Hacking OPEN

Vol.2 No.6
Issue 1/2014 (6) ISSN: 1733-7186

KALI LINUX

HOW TO INSTALL BACKTRACK 5 R3 ON VMWARE WORKSTATION 8

HOW TO USE NMAP

HOW TO USE NETMASK IN KALI LINUX

HOW TO USE SSLSTRIP

Dr.Web 9.0

for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search

www.drweb.com

Free 30-day trial: https://download.drweb.com

New features in Dr.Web 9.0 for Windows: http://products.drweb.com/9

FREE bonus — Dr.Web Mobile Security:
https://download.drweb.com/android

Accelerating Mobile Apps Growth

TapReason.com

TapReason

Kali Linux

Table of Contents

Dear Readers,

We are happy to present you another issue of Hakin9 Open. This time all of the articles are dedicated to the most known Linux distribution – Kali Linux. We are sure all of you know that this BackTrack successor is a great pentesting tool. We hope that our tutorials will help you to gain professional knowledge which will allow you to dive into deep water of hacking and pentesting.

In this very new issue you will find articles on how to use different tools on Kali Linux. This time you will deal with Nmap, Netmask, Ssldump, Sslstrip, and Uniscan. You will also learn how to install Backtrack 5 R3 on VMware workstation 8.

We would also like to thank to our friends from PenTest Magazine. We appreciate their help and we would like to invite you to visit their website pentestmag.com.

We wish you a good reading!

Ewelina Nazarczuk
Hakin9 Magazine Junior Product Manager
and Hakin9 Team

Editor in Chief: Ewelina Nazarczuk
ewelina.nazarczuk@hakin9.org

Editorial Advisory Board: John Webb, Marco Hermans, Gareth Watters, Peter Harmsen, Dhawal Desai, Kishore PV, Bamidele Ajayi

Proofreaders: Jeff Smith, Krzysztof Samborski

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic.@hakin9.org

Product Manager: Ewa Duranc
ewa.duranc@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Art. Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org
DTP: Ireneusz Pogroszewski

Marketing Director: Ewelina Nazarczuk
ewelina.nazarczuk@hakin9.org

Publisher: Hakin9 Media sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
NIP 95123253396
www.hakin9.org/en

How to Install Backtrack 5 R3 on VMware Workstation

by Rrajesh Kumar

With this article you will get knowledge on how to instal BackTrack 5. But this time installation will be launched on Virtual Machine (VMWare).

Step 1.

Go to *File* and click on *New Virtual Machine* (Figure 1).

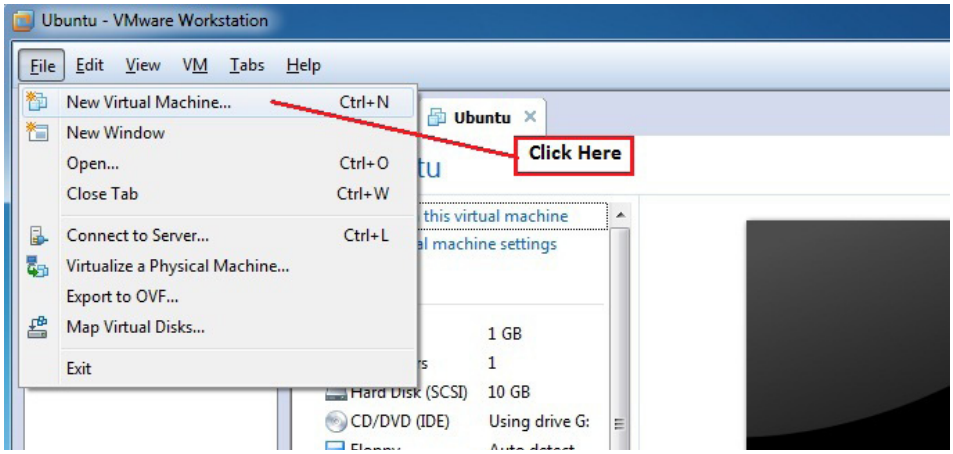


Figure 1. Creating a new virtual machine

Step 2.

Select *Typical* and click *Next* (Figure 2).

Figure 2. Selecting the type of configuration

Step 3.

Select DVD drive or ISO and click *Next* (Figure 3).

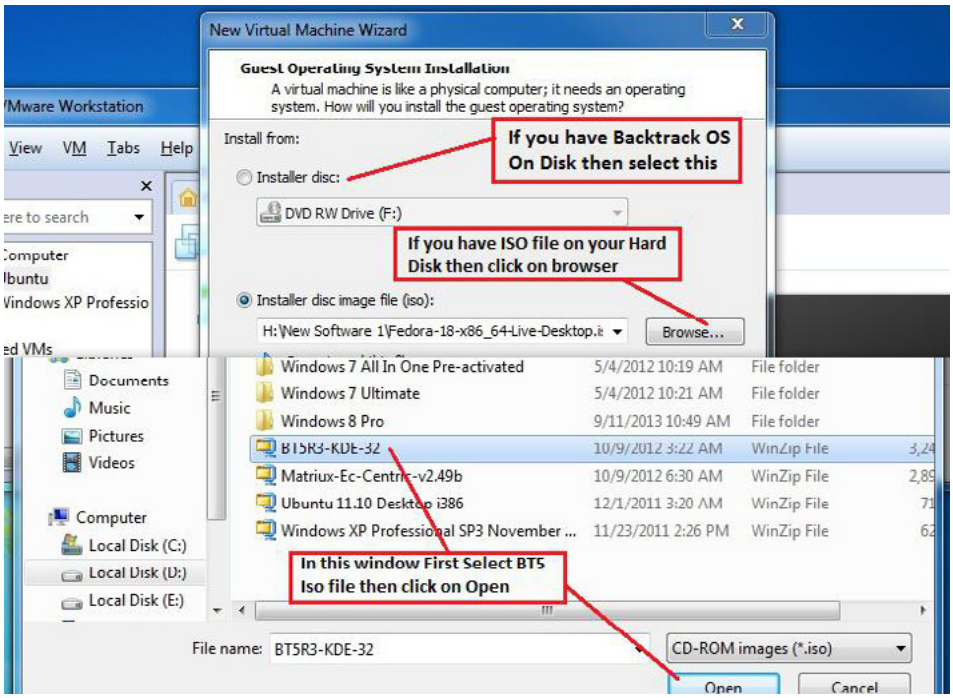


Figure 3. Selecting the information source

Step 4.

Click on *Next* (Figure 4).

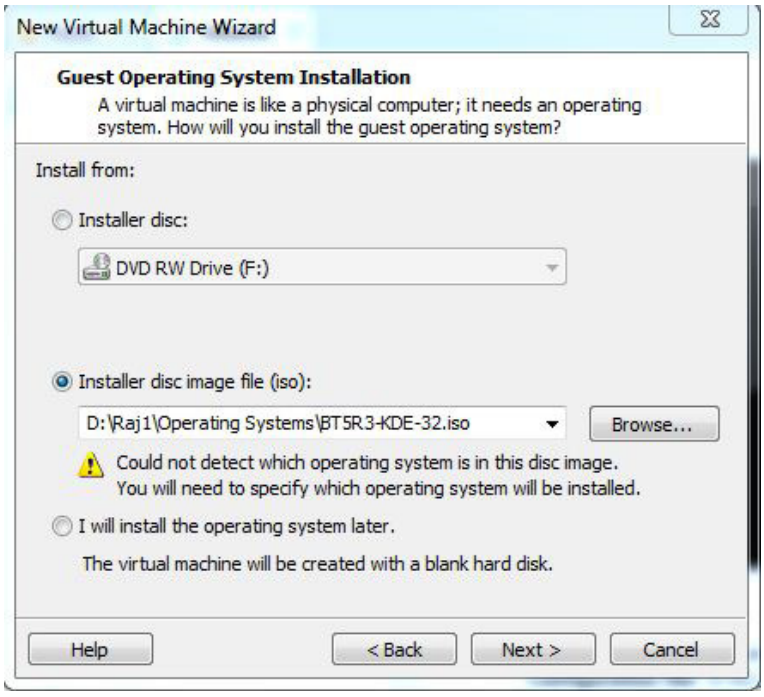


Figure 4. Continuing installation

Step 5.

Select *Linux*, choose your OS version (Ubuntu), and click *Next* (Figure 5).

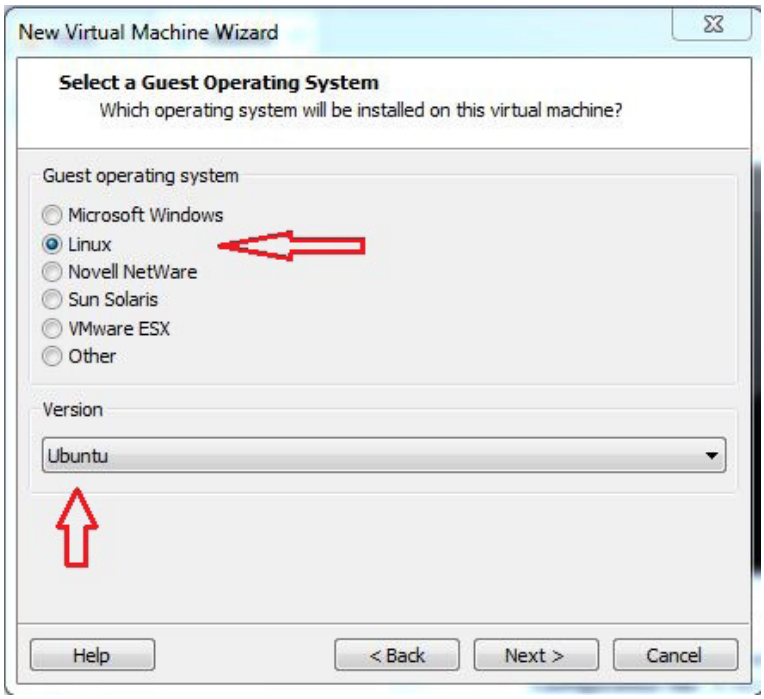


Figure 5. Specifying the OS that will be installed

Step 6.

You can change your virtual machine name and choose where do you want to install your OS (Figure 6).

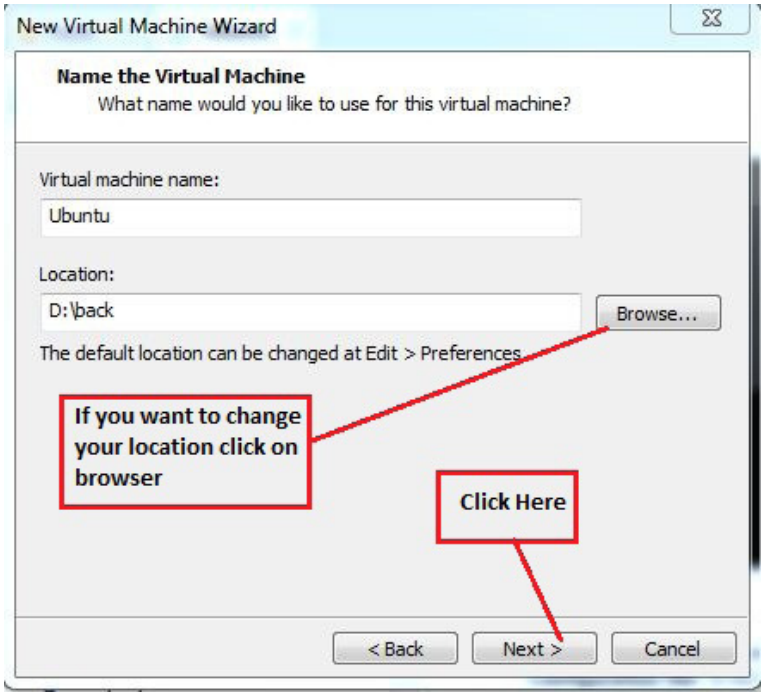


Figure 6. Setting the name and installation path

Step 7.

Change your OS installation disk size (it should be more than 20 GB) and click *Next* (Figure 7).

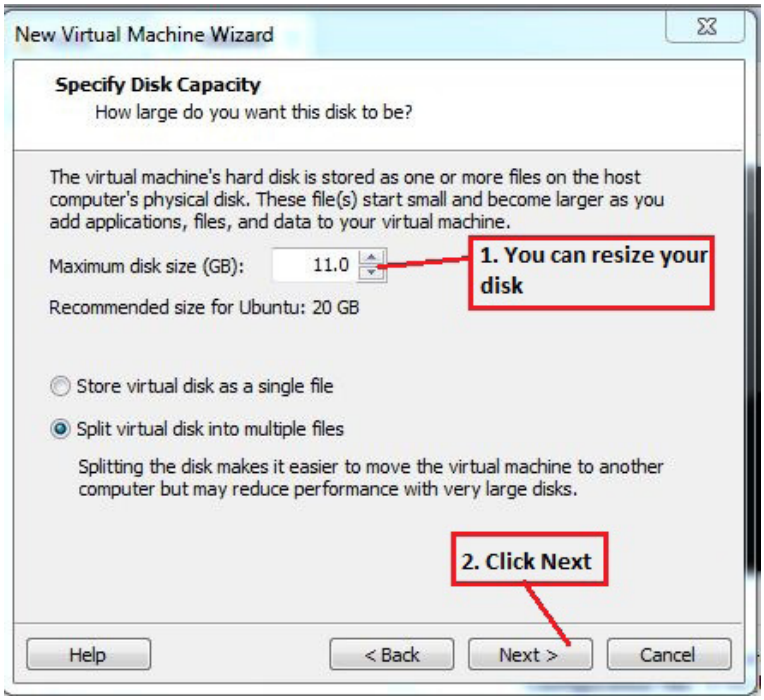


Figure 7. Changing installation disk size

Step 8.

Click on *Finish* (Figure 8).

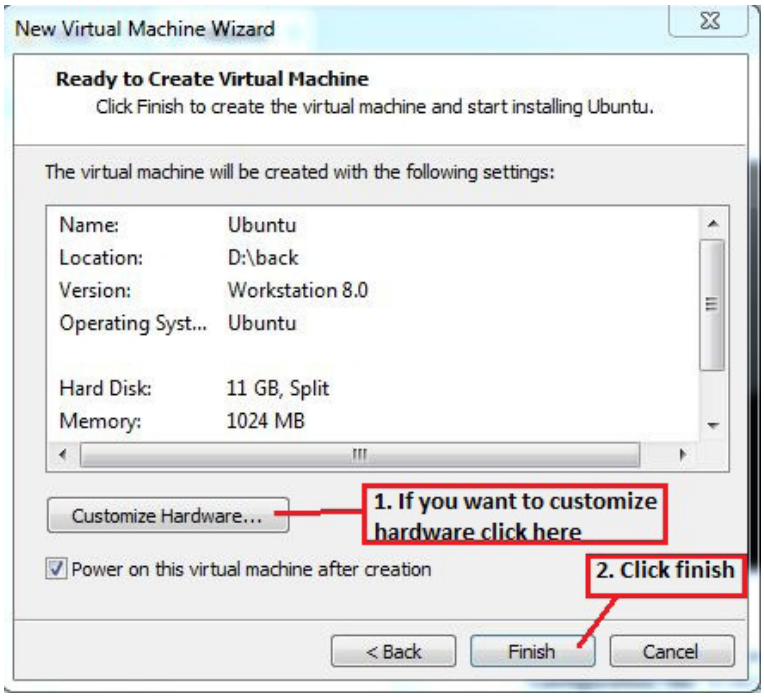


Figure 8. Ready to create the VM

Step 9.

Select *Text Mode* and hit *Enter* (Figure 9).

Figure 9. Boot mode select

Step 10.

After booting your ISO, a screen similar to Figure 10 will show. Type `startx` and hit *Enter*.

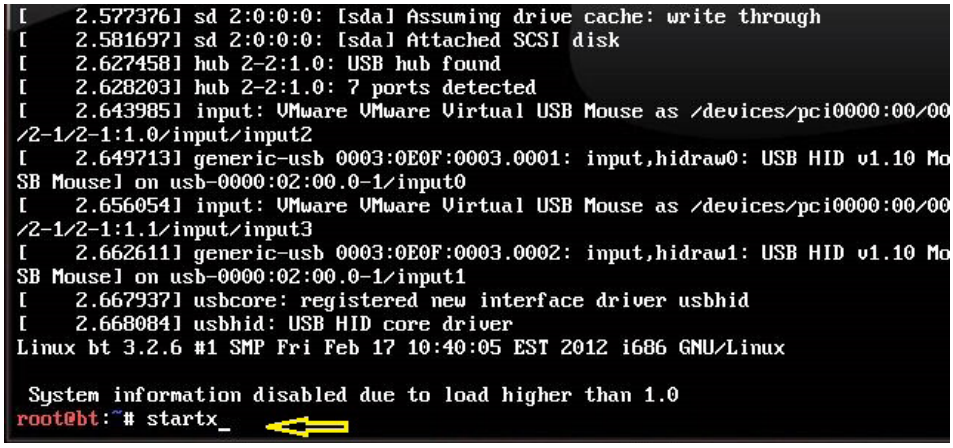


Figure 10. Screen visible after booting.

Step 11.

Loading (Figure 11).

Figure 11. Loading

Step 12.

Right click on the *Install BackTrack* icon and click *Open* (Figure 12).

Figure 12. Opening installation

Step 13.

Click *Forward* (Figure 13).

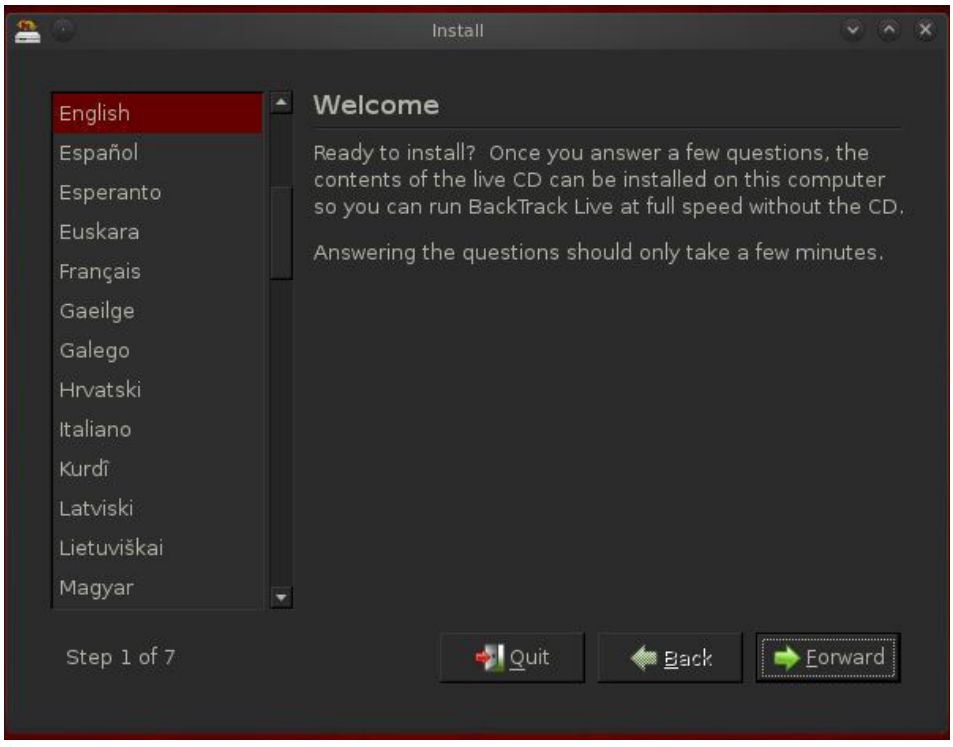


Figure 13. Step 1 – starting installation

Step 14.

Click *Forward* (Figure 14).

Figure 14. Choosing your location

Step 15.

Click *Forward* (Figure 15).

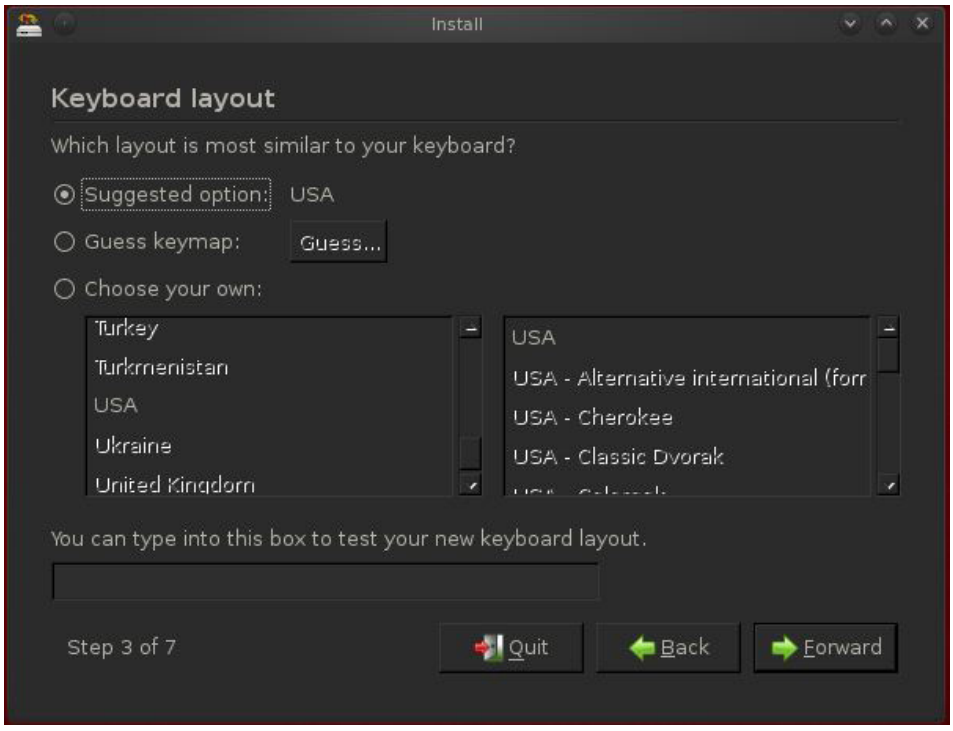


Figure 15. Keyboard layout selection

Step 16.

Here, we are choosing *Erase and use entire disk* because we have created a separate partition for our BT OS installation. This is good for installing OS on VMware. Click on *Forward* (Figure 16).

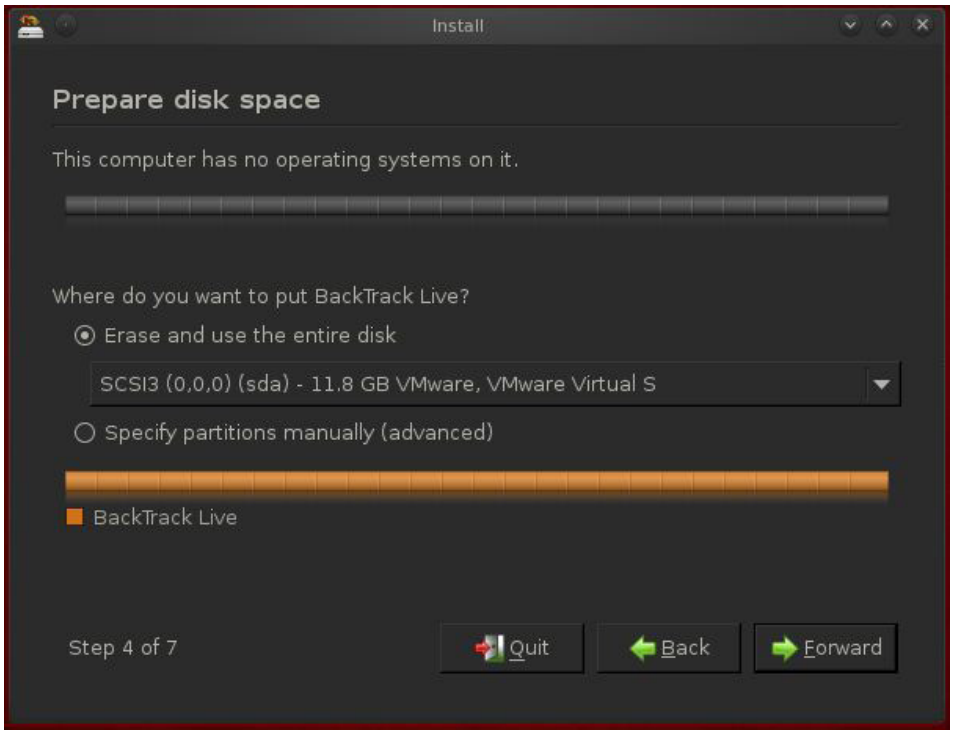


Figure 16. Preparing disk space

Step 17.

Click on *Install* (Figure 17).

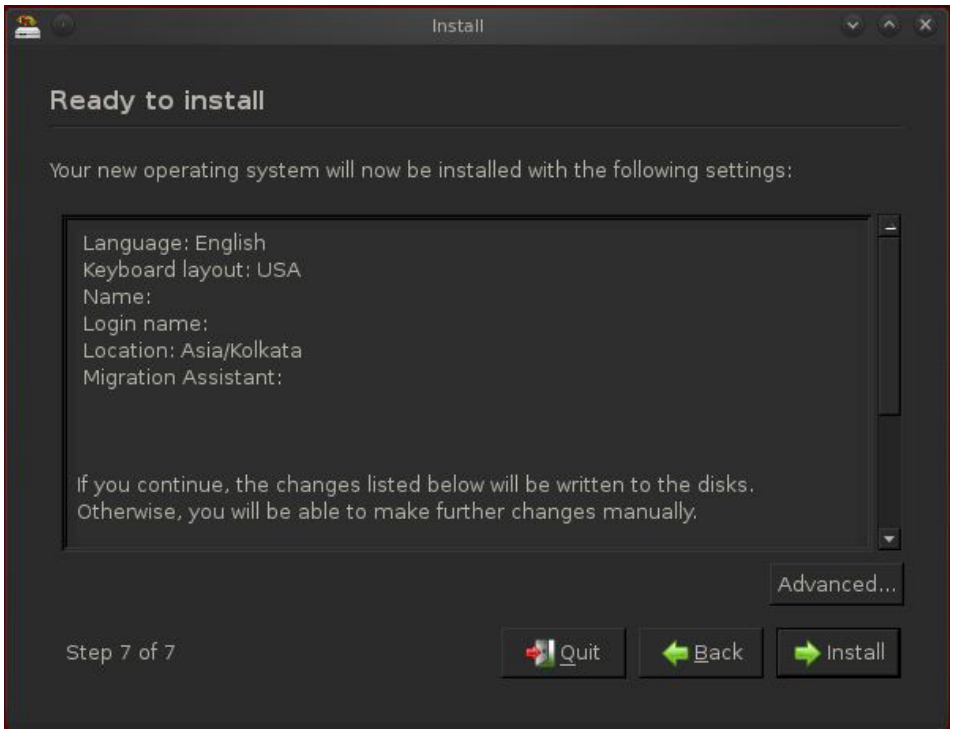


Figure 17. Ready to install

Step 18.

Installation starts (Figure 18).

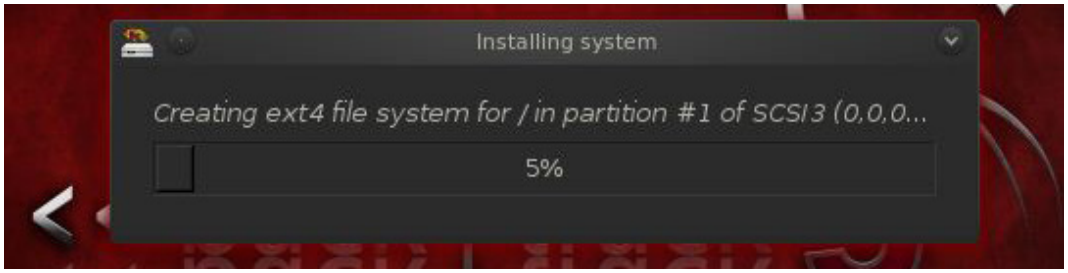


Figure 18. Installation starts

Step 19.

Installation completed. Click on *Restart Now* (Figure 19).

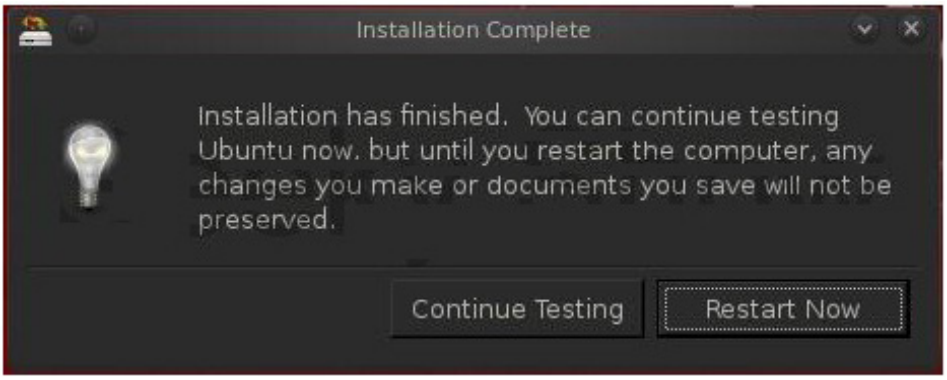


Figure 19. Installation complete

Step 20.

Now login with root and hit *Enter*. Our password will be `toor` (Figure 20).

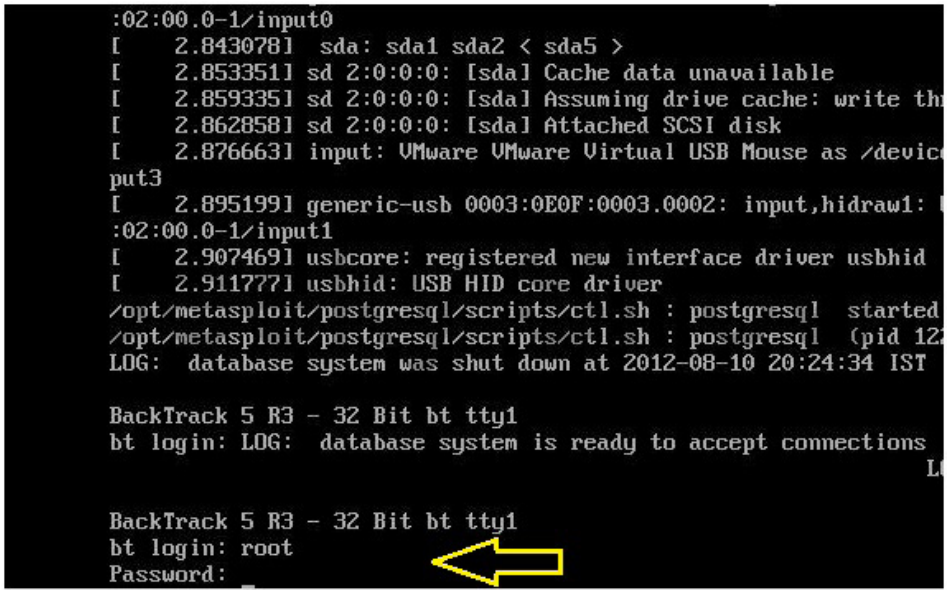


Figure 20. Setting login and password

Step 21.

Write `startx` and hit *Enter* (Figure 21).

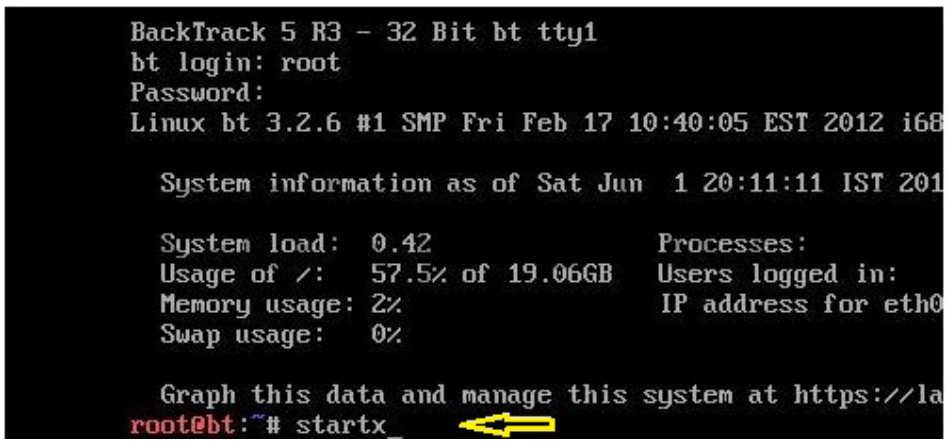


Figure 21. startx

Step 22.

Now, right click and delete the installation icon form your desktop (Figure 22).

Figure 22. Deleting the installation icon

Become a Big Data Master!

Over 45 HOW-TO, practical classes and tutorials to choose from!

Attend The 3rd Big Data TechCon!

The HOW-TO technical conference for professionals implementing Big Data



Come to Big Data TechCon to learn the best ways to:

- Process and analyze the real-time data pouring into your organization.
- Learn HOW TO integrate data collection technologies with data analytics and predictive analysis tools to produce the kind of workable information and reports your organization needs.
- Understand HOW TO leverage Big Data to help your organization today.
- Master Big Data tools and technologies like Hadoop, MapReduce, HBase, Cassandra, NoSQL databases, and more!
- Looking for Hadoop training? We have several Hadoop tutorials and dozens of Hadoop classes to get you started — or advanced classes to take you to the next level!

Big Data TECHCON Boston

March 31-April 2, 2014

www.BigDataTechCon.com

A BZ Media Event Big Data TechCon

How to Use Netmask in Kali Linux

by Rrajesh Kumar

Netmask is another simple tool which does one thing and that is, makes a ICMP netmask request. By determining the netmasks of various computers on a network, you can better map your subnet structure (www.question-defense.com).

Step 1. How to open

A. GUI Method (Figure 1).

Applications →Kali Linux → Information Gathering → Route Analysis → netmask

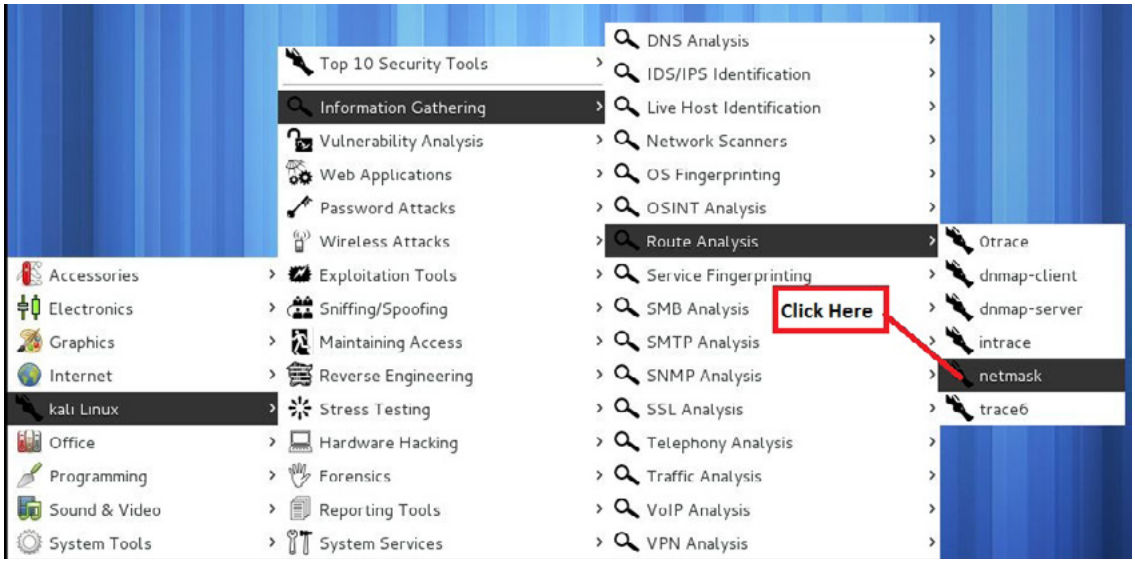


Figure 1. Opening netmask in the GUI

B. Open the terminal and type `netmask -h`. This command will open netmask with help options (Figure 2).

```
root@MrQuiety:~# netmask -h
This is netmask, an address netmask generation utility
Usage: netmask spec [spec ...]
  -h, --help                  Print a summary of the options
  -v, --version               Print the version number
  -d, --debug                 Print status/progress information
  -s, --standard              Output address/netmask pairs
  -c, --cidr                  Output CIDR format address lists
  -i, --cisco                 Output Cisco style address lists
  -r, --range                 Output ip address ranges
  -x, --hex                   Output address/netmask pairs in hex
  -o, --octal                 Output address/netmask pairs in octal
  -b, --binary                Output address/netmask pairs in binary
  -n, --nodns                 Disable DNS lookups for addresses
Definitions:
  a spec can be any of:
    address
    address:address
    address:+address
    address/mask
  an address can be any of:
    N           decimal number
    0N          octal number
    0xN         hex number
```

Figure 2. Opening netmask in the terminal

Step 2.

`-v` – this command is used to see the netmask version which is installed in your system (Figure 3).

Syntax – `netmask -v`

Figure 3. Checking the netmask version

Step 3.

This is the default search for a domain or IP (Figure 4).

Syntax – `netmask domain/IP`

Example – `netmask google.com`

Example – `netmask 192.168.237.129`

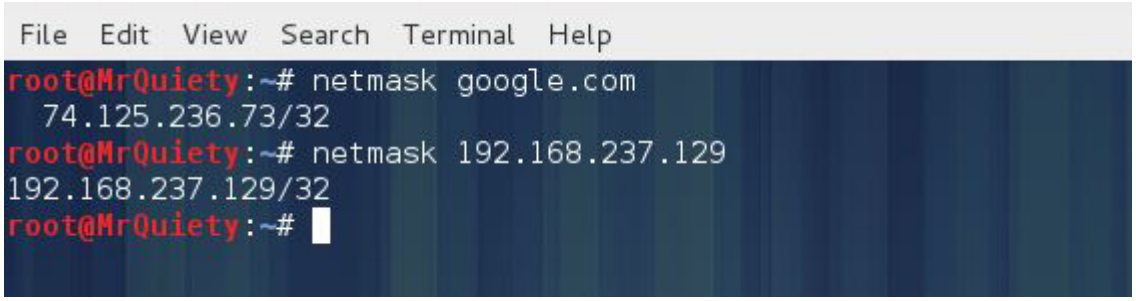


Figure 4. Search for domain or IP

Step 4.

Output address/netmask pairs (Figure 5).

Syntax – `netmask -s domain/IP`

Example – `netmask -s google.com`

Example – `netmask -s 192.168.237.129`

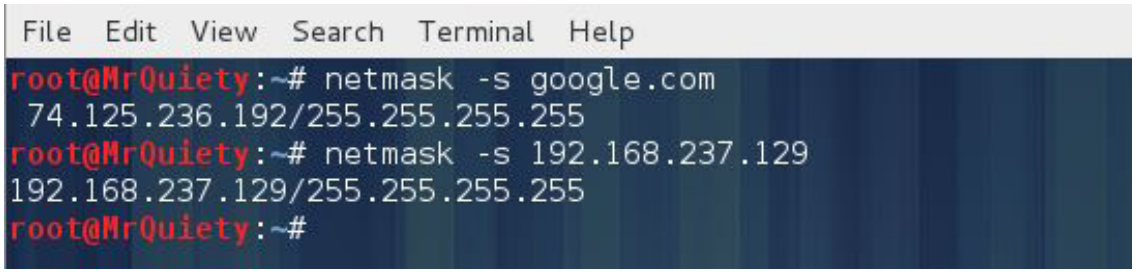


Figure 5. Output address/netmask pairs

Step 5.

Output CIDR format address lists (Figure 6).

Syntax – `netmask -c domain/IP`

Example – `netmask -c google.com`

Example – `netmask -c 192.168.237.129`

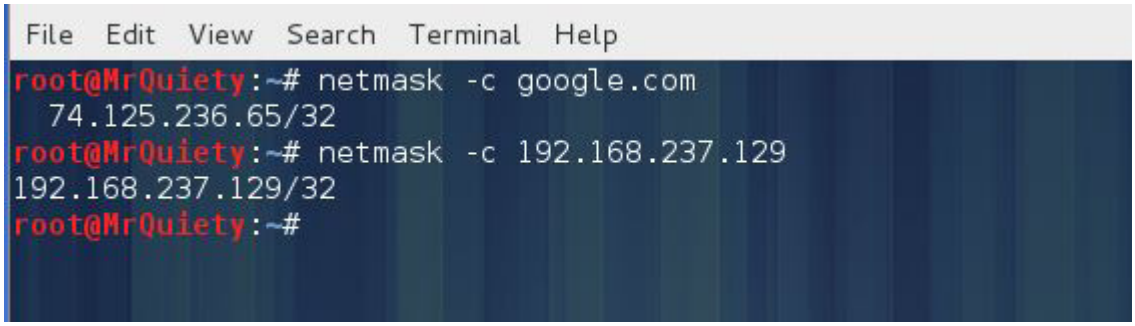


Figure 6. Output CIDR format address lists

Step 6.

Output Cisco style address lists (Figure 7).

Syntax – `netmask -i domain/IP`

Example – `netmask -i google.com`

Example – `netmask -i 192.168.237.129`

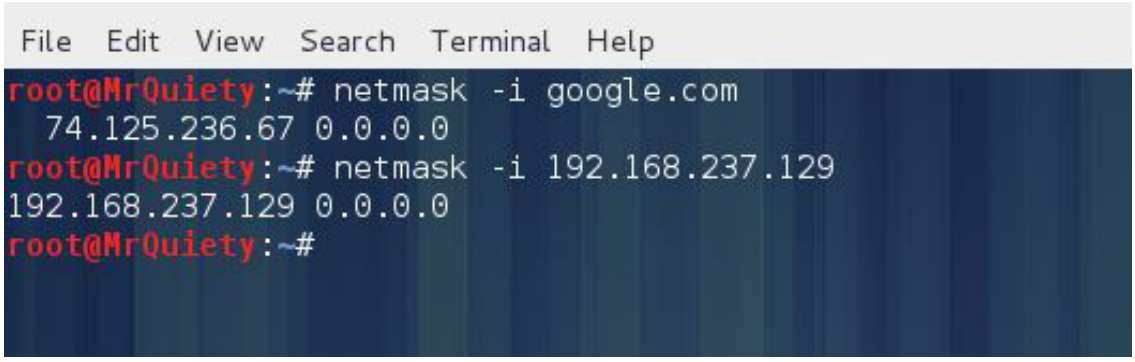


Figure 7. Output Cisco style address lists

Step 7.

Output IP address ranges (Figure 8).

Syntax – `netmask -r domain/IP`

Example – `netmask -r google.com`

Example – `netmask -r 192.168.237.129`

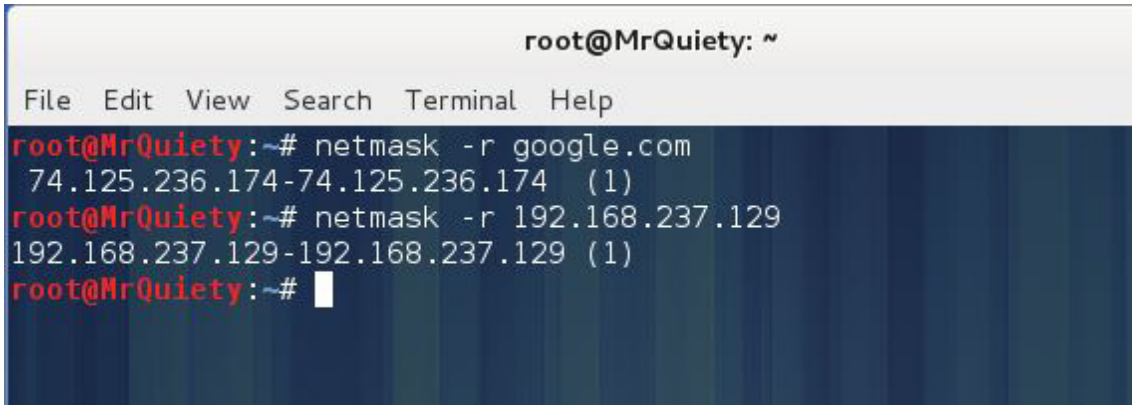


Figure 8. Output IP address ranges

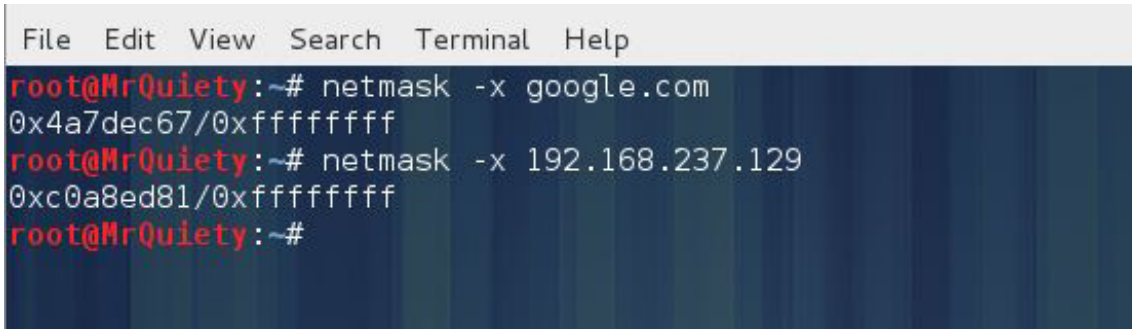


Figure 9. Output address/netmask pairs in hex

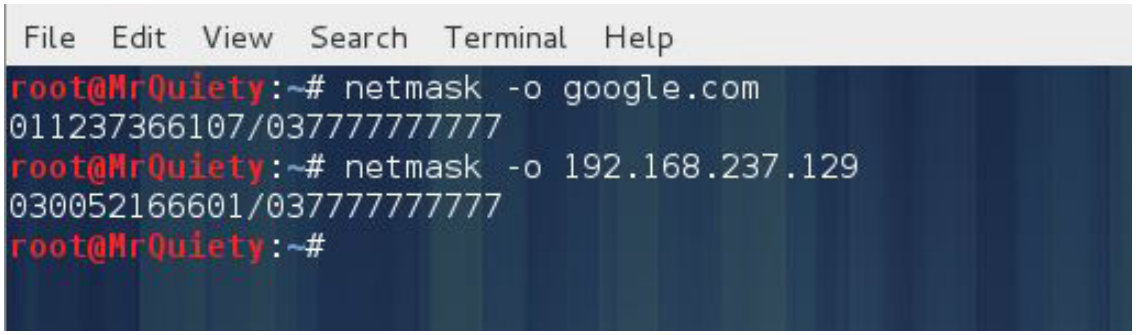


Figure 10. Output address/netmask pairs in octal

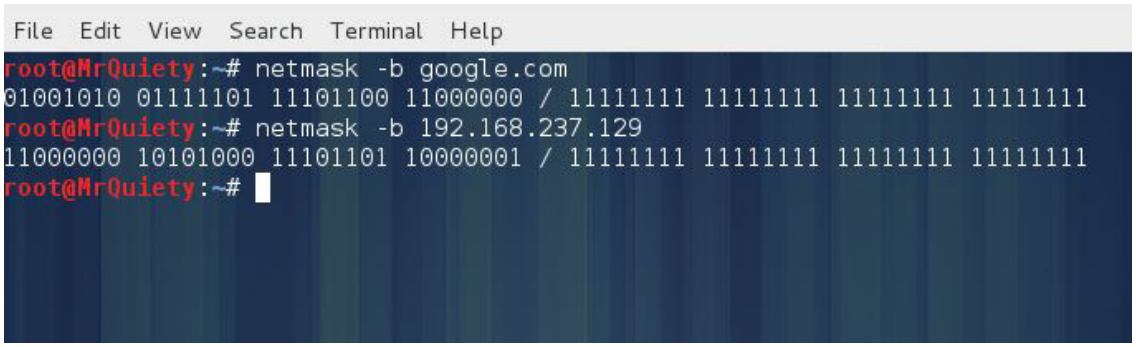


Figure 11. Output address/netmask pairs in binary

How to Use Nmap in Kali Linux

by Rrajesh Kumar

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime (nmap.org).

Step 1. How to open nmap

A. GUI method (Figure 1).

Applications → Information Gathering → DNS Analysis → nmap

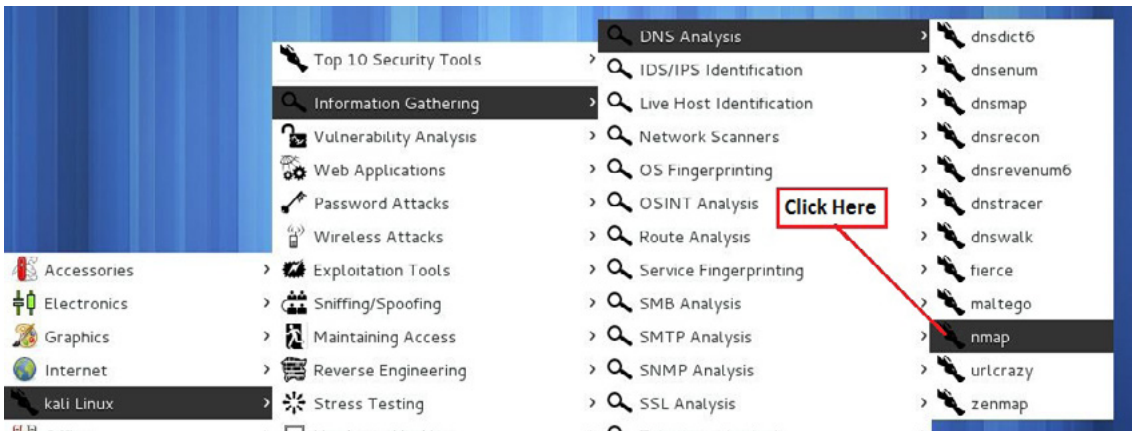


Figure 1. Opening nmap in the GUI

B. Open the terminal, type nmap, and hit *Enter* (Figure 2).

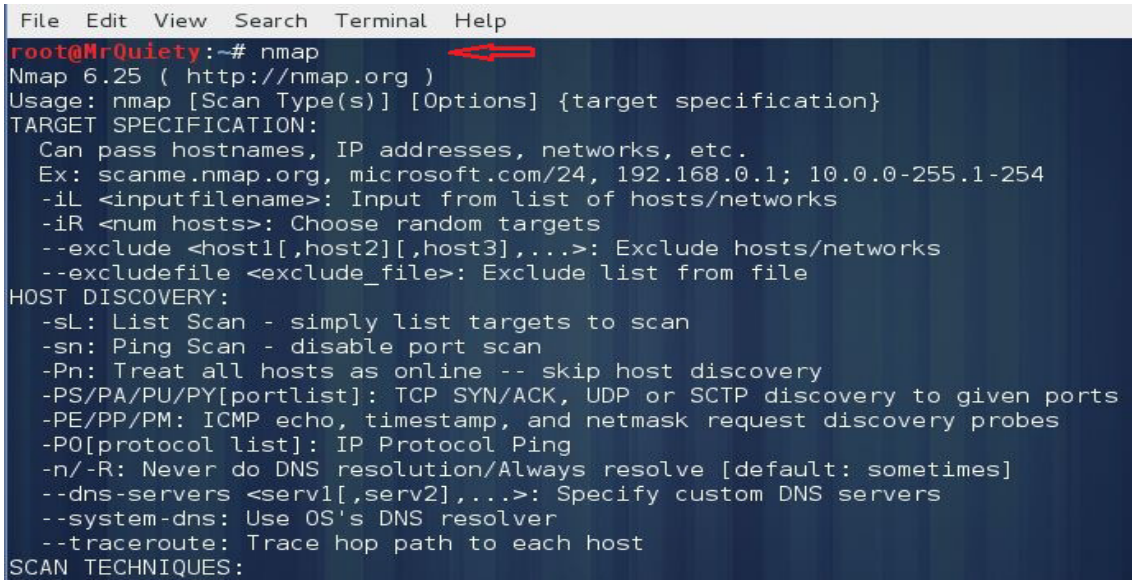


Figure 2. Opening nmap in the terminal

Step 2.

Scan a single IP address when the firewall is OFF/ON on the target PC (Figure 3).

Syntax – `nmap IP address/hostname`

Example – `nmap 192.168.237.129`

Example – `nmap google.com`

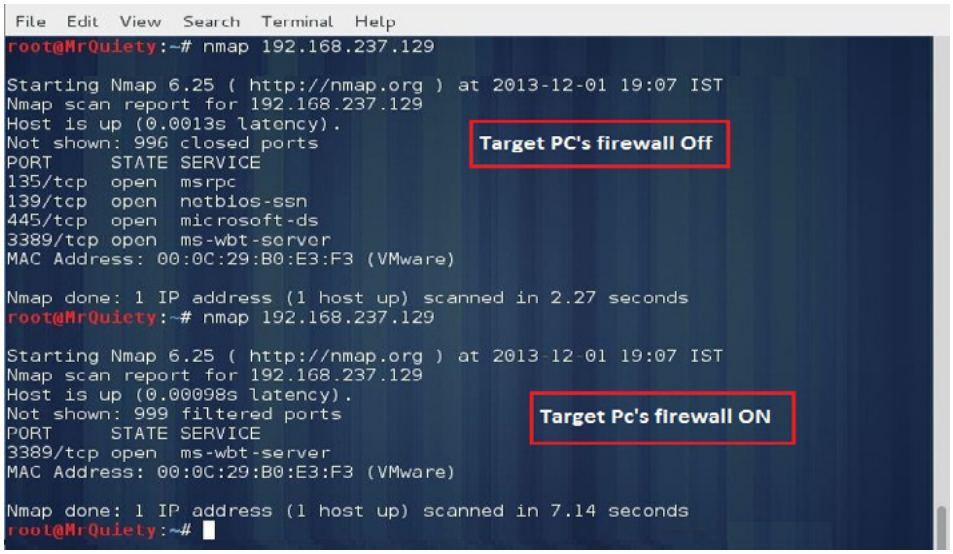


Figure 3. Scanning a single IP address with the firewall ON/OFF

Step 3.

Boost up your nmap scan – using this command you can decrease scan time (Figure 4).

Syntax – `nmap -F IP address`

Example – `nmap -F 192.168.237.129`

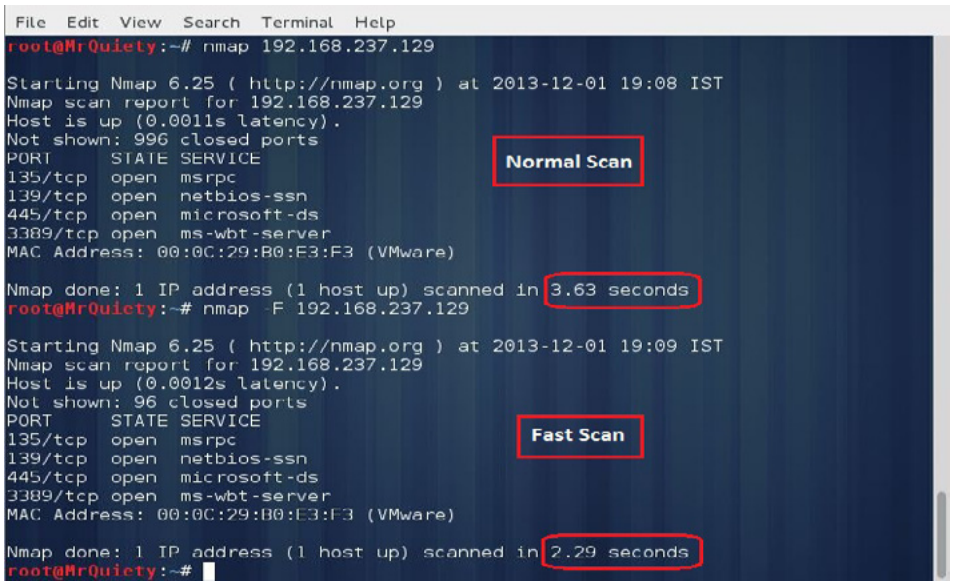


Figure 4. Decreasing scan time

Step 4.

Scan multiple IP addresses or subnet.

A. Scan a range of IP addresses (Figure 5).

Syntax – `nmap IP address range`

Example – `nmap 192.168.237.1-130`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap 192.168.237.1-130

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:10 IST
Nmap scan report for 192.168.237.1
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.237.2
Host is up (0.00074s latency).
Not shown: 999 closed ports
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:ED:D4:DE (VMware)

Nmap scan report for 192.168.237.128
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.237.128 are closed

Nmap scan report for 192.168.237.129
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 130 IP addresses (4 hosts up) scanned in 11.80 seconds
```

Figure 5. Scanning a range of IPs

B. Scan a range of IP addresses using a wildcard (Figure 6).

Example – `nmap 192.168.237.*`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap 192.168.237.*

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:12 IST
Nmap scan report for 192.168.237.1
Host is up (0.0073s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.237.2
Host is up (0.00070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:D4:DE (VMware)

Nmap scan report for 192.168.237.128
Host is up (0.000021s latency).
All 1000 scanned ports on 192.168.237.128 are closed

Nmap scan report for 192.168.237.129
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
```

Figure 6. Scanning a range of IPs using wildcard

C. Scan an entire subnet (Figure 7).

Example – `nmap 192.168.237.0/24`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap 192.168.237.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:13 IST
Nmap scan report for 192.168.237.1
Host is up (0.0058s latency).
All 1000 scanned ports on 192.168.237.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.237.2
Host is up (0.00091s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:ED:D4:DE (VMware)

Nmap scan report for 192.168.237.128
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.237.128 are closed

Nmap scan report for 192.168.237.129
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
```

Figure 7. Scanning entire subnet

Step 5.

This command is used to scan OS and version detection (Figure 8).

Example – `nmap -O 192.168.237.129`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap -O 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:14 IST
Nmap scan report for 192.168.237.129
Host is up (0.00096s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_s
erver_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
root@MrQuiety:~#
```

Figure 8. Scanning OS and itsversion

Step 6.

Scan all TCP ports in the target IP (Figure 9).

Example – `nmap -sT 192.168.237.129`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap -sT 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:15 IST
Nmap scan report for 192.168.237.129
Host is up (0.016s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@MrQuiety:~#
```

Figure 9. Scanning all TCP ports in target IP

Step 7.

Scan a firewall for security weakness.

A. Null scan – use TCP null scan to fool a firewall to generate a response (Figure 10).

Example – `nmap -sN 192.168.237.129`

B. Fin scan – use TCP Fin scan to check the firewall (Figure 10).

Example – `nmap -sF 192.168.237.129`

C. Use TCP Xmas scan to check firewall (Figure 10).

Example – `nmap -sX 192.168.237.129`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap -sN 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:16 IST
Nmap scan report for 192.168.237.129
Host is up (0.0011s latency).                                    A
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
root@MrQuiety:~# nmap -sF 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:16 IST
Nmap scan report for 192.168.237.129
Host is up (0.0010s latency).                                    B
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
root@MrQuiety:~# nmap -sX 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:16 IST
Nmap scan report for 192.168.237.129
Host is up (0.0011s latency).                                    C
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
root@MrQuiety:~#
```

Figure 10. Null, TCP Fin, and TCP Xmas scans

Step 8.

UDP scan – scan a host for UDP services. This scan is used to view open UDP ports (Figure 11).

Example – `nmap -sU 192.168.237.129`

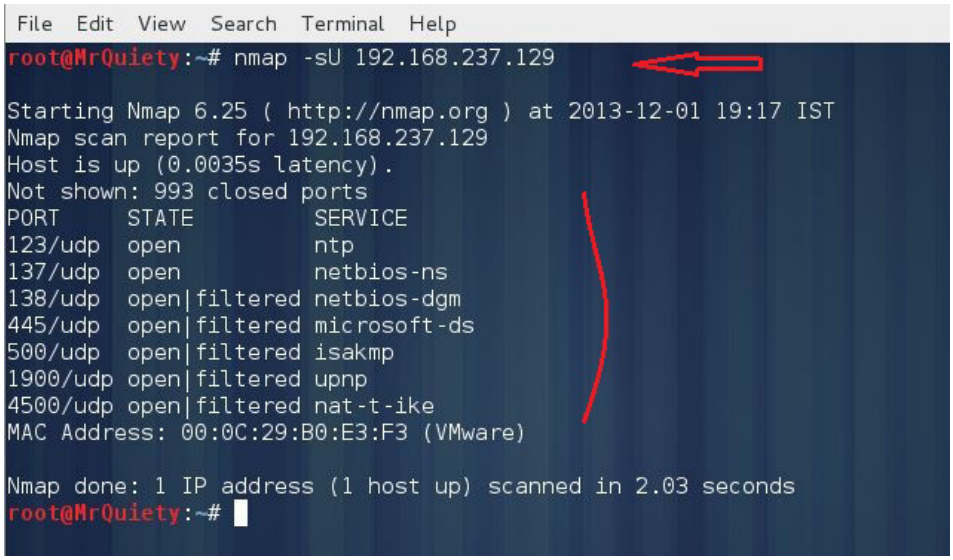


Figure 11. UDP scan

Step 9.

Scan for IP protocol – this type of scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines (Figure 12).

Example – `nmap -sO 192.168.237.129`

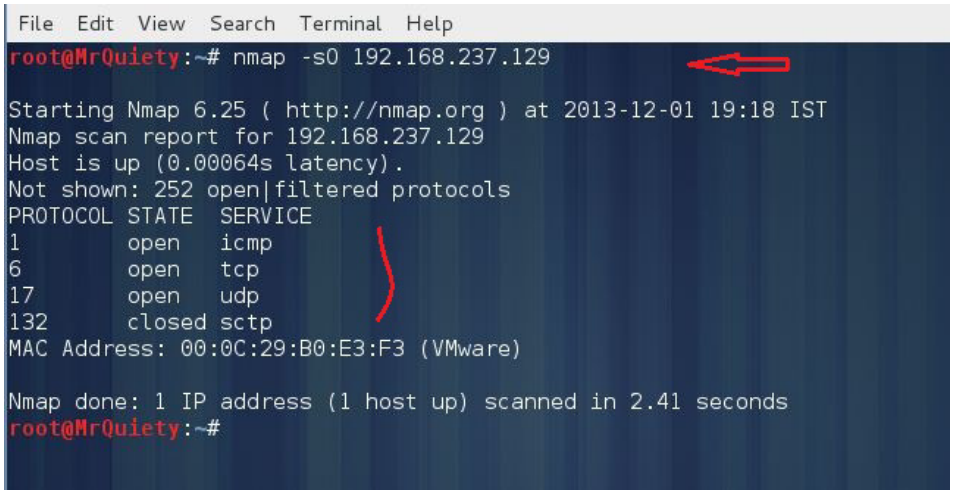


Figure 12. Scan for IP protocol

Step 10.

Detect remote services (server/domain) version numbers (Figure 13).

Example – `nmap -sV 192.168.237.129`

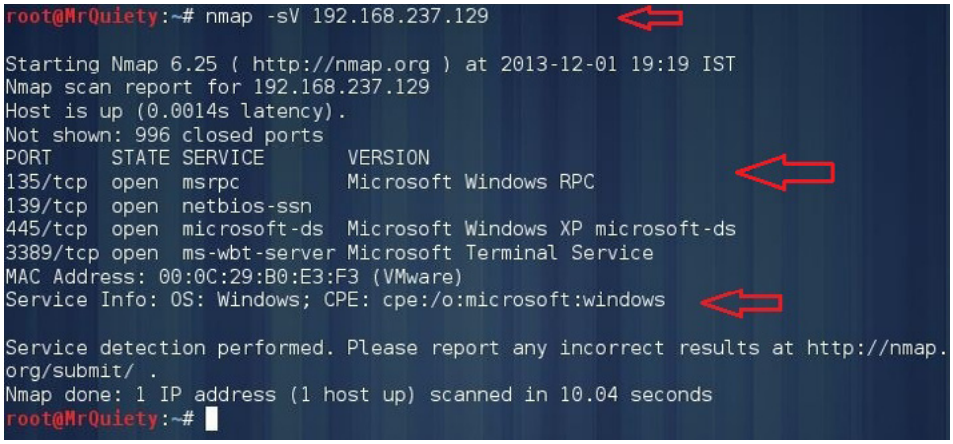


Figure 13. Detecting remote services

Step 11.

Find out the most commonly used TCP ports using TCP SYN Scan.

A. Stealthy scan (Figure 14).

Example – `nmap -sS 192.168.237.129`

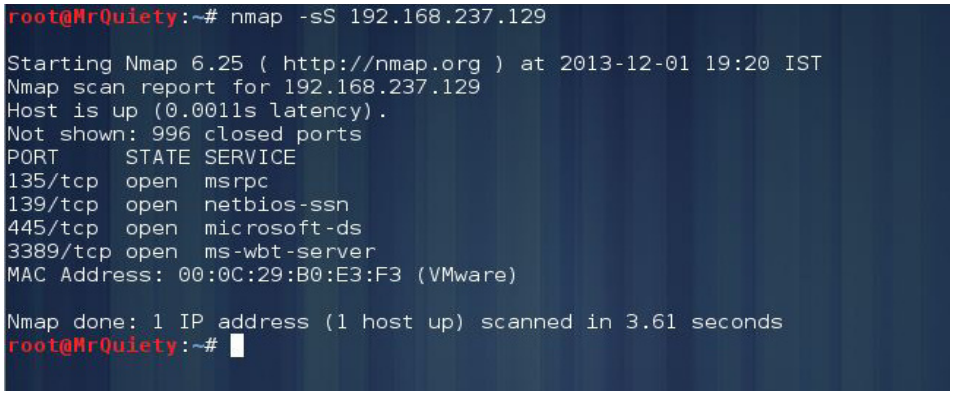


Figure 14. Stealthy TCP SYN scan

B. Find out the most commonly used TCP ports using TCP connect scan (Figure 15).

Example – `nmap -sT 192.168.237.129`

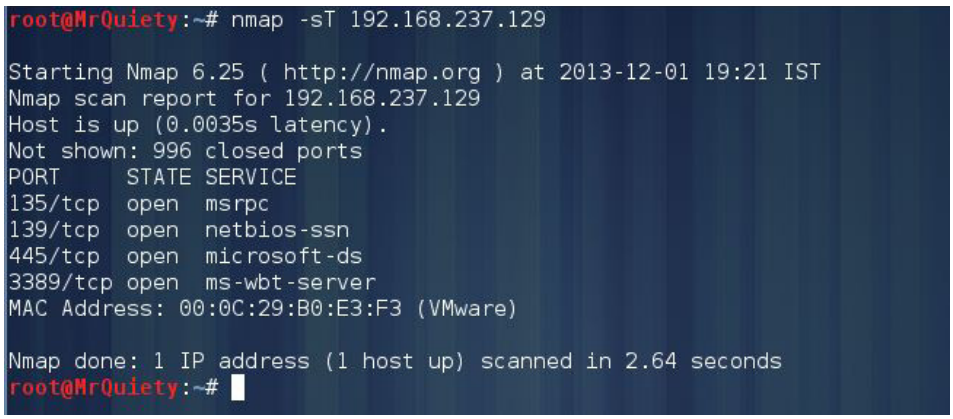


Figure 15. TCP connect scan

C. Find out the most commonly used TCP ports using TCP ACK scan (Figure 16).

Example – `nmap -sA 192.168.237.129`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap -sA 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:22 IST
Nmap scan report for 192.168.237.129
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.237.129 are unfiltered
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.65 seconds
root@MrQuiety:~#
```

Figure 16. TCP ACK scan

D. Find out the most commonly used TCP ports using TCP Window scan (Figure 17).

Example – `nmap -sW 192.168.237.129`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap -sW 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:23 IST
Nmap scan report for 192.168.237.129
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.50 seconds
root@MrQuiety:~#
```

Figure 17. TCP Window scan

E. Find out the most commonly used TCP ports using TCP Maimon scan (Figure 18).

Example – `nmap - sM 192.168.237.129`

```
File  Edit  View  Search  Terminal  Help
root@MrQuiety:~# nmap -sM 192.168.237.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-01 19:23 IST
Nmap scan report for 192.168.237.129
Host is up (0.0026s latency).
All 1000 scanned ports on 192.168.237.129 are closed
MAC Address: 00:0C:29:B0:E3:F3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
root@MrQuiety:~#
```

Figure 18. TCP Maimon scan

Step 12.

List scan – this command is used to list the targets to scan (Figure 19).

Example – `nmap -sL 192.168.237.129`

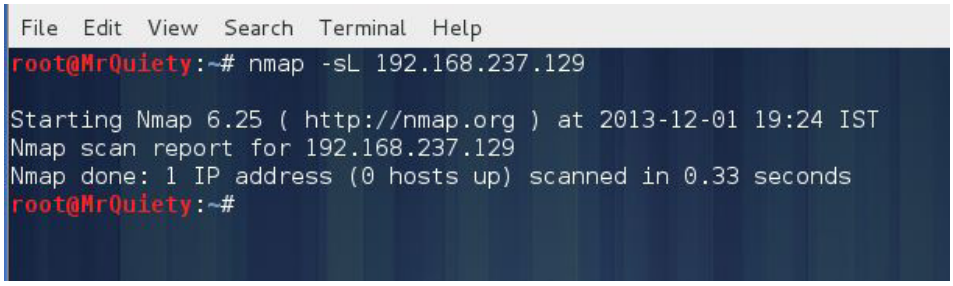


Figure 19. List scan

Step 13.

Host discovery or ping scan – scan a network and find out which servers and devices are up and running (Figure 20).

Example – `nmap -sP 192.168.237.0/24`

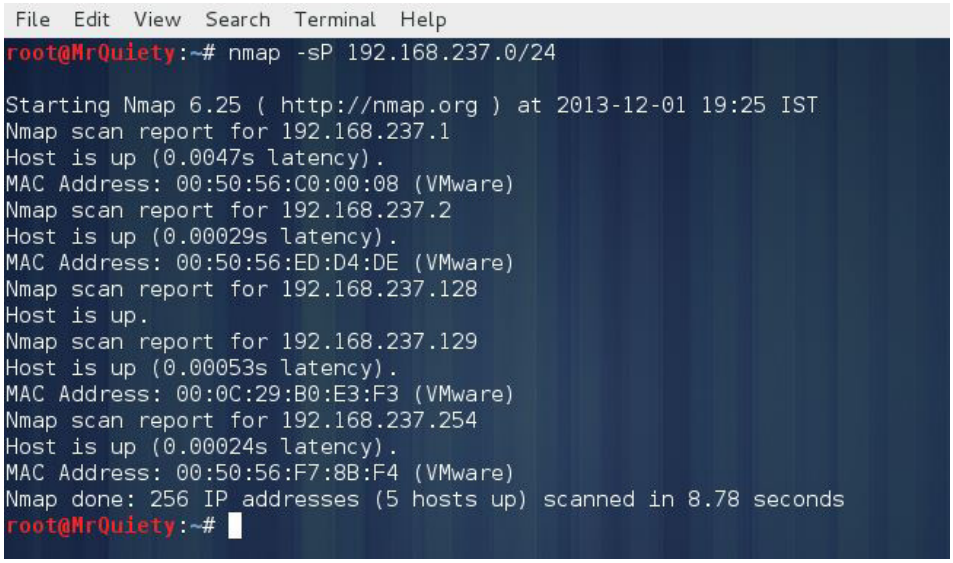


Figure 20. Ping scan

Step 14.

Scan a host when protected by the firewall (Figure 21).

Example – `nmap -PN 192.168.237.1`

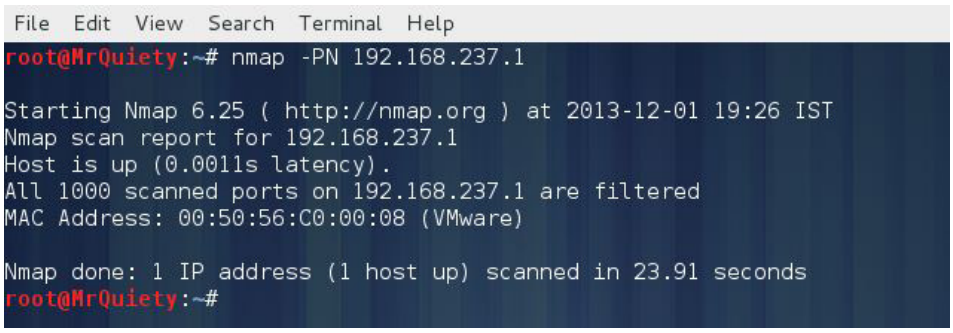
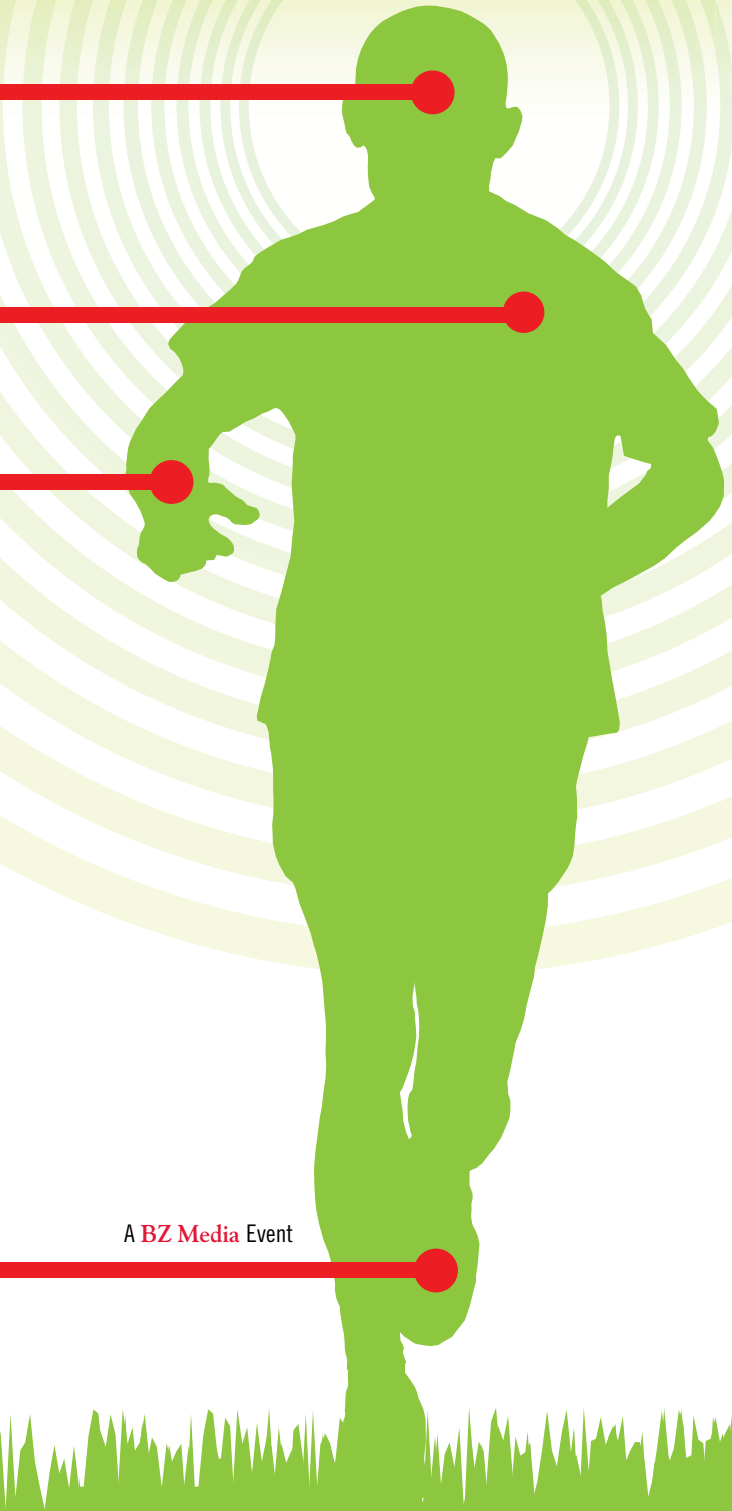


Figure 21. Scanning a host while protected by firewall

Join the Wearables Revolution!



Wearables DevCon

A conference for Designers, Builders and Developers of Wearable Computing Devices

Wearable computing devices are the Next Big Wave in technology. And the winning developers in the next decade are going to be the ones who take advantage of these new technologies EARLY and build the next generation of red-hot apps.

Choose from over 35 classes and tutorials!

- Learn how to develop apps for the coolest gadgets like Google Glass, FitBit, Pebble, the SmartWatch 2, Jawbone, and the Galaxy Gear SmartWatch
- Get practical answers to real problems, learn tangible steps to real-world implementation of the next generation of computing devices

March 5-7, 2014
San Francisco

WearablesDevCon.com

A BZ Media Event

How to Use Ssldump in Kali Linux

by Rrajesh Kumar

Ssldump is an SSL/TLS network protocol analyzer. It identifies TCP connections on the chosen network interface and attempts to interpret them as SSL/TLS traffic. When it identifies SSL/TLS traffic, it decodes the records and displays them in a textual form to stdout. If provided with the appropriate keying material, it will also decrypt the connections and display the application data traffic (www.rtfm.com).

Step 1. How to open

A. GUI Method (Figure 1).

Applications →Kali Linux → Information Gathering → SSL Analysis → ssldump

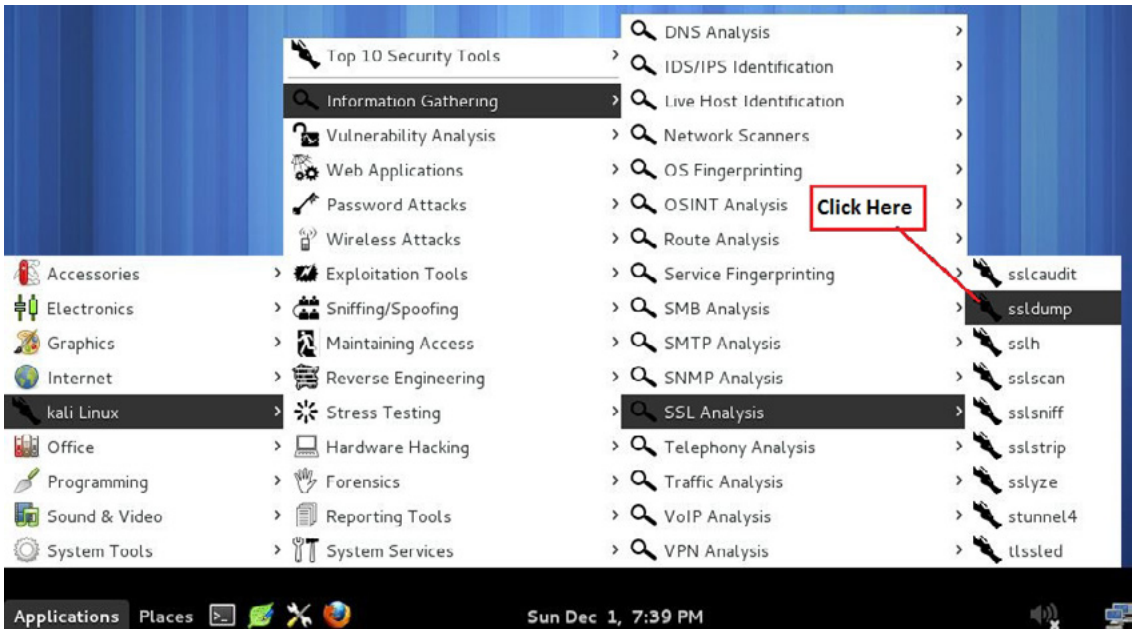


Figure 1. Opening ssldump in the GUI

B. Open the terminal and type `ssldump -h`. This command will open ssldump with help options (Figure 2).

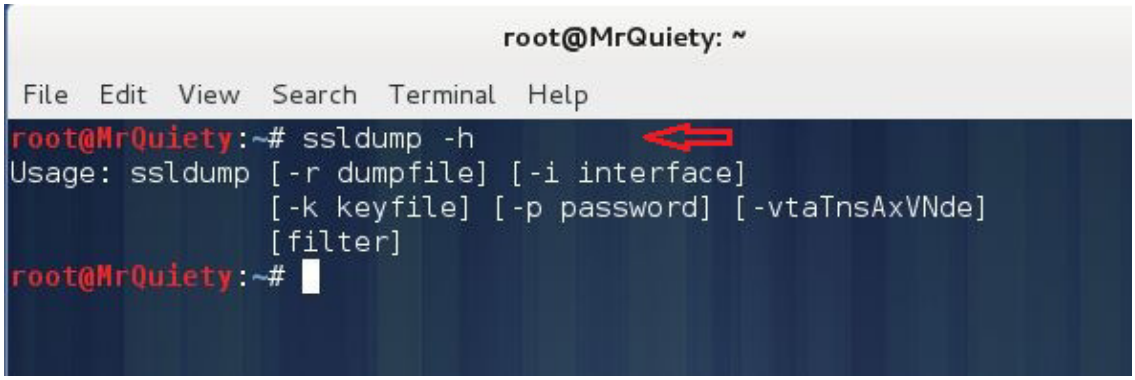


Figure 2. Opening ssldump in the terminal

Step 2.

This command is used to show the traffic (Figure 3).

Syntax – `ssldump -i interface port no`

Example – `ssldump -i eth0 port 80`

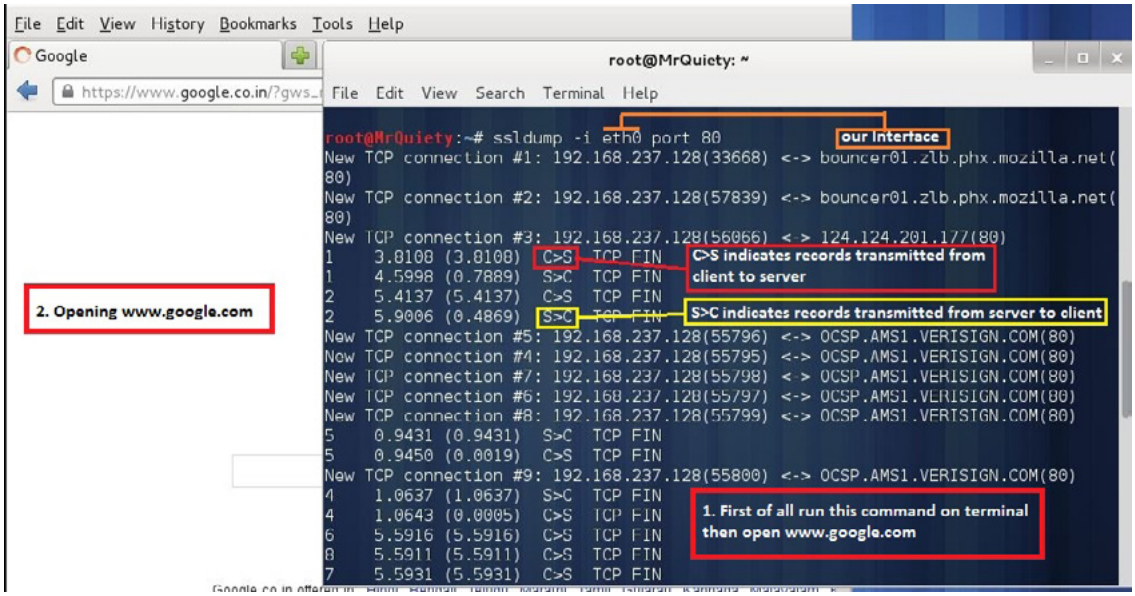


Figure 3. Showing the traffic

Step 3.

This command displays the application data traffic. This usually means decrypting it, but when `-d` is used, ssldump will also decode application data traffic before the SSL session initiates. This allows you to see HTTPS CONNECT behavior as well as SMTP STARTTLS. As a side effect, since ssldump can't tell whether plaintext is traffic before the initiation of an SSL connection or just a regular TCP connection, this allows you to use ssldump to sniff any TCP connection.

Ssldump will automatically detect ASCII data and display it directly on the screen. Non-ASCII data is displayed as hex dumps (Figure 4 & 5).

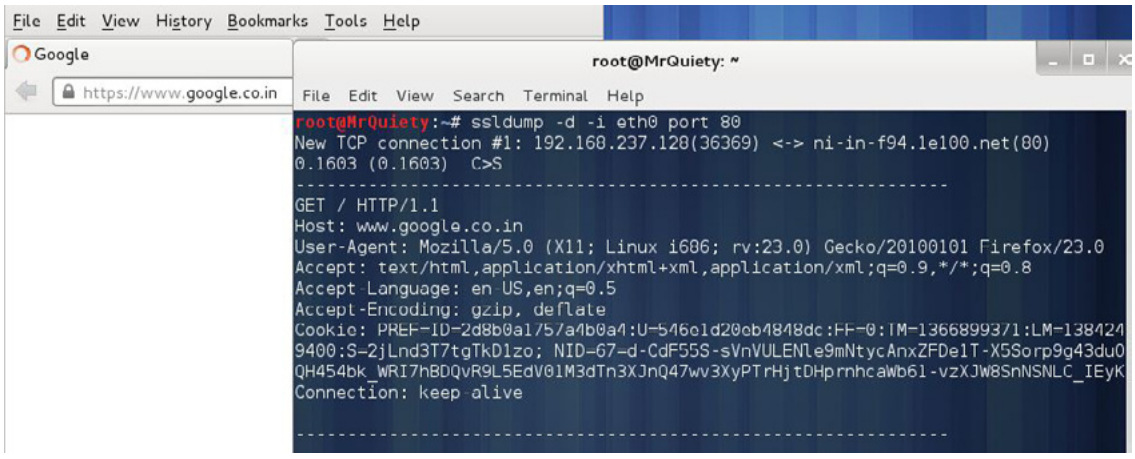


Figure 4. Application data traffic

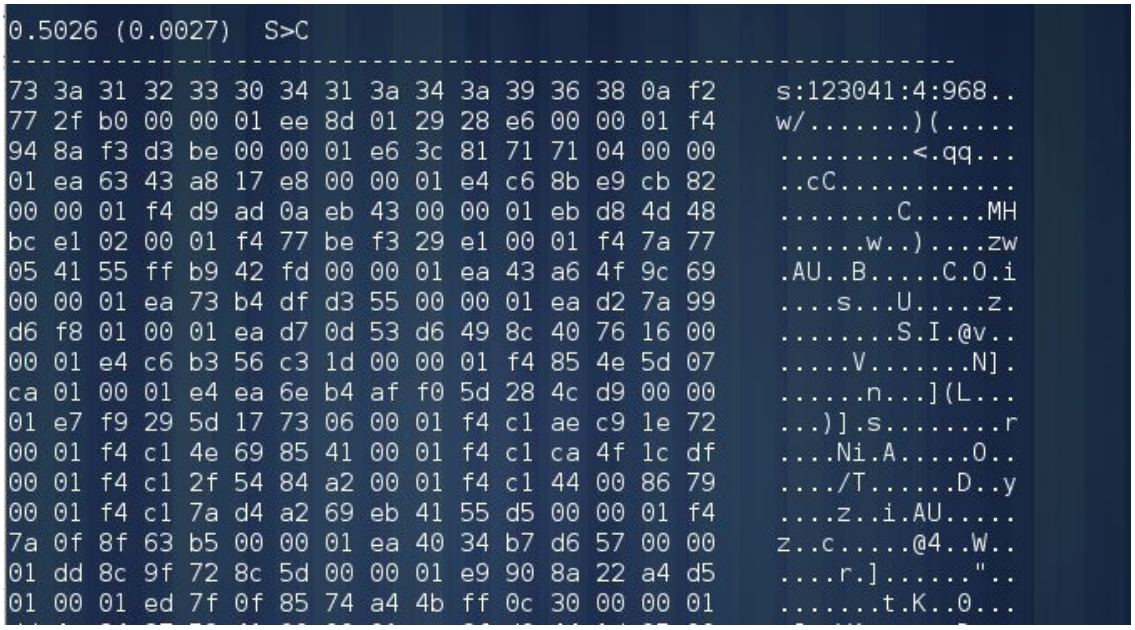


Figure 5. Non-ASCII application data traffic (hex dumps)

Step 4.

Print absolute timestamps instead of relative timestamps (Figure 6).

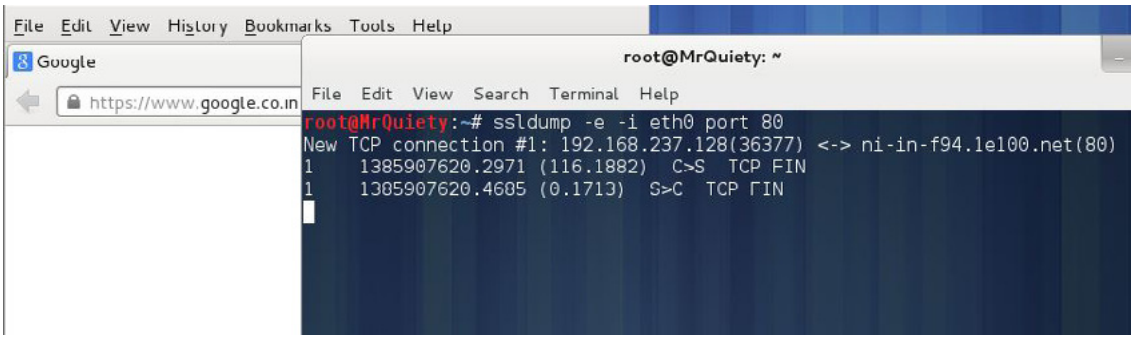


Figure 6. Absolute timestamps

Step 5.

The full SSL packet header. Ssldump may print record-specific data on the rest of the line. For handshake records, it prints the handshake message. Thus, this record is a certificate message. Ssldump chooses certain record types for further decoding. These are the ones that have proven to be most useful for debugging:

`ClientHello` – version, offered cipher suites, session ID (Figure 7).

`ServerHello` – version, session_id, chosen cipher suite, compression method (Figure 8).

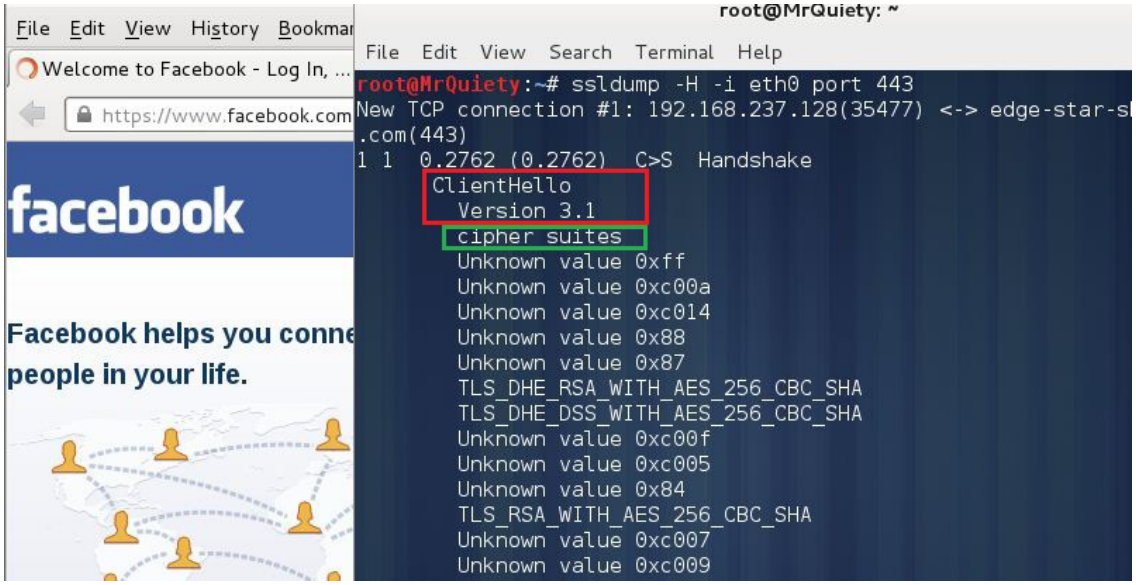


Figure 7. ClientHello

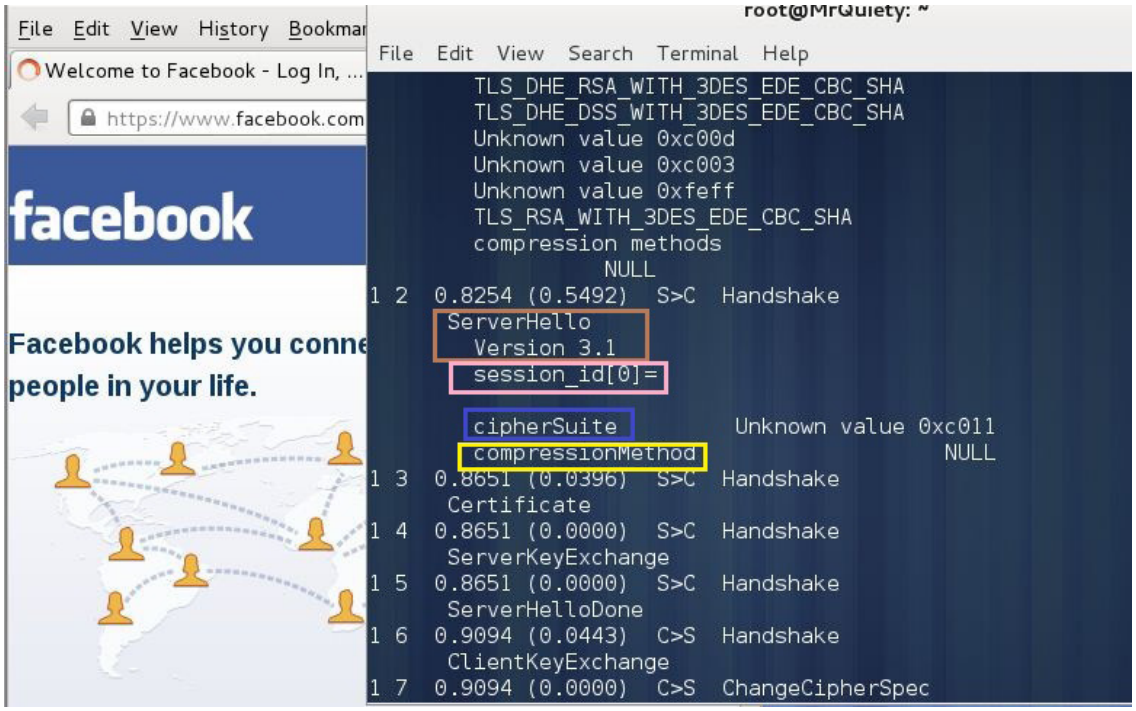


Figure 8. ServerHello

How to Use SSLStrip in Kali Linux

by Rrajesh Kumar

In this tutorial, we will use sslstrip for stealing passwords from any PC which is connected to LAN. SSLStrip basically hijacks HTTP traffic. Nowadays, it's a little difficult to steal the passwords from some websites.

Step 1. How to open

A. GUI Method (Figure 1).

Applications →Kali Linux → Information Gathering → SSL Analysis → sslstrip

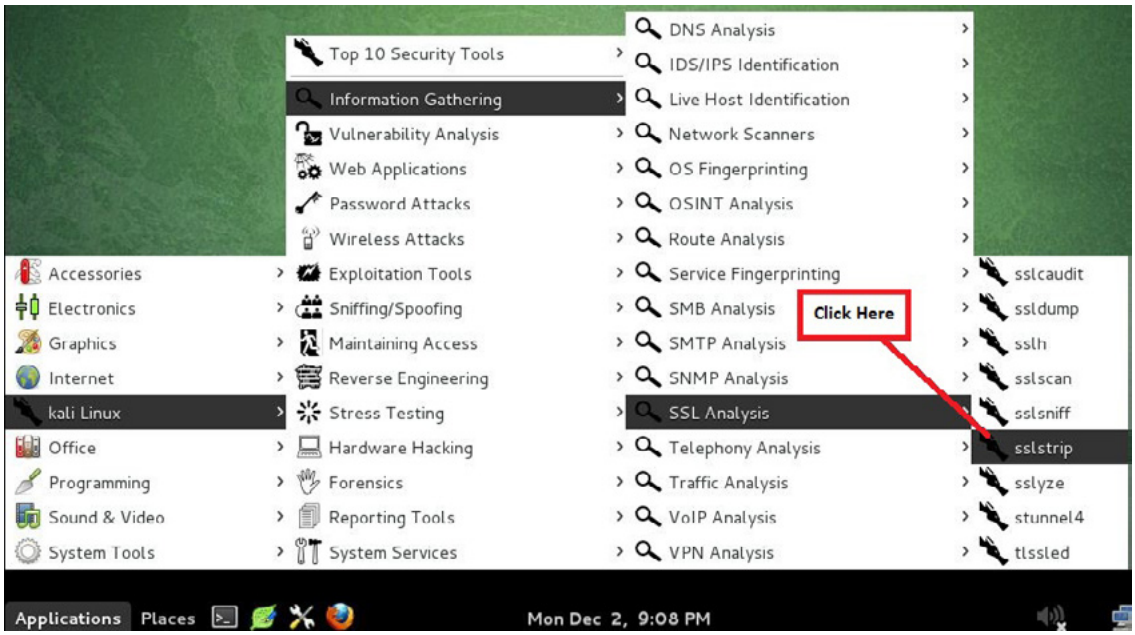


Figure 1. Opening SSLStrip in the GUI

B. Open the terminal and type `sslstrip -h`. This command will open SSLStrip with help options (Figure 2).

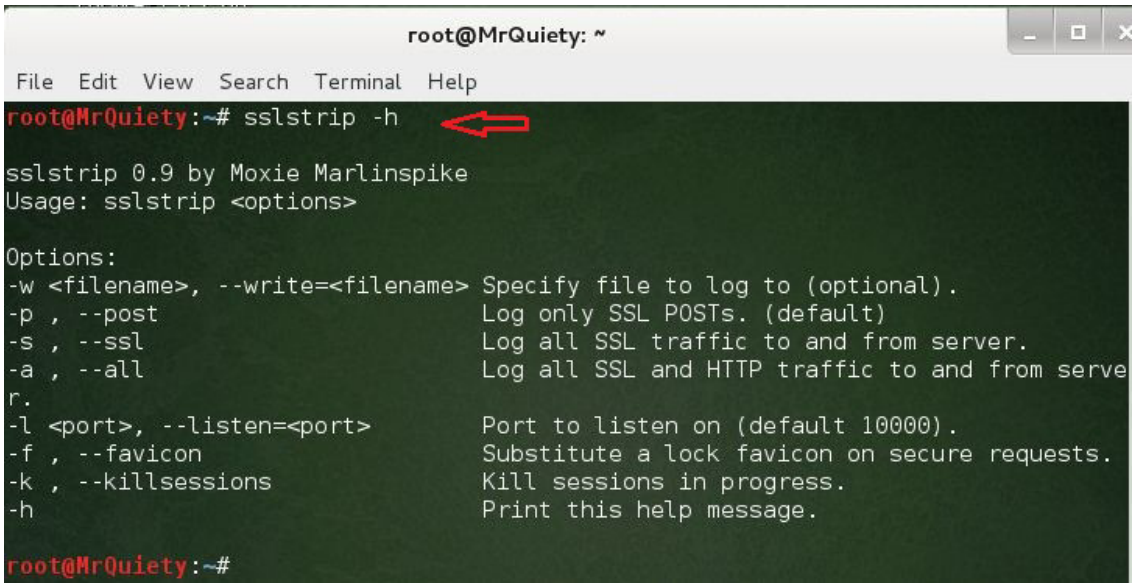


Figure 2. Opening SSLStrip in the terminal

Before starting SSLStrip, we need to do some other things for trapping our target:

- IP forwarding
- IP table for redirect 80 to 8080
- Finding gateway IP
- Finding target IP
- Arpspoof

Step 2.

This command is used to enable IP forwarding (Figure 3).

Syntax – `echo '1' > /proc/sys/net/ipv4/ip_forward`

Figure 3. IP forwarding

Step 3.

This command is used to redirect requests from port 80 to port 8080 to ensure our outgoing connections (from SSLStrip) get routed to the proper port (Figure 4).

Syntax – `iptables -t nat -A PREROUTING -p tcp -destination-port 80 -j REDIRECT -to-port 8080`

Figure 4. Redirecting requests from port 80 to port 8080

Step 4.

This command is used to find the gateway IP (Figure 5).

Syntax – `netstat -nr`

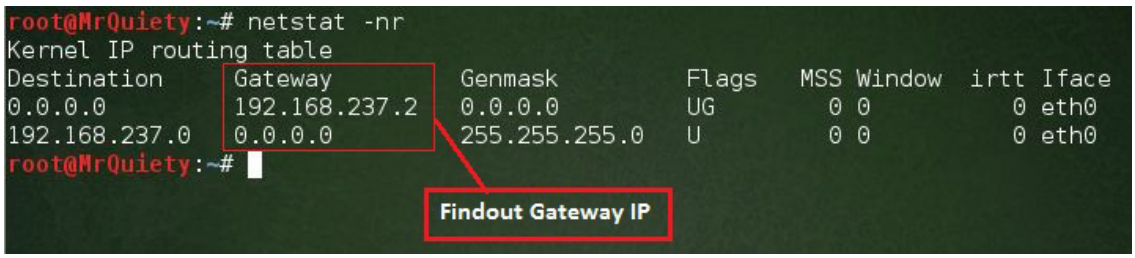


Figure 5. Finding gateway IP

Step 5.

This is our target OS (Windows XP). By using `ipconfig`, we got the target IP. I know you are thinking if I want to trap an unknown LAN PC, then how will we find out the IP address. Well, it's not that difficult, some social engineering can do your job. Come to the point on SSLStrip. Note the target IP (Figure 6).

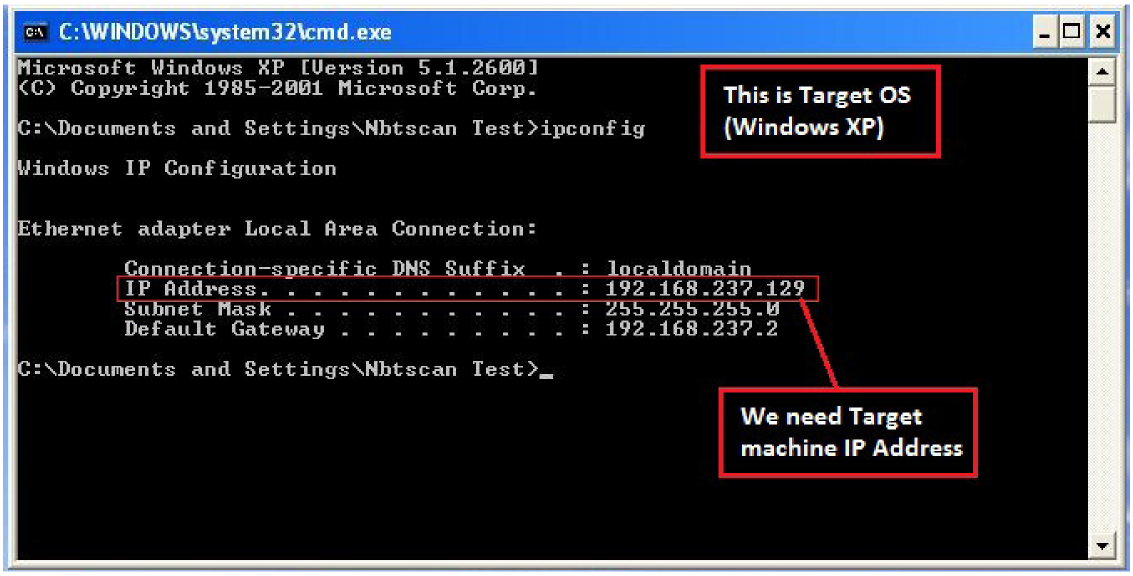


Figure 6. Getting target IP

Step 6.

This command is used to redirect all network HTTP traffic through our computer using ARPSpoof (don't forget to enable IP forwarding before this). See Figure 7.

Syntax – `arpspoof -i interface -t target IP -r gateway IP`

Example – `arpspoof -i eth0 -t 192.168.237.129 -r 192.168.237.2`

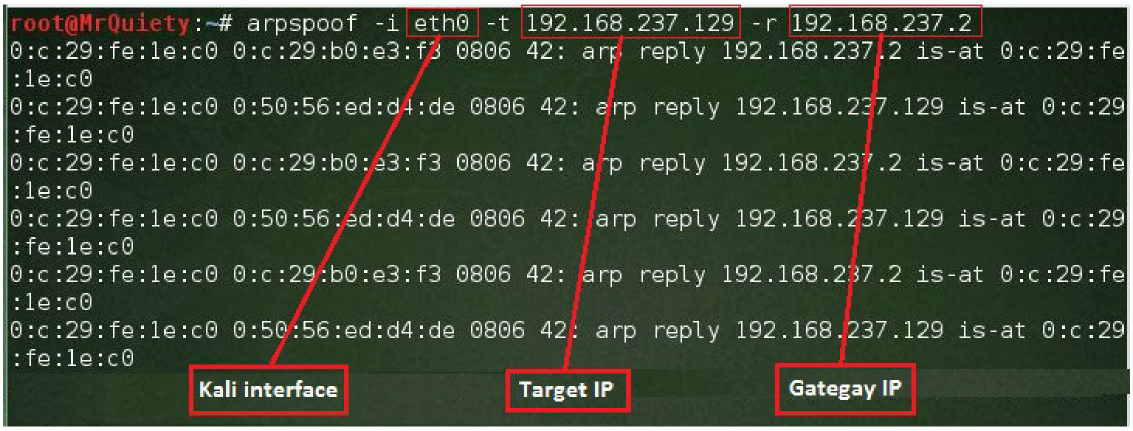


Figure 7. Redirecting all network HTTP traffic through our computer

Step 7.

Now, we need to open a new terminal because this terminal is running ARPSpoof and we can't stop it right now (Figure 8).

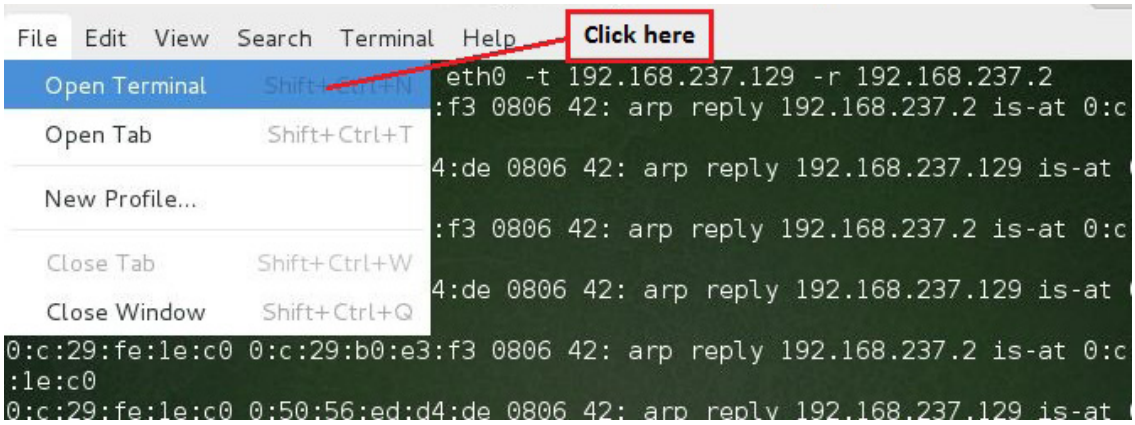


Figure 8. Opening new terminal

Step 8.

In the new terminal, use the following command. This command is used for listening on ports. `-l` tells the system to listen on specified port (Figure 9).

Syntax – `sslstrip -l 8080`

Figure 9. Listening on port 8080

Step 9.

Now, go to the target OS, open *www.gmail.com*, enter your username and password, then click on *Sign in*. It's the same as we are using it for checking our Gmail (Figure 10).

Figure 10. Logging on Gmail at the target PC

Step 10.

After clicking *Sign in* on the target OS, go to the attacker PC (Kali Linux). You will see that SSLStrip has captured some data. After finishing the capture, press Ctrl + C for stopping SSLStrip. Data is automatically saved in a file named `sslstrip.log` (Figures 11 & 12).

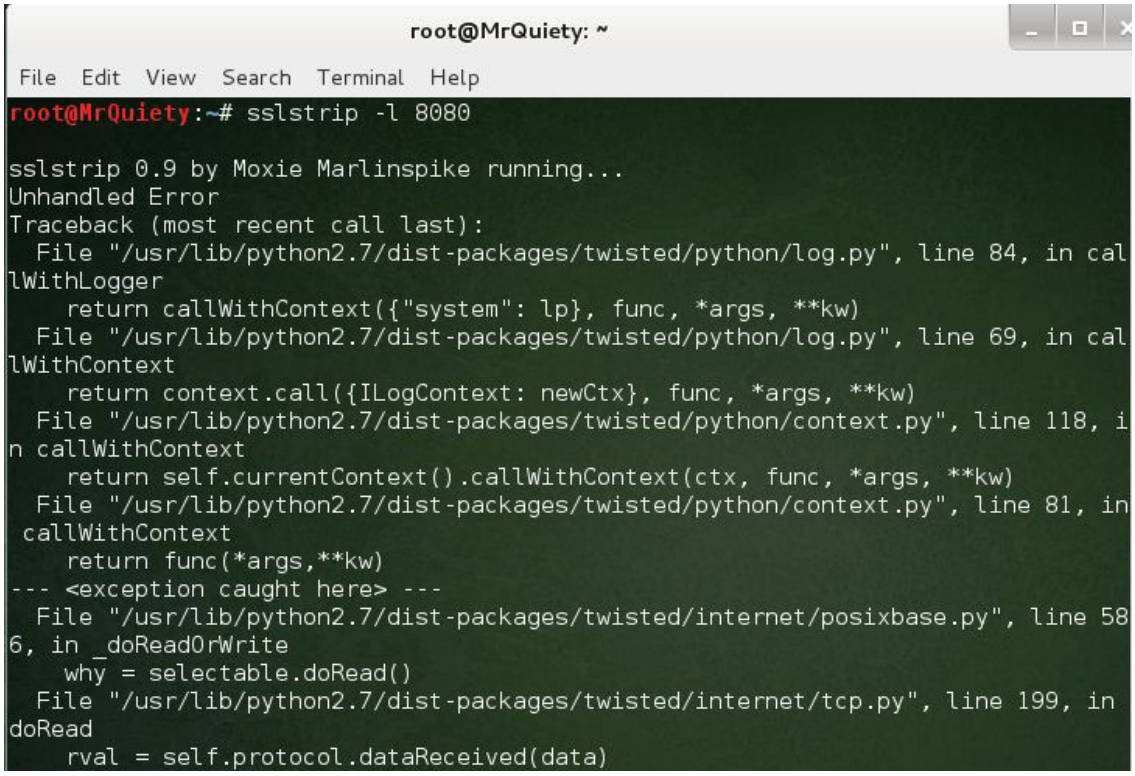


Figure 11. Data captured by SSLStrip (part 1)

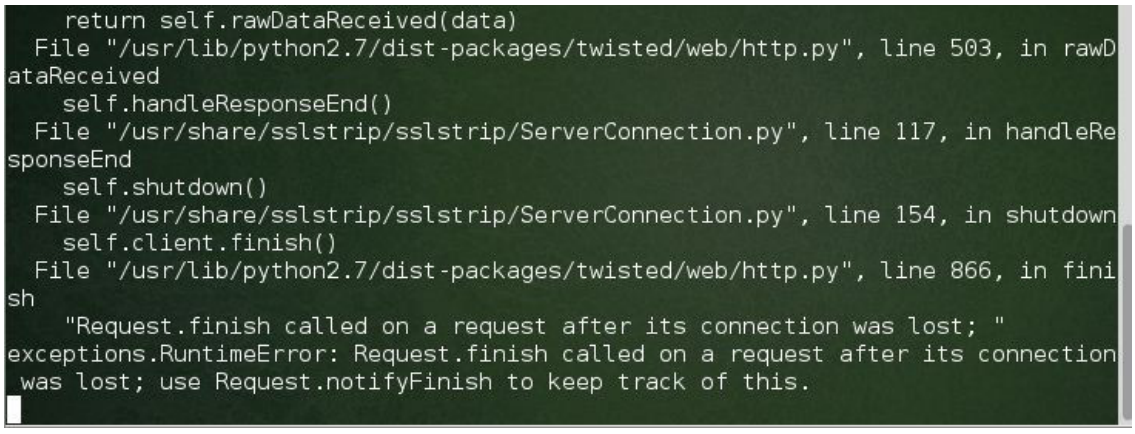


Figure 12. Data captured by SSLStrip (part 2)

Step 11.

Use the `ls` command so you can see the saved file as `sslstrip.log` (Figure 13).

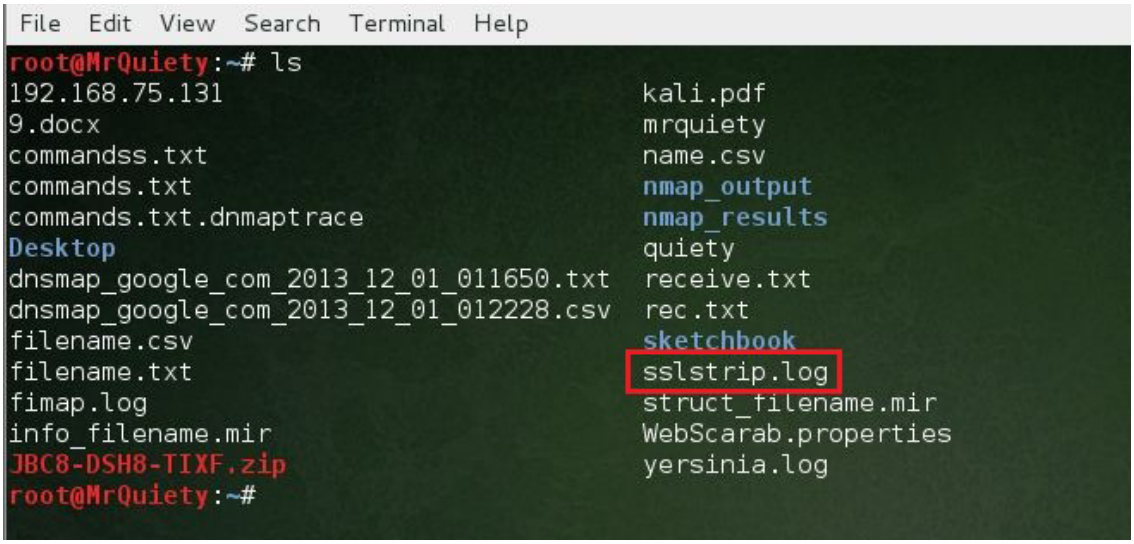


Figure 13. ls command

Step 12.

Use `cat` to open your `sslstrip.log` file and watch carefully. There are your victim's e-mail ID and password as shown in Figure 14.

Syntax – `cat sslstrip.log`

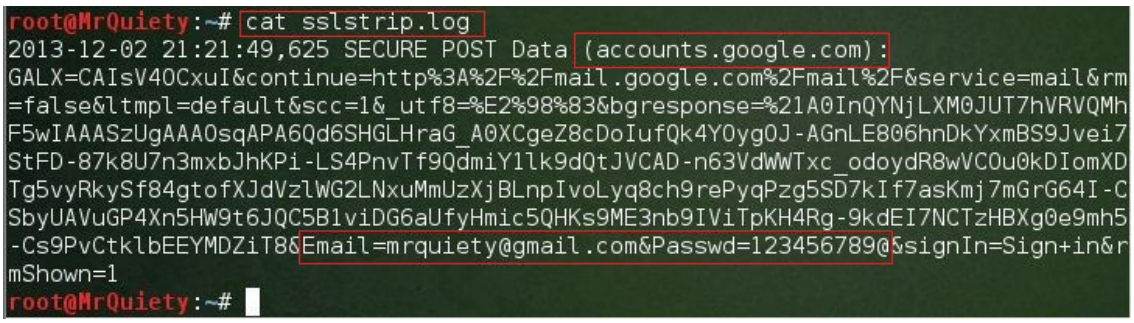


Figure 14. Victim e-mail and password captured

How to Use Uniscan-gui /Uniscan in Kali Linux

by Rrajesh Kumar

Uniscan is a simple Remote File Include, Local File Include, and Remote Command Execution vulnerability scanner.

Step 1. How to open

A. GUI Method (Figure 1).

Applications→ Kali Linux → Web Applications → Web Vulnerability Scanners → uniscan-gui

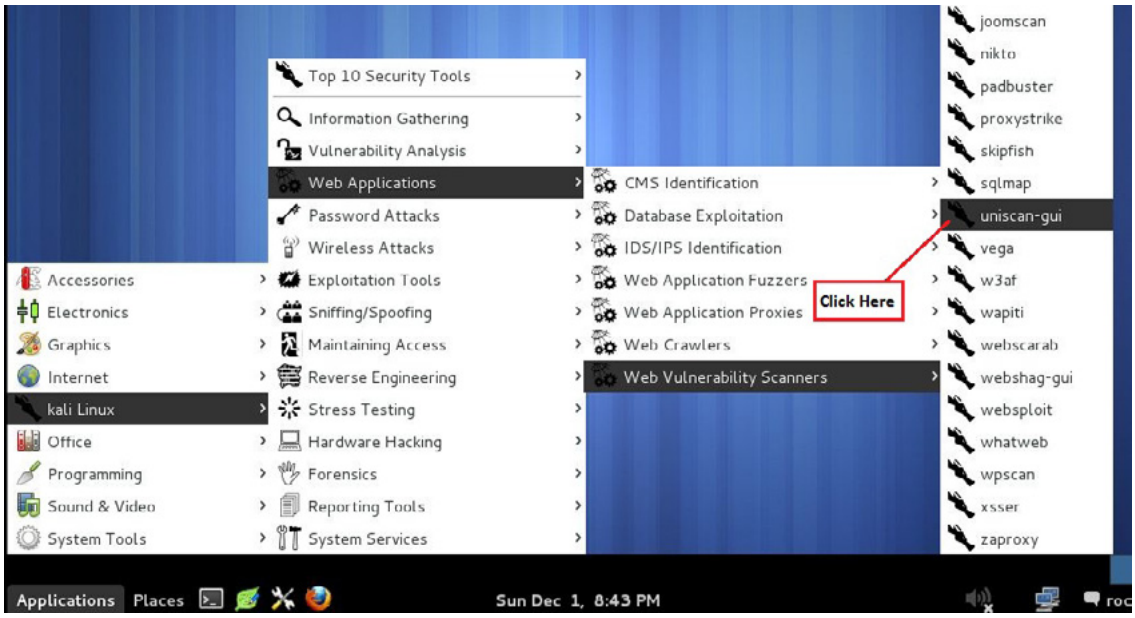


Figure 1. Opening Uniscan in the GUI

B. Open the terminal, type `uniscan-gui`, and hit *Enter* (Figure 2).

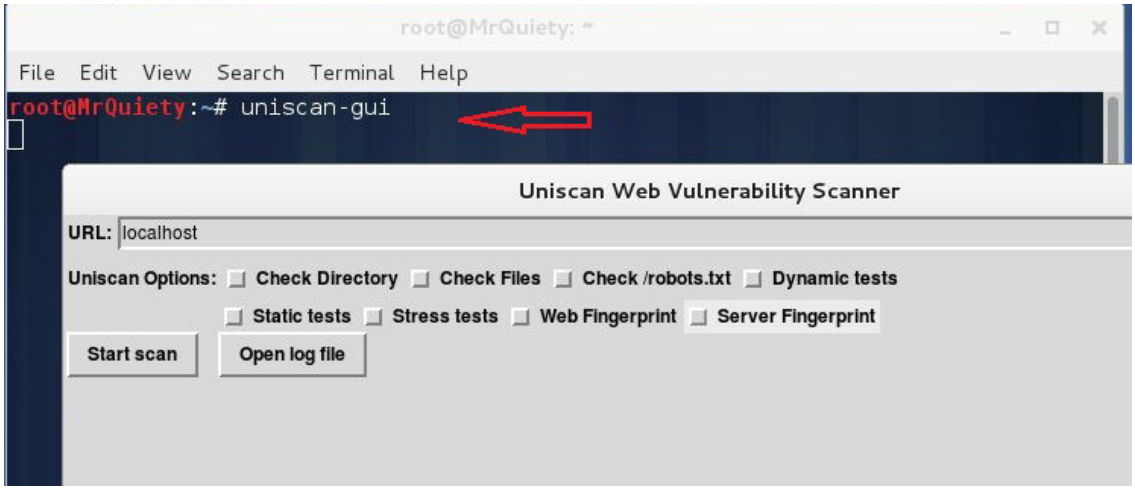


Figure 2. Opening Uniscan-gui in the terminal

C. Open the terminal, type `uniscan`, and hit *Enter* (Figure 3).

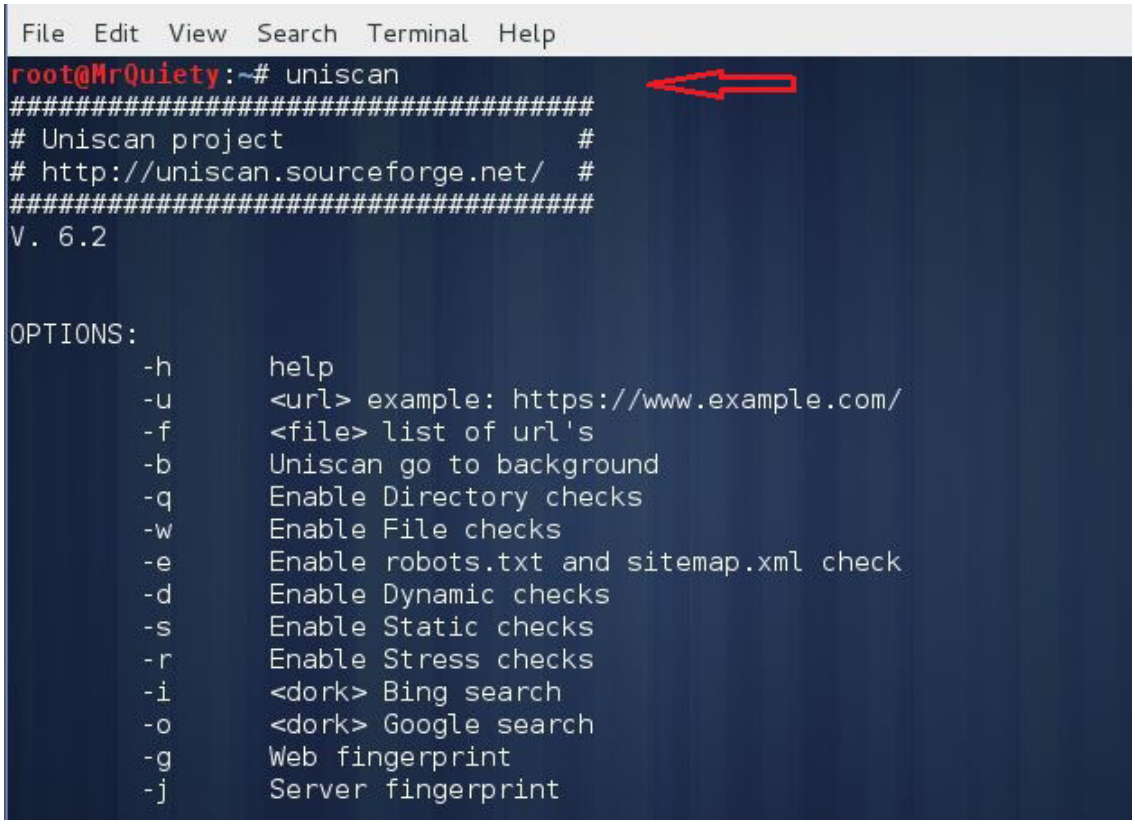


Figure 3. Opening Uniscan in the terminal

Step 2.

This command is used to scan the vulnerabilities on the target (Figure 4).

Syntax – `uniscan -u target host/IP -qweds`

Example – `uniscan -u www.hubbardbrook.org -qweds`

Here, `-q` – enable directory checks

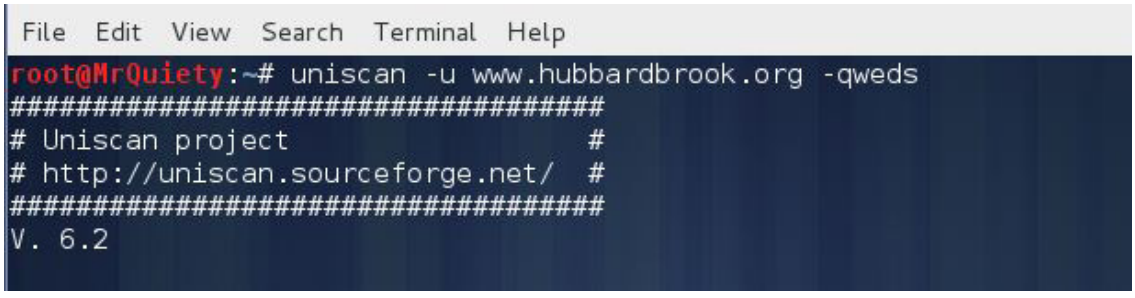


Figure 4. Scanning vulnerabilities on target

Step 2A.

Here, you can see the domain, server, and IP of the target URL, as well as the directory check result (Figure 5).

Figure 5. Domain, server, IP, and directory check result

Step 3.

You can see file check, check robots.txt , check sitemap.xml, and Crawler plugin (Figure 6).

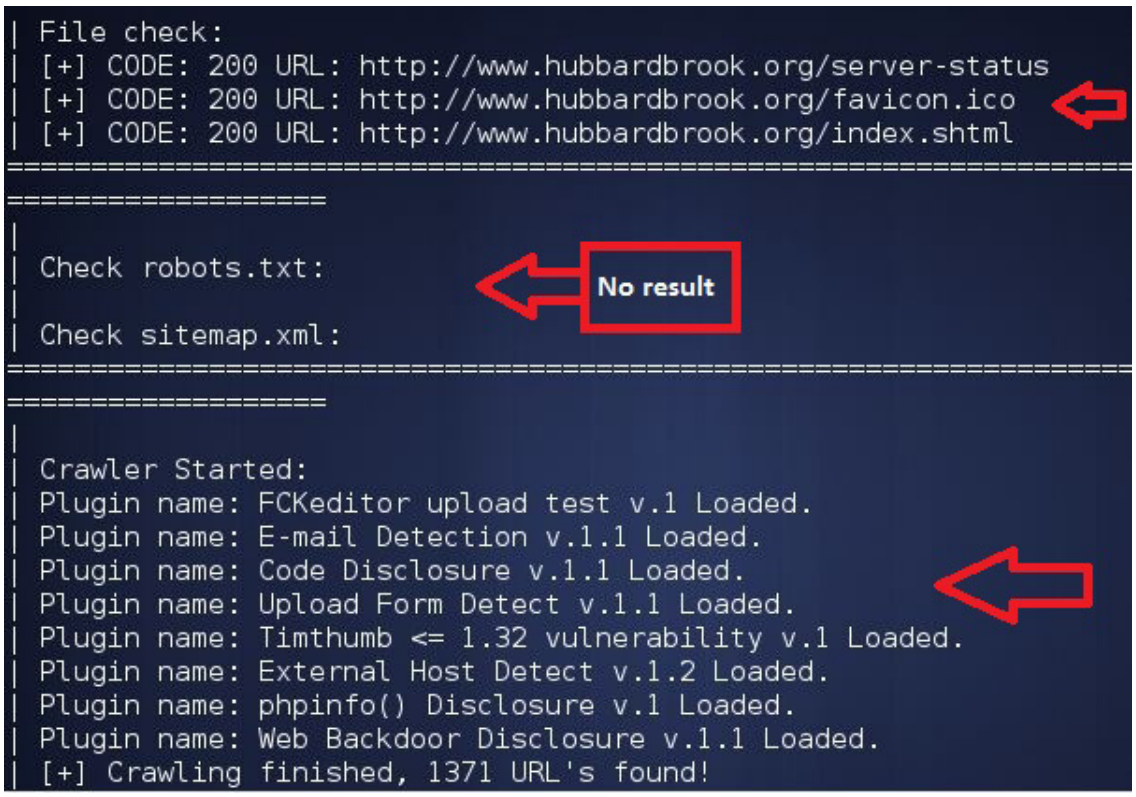


Figure 6. File check, check robots.txt, check sitemap.xml, and Crawler plugin

Step 4.

You can see FCKeditor file upload and e-mails information (Figure 7).

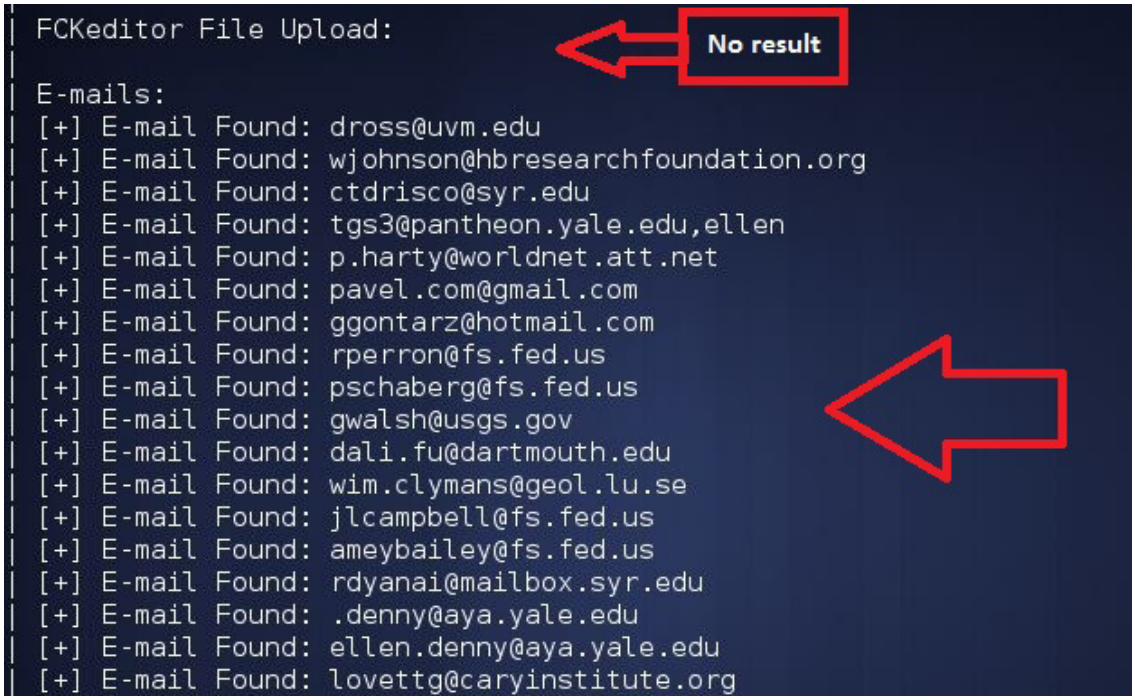


Figure 7. FCKeditor file upload and e-mails information

Step 5.

Source Code Disclosure (Figure 8).

Figure 8. Source Code Disclosure

Step 6.

Timthumb and external hosts (Figure 9).

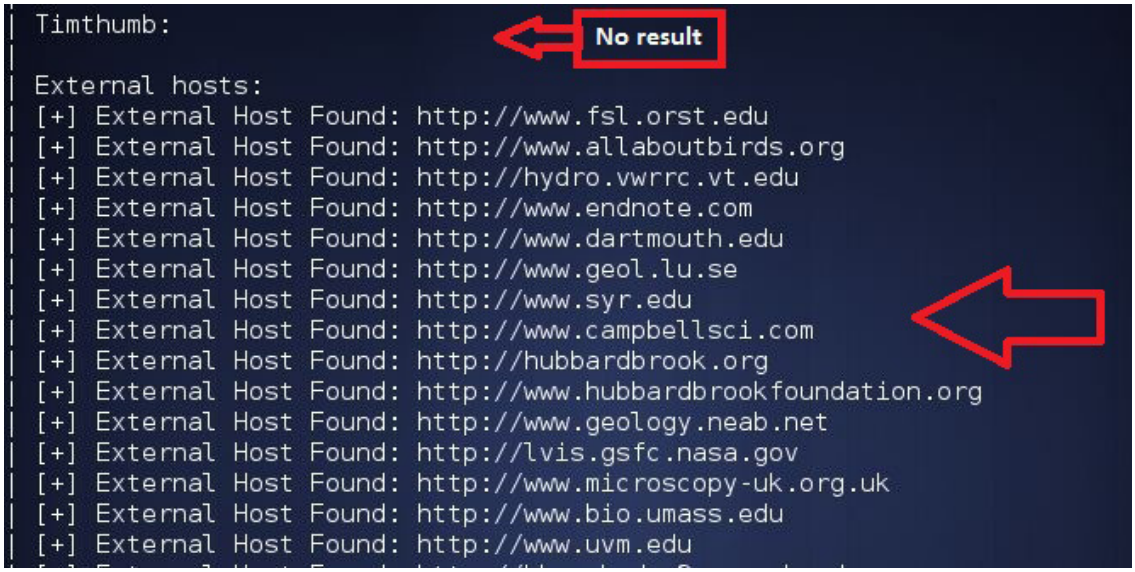


Figure 9. Timthumb and external hosts

Step 7.

PHPinfo () Disclosure and Web Backdoors (Figure 10).

Figure 10. PHPinfo () Disclosure and Web Backdoors

Step 8.

Dynamic test plugin names and FCKeditor tests (Figure 11).

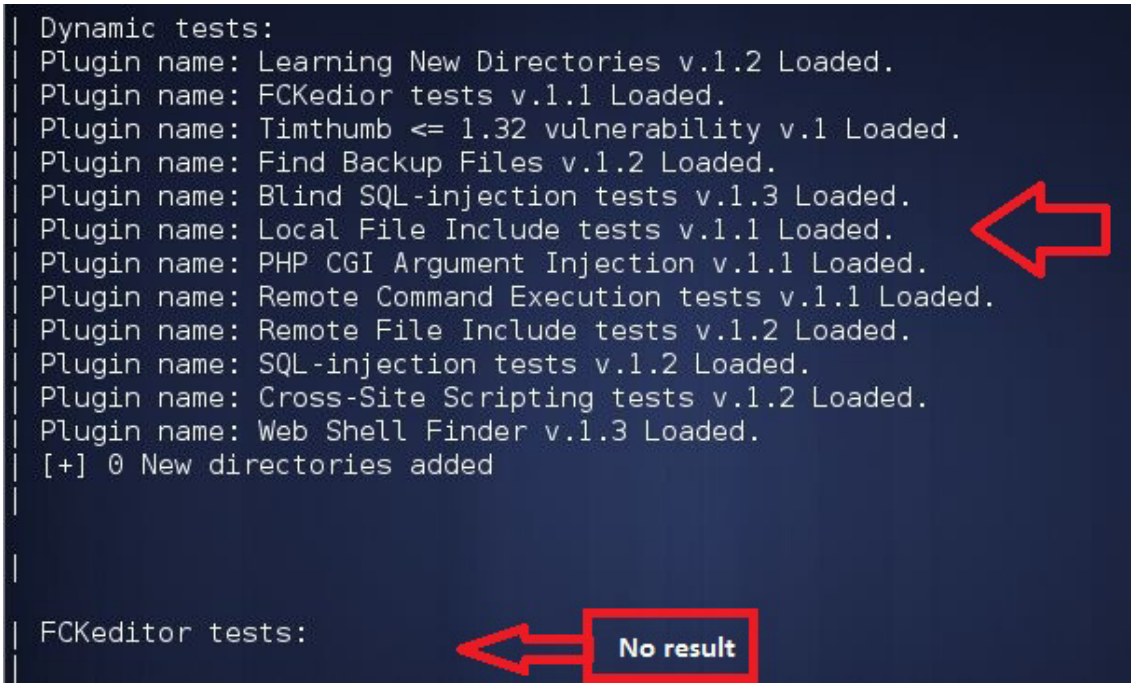


Figure 11. Dynamic test plugin names and FCKeditor tests

Step 9.

Timthumb < 1.33 vulnerability, Backup Files and Blind SQL Injection vulnerability information (Figure 12).

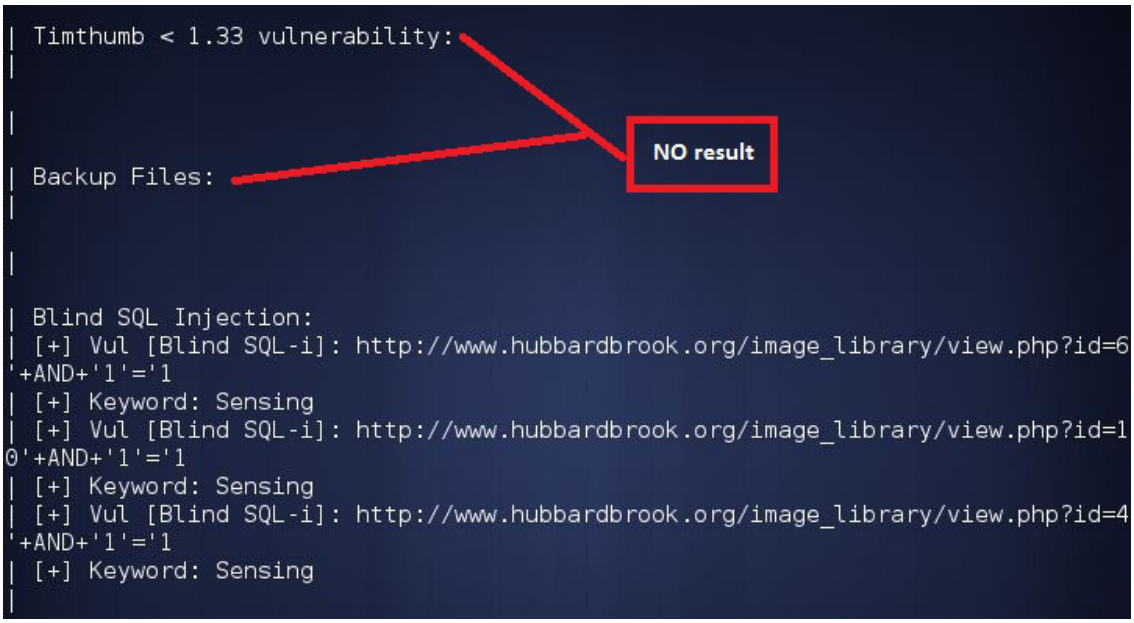


Figure 12. Timthumb < 1.33 vulnerability, Backup Files and Blind SQL Injection vulnerability information

Step 10.

Local File Include, PHP CGI Argument Injection, Remote Command Execution, Remote File Include, SQL Injection (Figure 13).

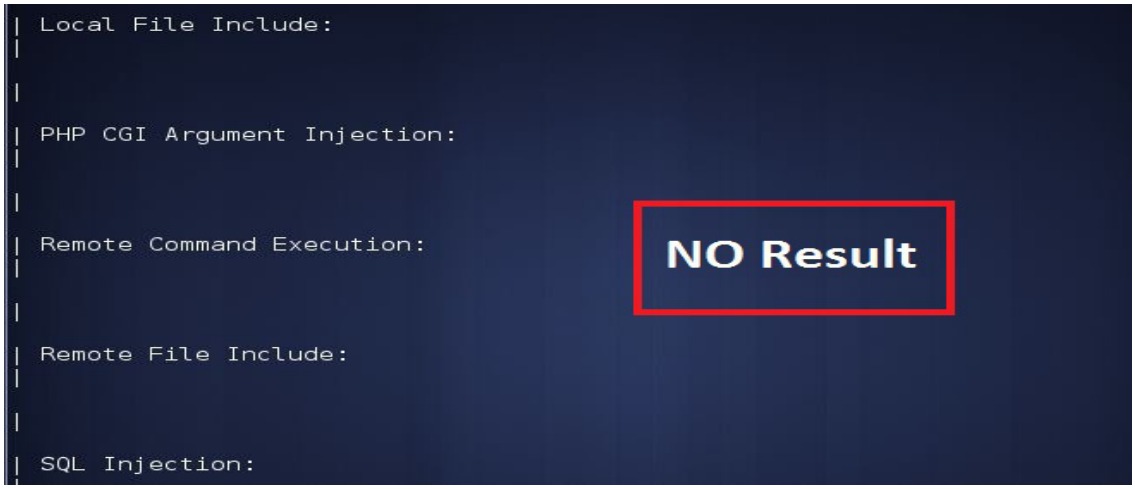


Figure 13. Local File Include, PHP CGI Argument Injection, Remote Command Execution, Remote File Include, SQL Injection

Step 11.

Web Shell Finder, Static test plugin names, Local file Include, Remote Command Execution (Figure 14).

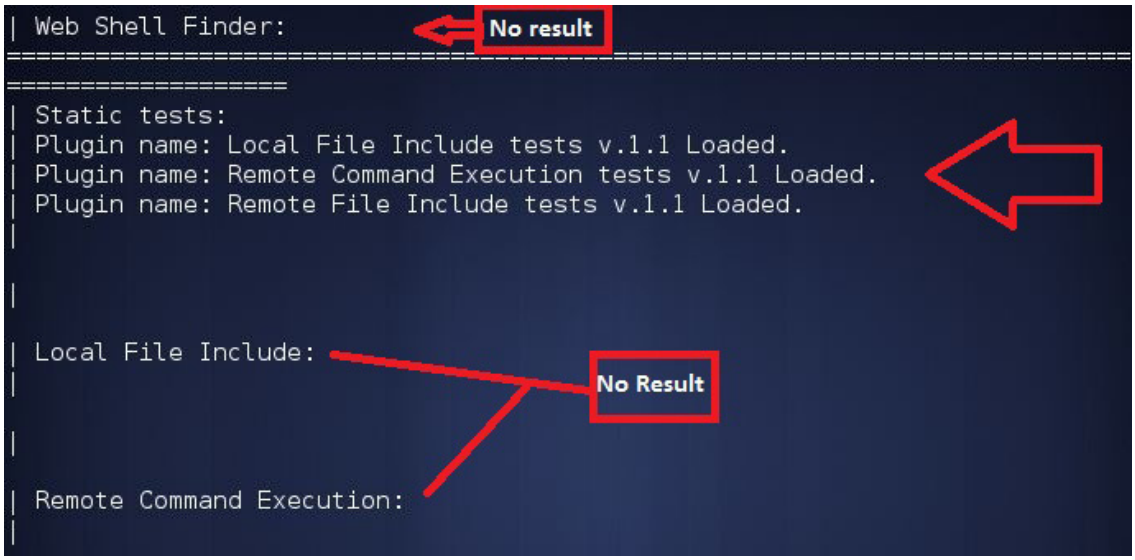


Figure 14. Web Shell Finder, Static test plugin names, Local file Include, Remote Command Execution

Step 12.

Remote File Include (Figure 15).

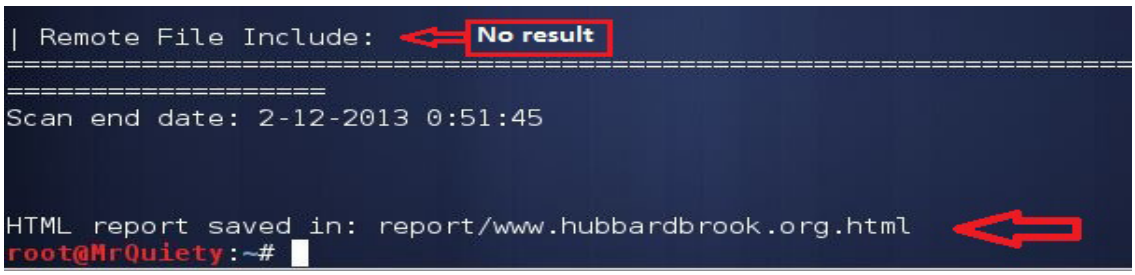


Figure 15. Remote File Include

Step 13.

Here we are starting Uniscan-gui. First of all, write your target URL in the *URL* field. Then, select the box from *Uniscan Options*. It depends on which type of scan and which plugin do you want to apply. Then, click `Start scan` and wait for the scan to finish. After completing, you have to click *Open log file*. There you can see your scan result (Figure 16).

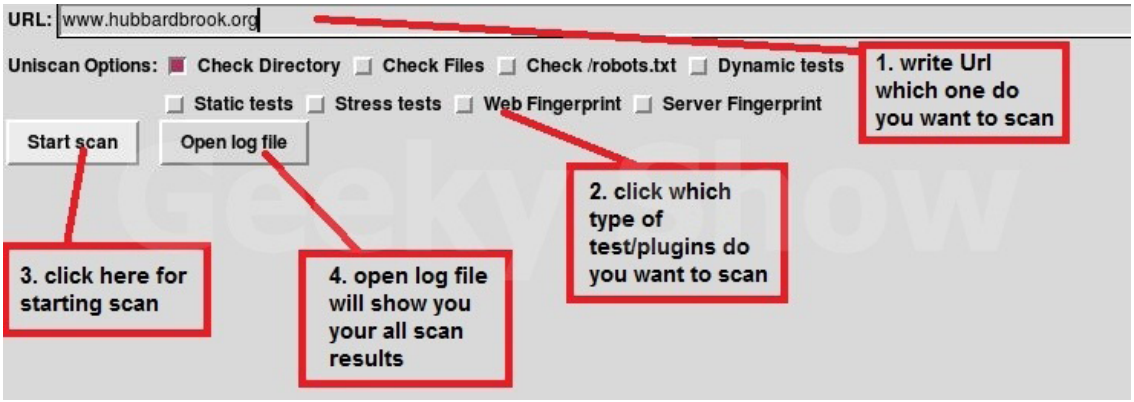


Figure 16. Scanning options

Step 14.

Open log file. Here, you can see your scan result (Figure 17).

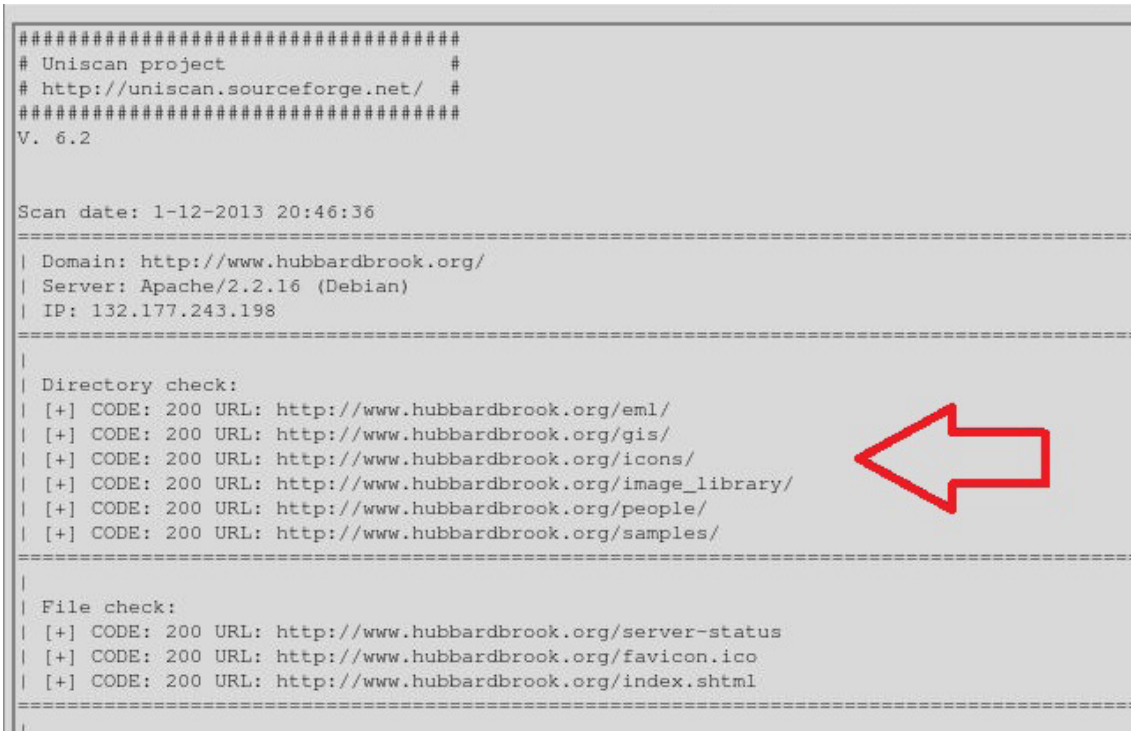
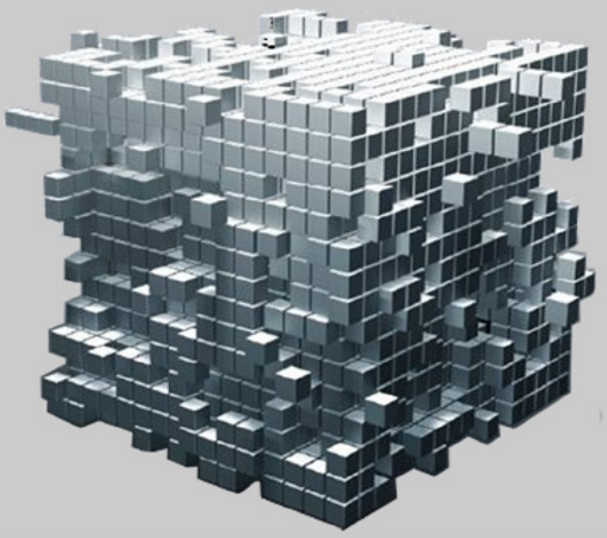


Figure 17. Log file – scan results



GoSecure!

penetration test_
vulnerability assessment_
computer forensics_

www.gosecure.it - info@gosecure.it
www.gosecure.it/blog

How to Install Android 4.3 on VM

by Rrajesh Kumar

In my previous article I teached you how to install BackTrack 5 on Virtual Machine. This time you will deal with Android 4.3. You will need just Android-x86-4.3.ISO and any Virtual Machine Software.

Requirements

- Android-x86-4.3.ISO
- Any Virtual Machine Software (recommended VM player & VM workstation)

Step 1.

Go to *File* and click on *New Virtual Machine* (Figure 1).

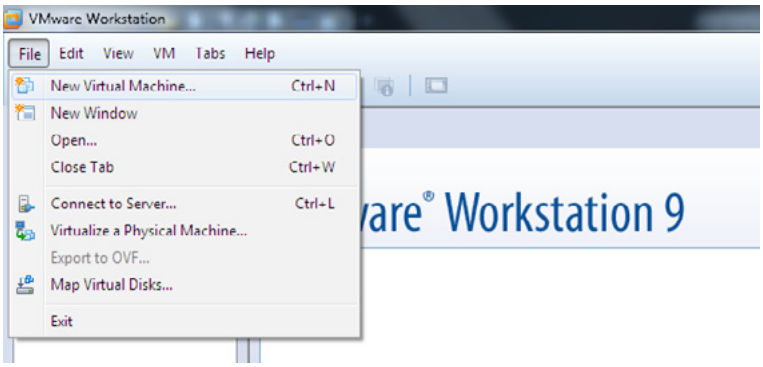


Figure 1. Creating a new virtual machine

Step 2.

Select *Typical* and click *Next* (Figure 2).

Figure 2. Choosing the type of configuration

Step 3.

Select the ISO file and click *Next* (Figure 3).

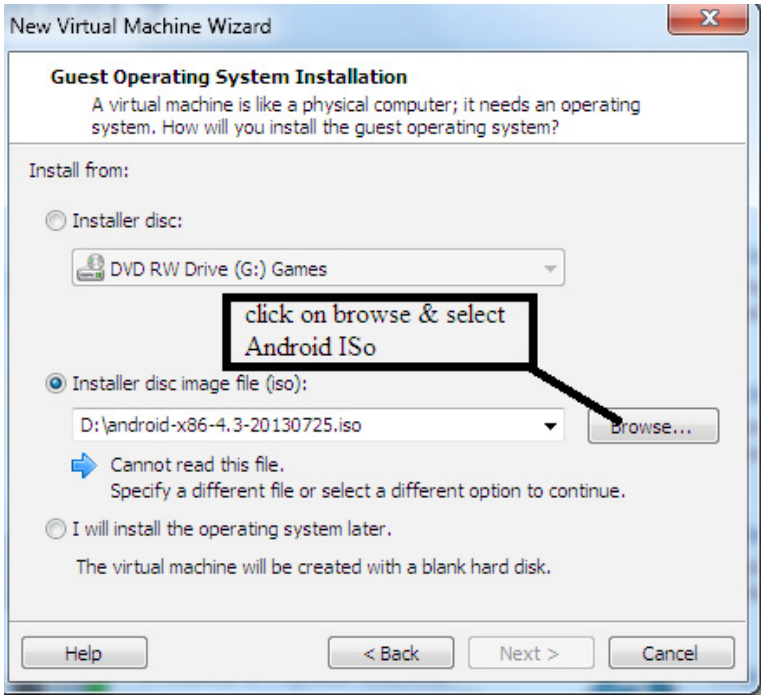


Figure 3. Selecting the ISO file

Step 4.

You can rename your OS and also you can choose where do you want to install it (Figure 4).

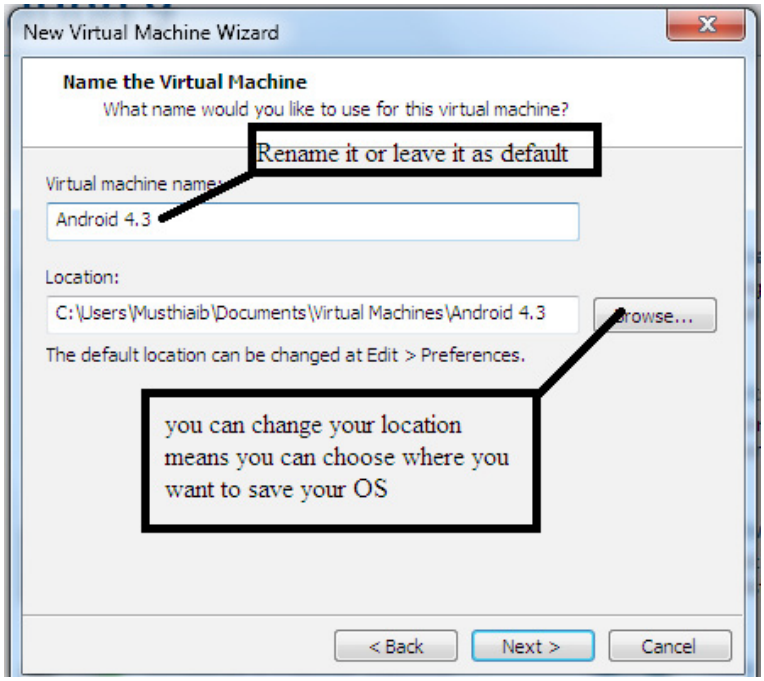


Figure 4. Choosing the installation path

Step 5.

Change your OS installation disk size (it should be more than 2 GB) for comfort and click *Next* (Figure 5).

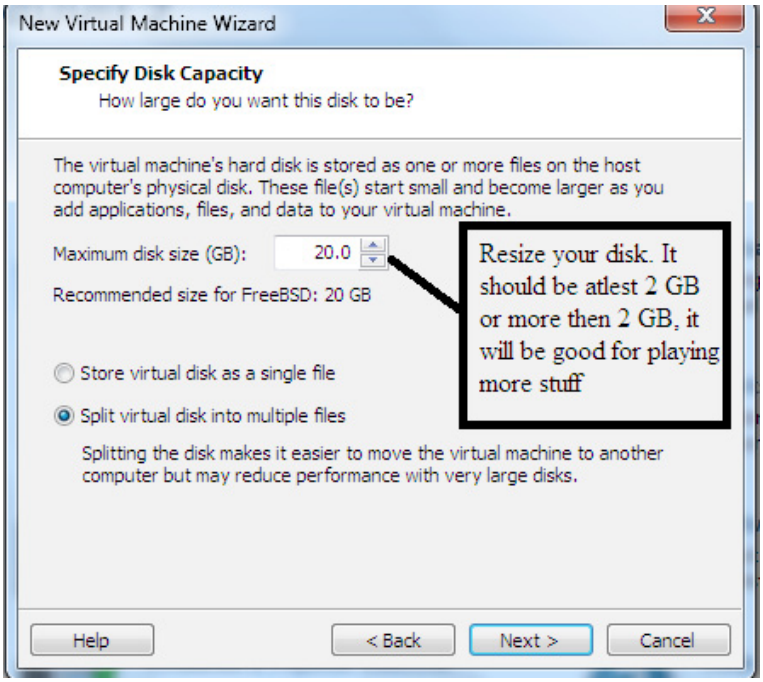


Figure 5. Changing your disk size

Step 6.

Click on *Finish* (Figure 6).

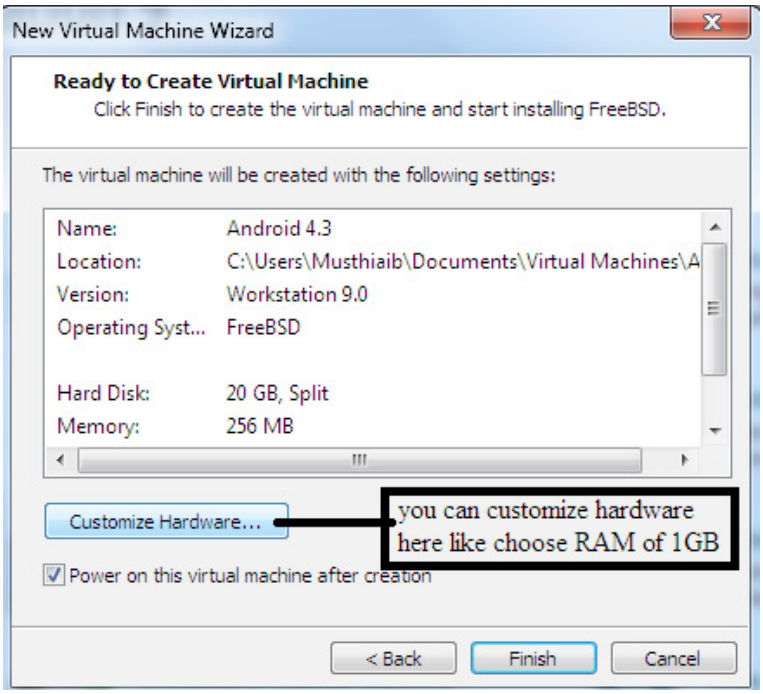


Figure 6. Finishing creating the VM

Step 7.

After booting your ISO, the screen similar to Figure 7 will show. Select *Installation* (Figure 7).

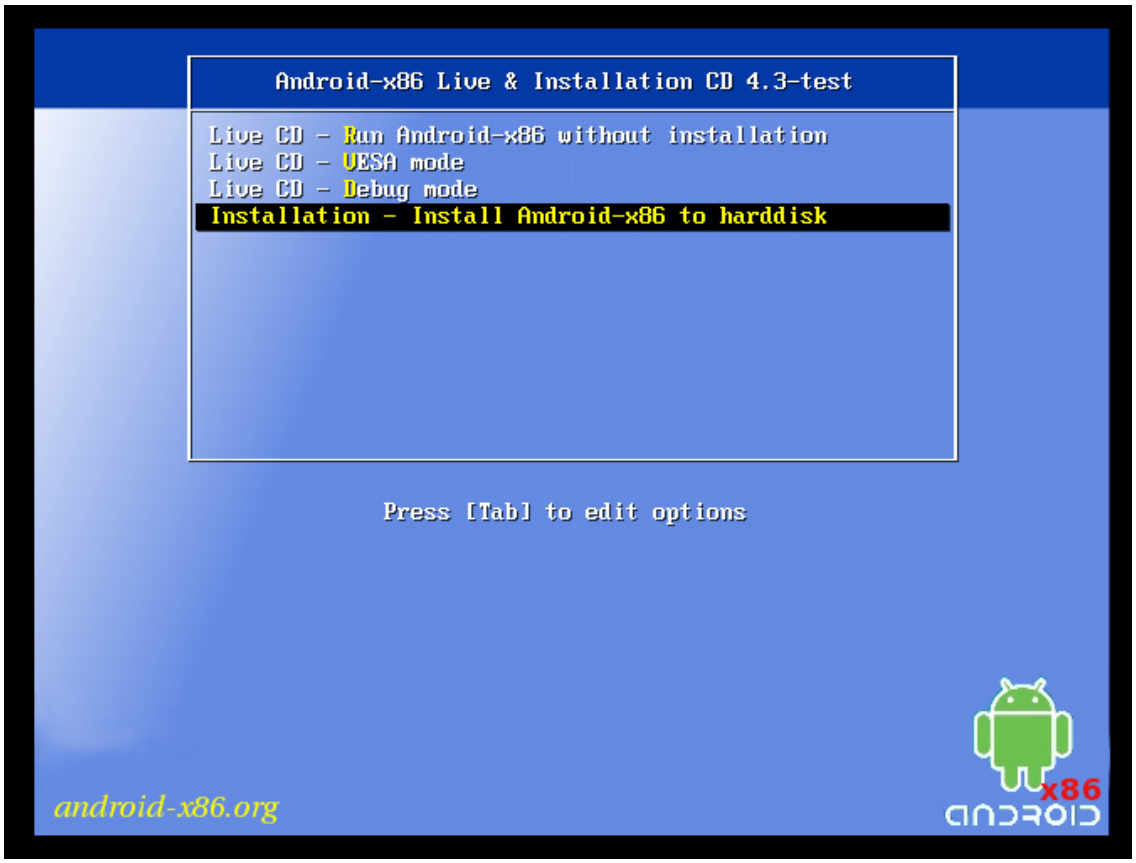


Figure 7. Starting the installation of the OS

Step 8.

Select *Create/Modify partitions* and click *OK* (Figure 8).

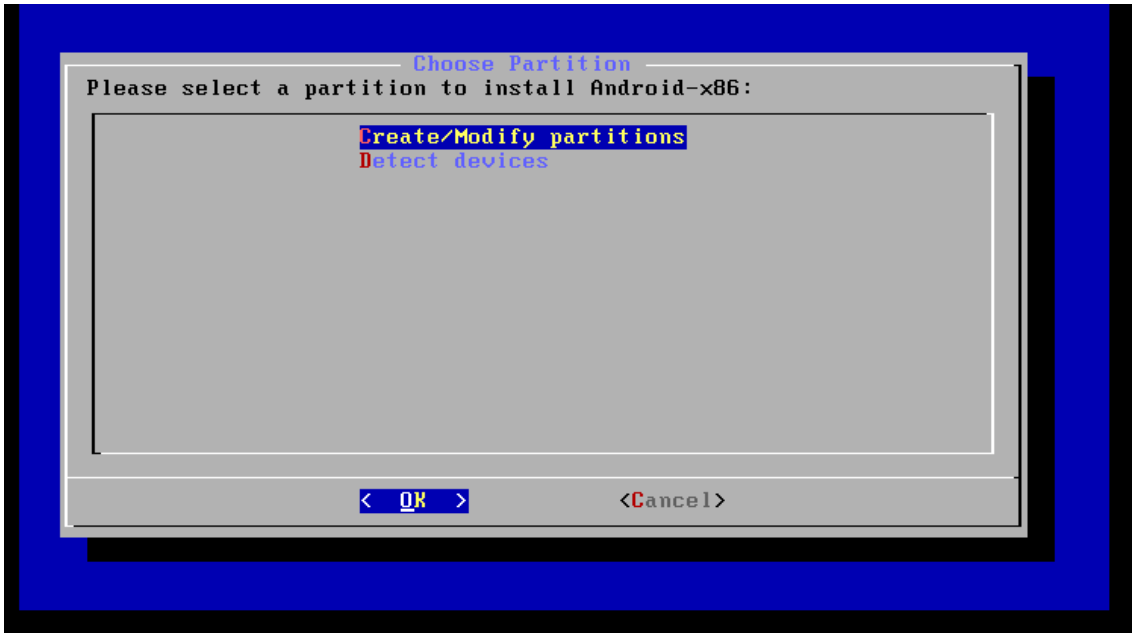


Figure 8. Creating or modifying partitions

Step 9.

Select *New* (Figure 9).

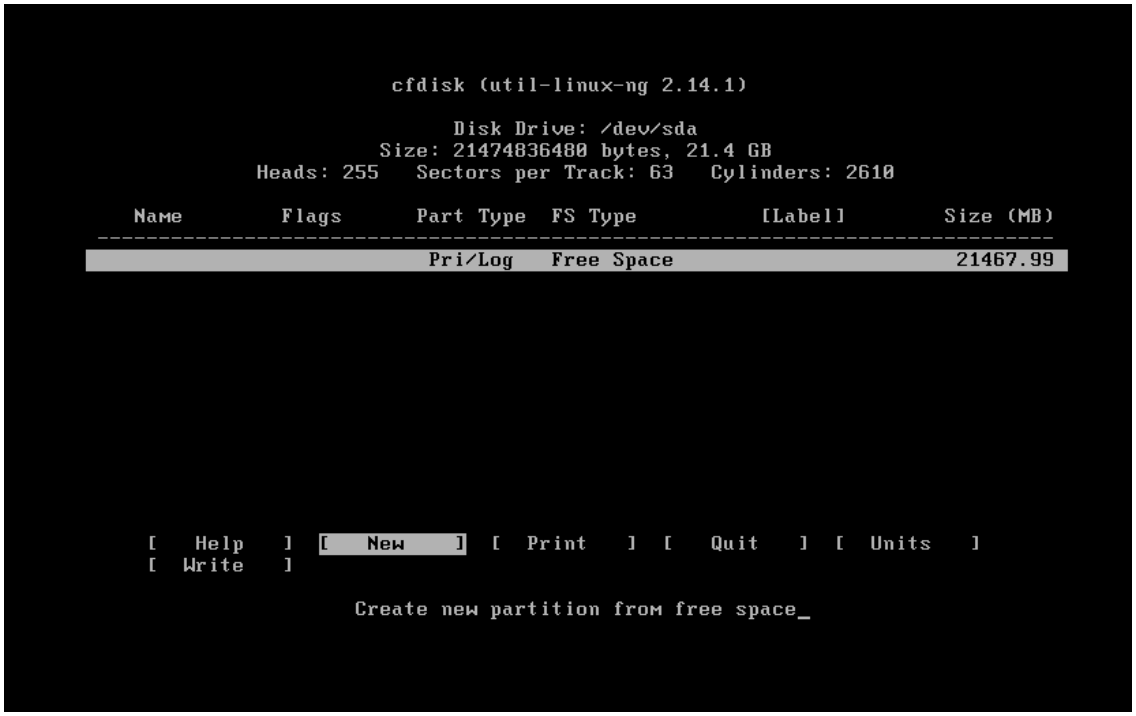


Figure 9. Creating a new partition

Step 10.

Select *Primary* (Figure 10).

Figure 10. Creating a primary partition

Step 11.

Let it be default and press *Enter* (Figure 11).

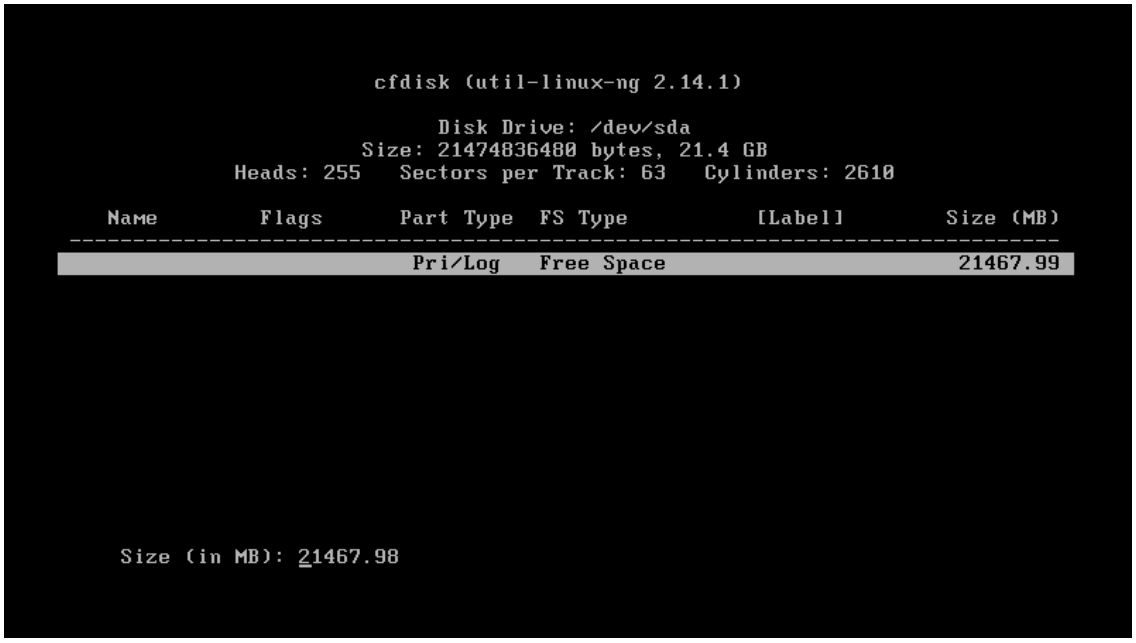


Figure 11. Default settings

Step 12.

Now select *Write* and press *Enter* (Figure 12).

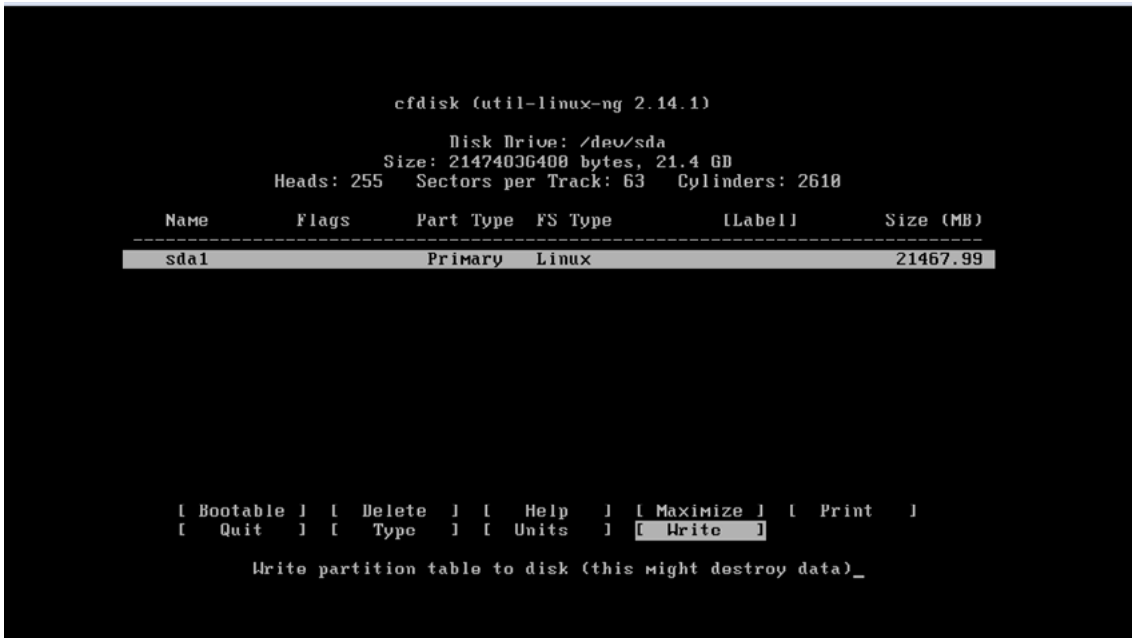


Figure 12. Selecting the Write option

Step 13.

Type *Yes* and press *Enter* (Figure 13).

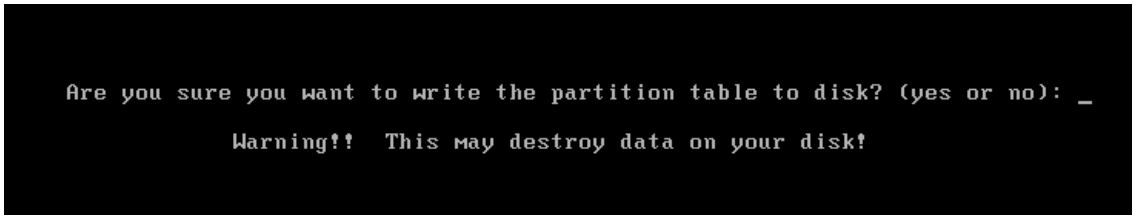


Figure 13. Writing the partition table to disk

Step 14.

Select *Quit* and press *Enter* (Figure 14).

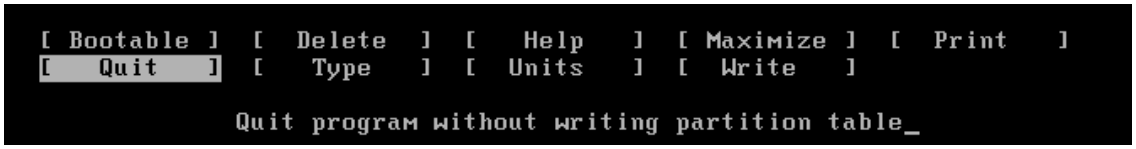


Figure 14. Quitting the program without writing partition table

Step 15.

Select `sda1` and press *Enter* (Figure 15).

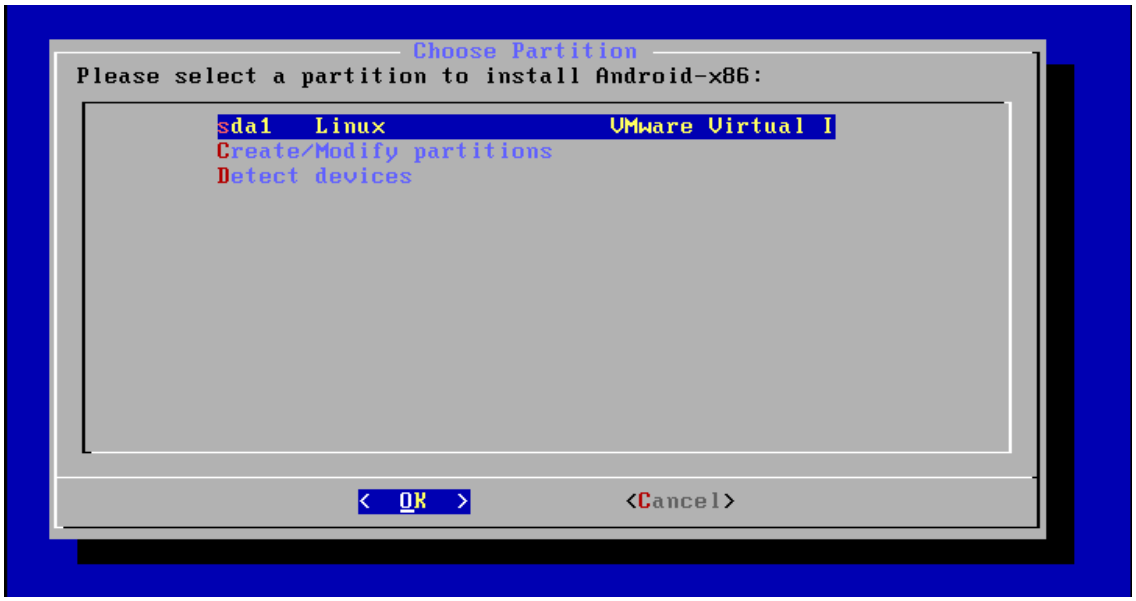


Figure 15. Selecting sda1

Step 16.

Select *ext3* and press *Enter* (Figure 16).

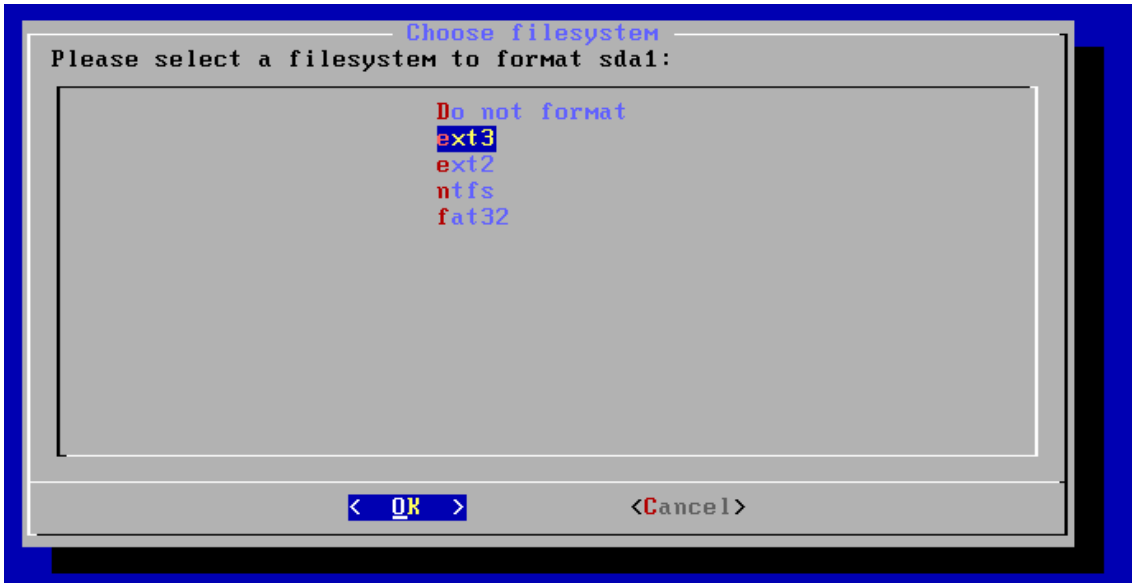


Figure 16. Selecting a filesystem to format sda1

Step 17.

Select *Yes* and press *Enter* (Figure 17).

Figure 17. Confirming formatting

Step 18.

Select *Yes* and press `Enter` (Figure 18).

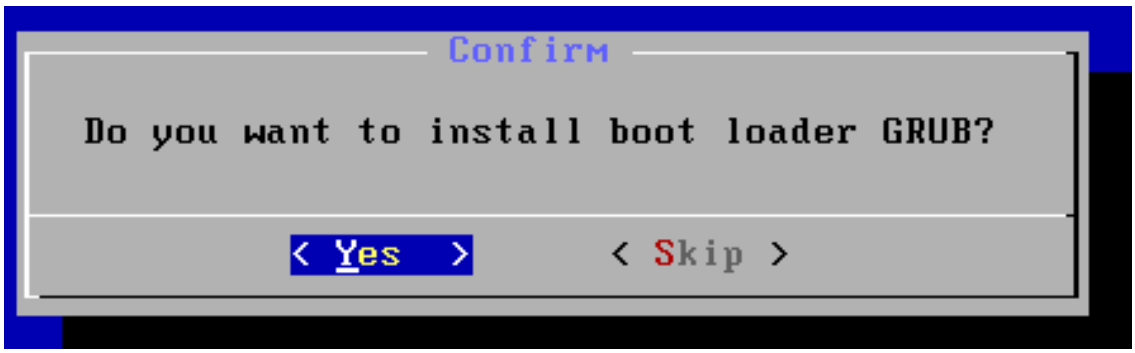


Figure 18. Installing GRUB

Step 19.

Select *Yes* and press *Enter* (Figure 19).

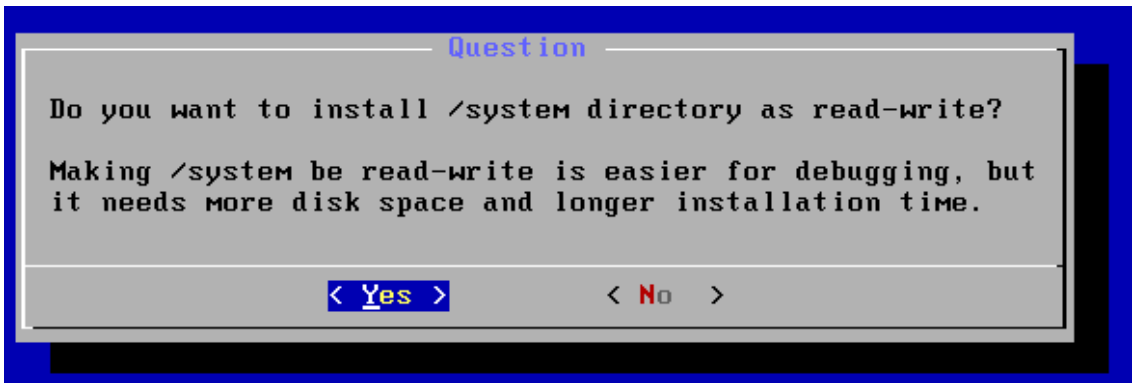


Figure 19. Installing /system directory as read-write

Step 20.

Select *Run Android-x86* and press *Enter* (Figure 20).

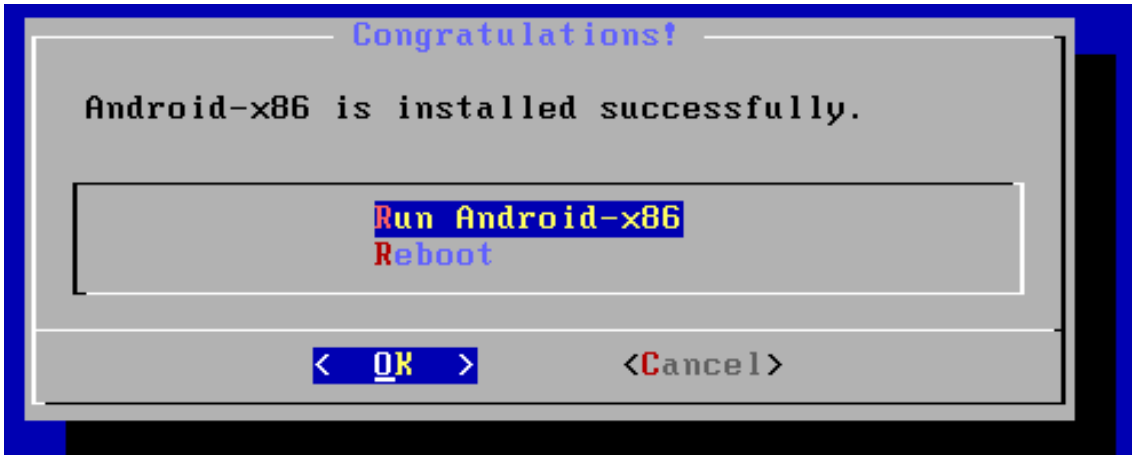


Figure 20. Running Android -x86

Step 21.

The booting has started (Figure 21). Be aware that it will take some time.

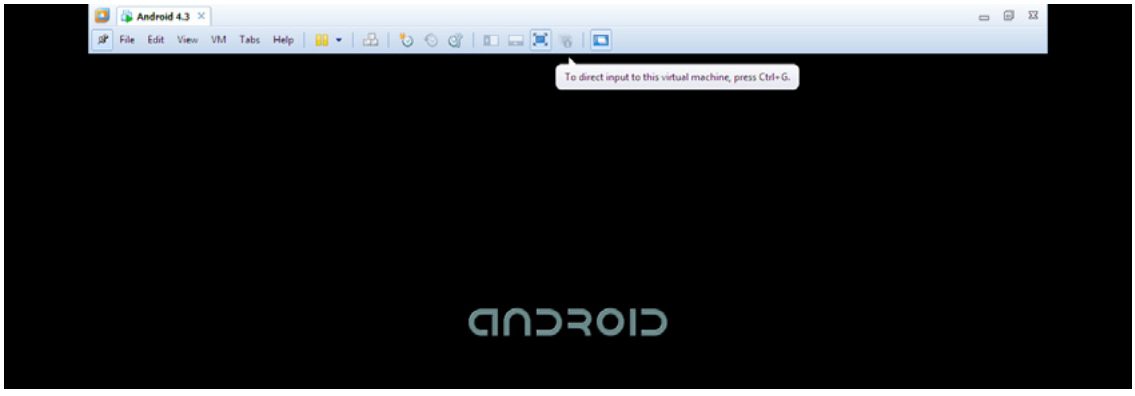


Figure 21. Boot screen

Step 22.

Select the language and click *Start* (Figure 22).

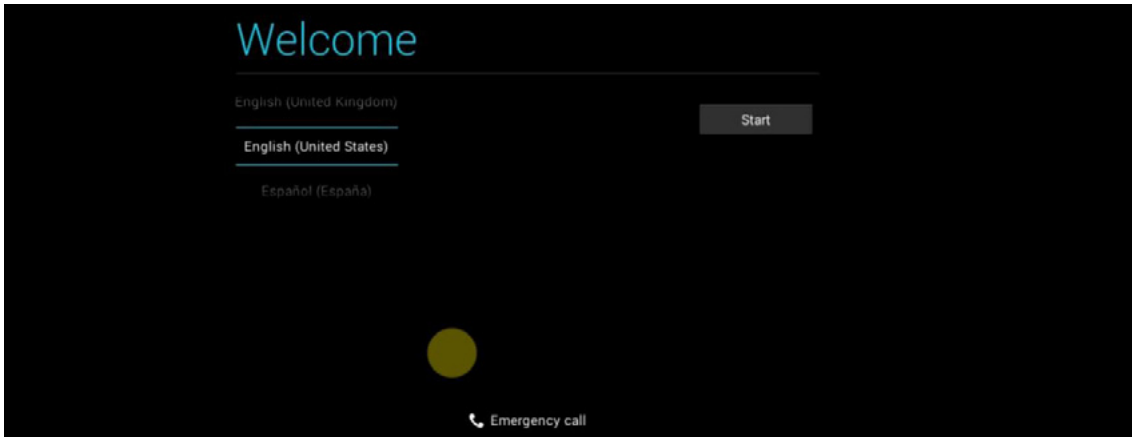


Figure 22. Language choice screen

Step 23.

It takes some time to load (Figure 23).

Figure 23. Loading

Step 24.

You can select the available network or just click *Skip* (Figure 24).

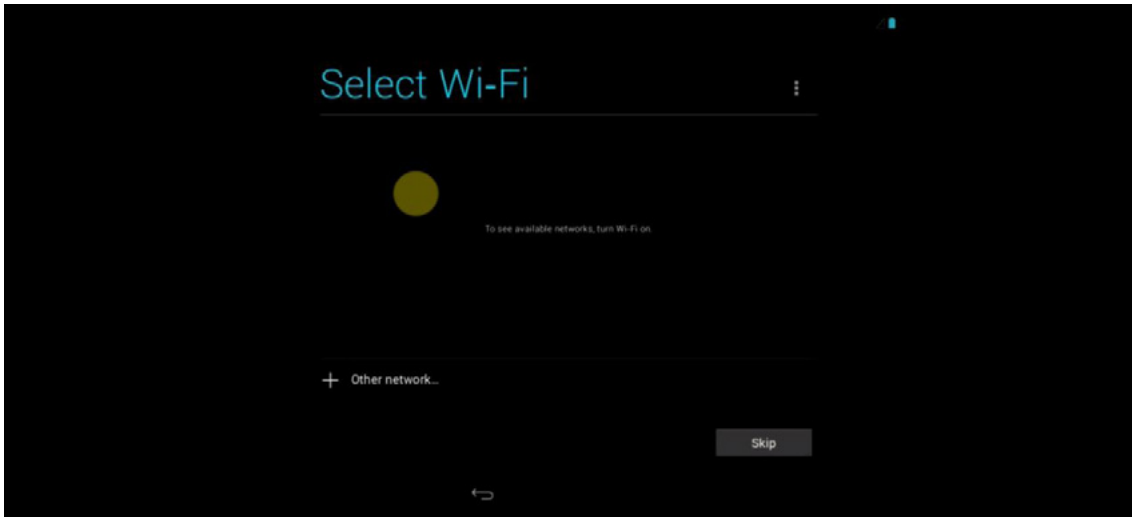


Figure 24. Choosing the network

Step 25.

Select *Yes* to setup your *Account* or No to set it up later (Figure 25).

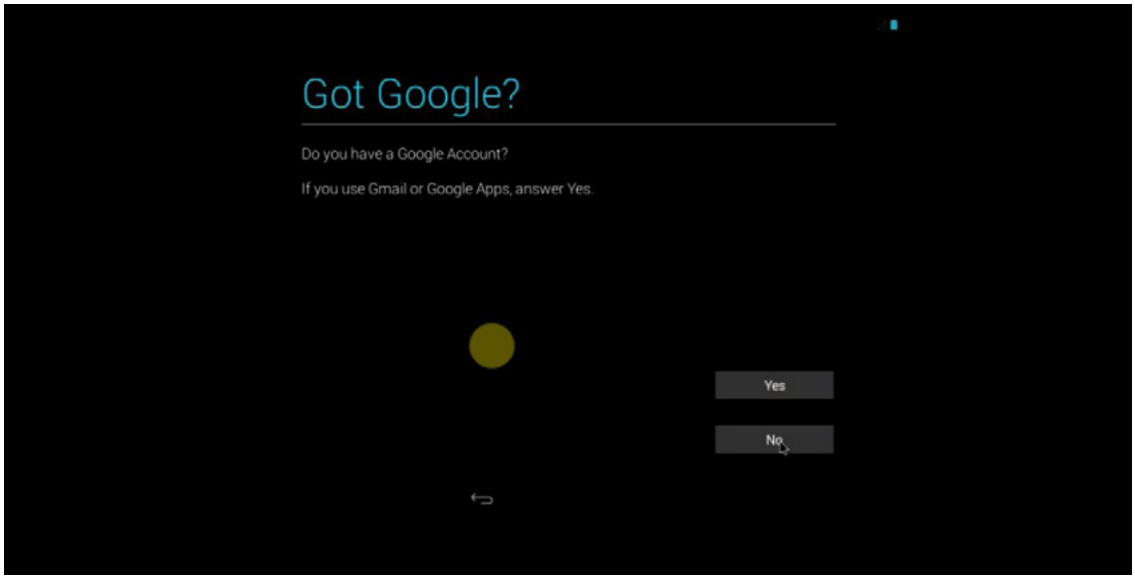


Figure 25. Setting up your Google account

Step 26.

Set the time and date. Then, click on the arrow (Figure 26).

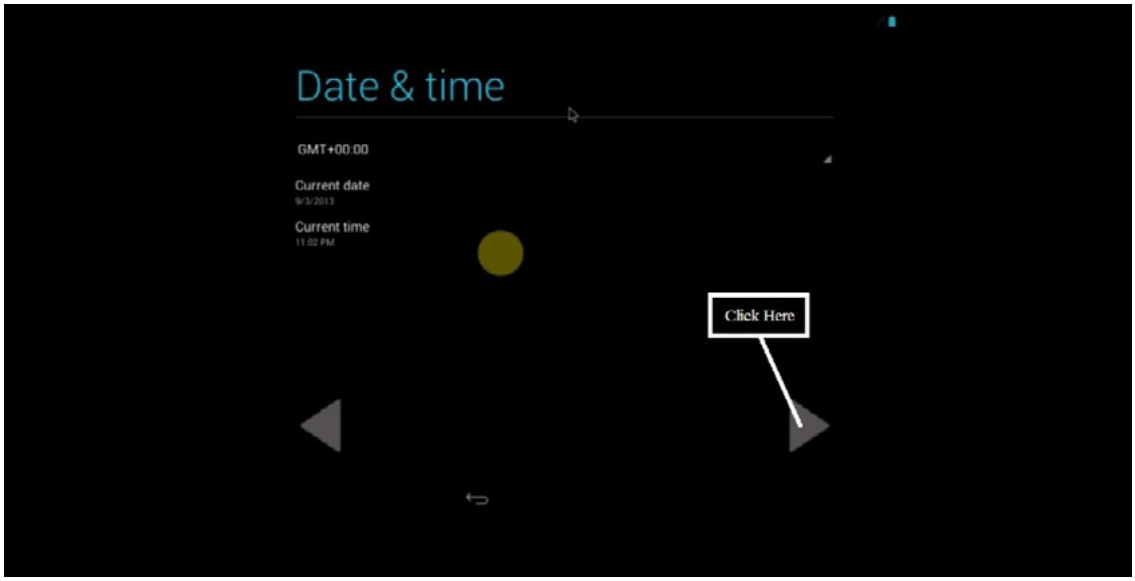


Figure 26. Setting date and time

Step 27.

Provide the username and click on the arrow (Figure 27).

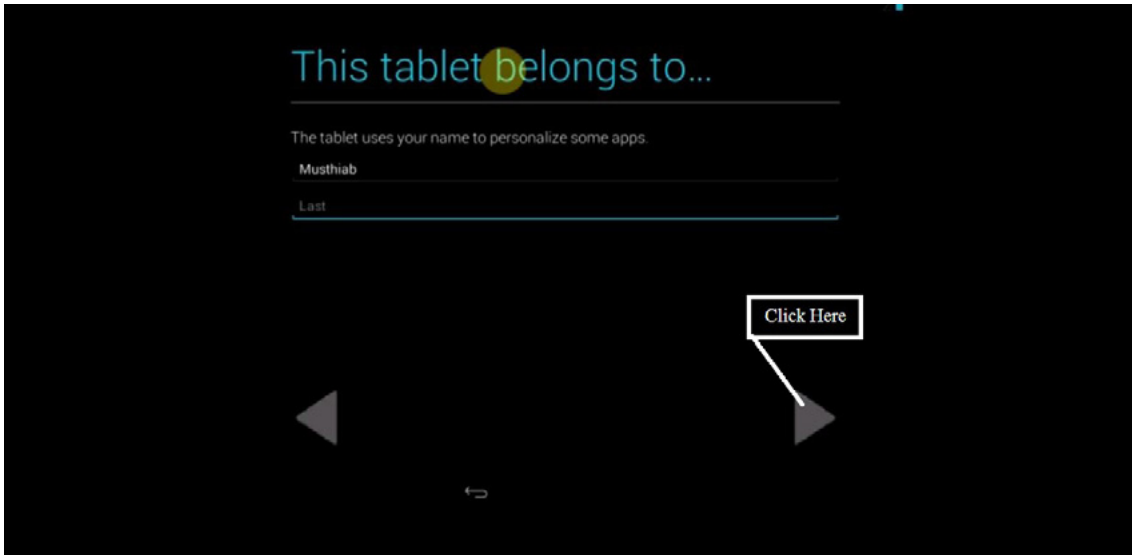


Figure 27. Providing the username

Step 28.

The desktop screen will appear (Figure 28).

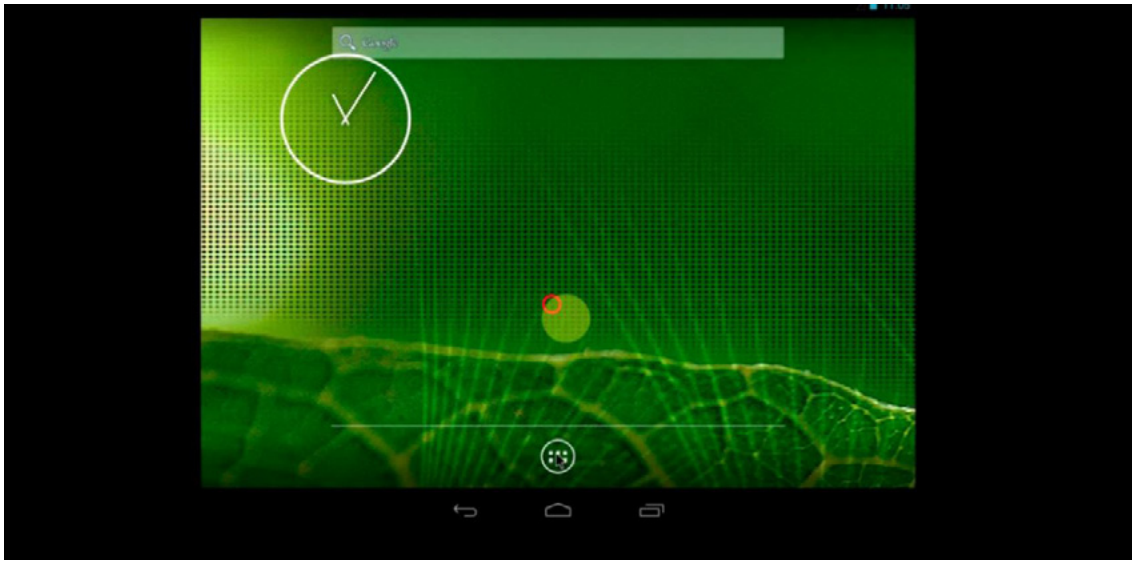


Figure 28. Desktop screen

Step 29.

You can take a look at the default applications (Figure 29).

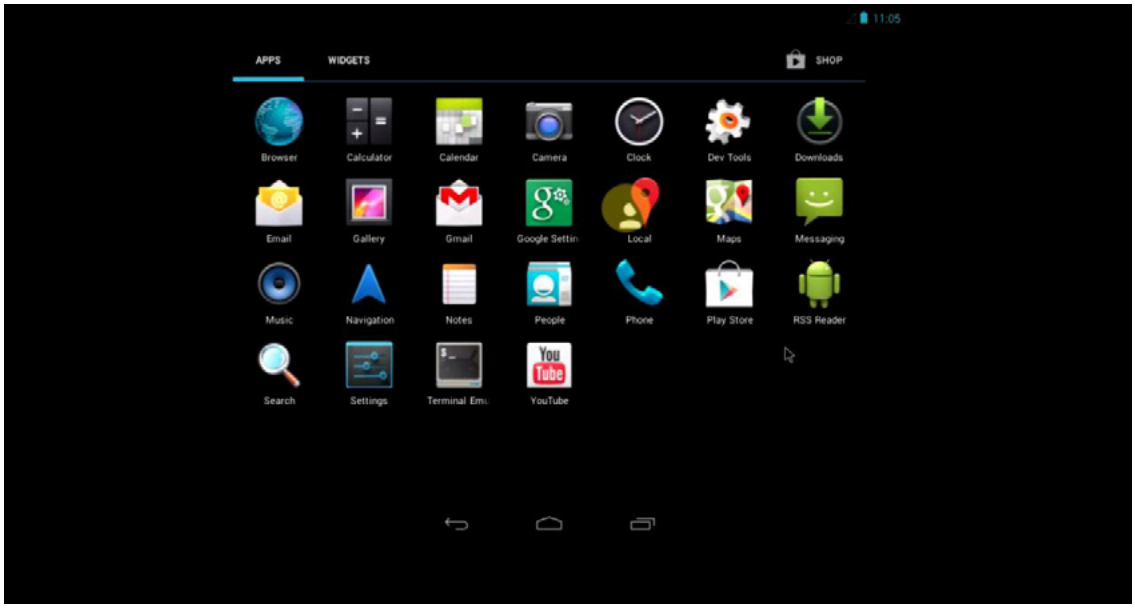


Figure 29. Default applications

Step 30.

You can check your Android version in *Settings* → *About tablet* (Figure 30).

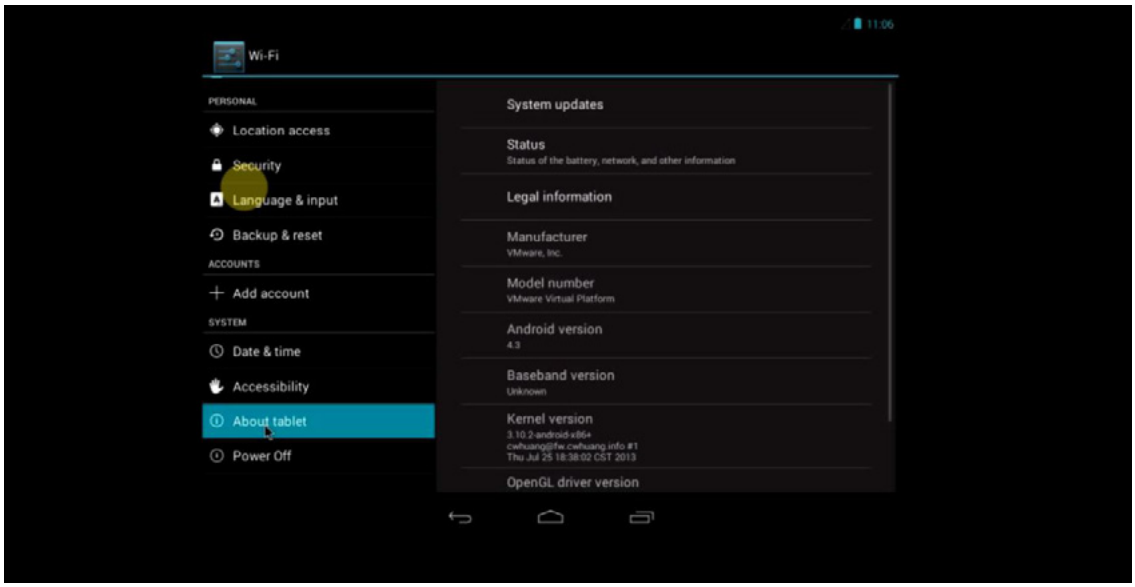


Figure 30. Checking your Android version

ANRC

A Cyber criminal can target and breach your organization's perimeter in less than a second from anywhere in the world ...

Are You Prepared?

ANRC delivers advanced cyber security training, consulting, and development services that provide our customers with peace of mind in an often confusing cyber security environment. ANRC's advanced security training program utilizes an intensive hands-on laboratory method of training taught by subject matter experts to provide Information Security professionals with the knowledge and skills necessary to defend against today's cyber-attacks and tomorrow's emerging threats.

ANRC's consulting and development services leverage team member knowledge and experience gained in the trenches while securing critical networks in the U.S. Department of Defense and large U.S. corporations. ANRC tailors these services to deliver computer security solutions specific to the needs of the customer's operational environment. Our approach emphasizes a close relationship with our clients as an integral part of our service. We believe we're all in the security battle together, and we view our customers as key members of our team in the fight.

TRAINING :: CONSULTING :: SOLUTIONS www.anrc-services.com

UPDATE NOW WITH STIG AUDITING

"IN SOME CASES **nipper studio** HAS VIRTUALLY **REMOVED** the NEED FOR a **MANUAL AUDIT**"

CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com

2012 Computing Security Awards WINNER Enterprise Security Solution of the Year

Security Products' GOVIES 2013 Government Security Awards

2012 Computing Security Awards WINNER Network Security Solution of the Year

www.titania.com