3. Scanning Networks

Network Scanning

Practical 1: Using netdiscover command in Kali Linux

Open a terminal window and enter command in following syntax:

netdiscover -i <interface>
netdiscover -r <range>

For example:
netdiscover -i eth0
netdiscover -i 192.168.0.0/24

Practical 2: Using NMAP

Open a terminal windows and enter command in following syntax:

nmap -sn <subnet>
nmap -sP <subnet>

For example:
nmap -sn 192.168.0.0/24
nmap -sP 192.168.0.0/24

Practical 3: Using angry ip scanner

Download and install angry ip scanner from following link:
http://angryip.org/download

To install it in Kali Linux, enter following command:

dpkg -i <filename.deb>

For example:
dpkg -i ipscan_3.5.1_i386.deb

After successful installation, you can run Angry IP scanner. There you can provide starting IP address and ending IP address. It will find out all the running IP addresses in given range. The running IP addresses will be shown as blue colour.

Port/Service Scanning

We use NMAP or ZenMAP for ports and services scanning. Both tools comes pre-installed on Kali Linux and available for all other platforms.

Note: You should not scan any website, domain or sub domain without prior agreements. Doing so could lead you in legal trouble. We use our own network and systems to perform scanning. You can scan “scanme.nmap.org” for learning purpose.

Practical 4: Simple IP scanning using NMAP

For a simple scanning using NMAP we don’t require any options. We just need to provide target IP or domain.

Scanning singe host:

nmap <IP address>
For example:
nmap 192.168.0.100 or nmap scanme.nmap.org

Scanning multiple host (Seperated by space):

nmap <IP address> <IP address> <IP address> . . .
For example:
nmap 192.168.0.100 192.168.0.105 nmap scanme.nmap.org

Scanning a range or subnet:

nmap <range> or nmap <subnet>
For example:
nmap 192.168.0.100-200
nmap 192.168.0.0/24

Scanning a list:

nmap -iL <filename.txt>
For example:
nmap -iL /root/Desktop/scan.txt

Note: You first need to create a list file that contains target IP addresses. In that new IP should be on new line.

Practical 5: Scanning for specific port numbers

nmap -p <ports> <target IP>

For example:
nmap -p 21,22,23,80 192.168.0.100

Practical 6: Scanning IPv6

nmap -6 <target IP>

For example:
nmap -6 fe80::45b0:5dde:c583:d7f5%6

Practical 7: OS detection scan

nmap -O <tatget IP>

For example:
nmap -O 192.168.0.100

Practical 8: Version scan

nmap -sV <target IP>

For example:
nmap -sV 192.168.0.100

Practical 9: traceroute scan

nmap --traceroute <target IP>

For example:
nmap –traceroute 192.168.0.100

Practical 10: Aggression scan

nmap -A <target IP>

For example:
nmap -A 192.168.0.100

Practical 11: Advanced NMAP Scans

TCP Connect (Full Open) Scan:

nmap -sT <target IP>

For example:
nmap -sT 192.168.0.100

Stealth (Half Open) Scan:

nmap -sS <target IP>

For example:
nmap -sS 192.168.0.100

XMAS Scan:

nmap -sX <target IP>

For example:
nmap -sX 192.168.0.100

Null Scan:

nmap -sN <target IP>

For example:
nmap -sN 192.168.0.100

Idle (Zombie) Scan:

nmap -Pn -sI <zombie IP> <target IP>

For example:
nmap -Pn -sI 192.168.0.105 192.168.0.100

UDP Scan:

nmap -sU <target IP>

For example:
nmap -sU 192.168.0.100

Vulnerability Assessment Scanning (VA)

Practical 12: VA using NMAP

nmap --script=vuln <target IP> -vv

For example:
nmap --script=vuln 192.168.0.100 -vv

Practical 13: VA using Nessus Home Edition

Step 1: Installation

Download and install nessus from following link:

https://www.tenable.com/products/nessus/select-your-operating-system

In Kali Linux, enter following command to install

dpkg -i <filename.deb>

For example:
dpkg -i Nessus-6.10.7-debian6_i386.deb

Step 2: Starting Nessus Server

Enter following command in Kali Linux

service nessusd start

Step 3: Using Nessus Web GUI for scanning

In your favourite web browser enter following URL to access nessus

https://localhost:8834

By following on screen instructions, you can perform vulnerability assessment scan with Nessus.