



SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

**Information Systems Security Audit & Control**

**4<sup>th</sup> Year 2<sup>nd</sup> Semester 2016**

Name: Harshanath W.W.D.K

SLIIT ID: IT13069032

Practical Session: WE Friday

Practical Number: Lab 3

Date of Evaluation : \_\_\_\_\_

Evaluators Signature : \_\_\_\_\_

# Kali Linux

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. Mati Aharoni, Devon Kearns and Raphaël Hertzog are the core developers.

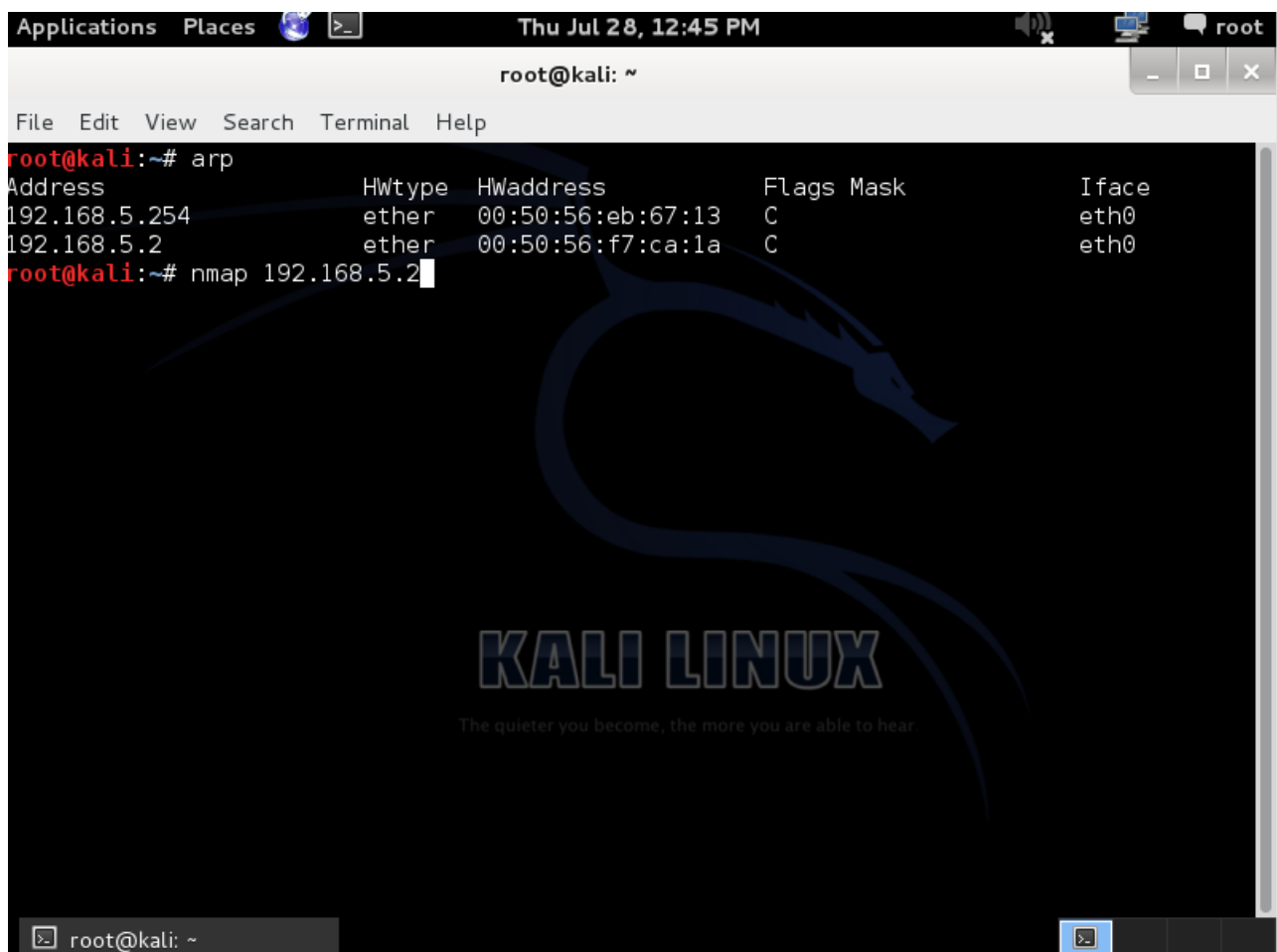
Kali Linux includes many well-known security tools, including

- Nmap
- Aircrack-ng
- Kismet
- Wireshark
- Metasploit Framework
- Burp suite
- John the Ripper
- Social Engineering Toolkit
- Airodump-ng

## Nmap Tool

Nmap (“Network Mapper”) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. 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. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

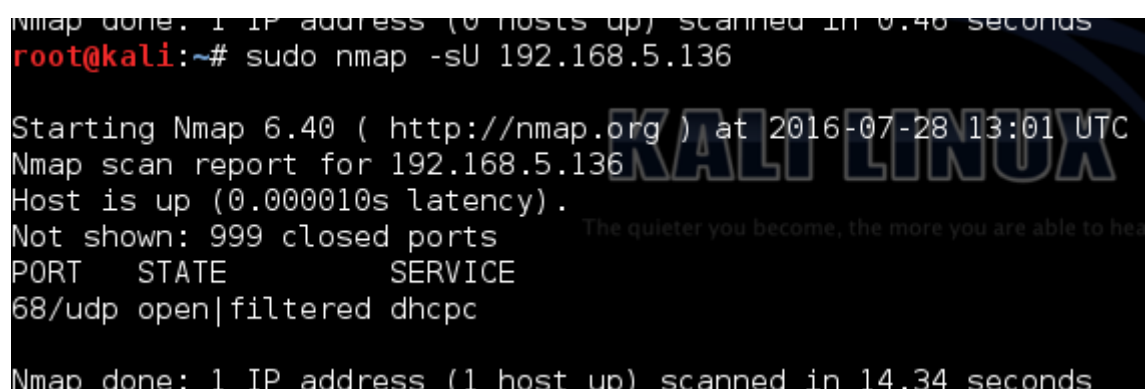
Use *arp* command to obtain the IP address of the machine



The screenshot shows a terminal window on a Kali Linux system. The window title is 'root@kali: ~'. The terminal output shows the command 'arp' being executed, which displays a table of ARP entries. The table has columns for Address, HWtype, HWaddress, Flags Mask, and Iface. The entries are for 192.168.5.254 and 192.168.5.2, both with HWtype 'ether' and Iface 'eth0'. The background of the terminal window features the Kali Linux logo and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear.'

```
root@kali:~# arp
Address          HWtype  HWaddress     Flags Mask    Iface
192.168.5.254    ether   00:50:56:eb:67:13  C             eth0
192.168.5.2      ether   00:50:56:f7:ca:1a  C             eth0
root@kali:~# nmap 192.168.5.2
```

Check UDP connection



The screenshot shows a terminal window on a Kali Linux system. The terminal output shows the command 'sudo nmap -sU 192.168.5.136' being executed. The output indicates that Nmap 6.40 is starting the scan at 2016-07-28 13:01 UTC. The scan report for 192.168.5.136 shows that the host is up (0.000010s latency). The output also shows 'Not shown: 999 closed ports' and '68/udp open|filtered dhcpc'. The background of the terminal window features the Kali Linux logo and the text 'KALI LINUX' and 'The quieter you become, the more you are able to hear.'

```
nmap done: 1 IP address (0 hosts up) scanned in 0.46 seconds
root@kali:~# sudo nmap -sU 192.168.5.136

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-28 13:01 UTC
Nmap scan report for 192.168.5.136
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc

Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
```

## Perform a sync scan

```
Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
root@kali:~# sudo nmap -sS 192.168.5.136

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-28 13:15 UTC
Nmap scan report for 192.168.5.136
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.5.136 are closed

Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
root@kali:~#
```

## Scan all TCP and UDP ports

```
root@kali:~# sudo nmap -n -PN -sT -sU -p 192.168.5.136

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-28 13:13 UTC
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
root@kali:~# sudo nmap -n -PN -sT -sU -p- 192.168.5.136

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-28 13:13 UTC
Nmap scan report for 192.168.5.136
Host is up (0.000048s latency).
Not shown: 131067 closed ports
PORT      STATE      SERVICE
60900/tcp  open      unknown
68/udp    open|filtered dhcpc
53182/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
root@kali:~#
```

## Scan of invalid TCP header sending

```
root@kali:~# sudo nmap -PN -p 80 -sN 192.168.5.136

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-28 13:17 UTC
Nmap scan report for 192.168.5.136
Host is up (0.000087s latency).
PORT      STATE      SERVICE
80/tcp    closed    http

Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
root@kali:~#
```

## Check the version of a running service

```
root@kali:~# sudo nmap -PN -p 80 -sV 192.168.5.136

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-28 13:21 UTC
Nmap scan report for 192.168.5.136
Host is up (0.000091s latency).
PORT      STATE      SERVICE VERSION
80/tcp    closed    http

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
root@kali:~#
```