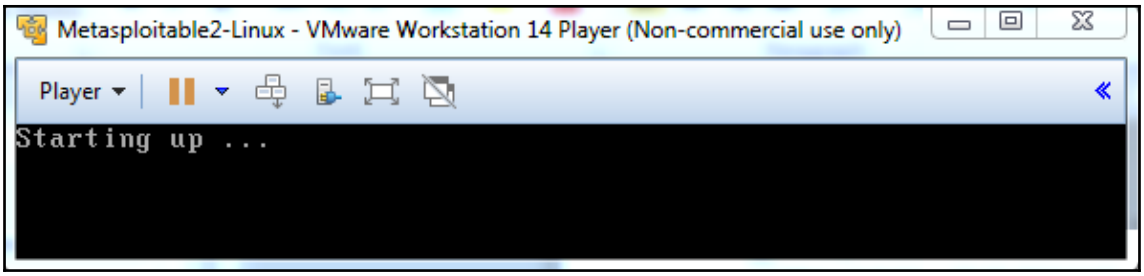

C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -sS -Pn 192.168.75.128 -v -d9
Trying to initialize Windows pcap engine
npcap service is already running.
wpcap.dll present, library version: Npcap version 0.99-r2, based on libpcap version 1.8.1
Starting Nmap 7.70 (https://nmap.org) at 2018-09-22 03:05 Arabian Standard Time
Fetchfile found C:\Program Files (x86)\Nmap\nmap-services
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
Fetchfile found C:\Program Files (x86)\Nmap\nmap.xsl
The max # of sockets we are using is: 0
-------------- Timing report --------------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0

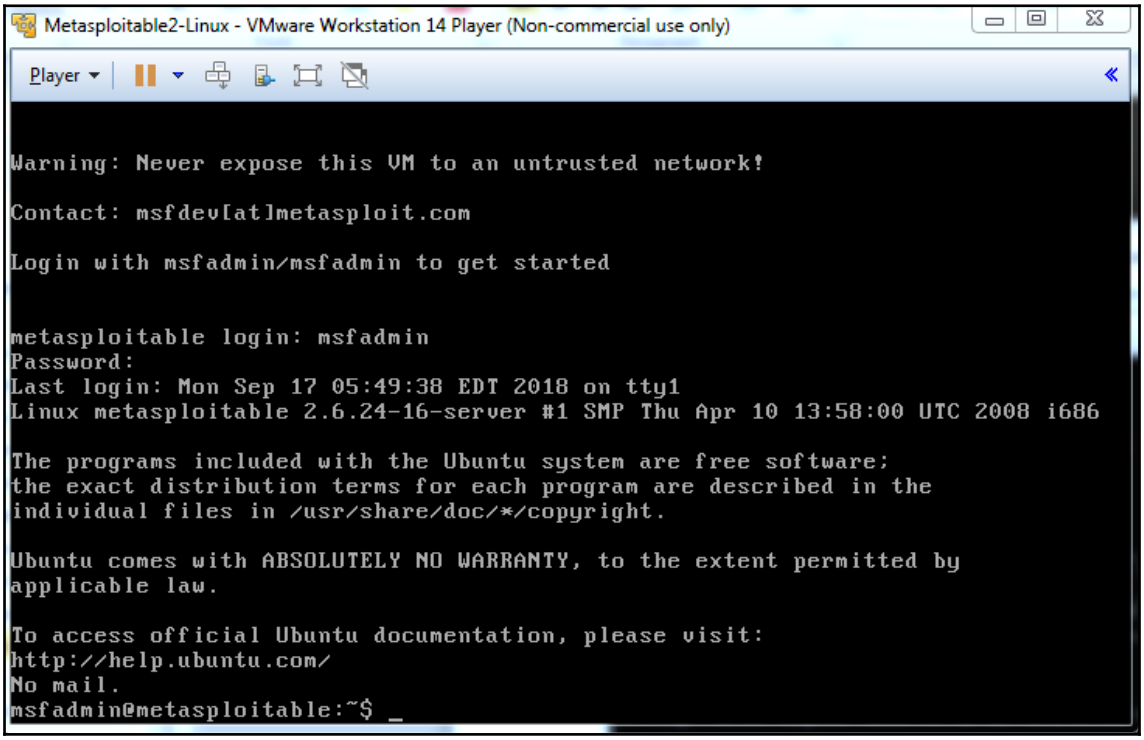
Fetchfile found C:\Program Files (x86)\Nmap\nmap-payloads
Initiating ARP Ping Scan at 03:06
Scanning 192.168.75.128 [1 port]
Packet capture filter (device eth5): arp and arp[18:4] = 0x005056C0 and arp[22:2] = 0x0008
SENT (2.5980s) ARP who-has 192.168.75.128 tell 192.168.75.1
TIMING STATS (2.5980s): IP: probes active/freshportsleft/retry_stack/outstanding/retranwait/onbench, cwnd/ssthresh/delay, timeout/srtt/rttvar/
Groupstats (1/1 incomplete): 1/*/*/*/*/* 10.00/75/* 200000/-1/-1
192.168.75.128: 1/0/0/1/0/0 10.00/75/0 200000/-1/-1
Current sending rates: 0.55 packets / s, 23.29 bytes / s.
Overall sending rates: 0.55 packets / s, 23.29 bytes / s.
RCVD (2.5980s) ARP reply 192.168.75.128 is-at 00:0C:29:74:1C:63
Found 192.168.75.128 in incomplete hosts list.
ultrascan_host_probe_update called for machine 192.168.75.128 state UNKNOWN -> HOST_UP (trynum 0 time: 3000)
Timeout vals: srtt: -1 rttvar: -1 to: 200000 delta 0 ==> srtt: 0 rttvar: 5000 to: 100000
Timeout vals: srtt: -1 rttvar: -1 to: 200000 delta 0 ==> srtt: 0 rttvar: 5000 to: 100000
Changing ping technique for 192.168.75.128 to ARP
Moving 192.168.75.128 to completed hosts list with 0 outstanding probes.
Changing global ping host to 192.168.75.128.
Completed ARP Ping Scan at 03:06, 1.81s elapsed (1 total hosts)
Overall sending rates: 0.55 packets / s, 23.26 bytes / s.
pcap stats: 2 packets received by filter, 0 dropped by kernel.
mass_rdns: Using DNS server 10.117.83.53
mass_rdns: Using DNS server 10.117.83.54


C:\Windows\system32\cmd.exe
C:\Users\admin>nmap -v --packet-trace -sS -Pn 192.168.75.128
Starting Nmap 7.70 (https://nmap.org) at 2018-09-22 03:09 Arabian Standard Time
Initiating ARP Ping Scan at 03:09
Scanning 192.168.75.128 [1 port]
SENT (2.6350s) ARP who-has 192.168.75.128 tell 192.168.75.1
RCVD (2.6350s) ARP reply 192.168.75.128 is-at 00:0C:29:74:1C:63
Completed ARP Ping Scan at 03:09, 1.86s elapsed (1 total hosts)

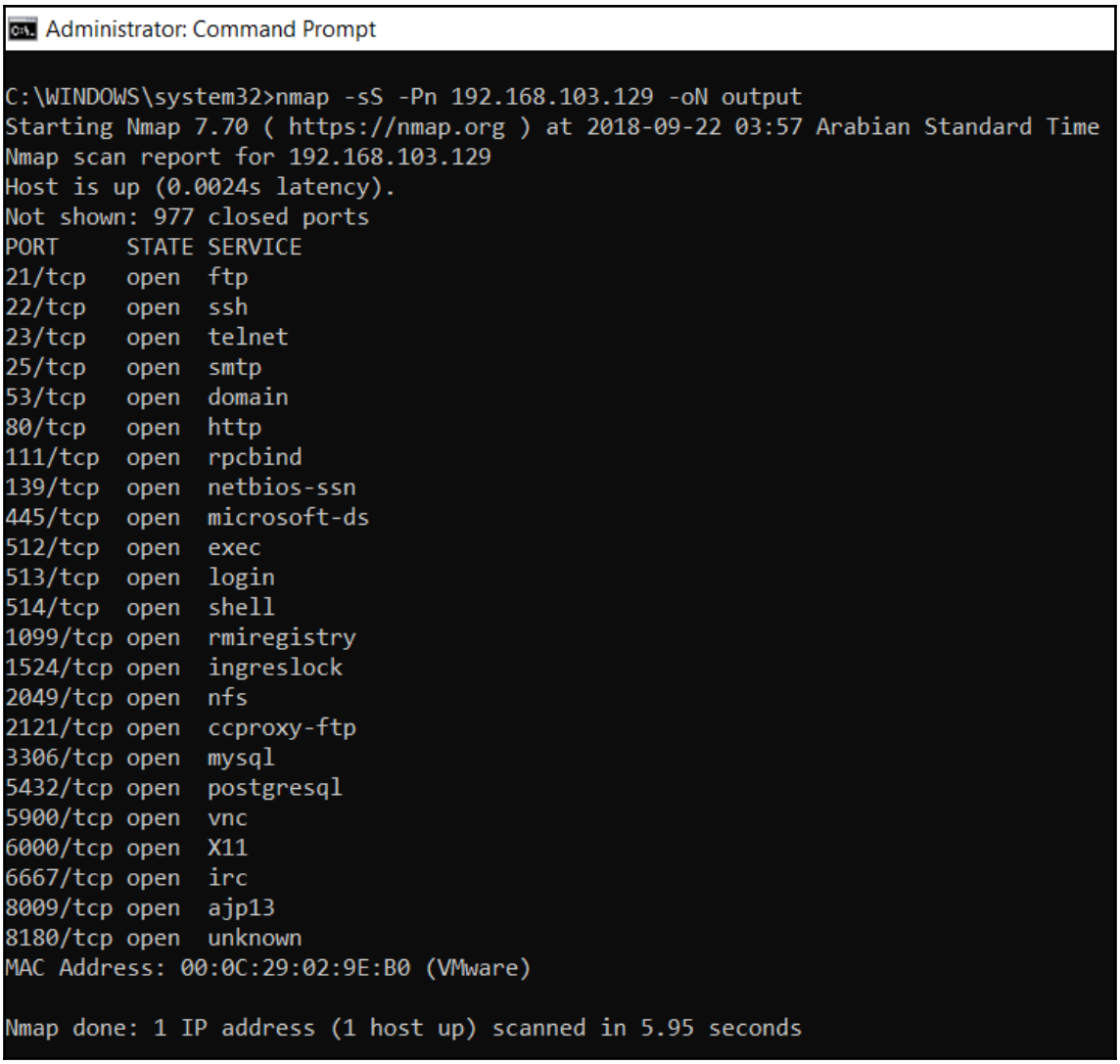

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\admin>nmap
Nmap 7.70 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] <target specification>
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags

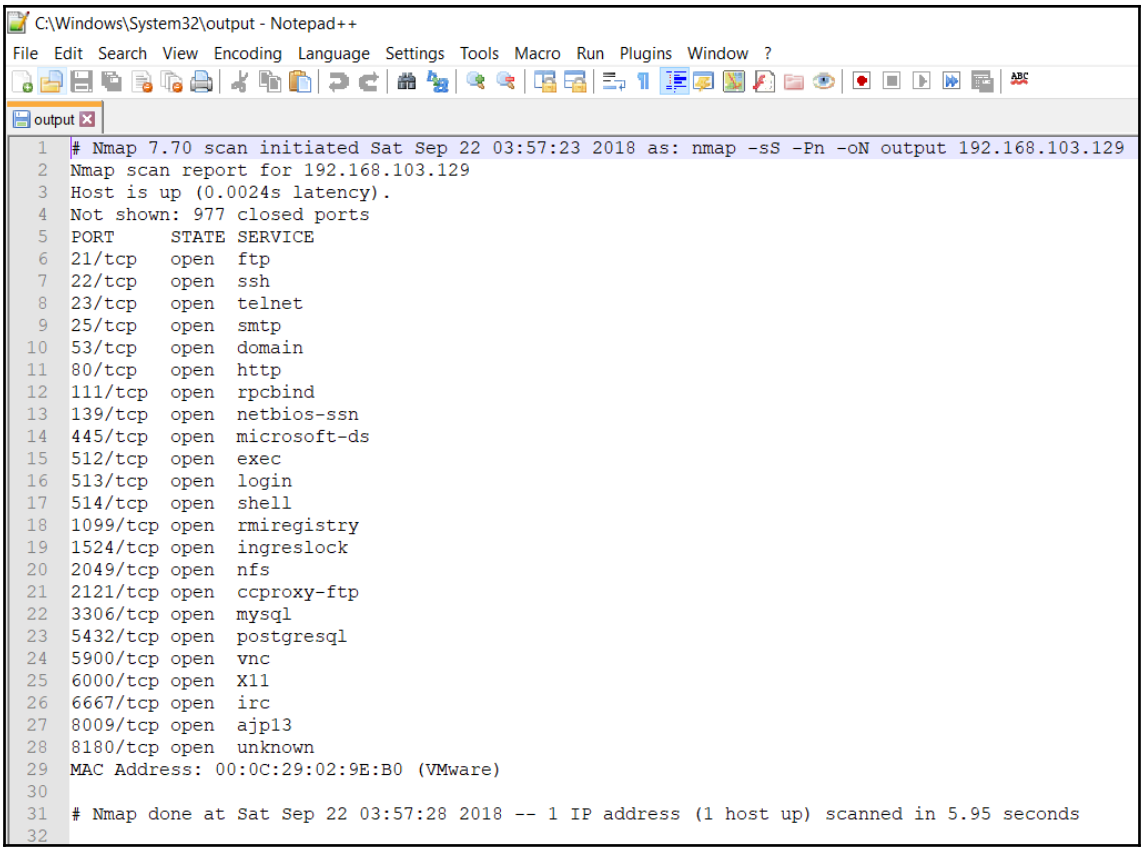

Metasploitable.nvram 04-09-2018 16:53 NVRAM File 9 KB
Metasploitable.vmdk 17-09-2018 13:48 VMware virtual dis... 18,81,024 KB
Metasploitable.vmsd 07-05-2010 14:46 VMSD File 0 KB
Metasploitable.vmx 17-09-2018 13:47 VMware virtual m... 3 KB
Metasploitable.vmxf 07-05-2010 14:46 VMXF File 1 KB


Metasploitable2-Linux - VMware Workstation 14 Player (Non-commercial use only)
Player
Starting up ...

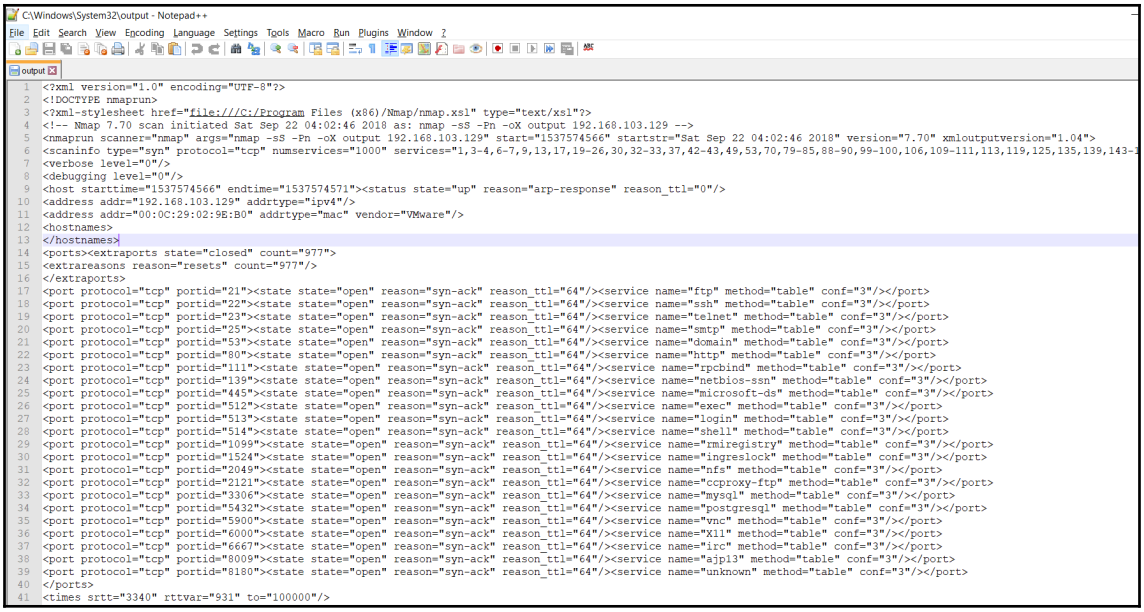

Metasploitable2-Linux - VMware Workstation 14 Player (Non-commercial use only)
Player
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Mon Sep 17 05:49:38 EDT 2018 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _

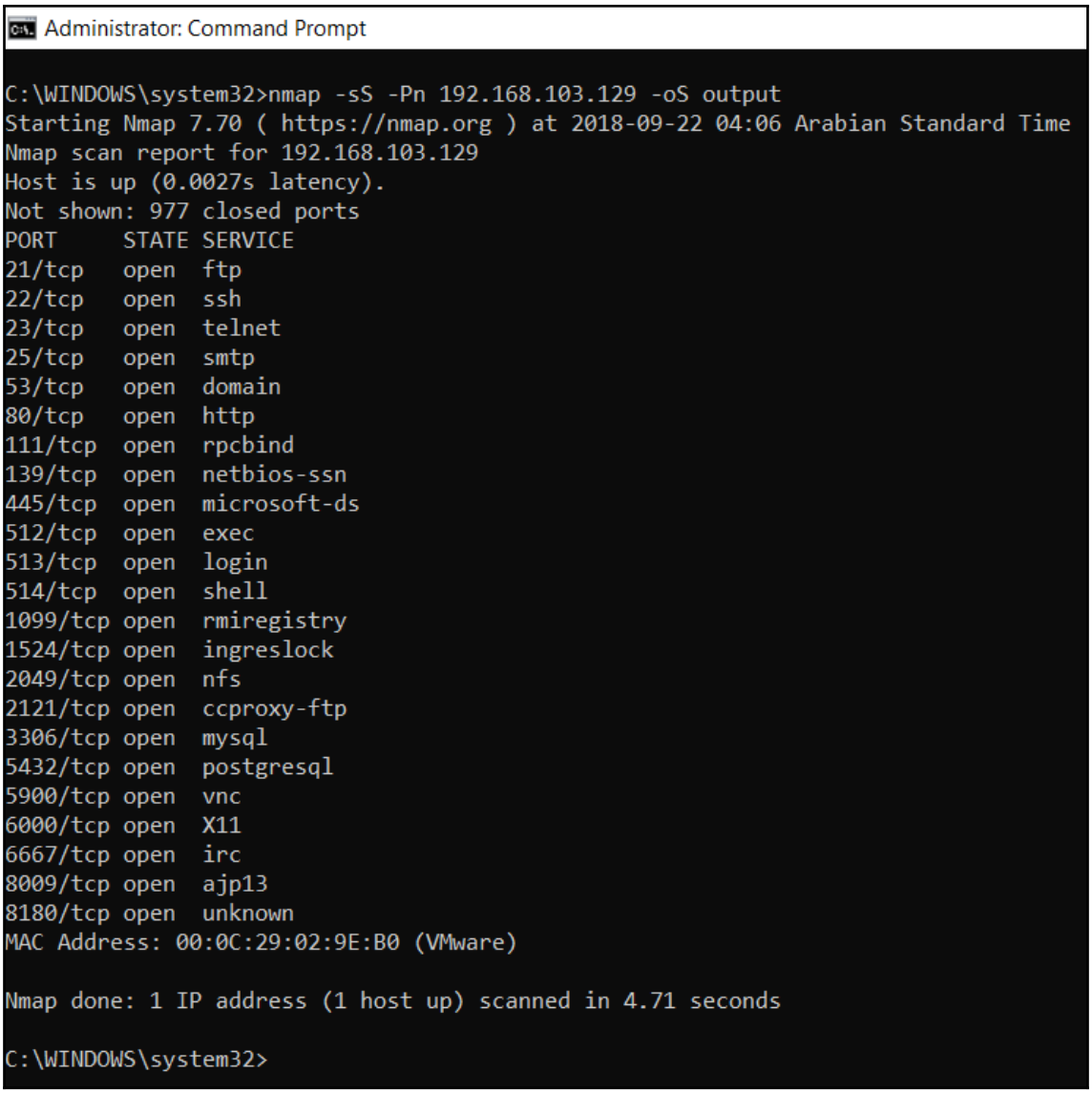
```
C:\WINDOWS\system32\cmd.exe

C:\>nmap -sS -Pn 192.168.103.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 03:52 Arabian Standard Time
Nmap scan report for 192.168.103.129
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:02:9E:B0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.81 seconds
```

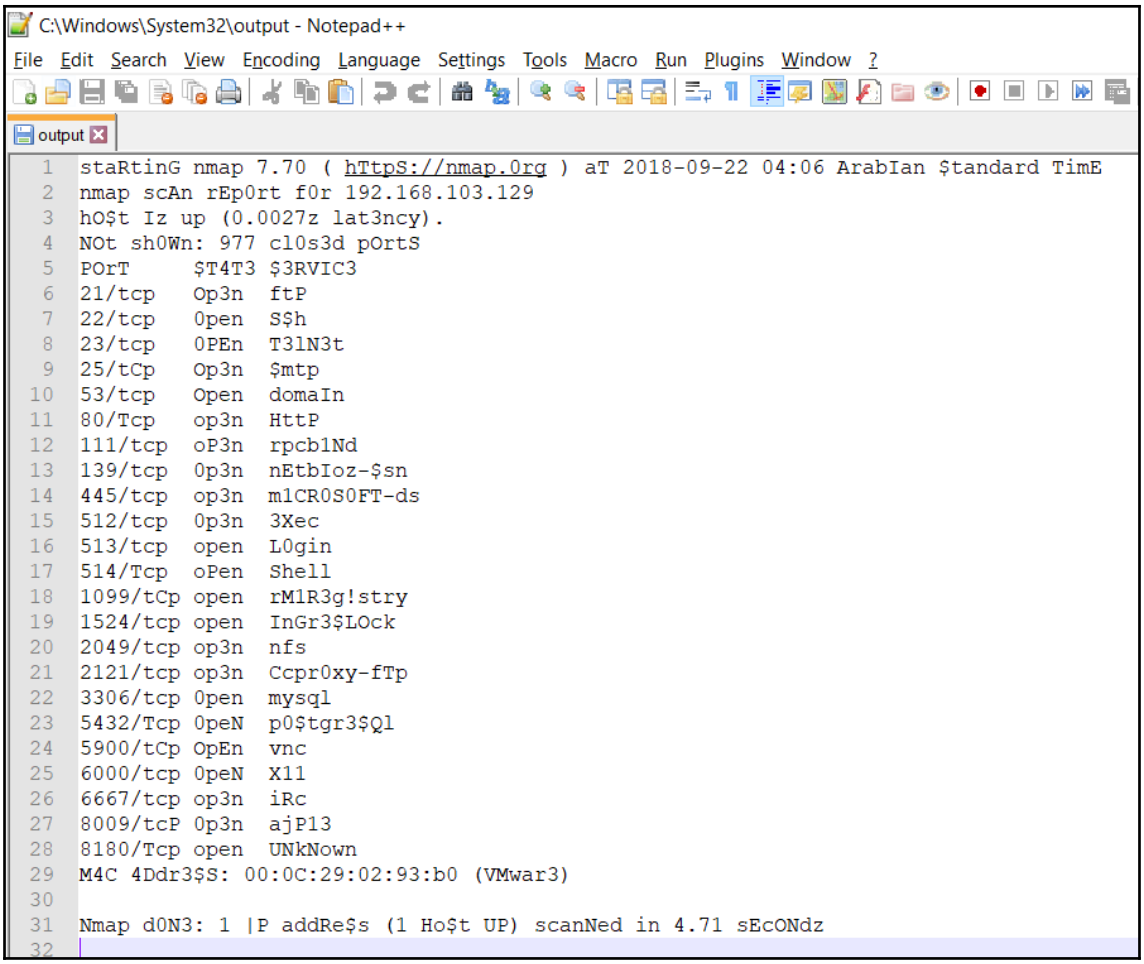

Administrator: Command Prompt
C:\WINDOWS\system32>nmap -sS -Pn 192.168.103.129 -oN output
Starting Nmap 7.70 (https://nmap.org) at 2018-09-22 03:57 Arabian Standard Time
Nmap scan report for 192.168.103.129
Host is up (0.0024s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:02:9E:B0 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds


C:\Windows\System32\output - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
output
Nmap 7.70 scan initiated Sat Sep 22 03:57:23 2018 as: nmap -sS -Pn -oN output 192.168.103.129
Nmap scan report for 192.168.103.129
Host is up (0.0024s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:02:9E:B0 (VMware)
Nmap done at Sat Sep 22 03:57:28 2018 -- 1 IP address (1 host up) scanned in 5.95 seconds

```
C:\WINDOWS\system32>nmap -sS -Pn 192.168.103.129 -oX output
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 04:02 Arabian Standard Time
Nmap scan report for 192.168.103.129
Host is up (0.0033s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:02:9E:B0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.49 seconds

C:\WINDOWS\system32>
```

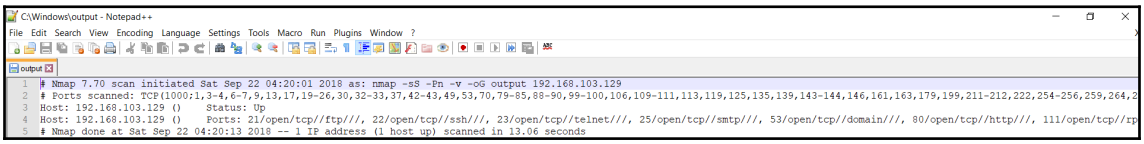

C:\Windows\System32\output - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
output
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///C:/Program Files (x86)/Nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.70 scan initiated Sat Sep 22 04:02:46 2018 as: nmap -sS -Pn -oX output 192.168.103.129 -->
<nmaprun scanner="nmap" args="nmap -sS -Pn -oX output 192.168.103.129" start="1537574566" startstr="Sat Sep 22 04:02:46 2018" version="7.70" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1537574566" endtime="1537574571"><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="192.168.103.129" addrtype="ipv4"/>
<address addr="00:0C:29:02:9E:B0" addrtype="mac" vendor="VMware"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="977">
<extrareasons reason="resets" count="977"/>
</extraports>
<port protocol="tcp" portid="21"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ftp" method="table" conf="3"/></port>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ssh" method="table" conf="3"/></port>
<port protocol="tcp" portid="23"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="telnet" method="table" conf="3"/></port>
<port protocol="tcp" portid="25"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="smtp" method="table" conf="3"/></port>
<port protocol="tcp" portid="53"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="domain" method="table" conf="3"/></port>
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" method="table" conf="3"/></port>
<port protocol="tcp" portid="111"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="rpcbind" method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="netbios-ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="microsoft-ds" method="table" conf="3"/></port>
<port protocol="tcp" portid="512"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="exec" method="table" conf="3"/></port>
<port protocol="tcp" portid="513"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="login" method="table" conf="3"/></port>
<port protocol="tcp" portid="514"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="shell" method="table" conf="3"/></port>
<port protocol="tcp" portid="1099"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="rmiregistry" method="table" conf="3"/></port>
<port protocol="tcp" portid="1524"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ingreslock" method="table" conf="3"/></port>
<port protocol="tcp" portid="2049"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="nfs" method="table" conf="3"/></port>
<port protocol="tcp" portid="2121"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ccproxy-ftp" method="table" conf="3"/></port>
<port protocol="tcp" portid="3306"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="mysql" method="table" conf="3"/></port>
<port protocol="tcp" portid="5432"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="postgresql" method="table" conf="3"/></port>
<port protocol="tcp" portid="5900"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="vnc" method="table" conf="3"/></port>
<port protocol="tcp" portid="6000"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="X11" method="table" conf="3"/></port>
<port protocol="tcp" portid="6667"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="irc" method="table" conf="3"/></port>
<port protocol="tcp" portid="8009"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ajp13" method="table" conf="3"/></port>
<port protocol="tcp" portid="8180"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="unknown" method="table" conf="3"/></port>
</ports>
<times srtt="3340" rttvar="931" to="100000"/>


Administrator: Command Prompt
C:\WINDOWS\system32>nmap -sS -Pn 192.168.103.129 -oS output
Starting Nmap 7.70 (https://nmap.org) at 2018-09-22 04:06 Arabian Standard Time
Nmap scan report for 192.168.103.129
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:02:9E:B0 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds
C:\WINDOWS\system32>

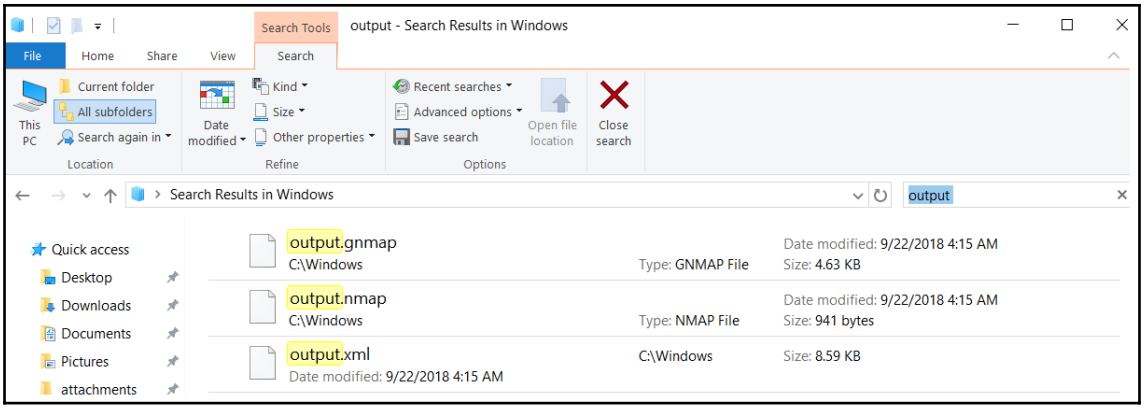

C:\Windows\System32\output - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
output
staRtinG nmap 7.70 (hTtpS://nmap.0rg) aT 2018-09-22 04:06 ArabIan $tandard TimE
nmap scAn rEp0rt f0r 192.168.103.129
hO$t Iz up (0.0027z lat3ncy).
NOt sh0Wn: 977 cl0s3d pOrtS
POrT $T4T3 $3RVIC3
21/tcp Op3n ftP
22/tcp 0pen S$h
23/tcp 0PEn T3lN3t
25/tCp Op3n $mtp
53/tcp Open domaIn
80/Tcp op3n HttP
111/tcp oP3n rpcb1Nd
139/tcp 0p3n nEtbIoz-$sn
445/tcp op3n m1CR0S0FT-ds
512/tcp 0p3n 3Xec
513/tcp open L0gin
514/Tcp oPen Shell
1099/tCp open rM1R3g!stry
1524/tcp open InGr3$LOck
2049/tcp op3n nfs
2121/tcp op3n Ccpr0xy-fTp
3306/tcp 0pen mysql
5432/Tcp 0peN p0$tgr3$Ql
5900/tCp OpEn vnc
6000/tcp 0peN X11
6667/tcp op3n iRc
8009/tcP 0p3n ajP13
8180/Tcp open UNkNown
M4C 4Ddr3$S: 00:0C:29:02:93:b0 (VMwar3)
Nmap d0N3: 1 |P addRe$s (1 Ho$t UP) scanNed in 4.71 sEcONdz

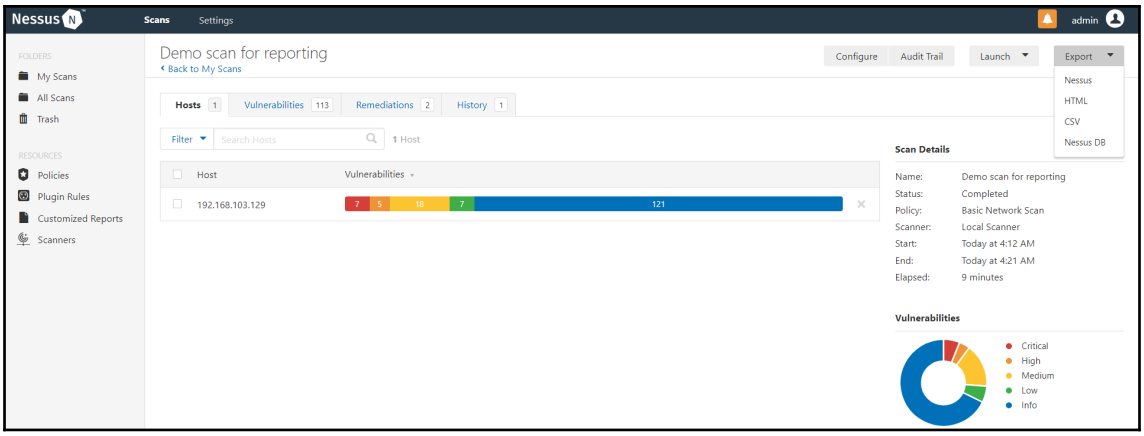
Administrator: Command Prompt

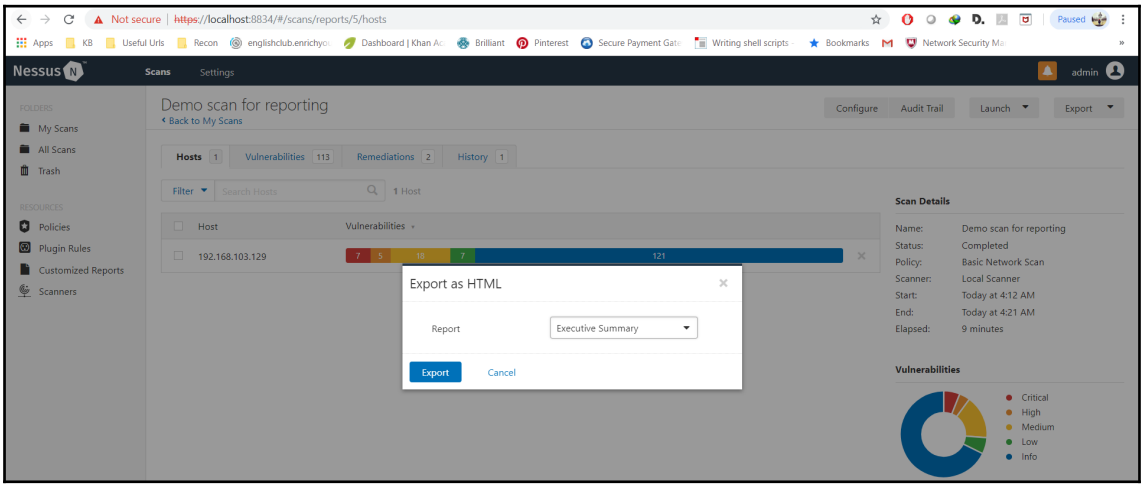
```
C:\Windows>nmap -sS -Pn -v 192.168.103.129 -oG output
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 04:20 Arabian Standard Time
Initiating ARP Ping Scan at 04:20
Scanning 192.168.103.129 [1 port]
Completed ARP Ping Scan at 04:20, 1.98s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:20
Completed Parallel DNS resolution of 1 host. at 04:20, 2.51s elapsed
Initiating SYN Stealth Scan at 04:20
Scanning 192.168.103.129 [1000 ports]
Discovered open port 139/tcp on 192.168.103.129
Discovered open port 53/tcp on 192.168.103.129
Discovered open port 25/tcp on 192.168.103.129
Discovered open port 5900/tcp on 192.168.103.129
Discovered open port 21/tcp on 192.168.103.129
Discovered open port 80/tcp on 192.168.103.129
Discovered open port 22/tcp on 192.168.103.129
Discovered open port 3306/tcp on 192.168.103.129
Discovered open port 111/tcp on 192.168.103.129
Discovered open port 23/tcp on 192.168.103.129
Discovered open port 445/tcp on 192.168.103.129
Discovered open port 8009/tcp on 192.168.103.129
Discovered open port 1099/tcp on 192.168.103.129
Discovered open port 512/tcp on 192.168.103.129
Discovered open port 6667/tcp on 192.168.103.129
Discovered open port 6000/tcp on 192.168.103.129
Discovered open port 1524/tcp on 192.168.103.129
Discovered open port 8180/tcp on 192.168.103.129
Discovered open port 5432/tcp on 192.168.103.129
Discovered open port 514/tcp on 192.168.103.129
Discovered open port 2121/tcp on 192.168.103.129
Discovered open port 2049/tcp on 192.168.103.129
Discovered open port 513/tcp on 192.168.103.129
Completed SYN Stealth Scan at 04:20, 0.36s elapsed (1000 total ports)
```

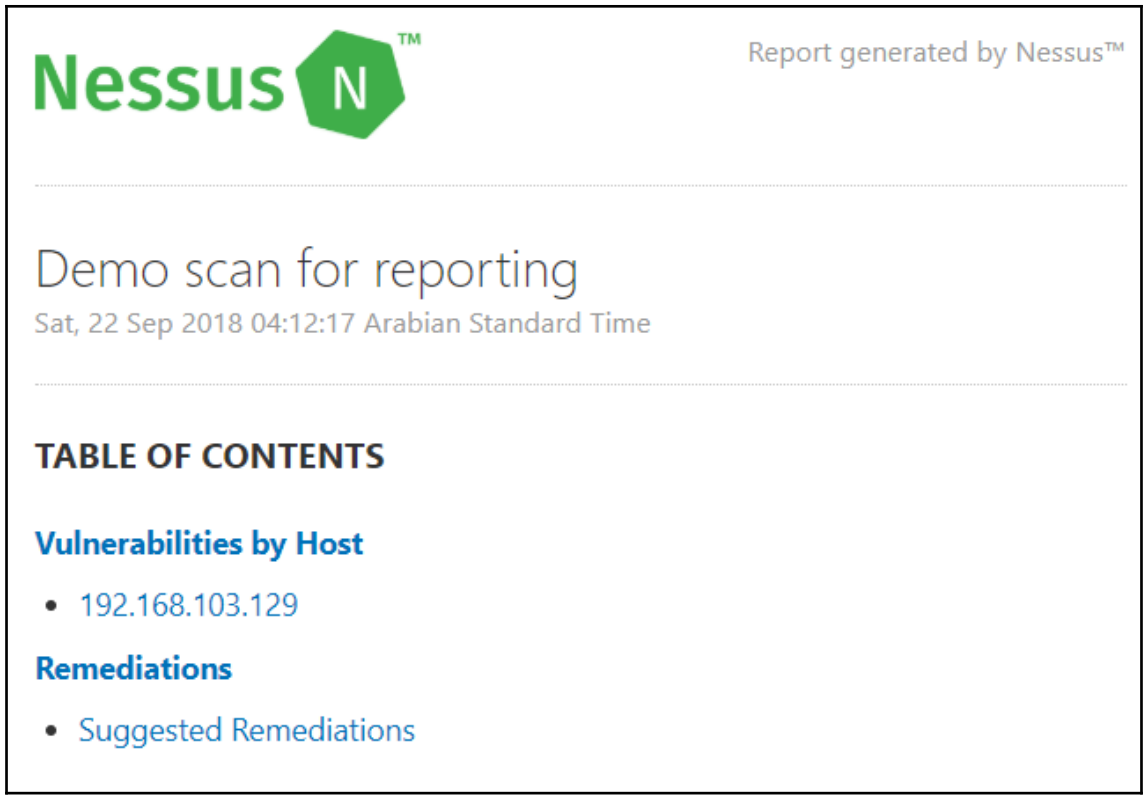


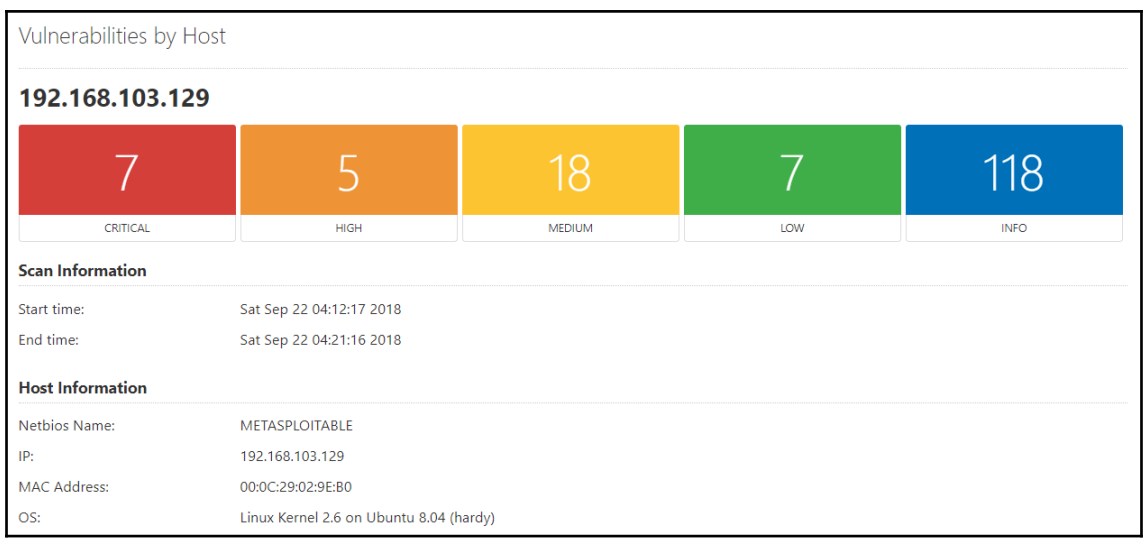
```
C:\Windows>nmap -sS -Pn -v 192.168.103.129 -oA output
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 04:15 Arabian Standard Time
Initiating ARP Ping Scan at 04:15
Scanning 192.168.103.129 [1 port]
Completed ARP Ping Scan at 04:15, 0.98s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:15
Completed Parallel DNS resolution of 1 host. at 04:15, 0.01s elapsed
Initiating SYN Stealth Scan at 04:15
Scanning 192.168.103.129 [1000 ports]
Discovered open port 139/tcp on 192.168.103.129
Discovered open port 445/tcp on 192.168.103.129
Discovered open port 5900/tcp on 192.168.103.129
Discovered open port 22/tcp on 192.168.103.129
Discovered open port 21/tcp on 192.168.103.129
Discovered open port 3306/tcp on 192.168.103.129
Discovered open port 80/tcp on 192.168.103.129
Discovered open port 23/tcp on 192.168.103.129
Discovered open port 111/tcp on 192.168.103.129
Discovered open port 25/tcp on 192.168.103.129
Discovered open port 53/tcp on 192.168.103.129
Discovered open port 513/tcp on 192.168.103.129
Discovered open port 1099/tcp on 192.168.103.129
Discovered open port 1524/tcp on 192.168.103.129
Discovered open port 2121/tcp on 192.168.103.129
Discovered open port 6667/tcp on 192.168.103.129
Discovered open port 8180/tcp on 192.168.103.129
Discovered open port 512/tcp on 192.168.103.129
Discovered open port 2049/tcp on 192.168.103.129
Discovered open port 514/tcp on 192.168.103.129
Discovered open port 8009/tcp on 192.168.103.129
Discovered open port 5432/tcp on 192.168.103.129
Discovered open port 6000/tcp on 192.168.103.129
Completed SYN Stealth Scan at 04:15, 0.14s elapsed (1000 total ports)
Nmap scan report for 192.168.103.129
Host is up (0.0026s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
```


output - Search Results in Windows
Search Tools
File
Home
Share
View
Search
Current folder
All subfolders
Search again in
This PC
Location
Date modified
Kind
Size
Other properties
Refine
Recent searches
Advanced options
Save search
Open file location
Close search
Options
Search Results in Windows
output
Quick access
Desktop
Downloads
Documents
Pictures
attachments
output.gnmap
C:\Windows
Type: GNMAP File
Date modified: 9/22/2018 4:15 AM
Size: 4.63 KB
output.nmap
C:\Windows
Type: NMAP File
Date modified: 9/22/2018 4:15 AM
Size: 941 bytes
output.xml
Date modified: 9/22/2018 4:15 AM
C:\Windows
Size: 8.59 KB


Nessus
Scans
Settings
admin
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Nessus
HTML
CSV
Nessus DB
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
7 5 18 7 121
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
My Scans
All Scans
Trash
Policies
Plugin Rules
Customized Reports
Scanners


Not secure
https://localhost:8834/#/scans/reports/5/hosts
Nessus
Scans
Settings
admin
Demo scan for reporting
Export as HTML
Report
Executive Summary
Export
Cancel
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
192.168.103.129
Scan Details
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus™
Report generated by Nessus™
Demo scan for reporting
Sat, 22 Sep 2018 04:12:17 Arabian Standard Time
TABLE OF CONTENTS
Vulnerabilities by Host
192.168.103.129
Remediations
Suggested Remediations


Vulnerabilities by Host
192.168.103.129
7
CRITICAL
5
HIGH
18
MEDIUM
7
LOW
118
INFO
Scan Information
Start time: Sat Sep 22 04:12:17 2018
End time: Sat Sep 22 04:21:16 2018
Host Information
Netbios Name: METASPLOITABLE
IP: 192.168.103.129
MAC Address: 00:0C:29:02:9E:B0
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	CWE:200

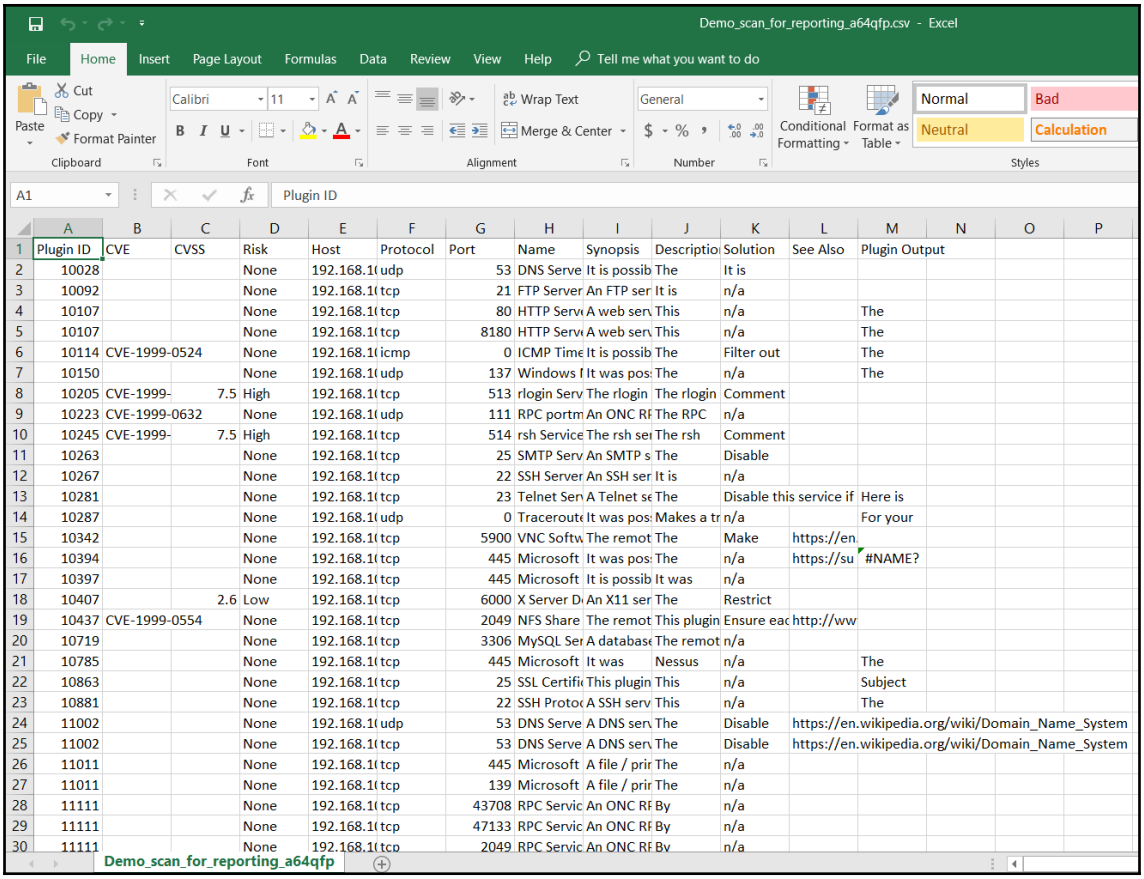
Plugin Information:

Published: 1999/08/01, Modified: 2018/08/10

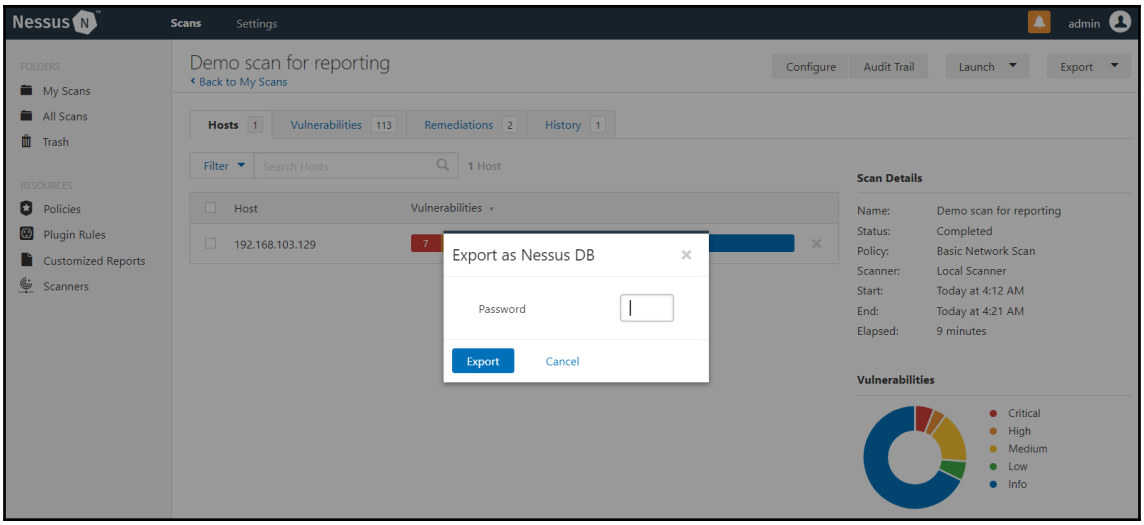
Plugin Output

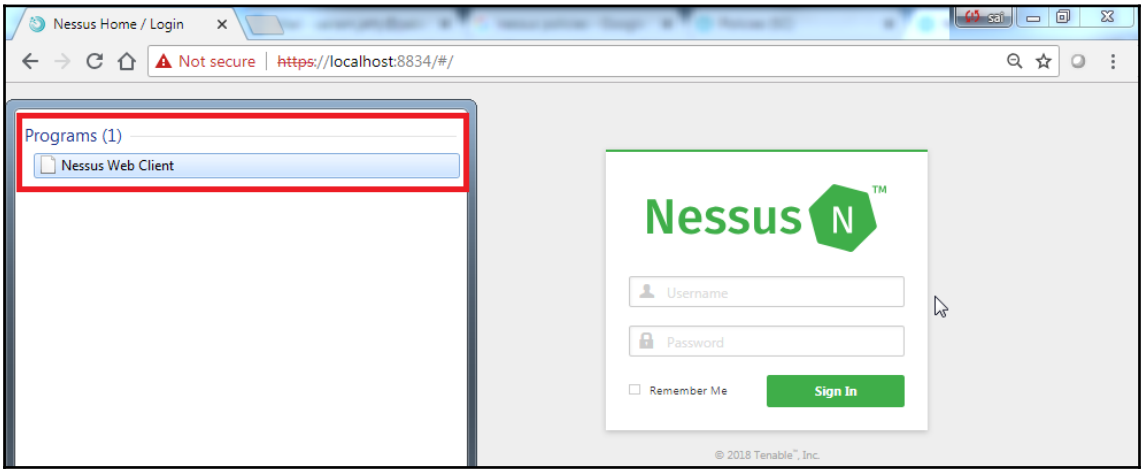
icmp/0

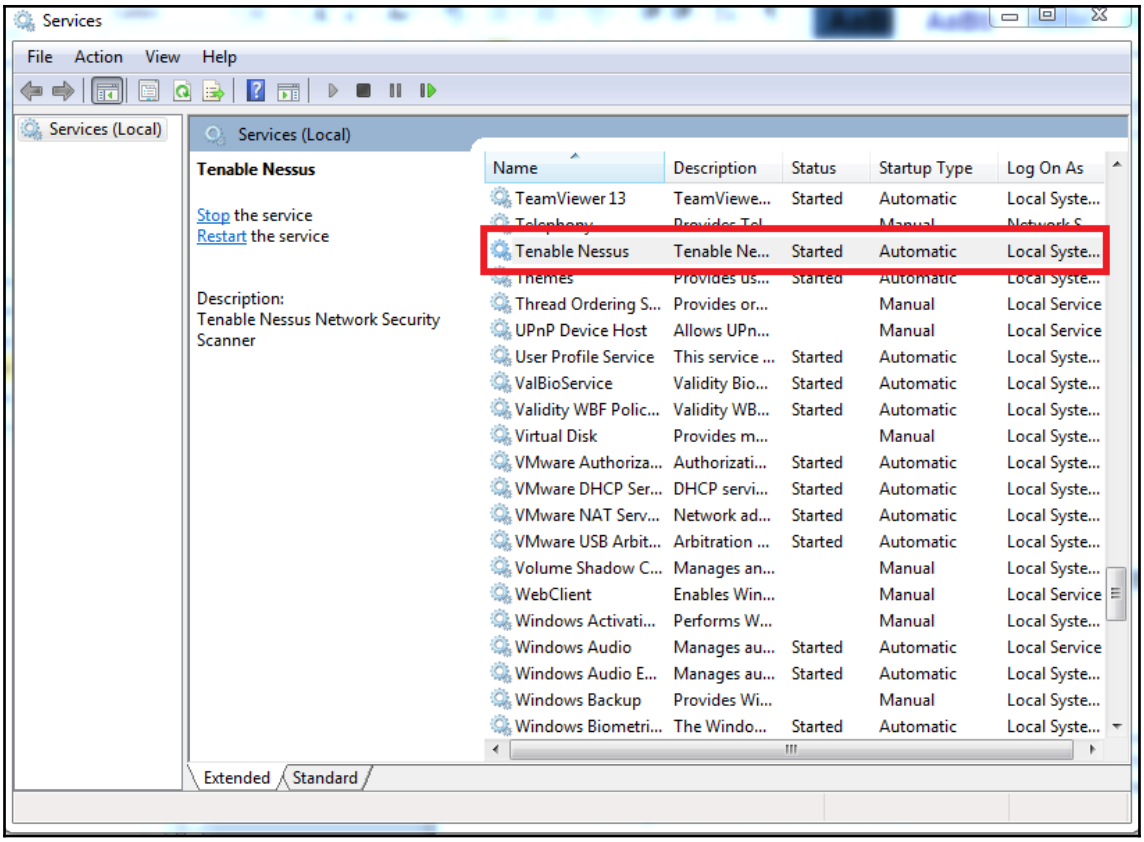
```
The difference between the local and remote clocks is -2 seconds.
```

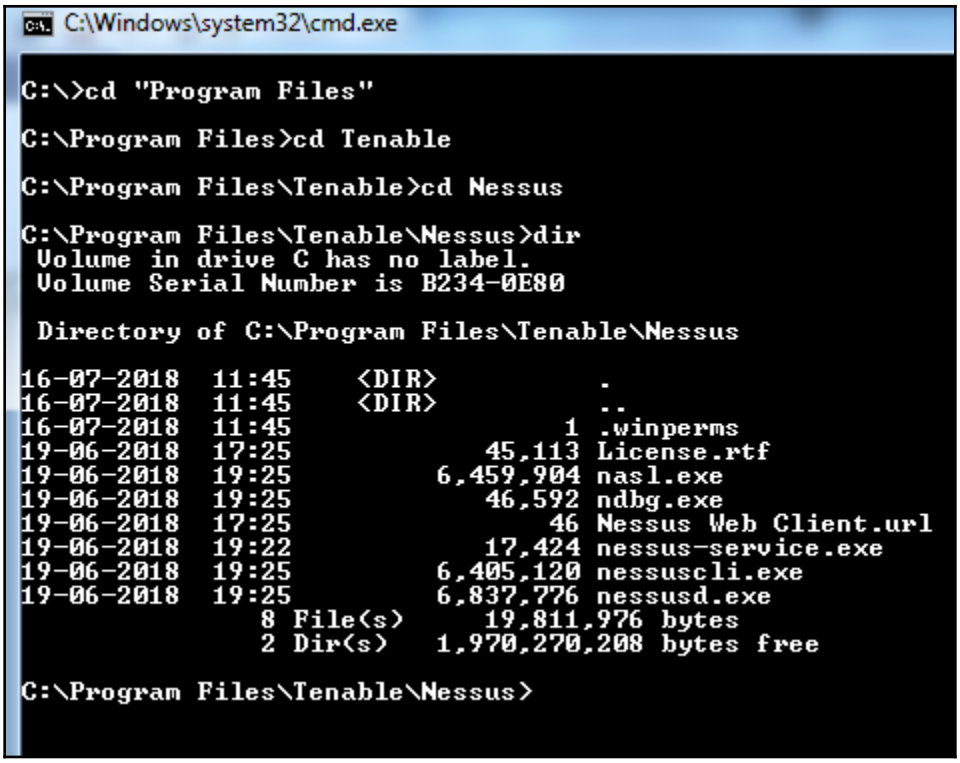


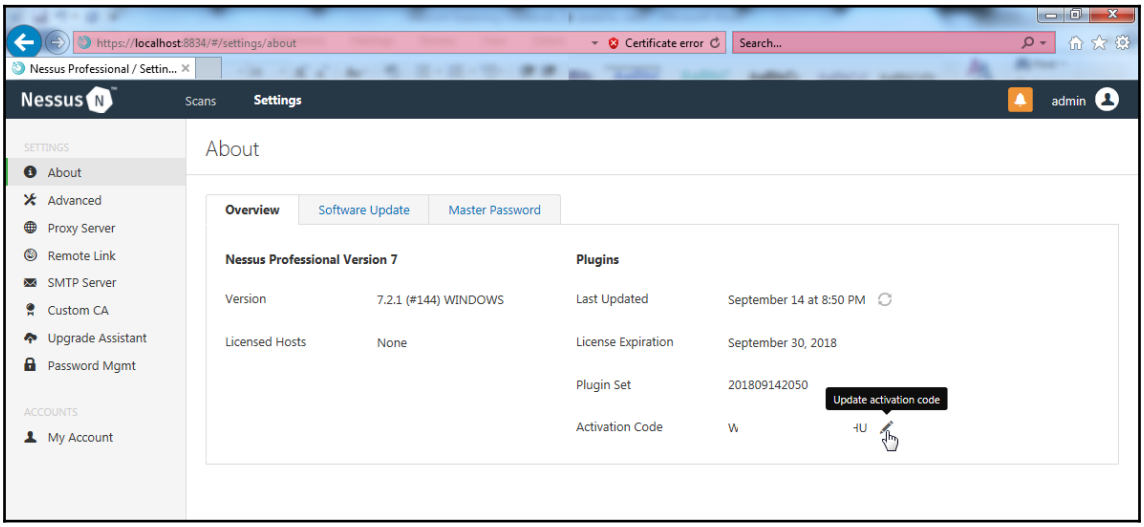
Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
10028			None	192.168.1(	udp	53	DNS Serve	It is possib	The	It is		
10092			None	192.168.1(	tcp	21	FTP Server	An FTP ser	It is	n/a		
10107			None	192.168.1(	tcp	80	HTTP Serv	A web ser	This	n/a		The
10107			None	192.168.1(	tcp	8180	HTTP Serv	A web ser	This	n/a		The
10114	CVE-1999-0524		None	192.168.1(	icmp	0	ICMP Time	It is possib	The	Filter out		The
10150			None	192.168.1(	udp	137	Windows I	It was pos	The	n/a		The
10205	CVE-1999-	7.5	High	192.168.1(	tcp	513	rlogin Serv	The rlogin	The rlogin	Comment		
10223	CVE-1999-0632		None	192.168.1(	udp	111	RPC portm	An ONC RI	The RPC	n/a		
10245	CVE-1999-	7.5	High	192.168.1(	tcp	514	rsh Service	The rsh se	The rsh	Comment		
10263			None	192.168.1(	tcp	25	SMTP Serv	An SMTP s	The	Disable		
10267			None	192.168.1(	tcp	22	SSH Server	An SSH ser	It is	n/a		
10281			None	192.168.1(	tcp	23	Telnet Ser	A Telnet se	The	Disable this service if		Here is
10287			None	192.168.1(	udp	0	Traceroute	It was pos	Makes a tr	n/a		For your
10342			None	192.168.1(	tcp	5900	VNC Softw	The remot	The	Make	https://en	
10394			None	192.168.1(	tcp	445	Microsoft	It was pos	The	n/a	https://su	#NAME?
10397			None	192.168.1(	tcp	445	Microsoft	It is possib	It was	n/a		
10407		2.6	Low	192.168.1(	tcp	6000	X Server D	An X11 ser	The	Restrict		
10437	CVE-1999-0554		None	192.168.1(	tcp	2049	NFS Share	The remot	This plugin	Ensure eac	http://ww	
10719			None	192.168.1(	tcp	3306	MySQL Ser	A database	The remot	n/a		
10785			None	192.168.1(	tcp	445	Microsoft	It was	Nessus	n/a		The
10863			None	192.168.1(	tcp	25	SSL Certifi	This plugin	This	n/a		Subject
10881			None	192.168.1(	tcp	22	SSH Protoc	A SSH serv	This	n/a		The
11002			None	192.168.1(	udp	53	DNS Serve	A DNS ser	The	Disable	https://en.wikipedia.org/wiki/Domain_Name_System	
11002			None	192.168.1(	tcp	53	DNS Serve	A DNS ser	The	Disable	https://en.wikipedia.org/wiki/Domain_Name_System	
11011			None	192.168.1(	tcp	445	Microsoft	A file / prir	The	n/a		
11011			None	192.168.1(	tcp	139	Microsoft	A file / prir	The	n/a		
11111			None	192.168.1(	tcp	43708	RPC Servic	An ONC RI	By	n/a		
11111			None	192.168.1(	tcp	47133	RPC Servic	An ONC RI	By	n/a		
11111			None	192.168.1(	tcp	2049	RPC Servic	An ONC RI	By	n/a		

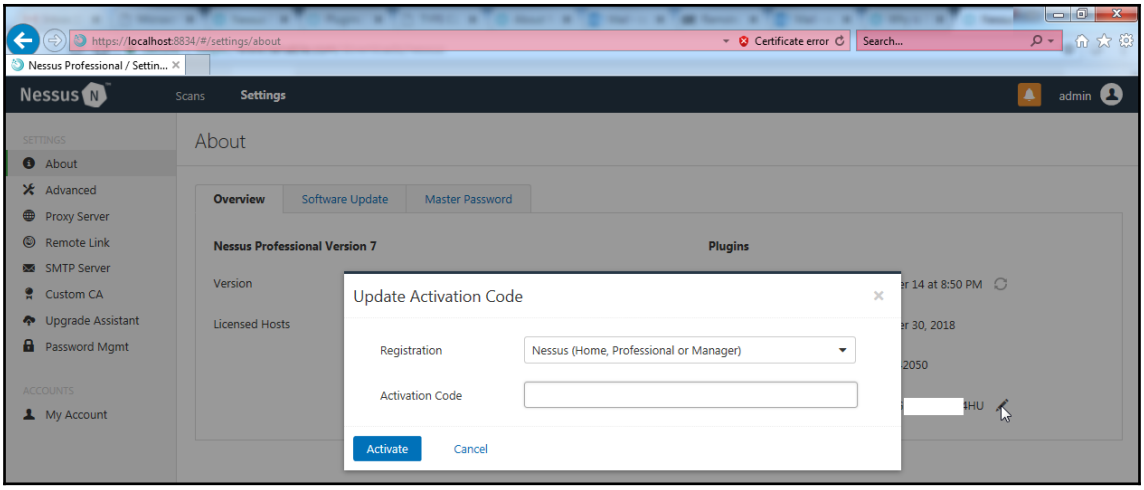

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
Export as Nessus DB
Password
Export
Cancel
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

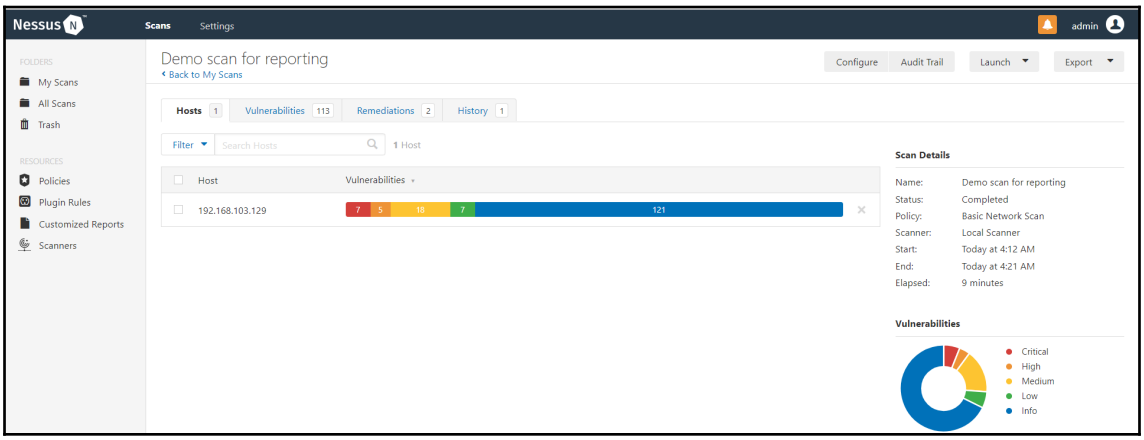

Nessus Home / Login
Not secure
https://localhost:8834/#/
Programs (1)
Nessus Web Client
Nessus
Username
Password
Remember Me
Sign In
© 2018 Tenable™, Inc.

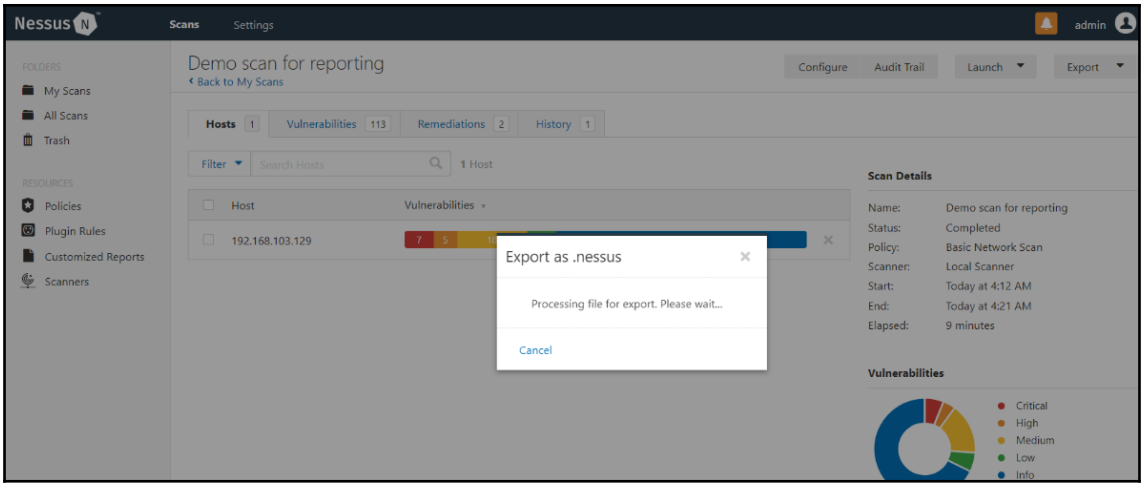

Services
File Action View Help
Services (Local)
Services (Local)
Tenable Nessus
Stop the service
Restart the service
Description:
Tenable Nessus Network Security Scanner
Name
Description
Status
Startup Type
Log On As
TeamViewer 13
TeamViewe...
Started
Automatic
Local Syste...
Tenable Nessus
Tenable Ne...
Started
Automatic
Local Syste...
Thread Ordering S...
Provides or...
Manual
Local Service
UPnP Device Host
Allows UPn...
Manual
Local Service
User Profile Service
This service ...
Started
Automatic
Local Syste...
ValBioService
Validity Bio...
Started
Automatic
Local Syste...
Validity WBF Polic...
Validity WB...
Started
Automatic
Local Syste...
Virtual Disk
Provides m...
Manual
Local Syste...
VMware Authoriza...
Authorizati...
Started
Automatic
Local Syste...
VMware DHCP Ser...
DHCP servi...
Started
Automatic
Local Syste...
VMware NAT Serv...
Network ad...
Started
Automatic
Local Syste...
VMware USB Arbit...
Arbitration ...
Started
Automatic
Local Syste...
Volume Shadow C...
Manages an...
Manual
Local Syste...
WebClient
Enables Win...
Manual
Local Service
Windows Activati...
Performs W...
Manual
Local Syste...
Windows Audio
Manages au...
Started
Automatic
Local Service
Windows Audio E...
Manages au...
Started
Automatic
Local Syste...
Windows Backup
Provides Wi...
Manual
Local Syste...
Windows Biometri...
The Windo...
Started
Automatic
Local Syste...
Extended
Standard

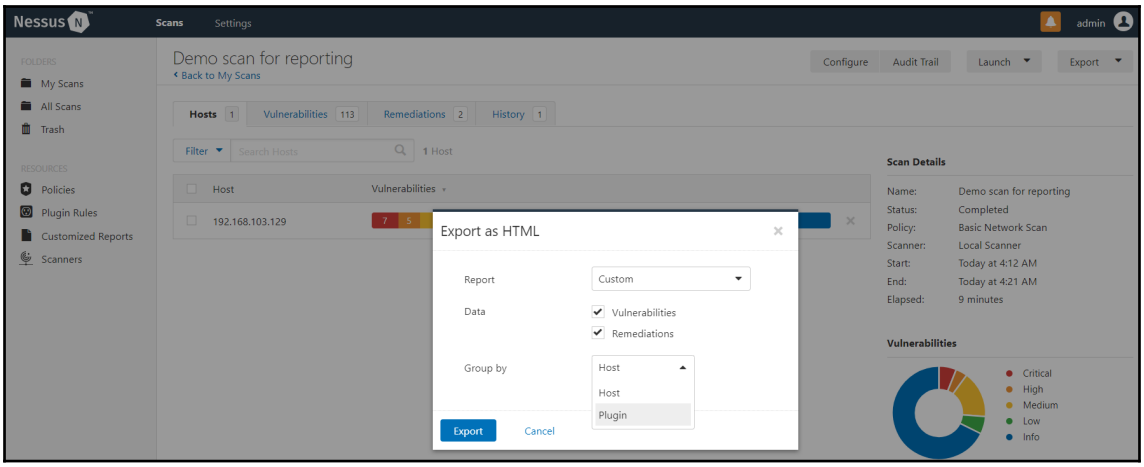

C:\Windows\system32\cmd.exe
C:\>cd "Program Files"
C:\Program Files>cd Tenable
C:\Program Files\Tenable>cd Nessus
C:\Program Files\Tenable\Nessus>dir
Volume in drive C has no label.
Volume Serial Number is B234-0E80
Directory of C:\Program Files\Tenable\Nessus
16-07-2018 11:45 <DIR> .
16-07-2018 11:45 <DIR> ..
16-07-2018 11:45 1 .winperms
19-06-2018 17:25 45,113 License.rtf
19-06-2018 19:25 6,459,904 nasl.exe
19-06-2018 19:25 46,592 ndbg.exe
19-06-2018 17:25 46 Nessus Web Client.url
19-06-2018 19:22 17,424 nessus-service.exe
19-06-2018 19:25 6,405,120 nessuscli.exe
19-06-2018 19:25 6,837,776 nessusd.exe
8 File(s) 19,811,976 bytes
2 Dir(s) 1,970,270,208 bytes free
C:\Program Files\Tenable\Nessus>

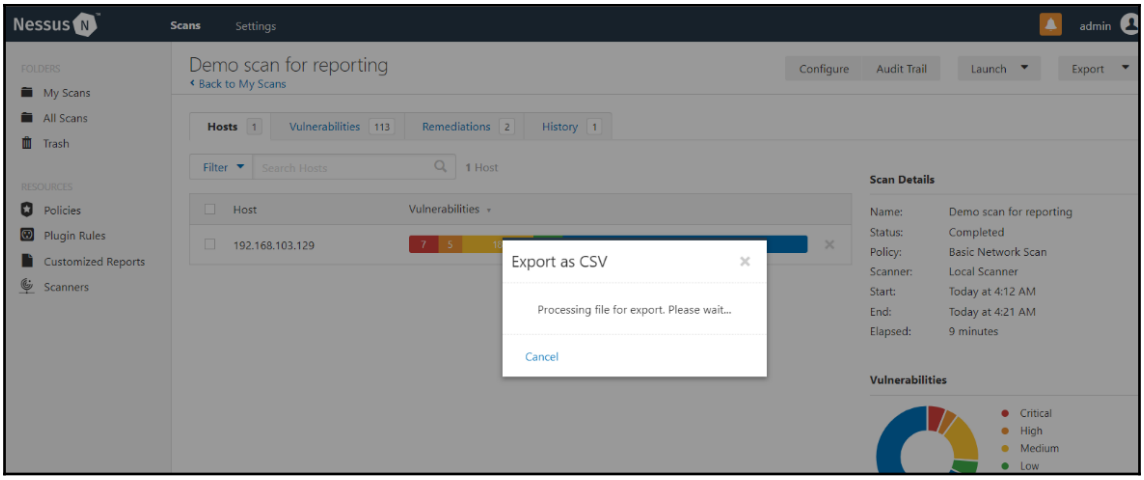

https://localhost:8834/#/settings/about
Certificate error
Search...
Nessus Professional / Settin...
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
ACCOUNTS
My Account
About
Overview
Software Update
Master Password
Nessus Professional Version 7
Version
7.2.1 (#144) WINDOWS
Licensed Hosts
None
Plugins
Last Updated
September 14 at 8:50 PM
License Expiration
September 30, 2018
Plugin Set
201809142050
Activation Code
Update activation code

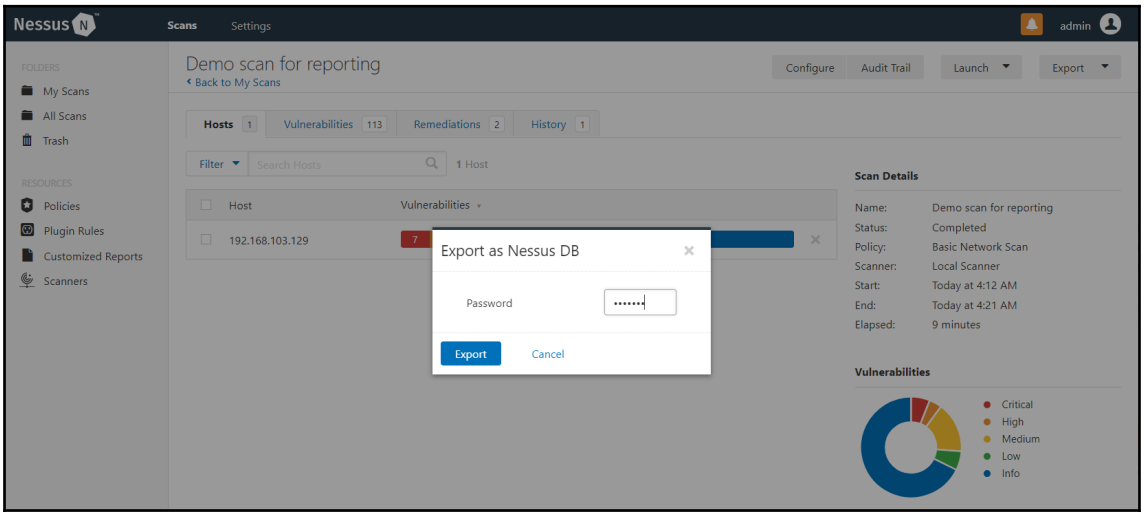

https://localhost:8834/#/settings/about
Certificate error
Search...
Nessus Professional / Settin...
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
ACCOUNTS
My Account
About
Overview
Software Update
Master Password
Nessus Professional Version 7
Plugins
Version
Licensed Hosts
Update Activation Code
Registration
Nessus (Home, Professional or Manager)
Activation Code
Activate
Cancel


Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
7
5
18
7
121
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

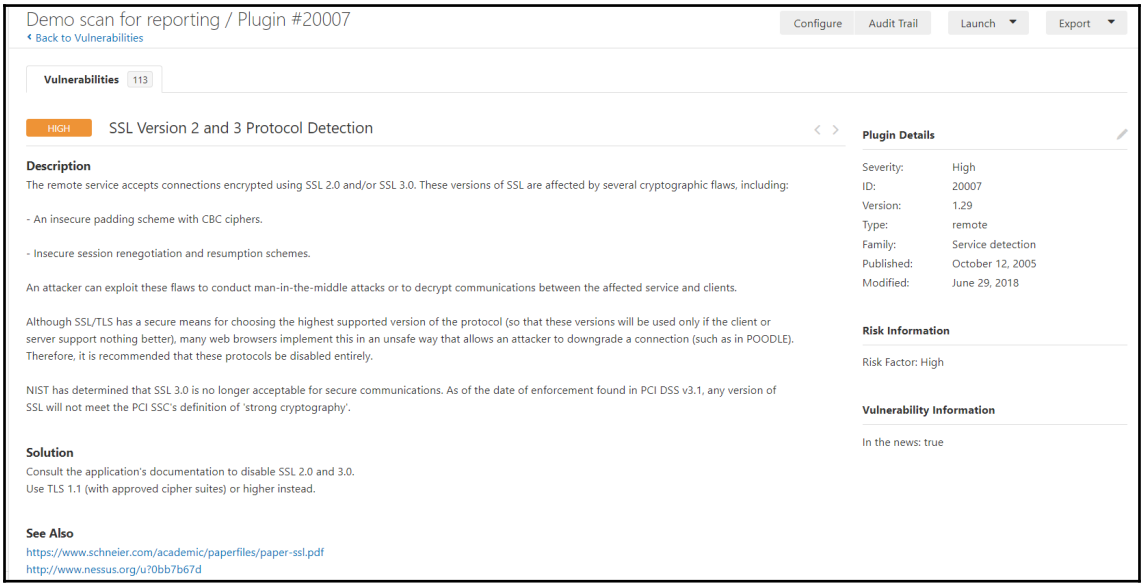

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
Export as .nessus
Processing file for export. Please wait...
Cancel
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

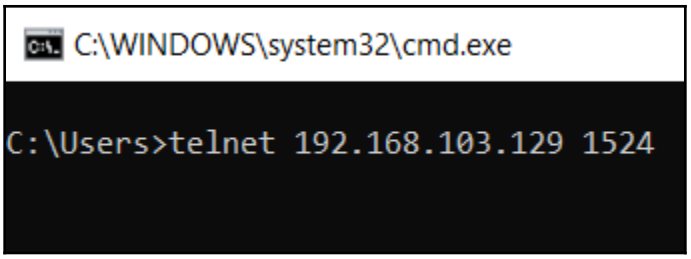

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
Export as HTML
Report
Custom
Data
Vulnerabilities
Remediations
Group by
Host
Host
Plugin
Export
Cancel
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

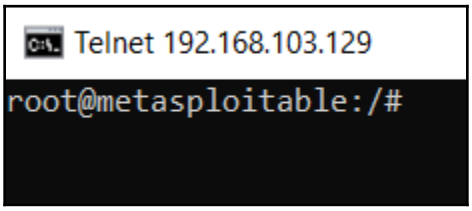

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
Export as CSV
Processing file for export. Please wait...
Cancel
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low


Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo scan for reporting
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 113
Remediations 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.103.129
Export as Nessus DB
Password
Export
Cancel
Scan Details
Name: Demo scan for reporting
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:12 AM
End: Today at 4:21 AM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Demo scan for reporting / Plugin #51988
Back to Vulnerabilities
Configure
Audit Trail
Launch
Export
Vulnerabilities 113
CRITICAL
Bind Shell Backdoor Detection
Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.
Output
Nessus was able to execute the command "id" using the following request :
This produced the following truncated output (limited to 10 lines) :
snip
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
snip
Port
Hosts
1524 / tcp / wild_shell
192.168.103.129
Plugin Details
Severity: Critical
ID: 51988
Version: 1.8
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: May 16, 2018
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C


Demo scan for reporting / Plugin #20007
Back to Vulnerabilities
Configure
Audit Trail
Launch
Export
Vulnerabilities 113
HIGH
SSL Version 2 and 3 Protocol Detection
Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.
Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.
See Also
https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?0bb7b67d
Plugin Details
Severity: High
ID: 20007
Version: 1.29
Type: remote
Family: Service detection
Published: October 12, 2005
Modified: June 29, 2018
Risk Information
Risk Factor: High
Vulnerability Information
In the news: true

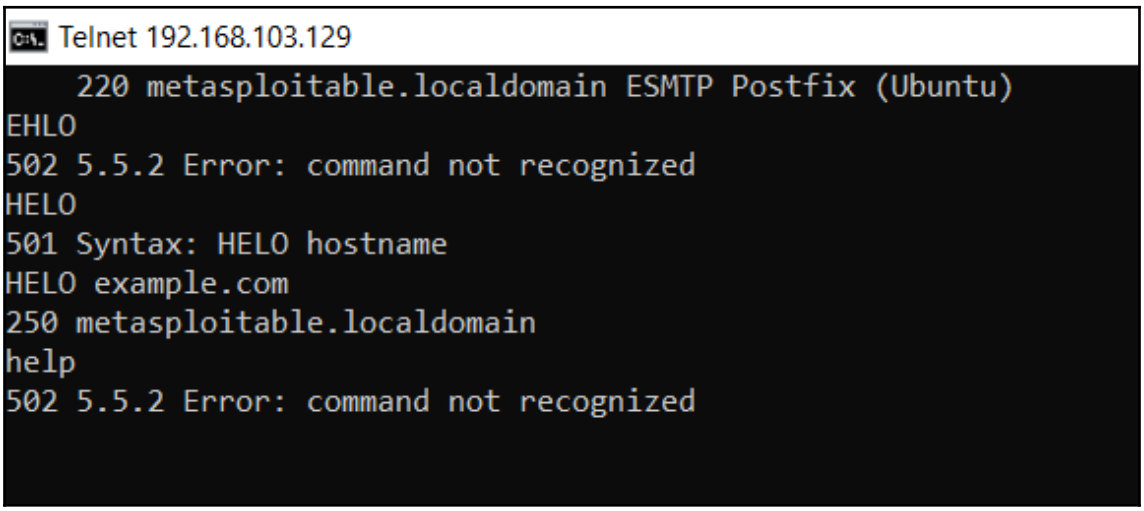





```
Telnet 192.168.103.129
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
                                    root@metasploitable:/# root@metasploitable:/#
```

```
C:\Windows>nmap -sV -script ssl-poodle -p 25 192.168.103.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 07:27 Arabian Standard Time
Nmap scan report for 192.168.103.129
Host is up (0.00s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
MAC Address: 00:0C:29:02:9E:B0 (VMware)
Service Info: Host:  metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.36 seconds
```

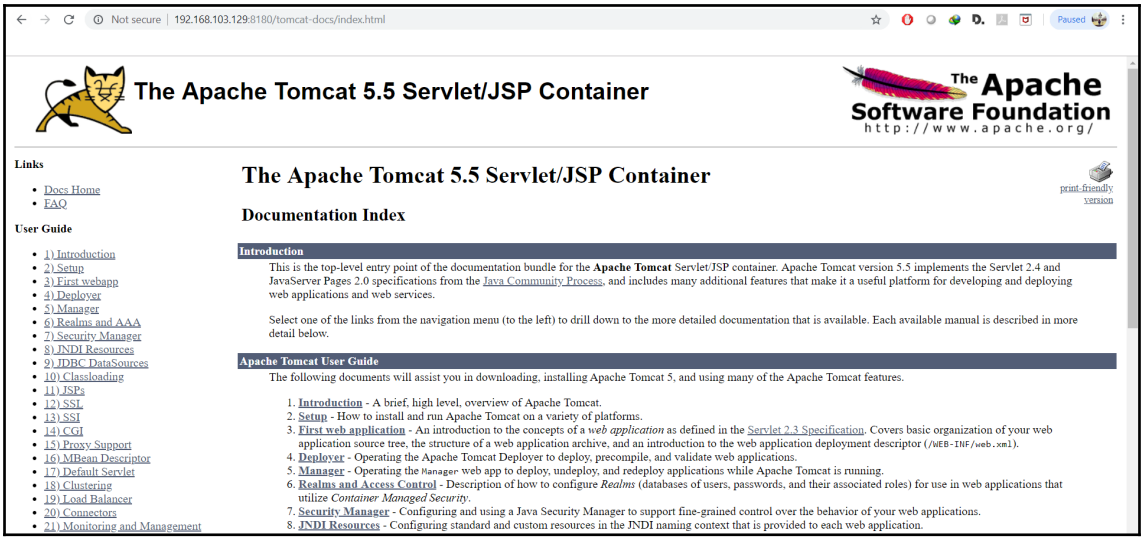
```
C:\Windows>nmap -script=ssl-enum-ciphers -p 25 192.168.103.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 07:33 Arabian Standard Time
Nmap scan report for 192.168.103.129
Host is up (0.00013s latency).

PORT   STATE SERVICE
25/tcp open  smtp
MAC Address: 00:0C:29:02:9E:B0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 50.98 seconds

C:\Windows>
```



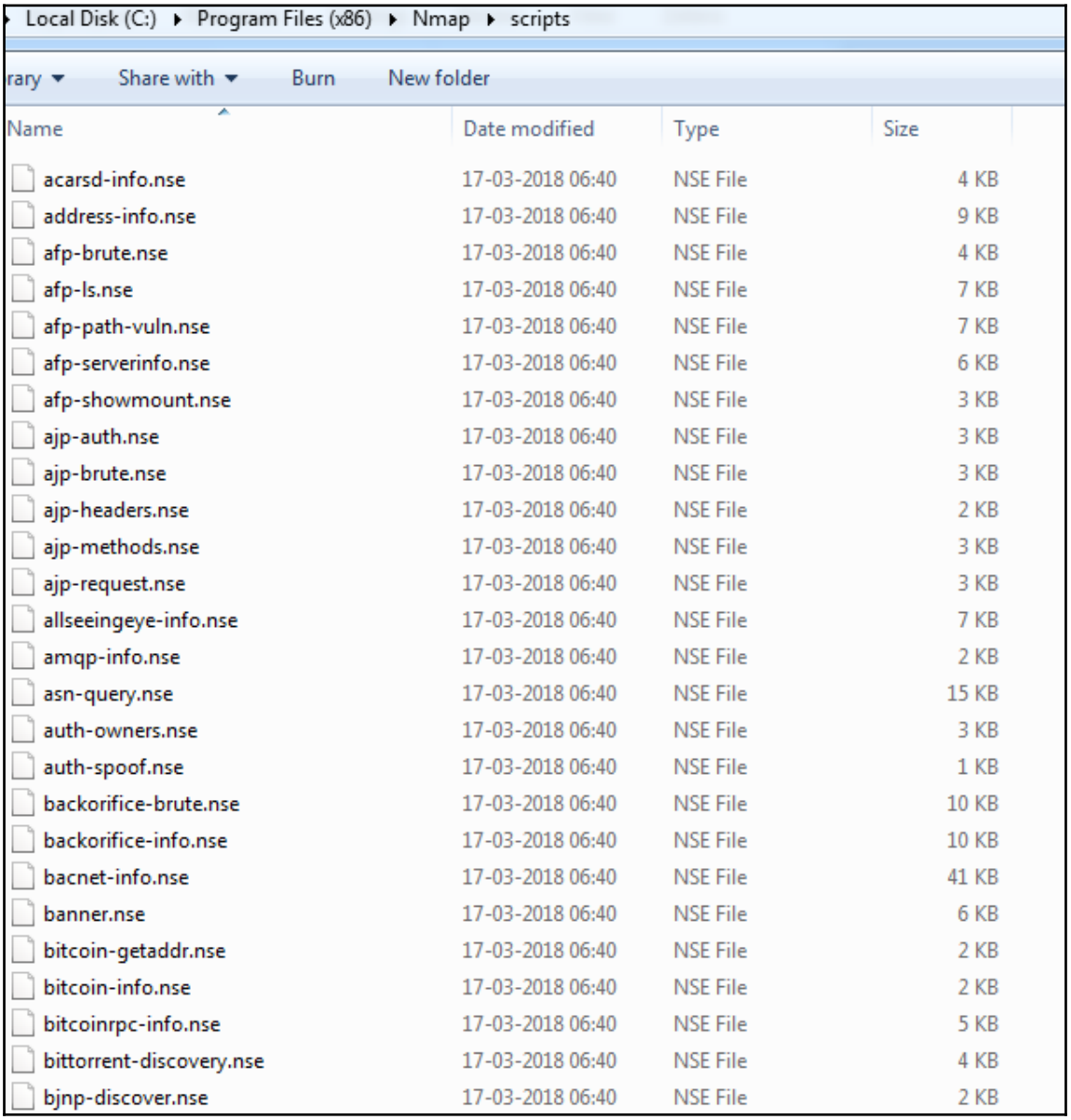
Output

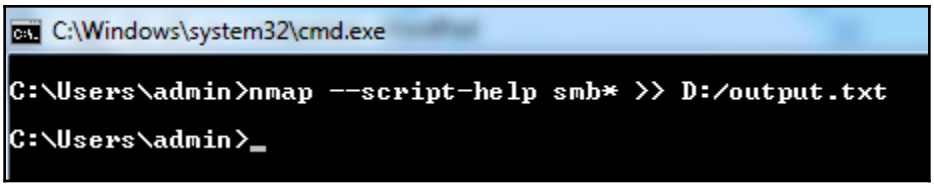
```
The following default files were found :

/tomcat-docs/index.html
/nessus-check/default-404-error-page.html
```

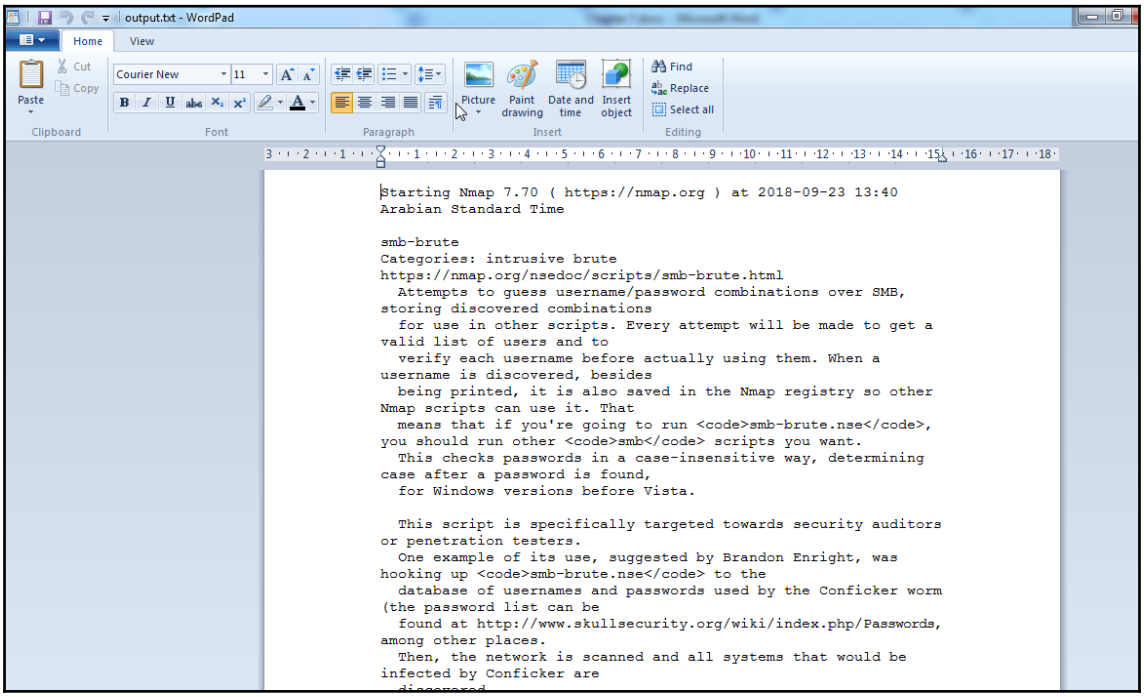
Port	Hosts
8180 / tcp / www	192.168.103.129

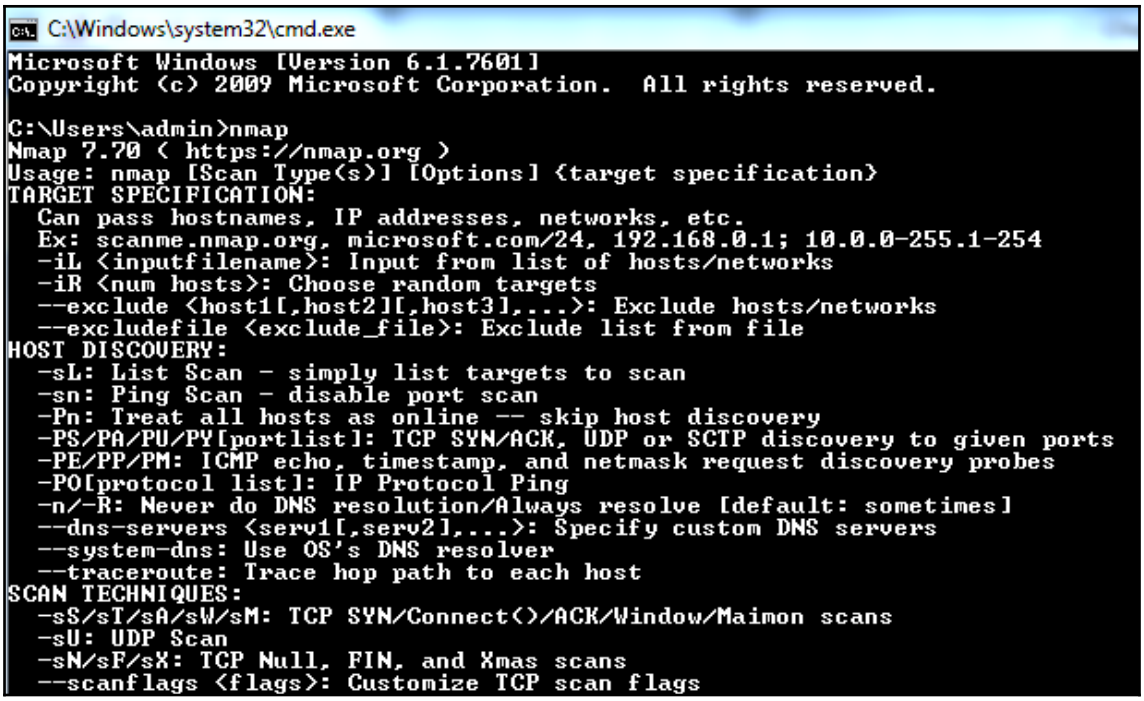


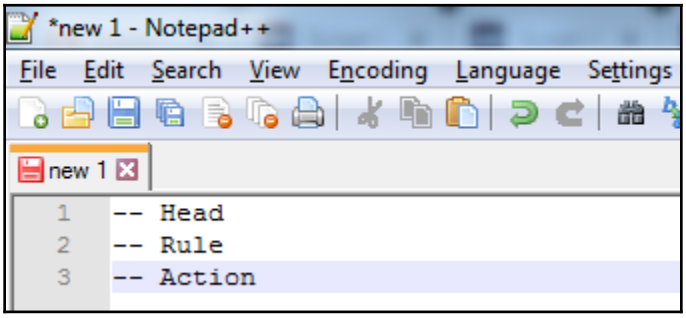
Chapter 7: Understanding the Customization and Optimization of Nessus and Nmap

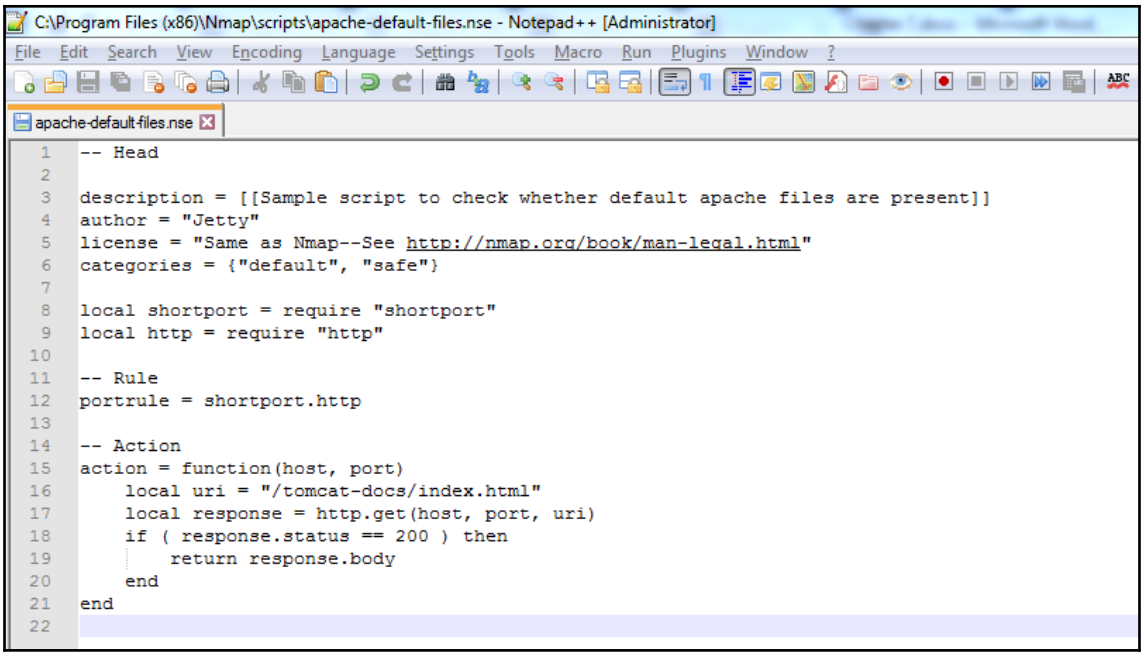



C:\Windows\system32\cmd.exe
C:\Users\admin>nmap --script-help smb* >> D:/output.txt
C:\Users\admin>


output.txt - WordPad
Home
View
Paste
Cut
Copy
Courier New
11
Picture
Paint drawing
Date and time
Insert object
Find
Replace
Select all
Clipboard
Font
Paragraph
Insert
Editing
Starting Nmap 7.70 (https://nmap.org) at 2018-09-23 13:40
Arabian Standard Time
smb-brute
Categories: intrusive brute
https://nmap.org/nsedoc/scripts/smb-brute.html
Attempts to guess username/password combinations over SMB,
storing discovered combinations
for use in other scripts. Every attempt will be made to get a
valid list of users and to
verify each username before actually using them. When a
username is discovered, besides
being printed, it is also saved in the Nmap registry so other
Nmap scripts can use it. That
means that if you're going to run <code>smb-brute.nse</code>,
you should run other <code>smb</code> scripts you want.
This checks passwords in a case-insensitive way, determining
case after a password is found,
for Windows versions before Vista.
This script is specifically targeted towards security auditors
or penetration testers.
One example of its use, suggested by Brandon Enright, was
hooking up <code>smb-brute.nse</code> to the
database of usernames and passwords used by the Conficker worm
(the password list can be
found at http://www.skullsecurity.org/wiki/index.php/Passwords,
among other places.
Then, the network is scanned and all systems that would be
infected by Conficker are

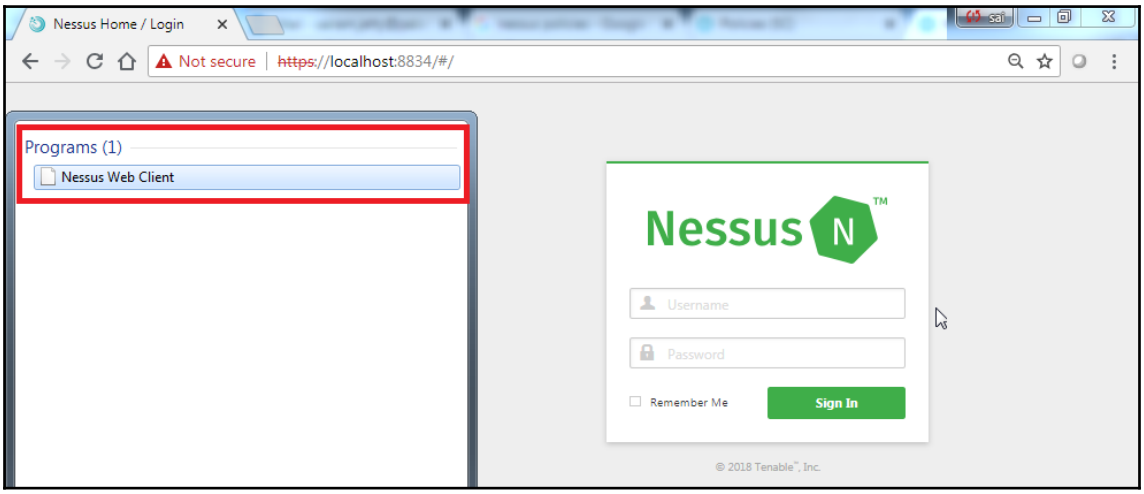

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\admin>nmap
Nmap 7.70 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] <target specification>
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags

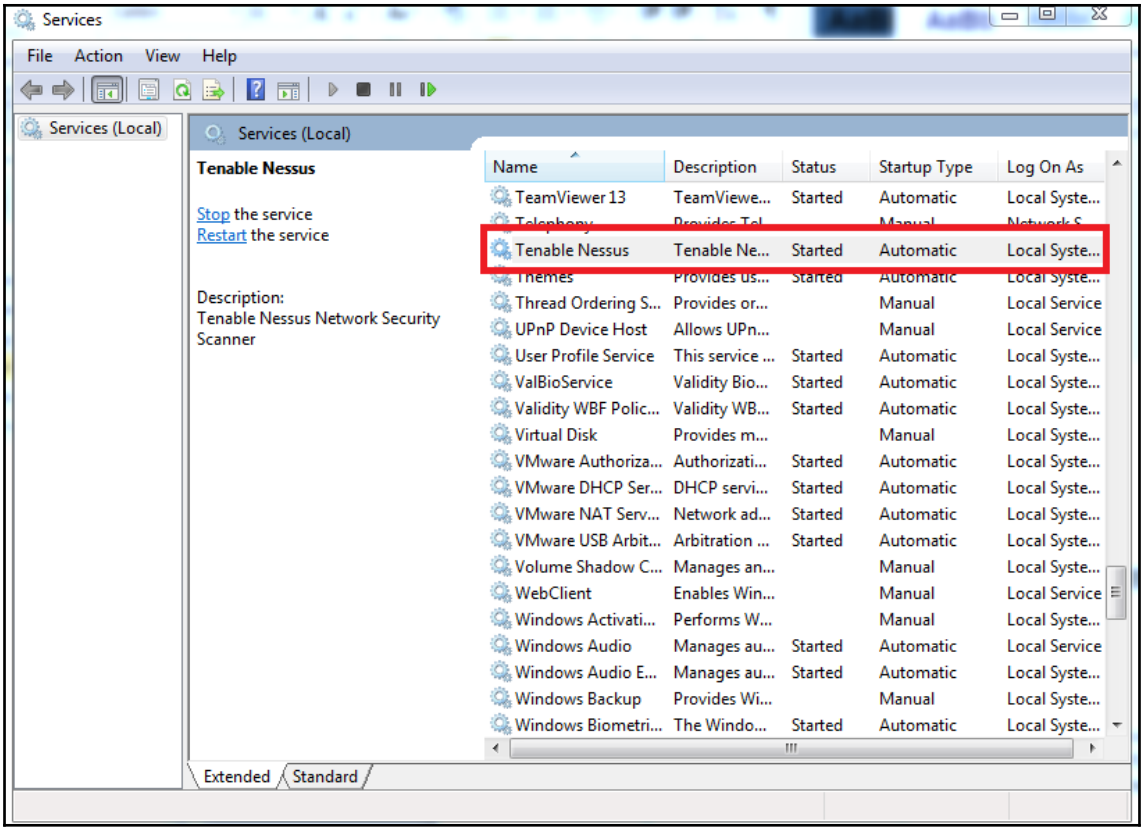

*new 1 - Notepad++
File Edit Search View Encoding Language Settings
new 1
1 -- Head
2 -- Rule
3 -- Action

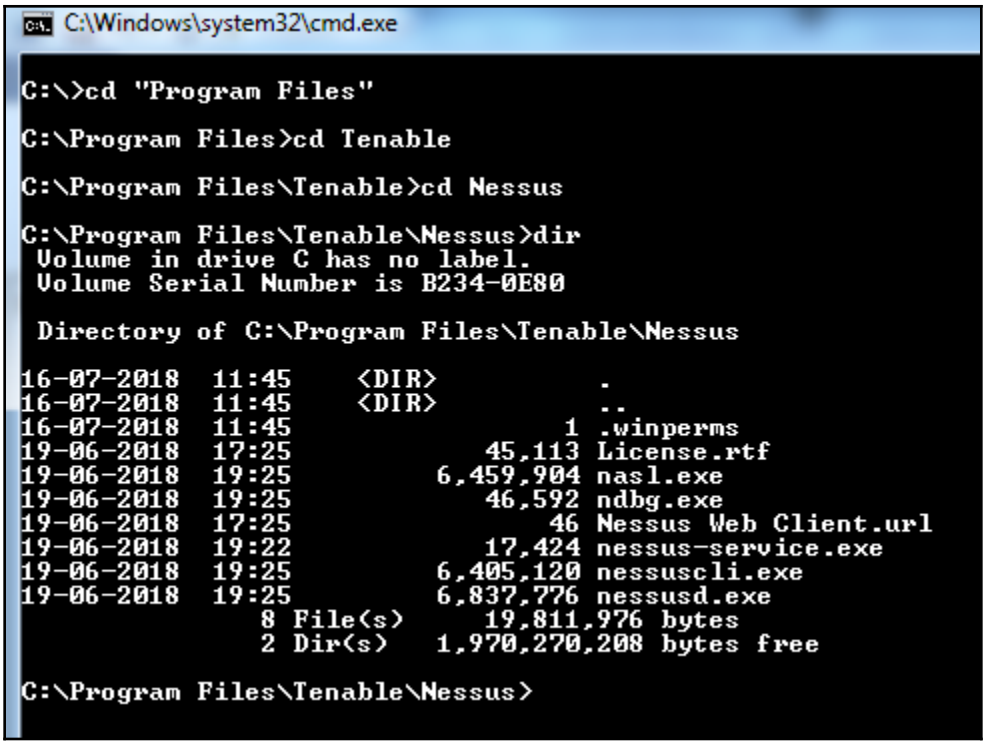

C:\Program Files (x86)\Nmap\scripts\apache-default-files.nse - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
apache-default-files.nse
1 -- Head
2
3 description = [[Sample script to check whether default apache files are present]]
4 author = "Jetty"
5 license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
6 categories = {"default", "safe"}
7
8 local shortport = require "shortport"
9 local http = require "http"
10
11 -- Rule
12 portrule = shortport.http
13
14 -- Action
15 action = function(host, port)
16 local uri = "/tomcat-docs/index.html"
17 local response = http.get(host, port, uri)
18 if (response.status == 200) then
19 return response.body
20 end
21 end
22

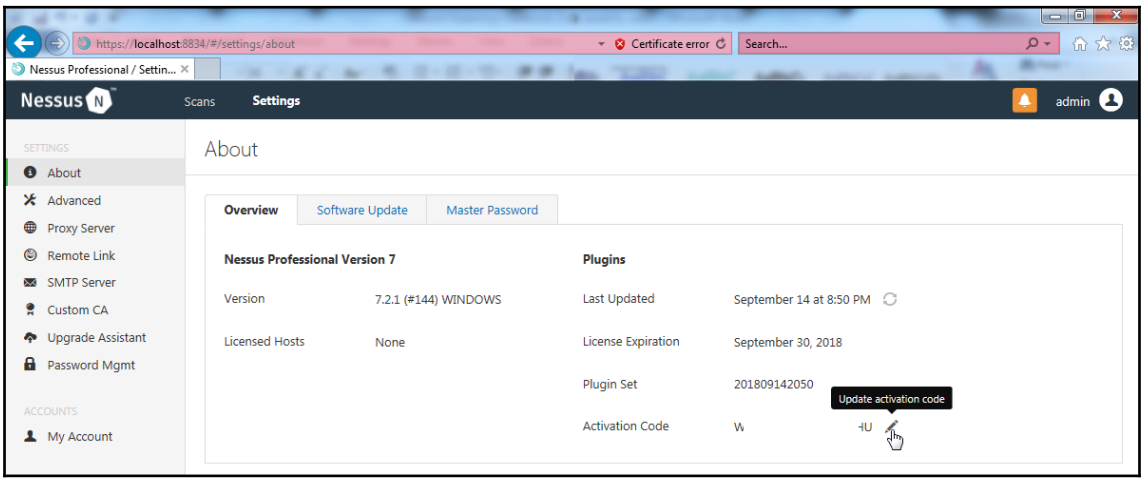

C:\Users\admin>nmap --script apache-default-files 192.168.75.128 -p8180 -v
Starting Nmap 7.70 (https://nmap.org) at 2018-09-23 15:54 Arabian Standard Time
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:54
Completed NSE at 15:54, 0.00s elapsed
Initiating ARP Ping Scan at 15:54
Scanning 192.168.75.128 [1 port]
Completed ARP Ping Scan at 15:54, 1.70s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:54
Completed Parallel DNS resolution of 1 host. at 15:54, 16.50s elapsed
Initiating SYN Stealth Scan at 15:54
Scanning 192.168.75.128 [1 port]
Discovered open port 8180/tcp on 192.168.75.128
Completed SYN Stealth Scan at 15:54, 0.01s elapsed (1 total ports)
NSE: Script scanning 192.168.75.128.
Initiating NSE at 15:54
Completed NSE at 15:54, 0.02s elapsed
Nmap scan report for 192.168.75.128
Host is up (0.00s latency).
PORT STATE SERVICE
8180/tcp open unknown
| apache-default-files: <html><head><META http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><title>The Apache Tomcat 5.5 Servlet/JSP Container - Documen
</title><meta value="Craig R. McClanahan" name="author"><meta value="craigmcc@apache.org" name="email"><meta value="Remy Maucherat" name="author"><meta value="remm@apac
="email"><meta value="Yoav Shapira" name="author"><meta value="yoavs@apache.org" name="email"></head><body vlink="#525D76" alink="#525D76" link="#525D76" text="#000000"
ffffff"><table cellspacing="0" width="100%" border="0"><!--PAGE HEADER--><tr><td><!--PROJECT LOGO--><img border="0" alt="
| The Apache Tomcat Servlet/JSP Container
| " align="right" src="./images/tomcat.gif"></td><td><h1>The Apache Tomcat 5.5 Servlet/JSP Container</h1></td><td><
GO--><img border="0" alt="Apache Logo" align="right" src="./images/asf-logo.gif"></td></tr></table><table cellspacing="4" width="10
0"><!--HEADER SEPARATOR--><tr><td colspan="2"><hr size="1" noshade></td></tr><tr><!--LEFT SIDE NAVIGATION--><td nowrap="true" valign="top" width="20%"> Links<
Docs Home
FAQ User Guide <a href="introducti
Introduction
2) Setup
3) First webapp
4) Deployer
href="manager-howto.html">5) Manager
6) Realms and AAA
7) Security Manager
ref="jndi-resources-howto.html">8) JNDI Resources
9) JDBC DataSources
<a href="class-loader-howto.
aseloading
11) JSPs
12) SSL
13) SSI
<a hre
.html">14) CGI
15) Proxy Support
16) MBean Descriptor
<a href="def
.html">17) Default Servlet
18) Clustering
19) Load Balancer
<a href="conn
>20) Connectors
21) Monitoring and Management
22) Logging
23) AP
i>24) Virtual Hosting Reference Release Notes
<
ig/index.html">Apache Tomcat Configuration
JK 1.2 Documentation
<a href="servletapi/index.htm
PI Javadocs
JSP API Javadocs Apache Tomcat Development Build
Changelog
Status
Developers
<a href="catalina/funcspecs
>Functional Specs.
Apache Tomcat Javadocs
Apache Jasper Javadocs
href="architecture/index.html">Architecture</td><!--RIGHT SIDE MAIN BODY--><td align="left" valign="top" width="80%"><table cellspacing="4" width="100%" b
r><td valign="top" align="left"><h1>The Apache Tomcat 5.5 Servlet/JSP Container</h1><h2>Documentation Index</h2></td><td nowrap="true" valign="top" align="right"><small
inter/index.html"><img alt="Printer Friendly Version" border="0" src="./images/printer.gif">
print-friendly
version
| </small></td></tr></table><table cellpadding="2" cellspacing="0" border="0"><tr><td bgcolor="#525D76"><font face="arial,helvetica,sanserif" co
">Introduction</td></tr><tr><td><blockquote>
|

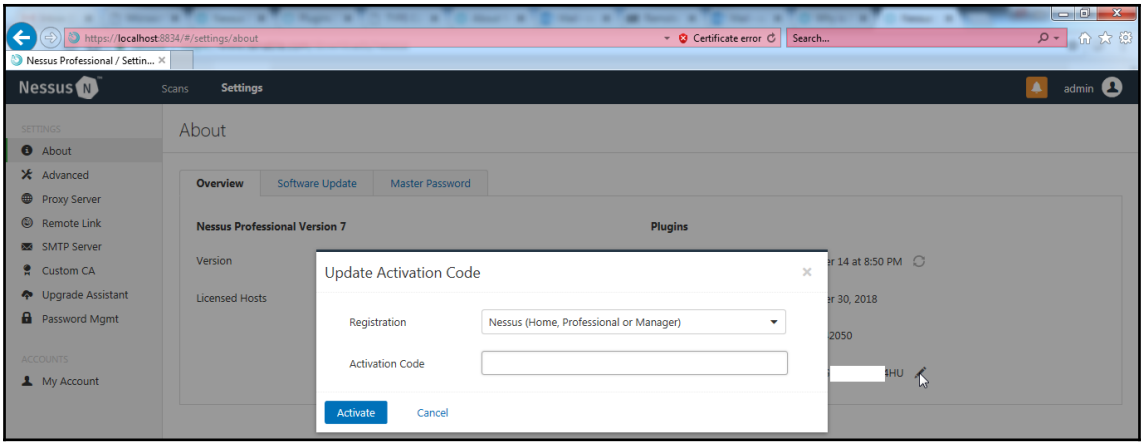
```
C:\Users\admin>nmap --script apache-default-files 192.168.75.128 -p8180 -v
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-23 16:07 Arabian Standard Time
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed
Initiating ARP Ping Scan at 16:07
Scanning 192.168.75.128 [1 port]
Completed ARP Ping Scan at 16:07, 1.77s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:07
Completed Parallel DNS resolution of 1 host. at 16:08, 16.50s elapsed
Initiating SYN Stealth Scan at 16:08
Scanning 192.168.75.128 [1 port]
Discovered open port 8180/tcp on 192.168.75.128
Completed SYN Stealth Scan at 16:08, 0.00s elapsed (1 total ports)
NSE: Script scanning 192.168.75.128.
Initiating NSE at 16:08
Completed NSE at 16:08, 0.01s elapsed
Nmap scan report for 192.168.75.128
Host is up (0.00088s latency).

PORT     STATE SERVICE
8180/tcp open  unknown
|_apache-default-files: vulnerable
MAC Address: 00:0C:29:74:1C:63 (VMware)

NSE: Script Post-scanning.
Initiating NSE at 16:08
Completed NSE at 16:08, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 33.60 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

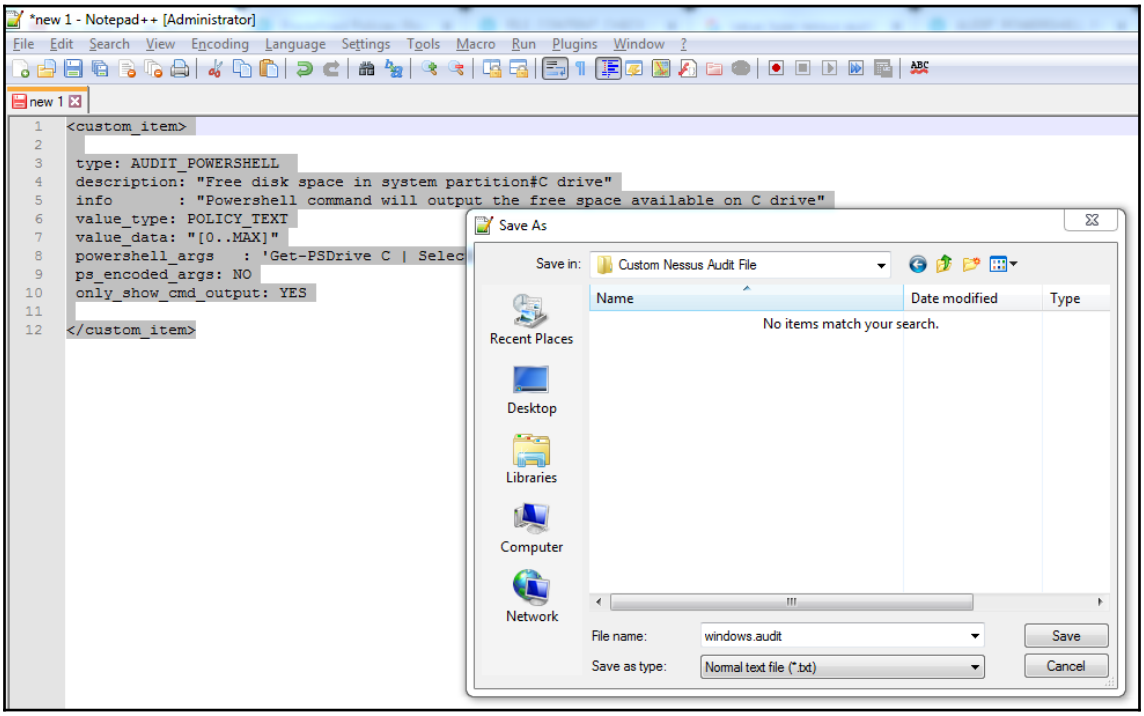


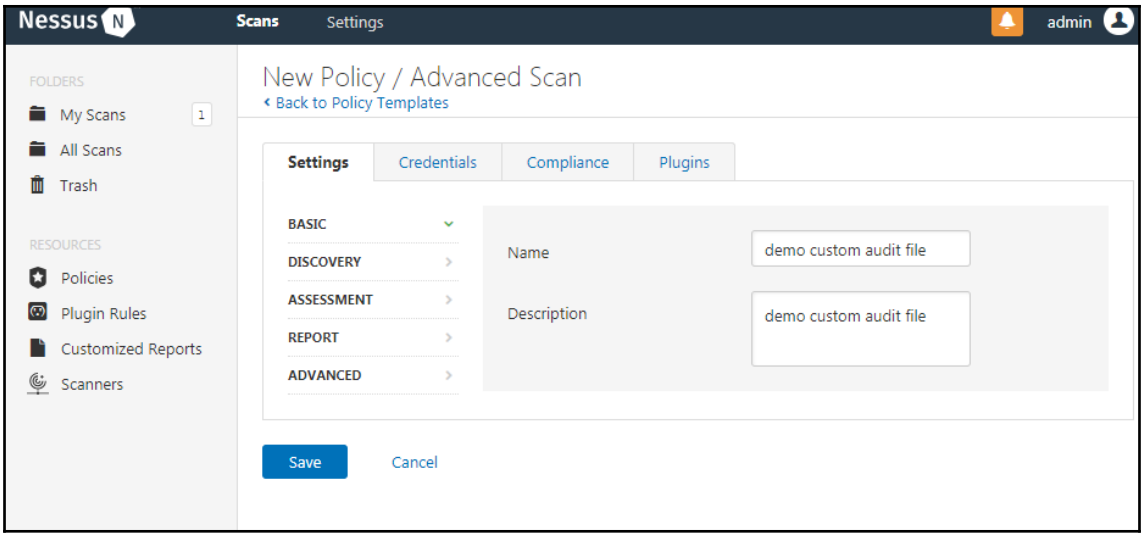

Services
File Action View Help
Services (Local)
Services (Local)
Tenable Nessus
Stop the service
Restart the service
Description:
Tenable Nessus Network Security Scanner
Name
Description
Status
Startup Type
Log On As
TeamViewer 13
TeamViewe...
Started
Automatic
Local Syste...
Tenable Nessus
Tenable Ne...
Started
Automatic
Local Syste...
Thread Ordering S...
Provides or...
Manual
Local Service
UPnP Device Host
Allows UPn...
Manual
Local Service
User Profile Service
This service ...
Started
Automatic
Local Syste...
ValBioService
Validity Bio...
Started
Automatic
Local Syste...
Validity WBF Polic...
Validity WB...
Started
Automatic
Local Syste...
Virtual Disk
Provides m...
Manual
Local Syste...
VMware Authoriza...
Authorizati...
Started
Automatic
Local Syste...
VMware DHCP Ser...
DHCP servi...
Started
Automatic
Local Syste...
VMware NAT Serv...
Network ad...
Started
Automatic
Local Syste...
VMware USB Arbit...
Arbitration ...
Started
Automatic
Local Syste...
Volume Shadow C...
Manages an...
Manual
Local Syste...
WebClient
Enables Win...
Manual
Local Service
Windows Activati...
Performs W...
Manual
Local Syste...
Windows Audio
Manages au...
Started
Automatic
Local Service
Windows Audio E...
Manages au...
Started
Automatic
Local Syste...
Windows Backup
Provides Wi...
Manual
Local Syste...
Windows Biometri...
The Windo...
Started
Automatic
Local Syste...
Extended
Standard

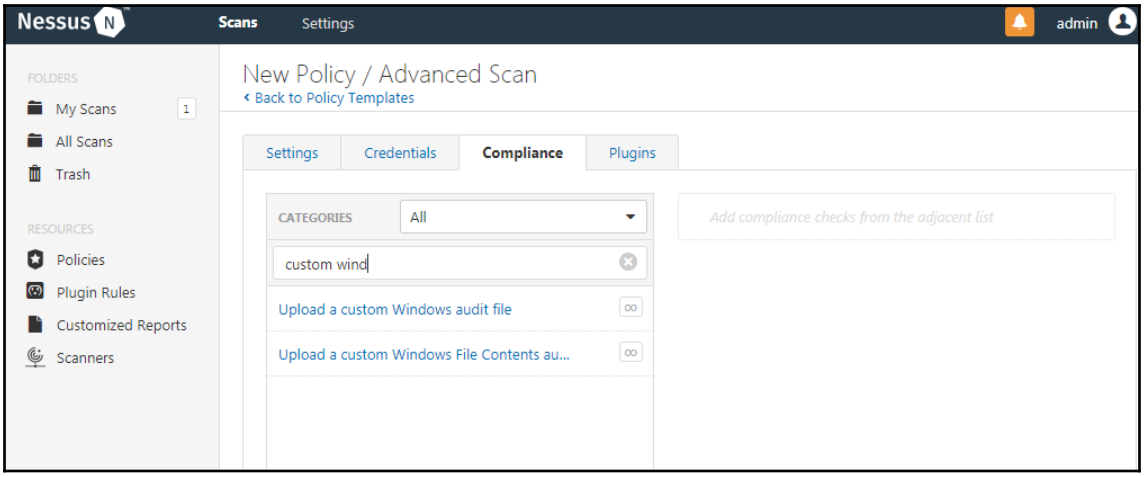

C:\Windows\system32\cmd.exe
C:\>cd "Program Files"
C:\Program Files>cd Tenable
C:\Program Files\Tenable>cd Nessus
C:\Program Files\Tenable\Nessus>dir
Volume in drive C has no label.
Volume Serial Number is B234-0E80
Directory of C:\Program Files\Tenable\Nessus
16-07-2018 11:45 <DIR> .
16-07-2018 11:45 <DIR> ..
16-07-2018 11:45 1 .winperms
19-06-2018 17:25 45,113 License.rtf
19-06-2018 19:25 6,459,904 nasl.exe
19-06-2018 19:25 46,592 ndbg.exe
19-06-2018 17:25 46 Nessus Web Client.url
19-06-2018 19:22 17,424 nessus-service.exe
19-06-2018 19:25 6,405,120 nessuscli.exe
19-06-2018 19:25 6,837,776 nessusd.exe
8 File(s) 19,811,976 bytes
2 Dir(s) 1,970,270,208 bytes free
C:\Program Files\Tenable\Nessus>

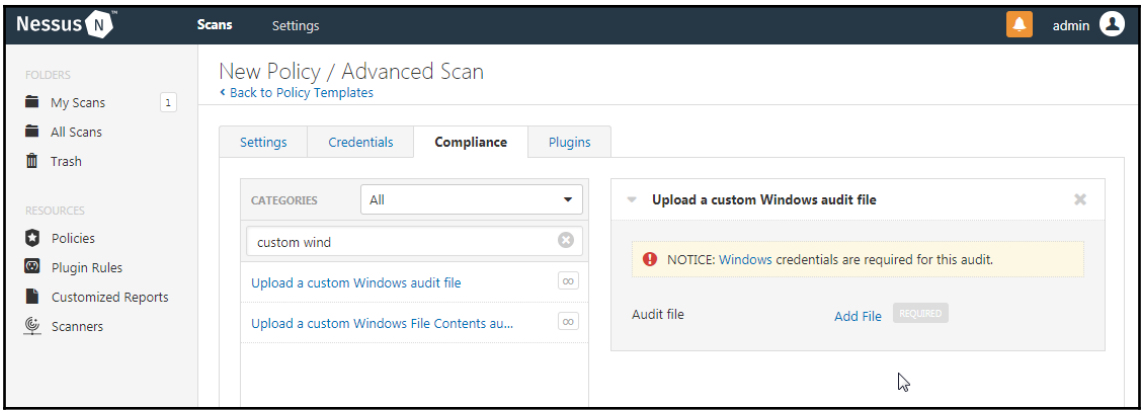

https://localhost:8834/#/settings/about
Certificate error
Search...
Nessus Professional / Settin...
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
ACCOUNTS
My Account
About
Overview
Software Update
Master Password
Nessus Professional Version 7
Version
7.2.1 (#144) WINDOWS
Licensed Hosts
None
Plugins
Last Updated
September 14 at 8:50 PM
License Expiration
September 30, 2018
Plugin Set
201809142050
Activation Code
Update activation code

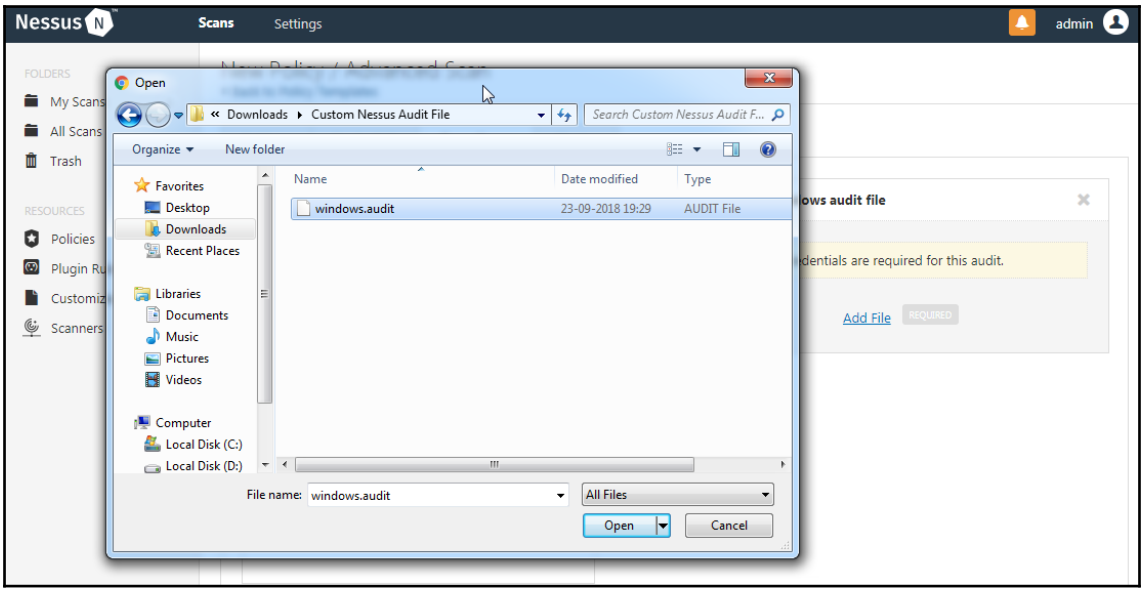

Nessus Professional / Settin...
Nessus
Scans
Settings
admin
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
My Account
Overview
Software Update
Master Password
Nessus Professional Version 7
Plugins
Version
Licensed Hosts
Update Activation Code
Registration
Nessus (Home, Professional or Manager)
Activation Code
Activate
Cancel

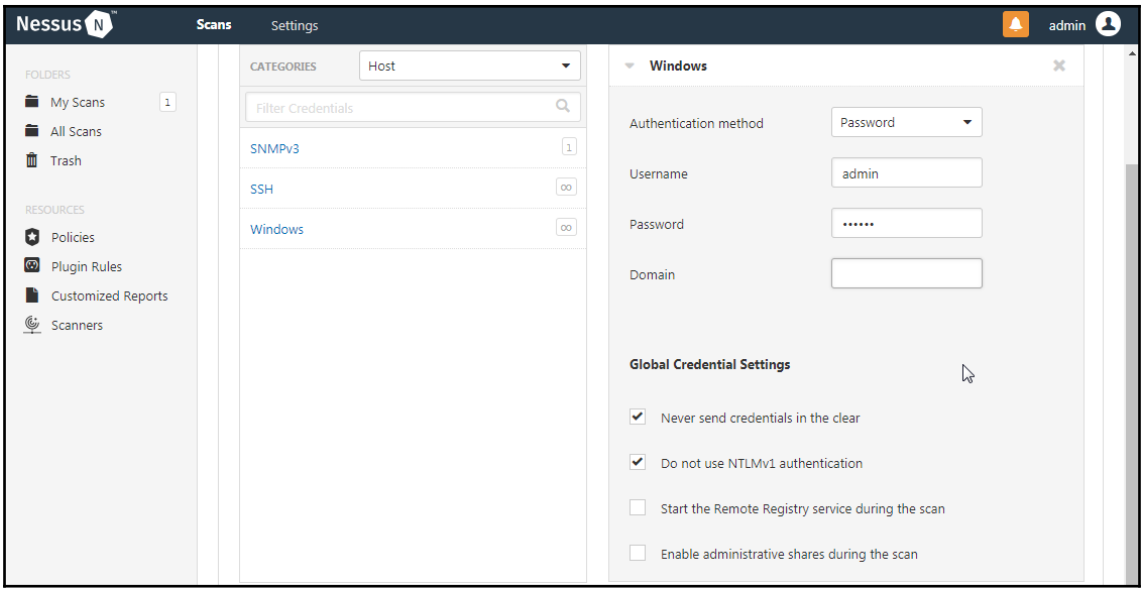

*new 1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
<custom_item>
type: AUDIT_POWERSHELL
description: "Free disk space in system partition#C drive"
info : "Powershell command will output the free space available on C drive"
value_type: POLICY_TEXT
value_data: "[0..MAX]"
powershell_args : 'Get-PSDrive C | Selec
ps_encoded_args: NO
only_show_cmd_output: YES
</custom_item>
Save As
Save in:
Custom Nessus Audit File
Recent Places
Desktop
Libraries
Computer
Network
Name
Date modified
Type
No items match your search.
File name:
windows.audit
Save as type:
Normal text file (*.txt)
Save
Cancel

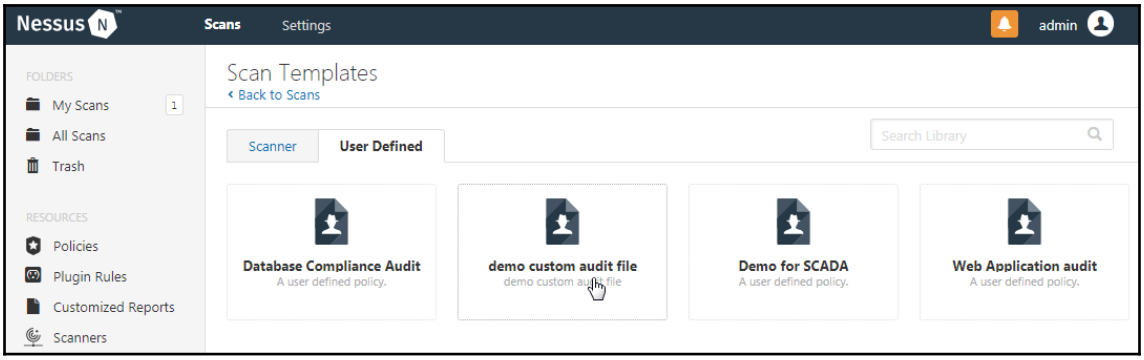

Nessus
Scans
Settings
admin
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
demo custom audit file
Description
demo custom audit file
Save
Cancel

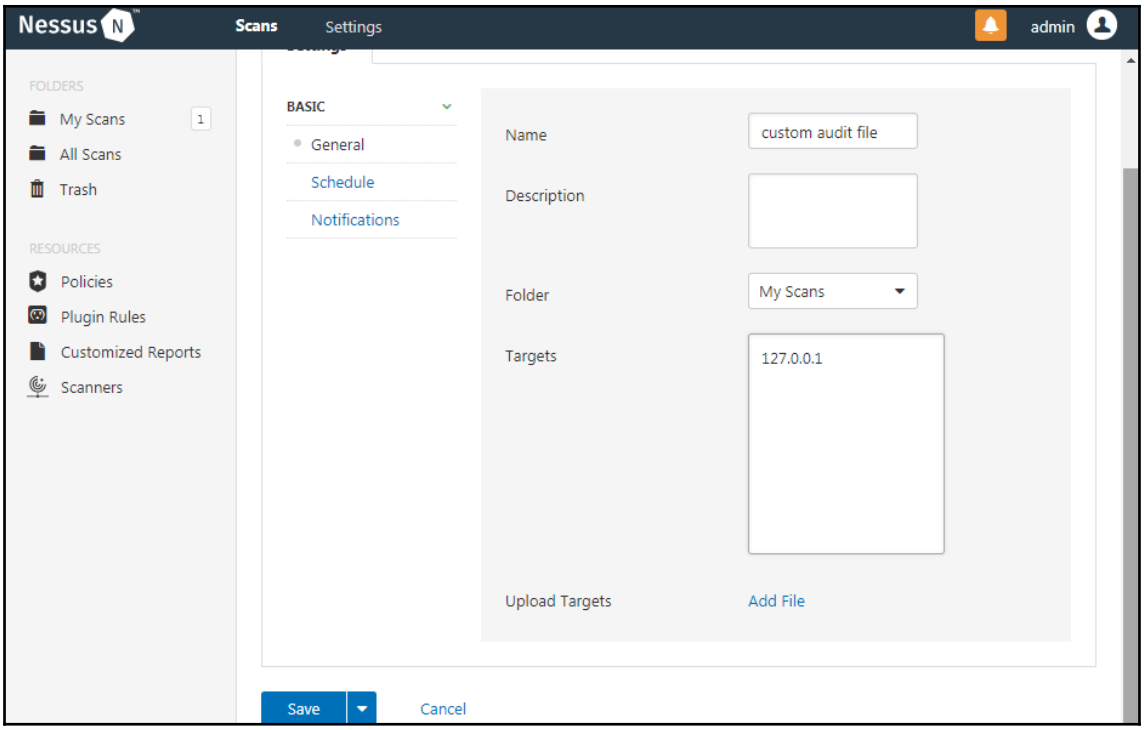

Nessus
Scans
Settings
admin
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
CATEGORIES
All
custom wind
Upload a custom Windows audit file
Upload a custom Windows File Contents au...
Add compliance checks from the adjacent list


Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Advanced Scan
Back to Policy Templates
Settings
Credentials
Compliance
Plugins
CATEGORIES
All
custom wind
Upload a custom Windows audit file
Upload a custom Windows File Contents au...
Upload a custom Windows audit file
NOTICE: Windows credentials are required for this audit.
Audit file
Add File
REQUIRED

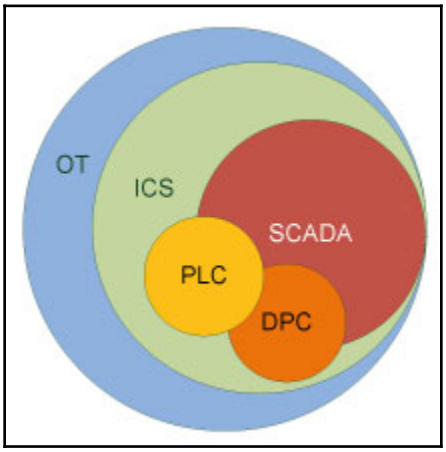

Nessus
Scans
Settings
admin
Open
Downloads
Custom Nessus Audit File
Search Custom Nessus Audit F...
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Name
Date modified
Type
windows.audit
23-09-2018 19:29
AUDIT File
File name:
windows.audit
All Files
Open
Cancel
Add File
REQUIRED

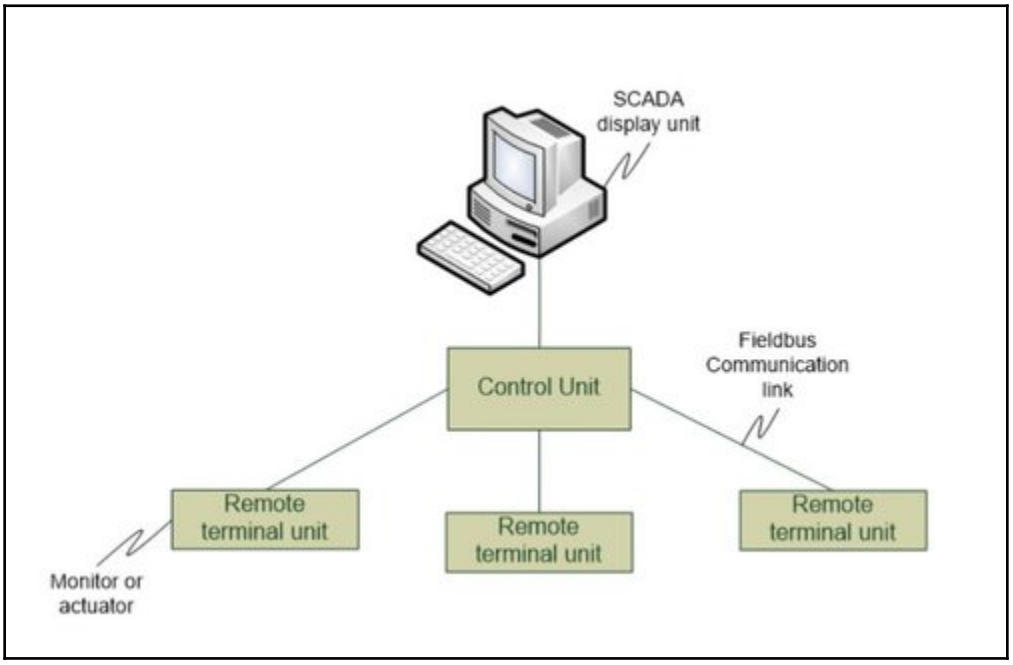

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
Windows
Authentication method
Password
Username
admin
Password
Domain
Global Credential Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan
Enable administrative shares during the scan

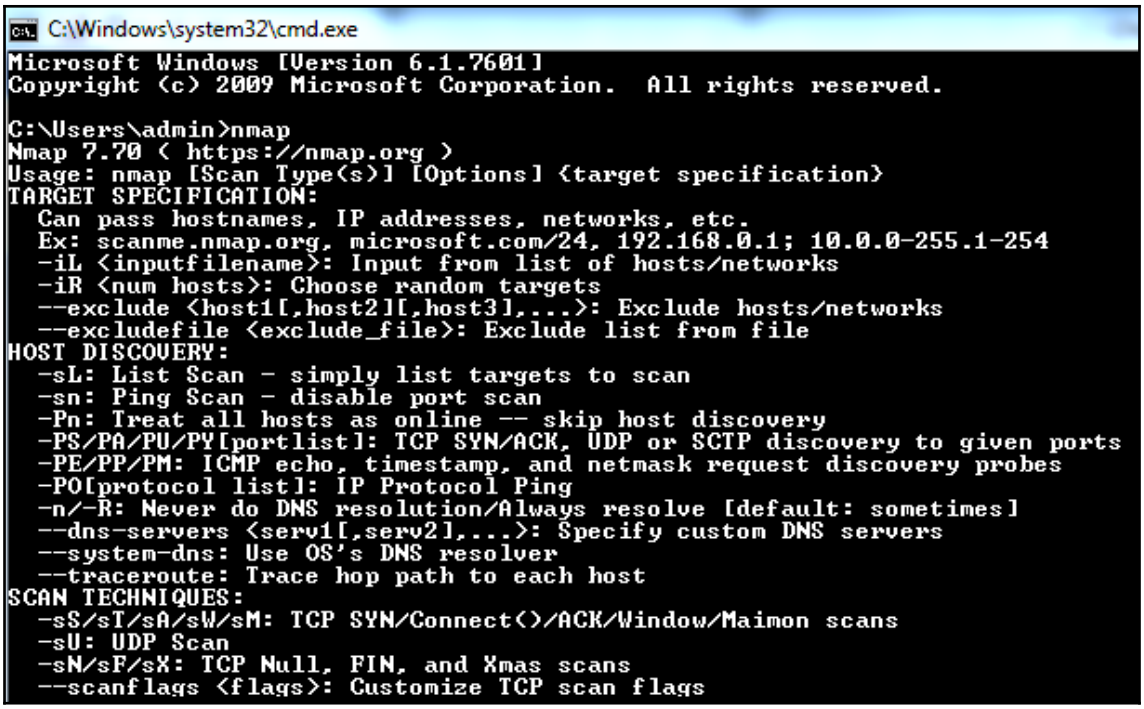

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
Database Compliance Audit
A user defined policy.
demo custom audit file
Demo for SCADA
A user defined policy.
Web Application audit
A user defined policy.

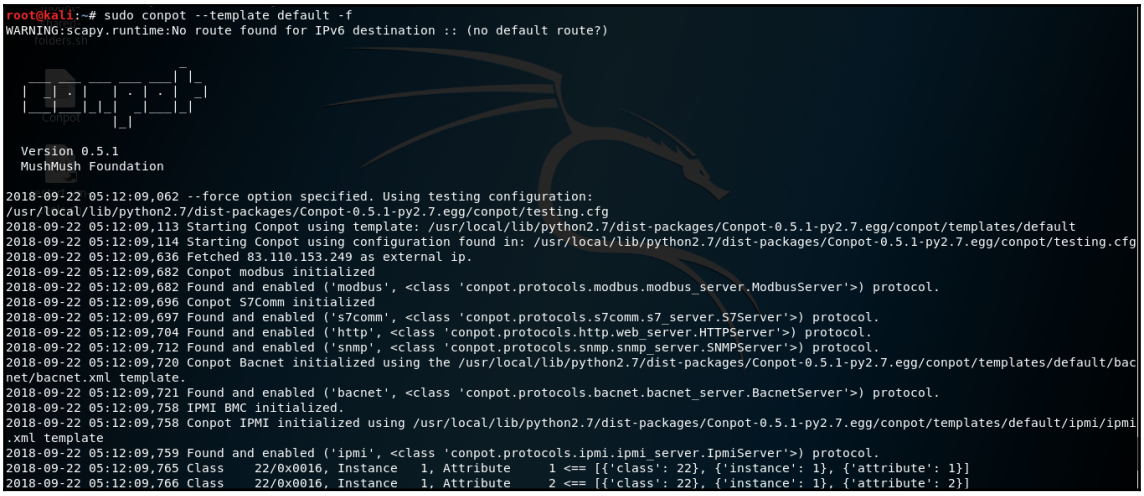

Nessus
Scans
Settings
admin
FOLDERS
My Scans
1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
BASIC
General
Schedule
Notifications
Name
custom audit file
Description
Folder
My Scans
Targets
127.0.0.1
Upload Targets
Add File
Save
Cancel

Chapter 8: Network Scanning for IoT, SCADA/ICS





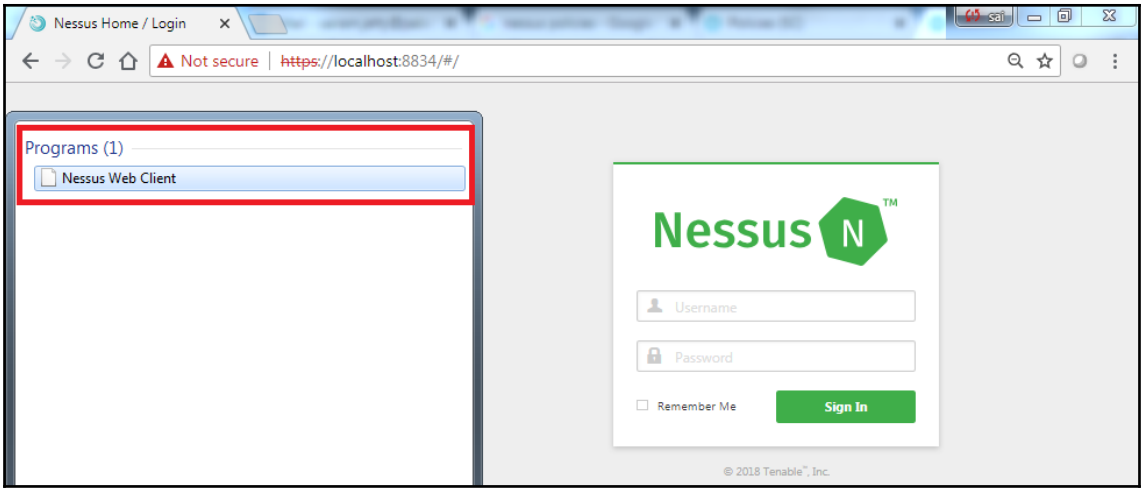

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\admin>nmap
Nmap 7.70 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags

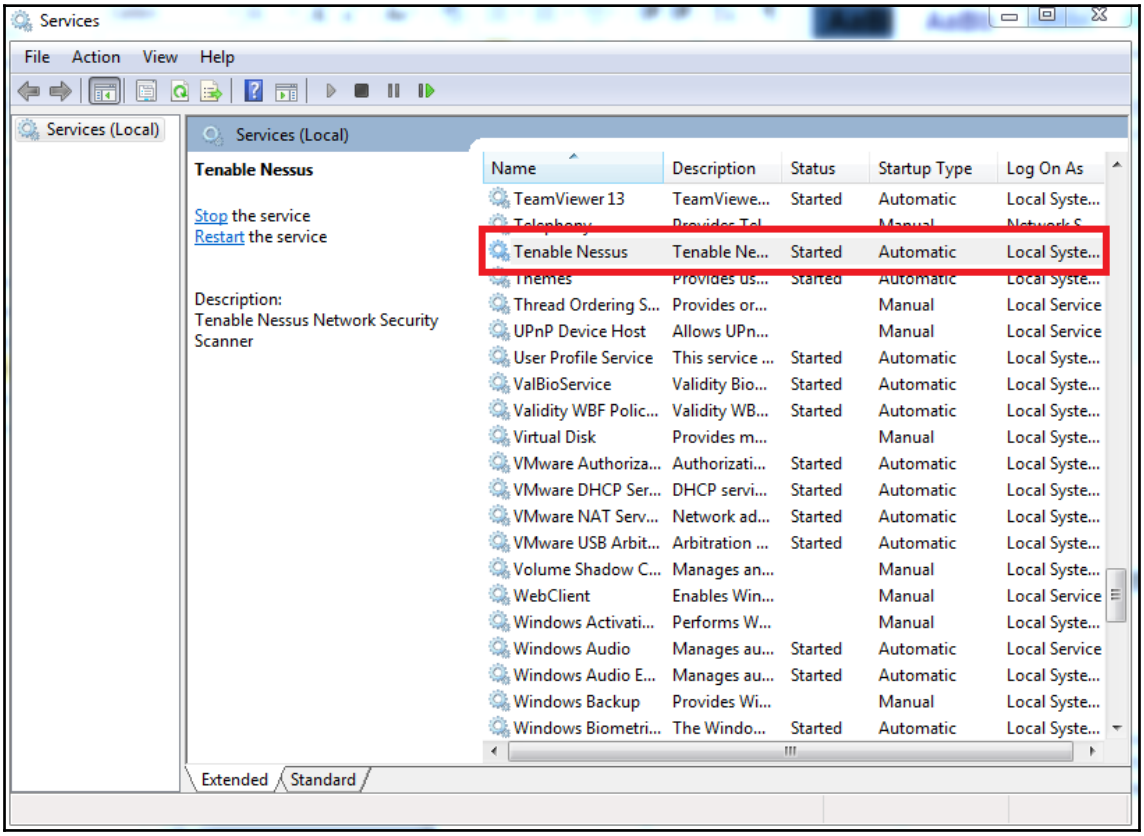

root@kali:~# sudo conpot --template default -f
WARNING:scapy.runtime:No route found for IPv6 destination :: (no default route?)
Conpot
Version 0.5.1
MushMush Foundation
2018-09-22 05:12:09,062 --force option specified. Using testing configuration:
/usr/local/lib/python2.7/dist-packages/Conpot-0.5.1-py2.7.egg/conpot/testing.cfg
2018-09-22 05:12:09,113 Starting Conpot using template: /usr/local/lib/python2.7/dist-packages/Conpot-0.5.1-py2.7.egg/conpot/templates/default
2018-09-22 05:12:09,114 Starting Conpot using configuration found in: /usr/local/lib/python2.7/dist-packages/Conpot-0.5.1-py2.7.egg/conpot/testing.cfg
2018-09-22 05:12:09,636 Fetched 83.110.153.249 as external ip.
2018-09-22 05:12:09,682 Conpot modbus initialized
2018-09-22 05:12:09,682 Found and enabled ('modbus', <class 'conpot.protocols.modbus.modbus_server.ModbusServer'>) protocol.
2018-09-22 05:12:09,696 Conpot S7Comm initialized
2018-09-22 05:12:09,697 Found and enabled ('s7comm', <class 'conpot.protocols.s7comm.s7_server.S7Server'>) protocol.
2018-09-22 05:12:09,704 Found and enabled ('http', <class 'conpot.protocols.http.web_server.HTTPServer'>) protocol.
2018-09-22 05:12:09,712 Found and enabled ('snmp', <class 'conpot.protocols.snmp.snmp_server.SNMPServer'>) protocol.
2018-09-22 05:12:09,720 Conpot Bacnet initialized using the /usr/local/lib/python2.7/dist-packages/Conpot-0.5.1-py2.7.egg/conpot/templates/default/bacnet/bacnet.xml template.
2018-09-22 05:12:09,721 Found and enabled ('bacnet', <class 'conpot.protocols.bacnet.bacnet_server.BacnetServer'>) protocol.
2018-09-22 05:12:09,758 IPMI BMC initialized.
2018-09-22 05:12:09,758 Conpot IPMI initialized using /usr/local/lib/python2.7/dist-packages/Conpot-0.5.1-py2.7.egg/conpot/templates/default/ipmi/ipmi.xml template
2018-09-22 05:12:09,759 Found and enabled ('ipmi', <class 'conpot.protocols.ipmi.ipmi_server.IpmiServer'>) protocol.
2018-09-22 05:12:09,765 Class 22/0x0016, Instance 1, Attribute 1 <== [{'class': 22}, {'instance': 1}, {'attribute': 1}]
2018-09-22 05:12:09,766 Class 22/0x0016, Instance 1, Attribute 2 <== [{'class': 22}, {'instance': 1}, {'attribute': 2}]

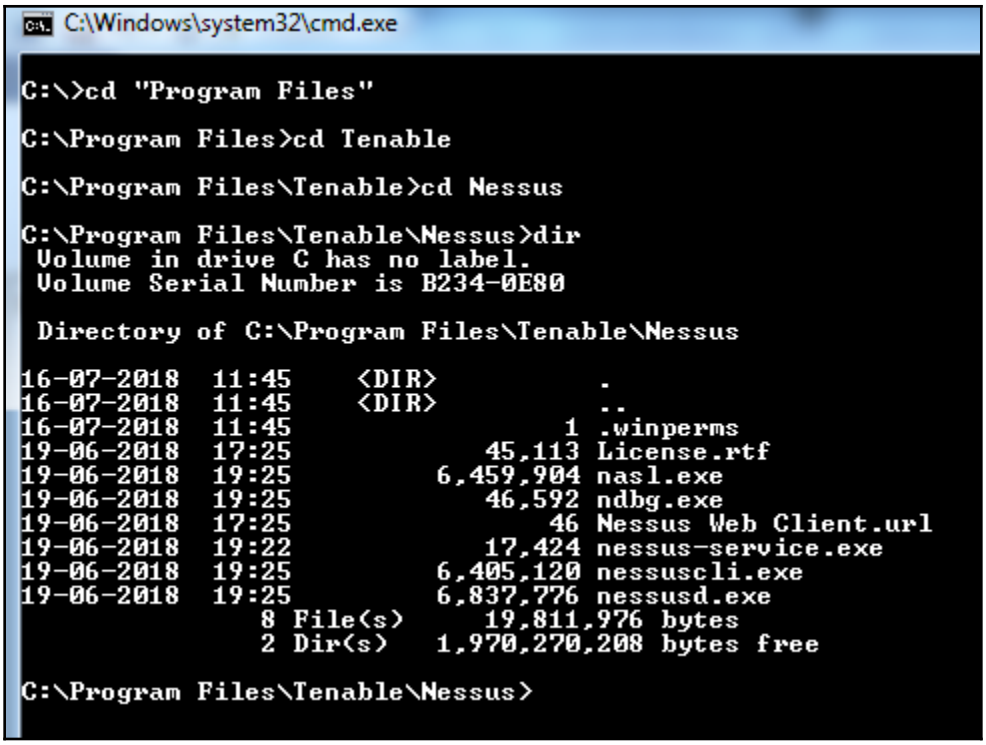
```
C:\Users\admin>nmap --script s7-info.nse -p 102 192.168.75.133
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 13:15 Arabian Standard Time
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 13:15 (0:00:00 remaining)
Nmap scan report for 192.168.75.133
Host is up (0.00s latency).

PORT    STATE SERVICE
102/tcp open  iso-tsap
| s7-info:
|   Version: 0.0
|   System Name: Technodrome
|   Module Type: Siemens, SIMATIC, S7-200
|   Serial Number: 88111222
|   Plant Identification: Mouser Factory
|_  Copyright: Original Siemens Equipment
MAC Address: 00:0C:29:74:28:93 (VMware)
Service Info: Device: specialized

Nmap done: 1 IP address (1 host up) scanned in 18.84 seconds

C:\Users\admin>
```

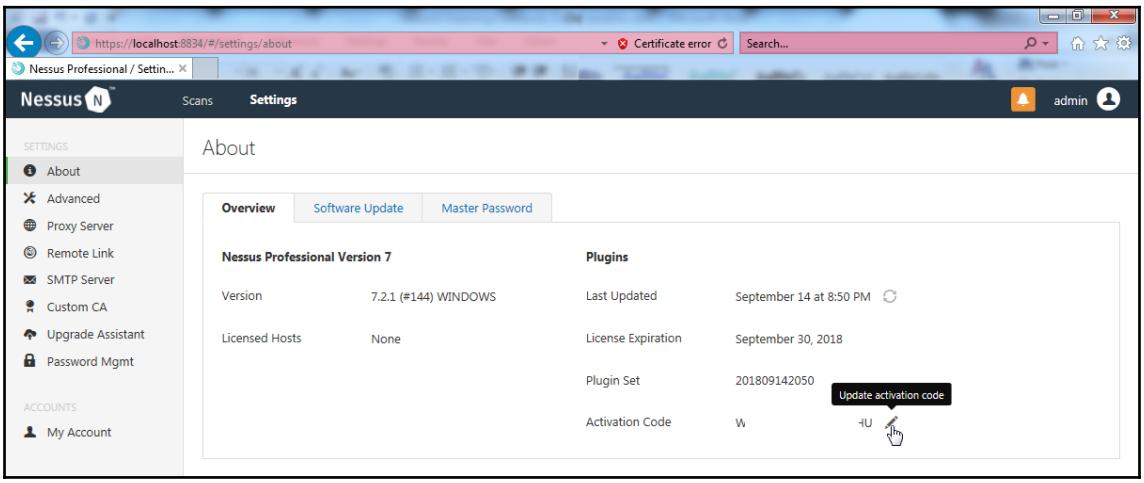
```
C:\Users\admin>nmap --script modbus-discover.nse --script-args='modbus-discover.aggressive=true' -p 502 192.168.75.133
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-22 13:17 Arabian Standard Time
Nmap scan report for 192.168.75.133
Host is up (0.00s latency).

PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid 0x1:
|     Slave ID data: <unknown>
|_    Device identification: Siemens SIMATIC S7-200
MAC Address: 00:0C:29:74:28:93 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.66 seconds

C:\Users\admin>
```

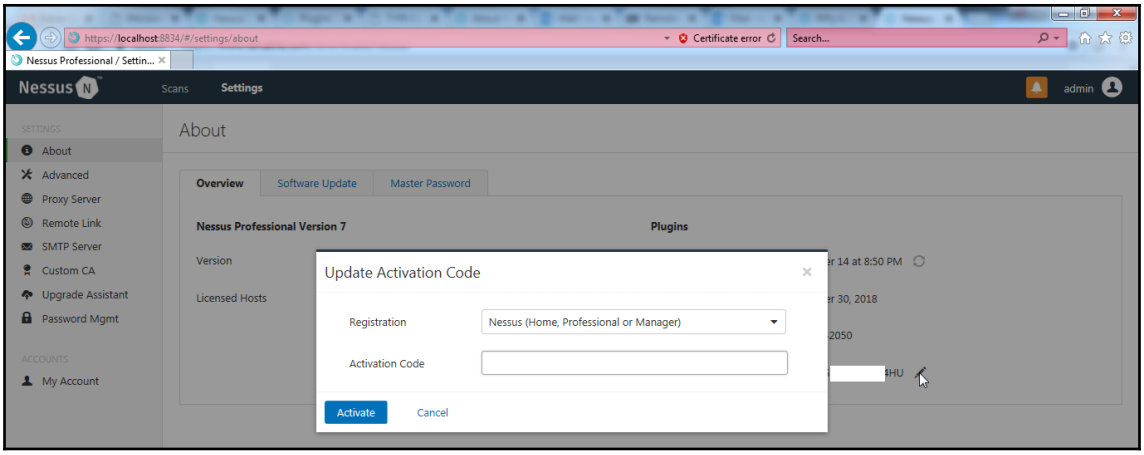
README.md	Added more checks to CommunicationsProcessor
Siemens-CommunicationsProcessor.nse	Added support for more versions
Siemens-HMI-miniweb.nse	Added more checks to CommunicationsProcessor
Siemens-SIMATIC-PLC-S7.nse	Added support for SCALANCE XF Family
Siemens-Scalance-module.nse	Added Siemens SCALANCE network devices
Siemens-WINCC.nse	Siemens WINCC discovery support added

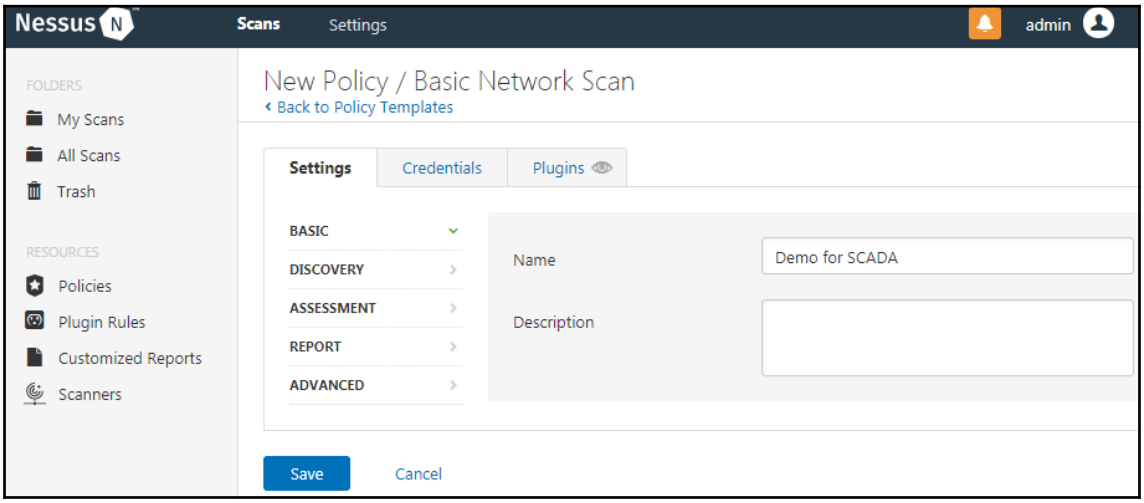

Nessus Home / Login
Not secure
https://localhost:8834/#/
Programs (1)
Nessus Web Client
Nessus
Username
Password
Remember Me
Sign In
© 2018 Tenable™, Inc.

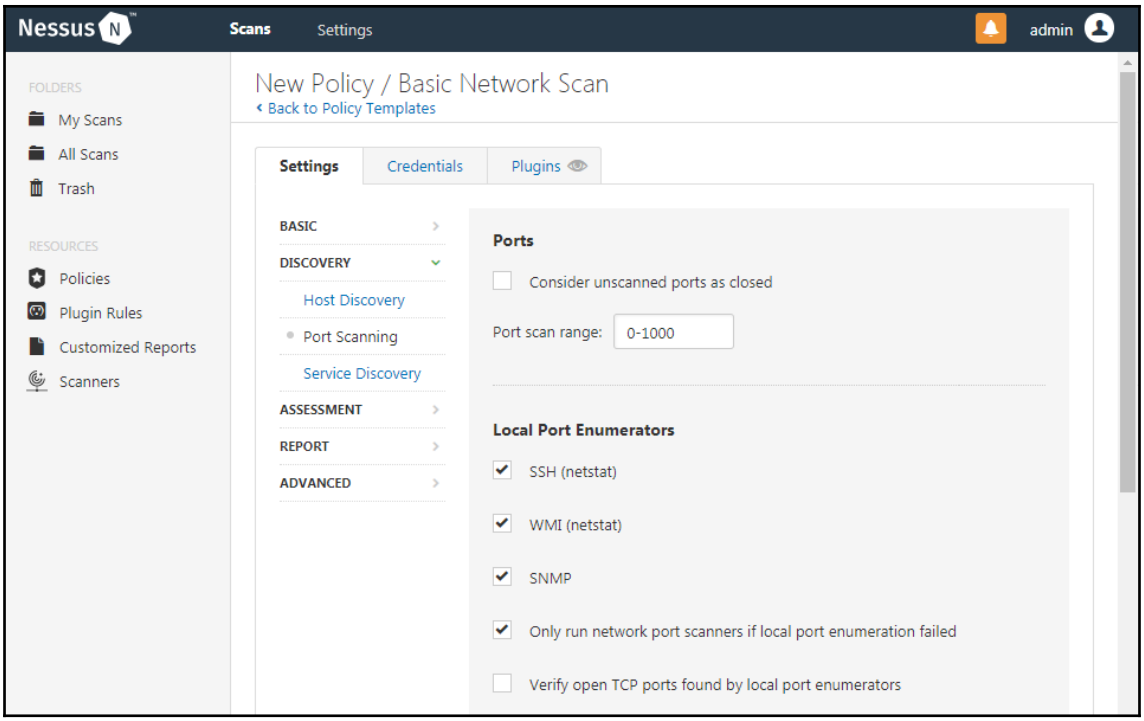

Services
File Action View Help
Services (Local)
Services (Local)
Tenable Nessus
Stop the service
Restart the service
Description:
Tenable Nessus Network Security Scanner
Name
Description
Status
Startup Type
Log On As
TeamViewer 13
TeamViewe...
Started
Automatic
Local Syste...
Tenable Nessus
Tenable Ne...
Started
Automatic
Local Syste...
Thread Ordering S...
Provides or...
Manual
Local Service
UPnP Device Host
Allows UPn...
Manual
Local Service
User Profile Service
This service ...
Started
Automatic
Local Syste...
ValBioService
Validity Bio...
Started
Automatic
Local Syste...
Validity WBF Polic...
Validity WB...
Started
Automatic
Local Syste...
Virtual Disk
Provides m...
Manual
Local Syste...
VMware Authoriza...
Authorizati...
Started
Automatic
Local Syste...
VMware DHCP Ser...
DHCP servi...
Started
Automatic
Local Syste...
VMware NAT Serv...
Network ad...
Started
Automatic
Local Syste...
VMware USB Arbit...
Arbitration ...
Started
Automatic
Local Syste...
Volume Shadow C...
Manages an...
Manual
Local Syste...
WebClient
Enables Win...
Manual
Local Service
Windows Activati...
Performs W...
Manual
Local Syste...
Windows Audio
Manages au...
Started
Automatic
Local Service
Windows Audio E...
Manages au...
Started
Automatic
Local Syste...
Windows Backup
Provides Wi...
Manual
Local Syste...
Windows Biometri...
The Windo...
Started
Automatic
Local Syste...
Extended
Standard

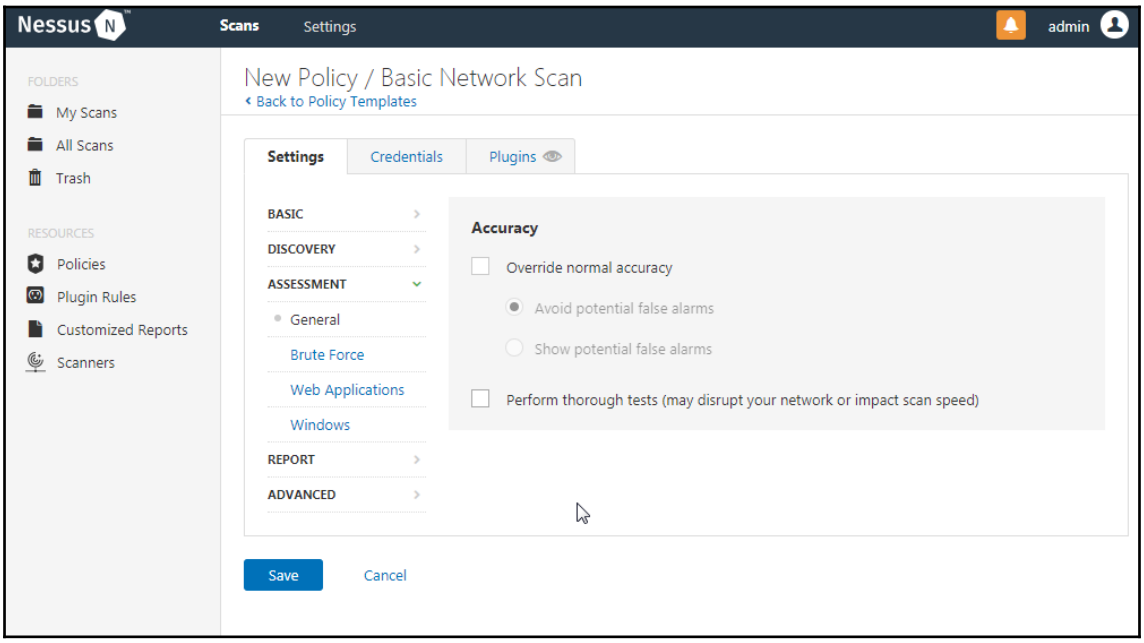

C:\Windows\system32\cmd.exe
C:\>cd "Program Files"
C:\Program Files>cd Tenable
C:\Program Files\Tenable>cd Nessus
C:\Program Files\Tenable\Nessus>dir
Volume in drive C has no label.
Volume Serial Number is B234-0E80
Directory of C:\Program Files\Tenable\Nessus
16-07-2018 11:45 <DIR> .
16-07-2018 11:45 <DIR> ..
16-07-2018 11:45 1 .winperms
19-06-2018 17:25 45,113 License.rtf
19-06-2018 19:25 6,459,904 nasl.exe
19-06-2018 19:25 46,592 ndbg.exe
19-06-2018 17:25 46 Nessus Web Client.url
19-06-2018 19:22 17,424 nessus-service.exe
19-06-2018 19:25 6,405,120 nessuscli.exe
19-06-2018 19:25 6,837,776 nessusd.exe
8 File(s) 19,811,976 bytes
2 Dir(s) 1,970,270,208 bytes free
C:\Program Files\Tenable\Nessus>

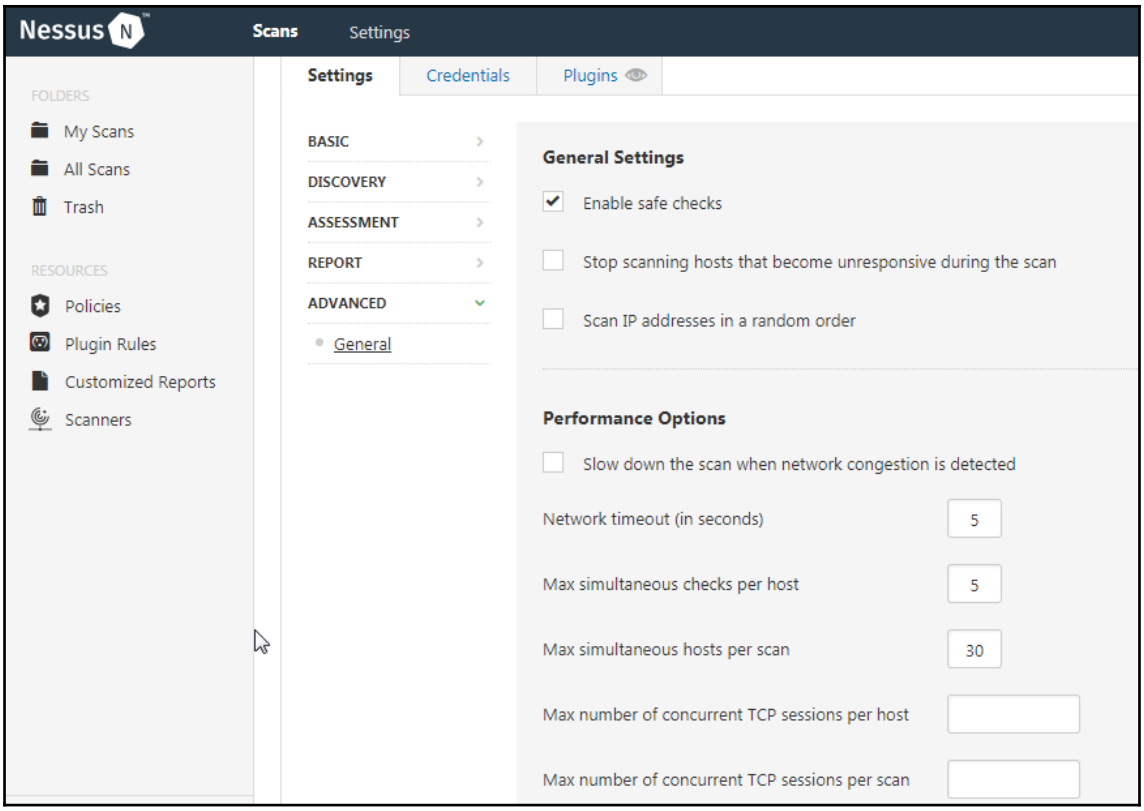

https://localhost:8834/#/settings/about
Certificate error
Search...
Nessus Professional / Settin...
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
ACCOUNTS
My Account
About
Overview
Software Update
Master Password
Nessus Professional Version 7
Version
7.2.1 (#144) WINDOWS
Licensed Hosts
None
Plugins
Last Updated
September 14 at 8:50 PM
License Expiration
September 30, 2018
Plugin Set
201809142050
Activation Code
Update activation code

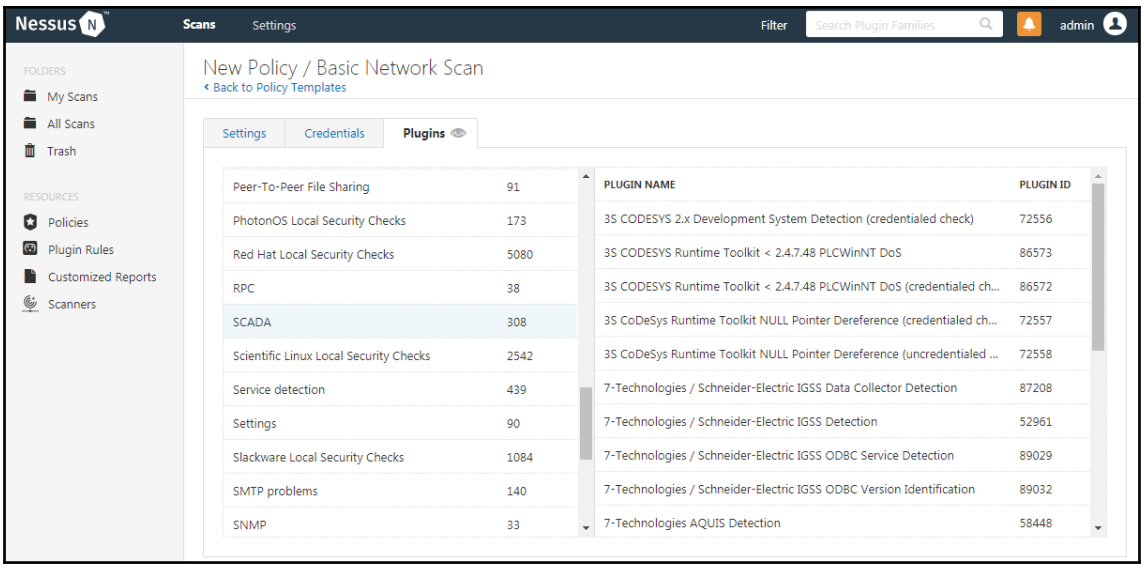

https://localhost:8834/#/settings/about
Certificate error
Search...
Nessus Professional / Settin...
Nessus
Scans
Settings
admin
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
Upgrade Assistant
Password Mgmt
ACCOUNTS
My Account
About
Overview
Software Update
Master Password
Nessus Professional Version 7
Plugins
Version
Licensed Hosts
Update Activation Code
Registration
Nessus (Home, Professional or Manager)
Activation Code
Activate
Cancel

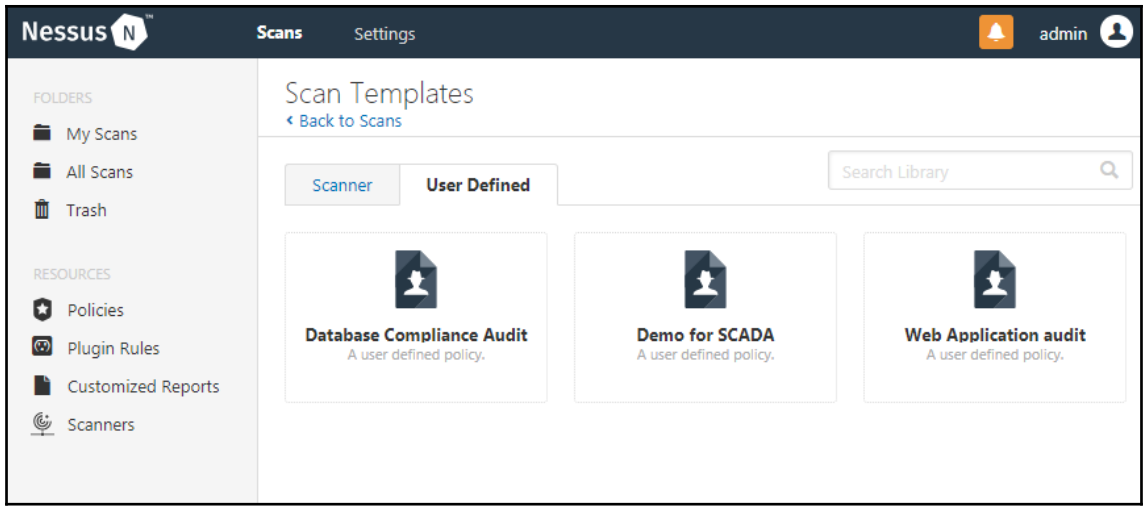

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Demo for SCADA
Description
Save
Cancel

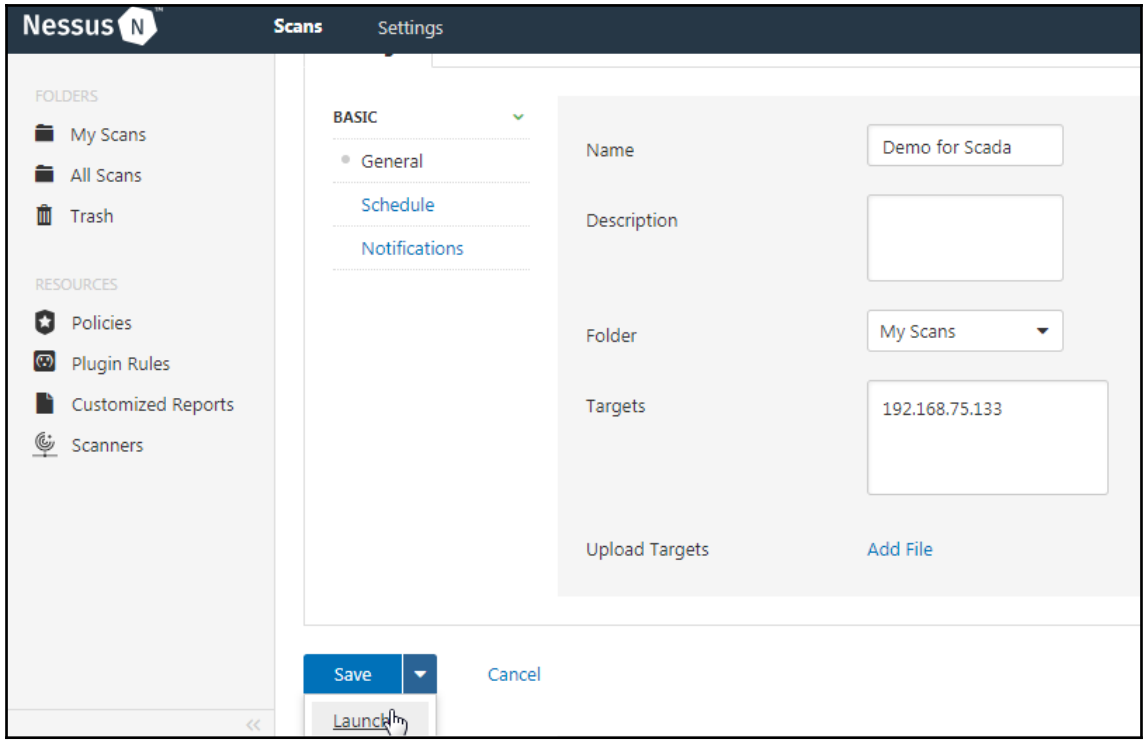

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Ports
Consider unscanned ports as closed
Port scan range:
0-1000
Local Port Enumerators
SSH (netstat)
WMI (netstat)
SNMP
Only run network port scanners if local port enumeration failed
Verify open TCP ports found by local port enumerators

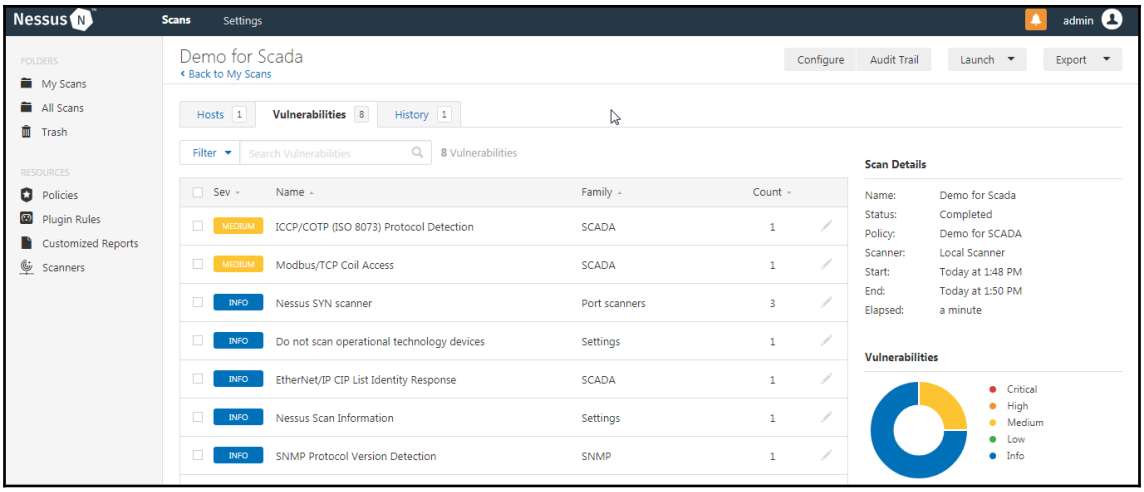

Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
General
Brute Force
Web Applications
Windows
REPORT
ADVANCED
Accuracy
Override normal accuracy
Avoid potential false alarms
Show potential false alarms
Perform thorough tests (may disrupt your network or impact scan speed)
Save
Cancel

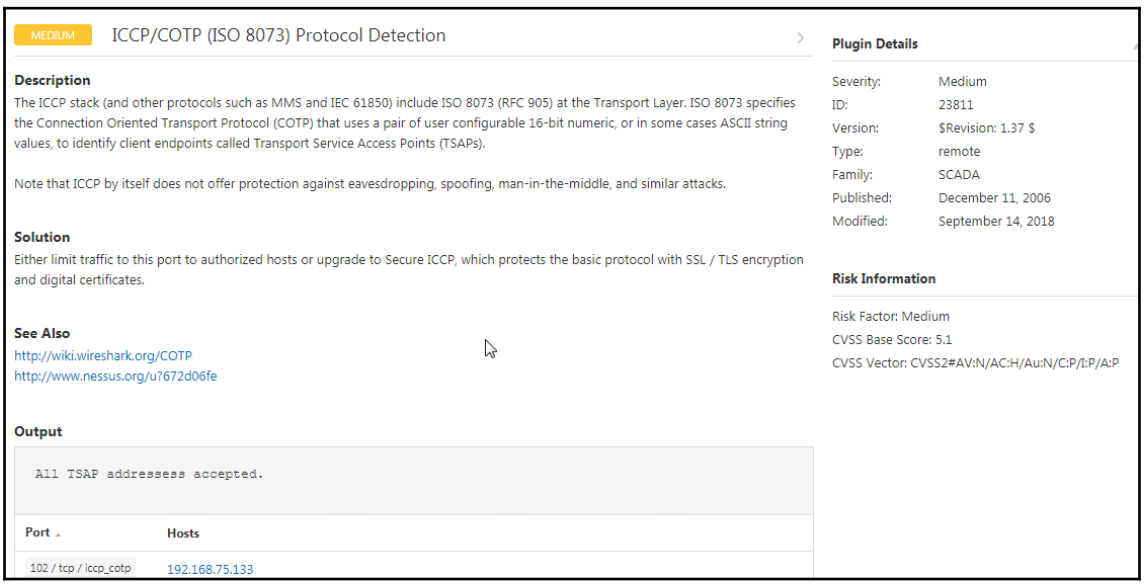

Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
General
General Settings
Enable safe checks
Stop scanning hosts that become unresponsive during the scan
Scan IP addresses in a random order
Performance Options
Slow down the scan when network congestion is detected
Network timeout (in seconds)
5
Max simultaneous checks per host
5
Max simultaneous hosts per scan
30
Max number of concurrent TCP sessions per host
Max number of concurrent TCP sessions per scan

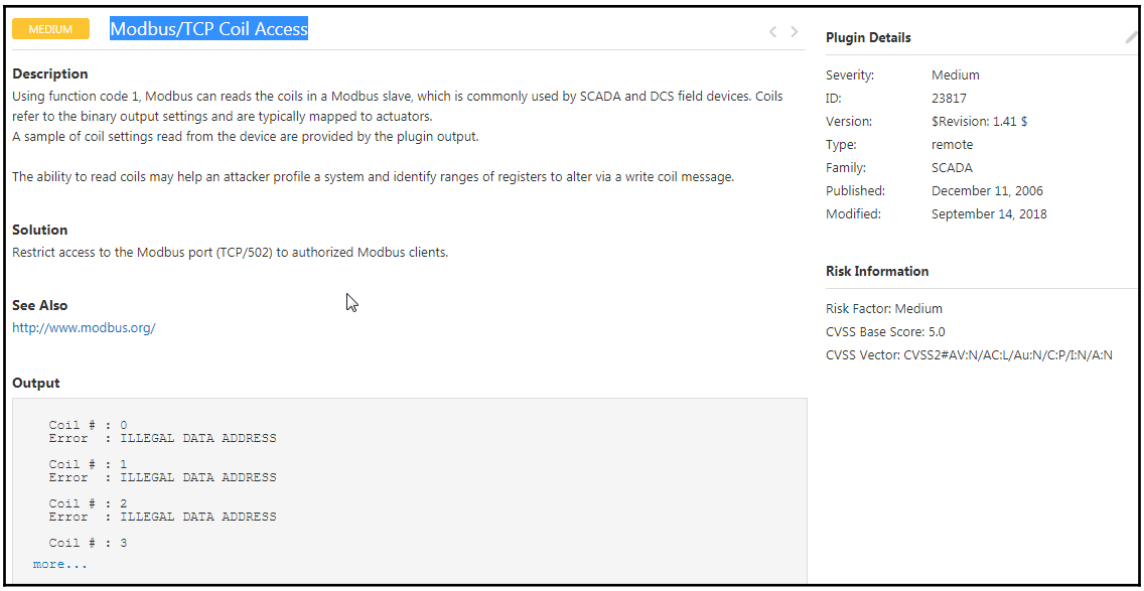

Nessus
Scans
Settings
Filter
Search Plugin Families
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Policy / Basic Network Scan
Back to Policy Templates
Settings
Credentials
Plugins
Peer-To-Peer File Sharing 91
PhotonOS Local Security Checks 173
Red Hat Local Security Checks 5080
RPC 38
SCADA 308
Scientific Linux Local Security Checks 2542
Service detection 439
Settings 90
Slackware Local Security Checks 1084
SMTP problems 140
SNMP 33
PLUGIN NAME
PLUGIN ID
3S CODESYS 2.x Development System Detection (credentialed check) 72556
3S CODESYS Runtime Toolkit < 2.4.7.48 PLCWinNT DoS 86573
3S CODESYS Runtime Toolkit < 2.4.7.48 PLCWinNT DoS (credentialed ch... 86572
3S CoDeSys Runtime Toolkit NULL Pointer Dereference (credentialed ch... 72557
3S CoDeSys Runtime Toolkit NULL Pointer Dereference (uncredentialed ... 72558
7-Technologies / Schneider-Electric IGSS Data Collector Detection 87208
7-Technologies / Schneider-Electric IGSS Detection 52961
7-Technologies / Schneider-Electric IGSS ODBC Service Detection 89029
7-Technologies / Schneider-Electric IGSS ODBC Version Identification 89032
7-Technologies AQUIS Detection 58448


Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
Database Compliance Audit
A user defined policy.
Demo for SCADA
A user defined policy.
Web Application audit
A user defined policy.


Nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
BASIC
General
Schedule
Notifications
Name
Demo for Scada
Description
Folder
My Scans
Targets
192.168.75.133
Upload Targets
Add File
Save
Cancel
Launch


Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Demo for Scada
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 1
Vulnerabilities 8
History 1
Filter
Search Vulnerabilities
8 Vulnerabilities
Sev
Name
Family
Count
MEDIUM ICCP/COTP (ISO 8073) Protocol Detection SCADA 1
MEDIUM Modbus/TCP Coil Access SCADA 1
INFO Nessus SYN scanner Port scanners 3
INFO Do not scan operational technology devices Settings 1
INFO EtherNet/IP CIP List Identity Response SCADA 1
INFO Nessus Scan Information Settings 1
INFO SNMP Protocol Version Detection SNMP 1
Scan Details
Name: Demo for Scada
Status: Completed
Policy: Demo for SCADA
Scanner: Local Scanner
Start: Today at 1:48 PM
End: Today at 1:50 PM
Elapsed: a minute
Vulnerabilities
Critical
High
Medium
Low
Info


MEDIUM
ICCP/COTP (ISO 8073) Protocol Detection
Description
The ICCP stack (and other protocols such as MMS and IEC 61850) include ISO 8073 (RFC 905) at the Transport Layer. ISO 8073 specifies the Connection Oriented Transport Protocol (COTP) that uses a pair of user configurable 16-bit numeric, or in some cases ASCII string values, to identify client endpoints called Transport Service Access Points (TSAPs).
Note that ICCP by itself does not offer protection against eavesdropping, spoofing, man-in-the-middle, and similar attacks.
Solution
Either limit traffic to this port to authorized hosts or upgrade to Secure ICCP, which protects the basic protocol with SSL / TLS encryption and digital certificates.
See Also
http://wiki.wireshark.org/COTP
http://www.nessus.org/u?672d06fe
Output
All TSAP addressess accepted.
Port
Hosts
102 / tcp / iccp_cotp
192.168.75.133
Plugin Details
Severity: Medium
ID: 23811
Version: $Revision: 1.37 $
Type: remote
Family: SCADA
Published: December 11, 2006
Modified: September 14, 2018
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.1
CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P


MEDIUM
Modbus/TCP Coil Access
Description
Using function code 1, Modbus can reads the coils in a Modbus slave, which is commonly used by SCADA and DCS field devices. Coils refer to the binary output settings and are typically mapped to actuators.
A sample of coil settings read from the device are provided by the plugin output.
The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.
Solution
Restrict access to the Modbus port (TCP/502) to authorized Modbus clients.
See Also
http://www.modbus.org/
Output
Coil # : 0
Error : ILLEGAL DATA ADDRESS
Coil # : 1
Error : ILLEGAL DATA ADDRESS
Coil # : 2
Error : ILLEGAL DATA ADDRESS
Coil # : 3
more...
Plugin Details
Severity: Medium
ID: 23817
Version: $Revision: 1.41 $
Type: remote
Family: SCADA
Published: December 11, 2006
Modified: September 14, 2018
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N


root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
M S F
=[metasploit v4.16.7-dev]
+ -- --=[1683 exploits - 964 auxiliary - 299 post]
+ -- --=[498 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]

```
msf > search scada
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/admin/http/scadabr_credential_dump          2017-05-28       normal     ScadaBR Credentials Dumper
   auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli  2014-04-08   normal     Advantech WebAccess DBVisitor.dll ChartThemeConf
ig SQL Injection
   auxiliary/admin/scada/ge_proficy_substitute_traversal  2013-01-22      normal     GE Proficy Cimplicity WebView substitute.bcl Dir
ectory Traversal
   auxiliary/admin/scada/modicon_command                 2012-04-05       normal     Schneider Modicon Remote START/STOP Command
   auxiliary/admin/scada/modicon_password_recovery       2012-01-19       normal     Schneider Modicon Quantum Password Recovery
   auxiliary/admin/scada/modicon_stux_transfer           2012-04-05       normal     Schneider Modicon Ladder Logic Upload/Download
   auxiliary/admin/scada/moxa_credentials_recovery       2015-07-28       normal     Moxa Device Credential Retrieval
   auxiliary/admin/scada/multi_cip_command               2012-01-19       normal     Allen-Bradley/Rockwell Automation EtherNet/IP CI
P Commands
   auxiliary/admin/scada/phoenix_command                 2015-05-20       normal     PhoenixContact PLC Remote START/STOP Command
   auxiliary/admin/scada/yokogawa_bkbcopyd_client        2014-08-09       normal     Yokogawa BKBCopyD.exe Client
```

```
msf > search modbus
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   auxiliary/admin/scada/modicon_command         2012-04-05       normal  Schneider Modicon Remote START/STOP Command
   auxiliary/admin/scada/modicon_stux_transfer   2012-04-05       normal  Schneider Modicon Ladder Logic Upload/Download
   auxiliary/scanner/scada/modbus_findunitid     2012-10-28       normal  Modbus Unit ID and Station ID Enumerator
   auxiliary/scanner/scada/modbusclient                           normal  Modbus Client Utility
   auxiliary/scanner/scada/modbusdetect          2011-11-01       normal  Modbus Version Scanner
```

```
msf > use auxiliary/scanner/scada/modbusdetect
msf auxiliary(modbusdetect) > show options

Module options (auxiliary/scanner/scada/modbusdetect):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      502              yes       The target port (TCP)
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    10               yes       Timeout for the network probe
   UNIT_ID    1                yes       ModBus Unit Identifier, 1..255, most often 1

msf auxiliary(modbusdetect) >
```

```
msf auxiliary(modbusdetect) > set RHOSTS 192.168.75.133
RHOSTS => 192.168.75.133
msf auxiliary(modbusdetect) > exploit

[+] 192.168.75.133:502    - 192.168.75.133:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(modbusdetect) >
```