crackchester crackchester crackchester

Introduction To Ethical Hacking

NMap/Port Detection

Workshop 2 - 20/10/2022

Kali Linux

To save time in future workshops, and to provide you with a suitable toolkit, we recommend installing a kali linux VM. Kali linux is a debian distribution designed for penetration testing. If you don't have a VM framework, we recommend either VMware or Virtualbox, this will be the program you use to launch the Virtual Machine. After you have your VM software installed

1. Head to https://www.kali.org/get-kali/ and select Virtual Machines
2. Select your VM software and press the download button
3. Once this download is complete, extract the file
4. Launch your VM software and press Add, then select the Machine image we just extracted
5. Adjust the settings to suit your system
6. Once installed, boot up the VM
7. Login to Kali using the Username & Password: kali / kali

Unlike Most VMs Kali is a very specialised tool, for this reason we recommend that you don't use tools that you are not familiar with, as many of them can be unsafe if used incorrectly. If you want to learn more about kali and it's tools feel free to message the society discord and we'll try to get back to you!

Network Reconnaissance

There are two types of network reconnaissance, passive and active

With active reconnaissance you will be legally liable if you are acting maliciously

Should only be used on networks with permission

Passive reconnaissance is not illegal

There are sites and services for this

Kali Linux

Kali Linux is an open-source, Linux distribution with a suite of tools useful for penetration testing and digital forensics.

It allows for network reconnaissance using the tool nmap

NMap

Useful for discovering networks and showing vulnerabilities.

Checks a network for hosts and services and send information to these

Read and interpret the response to create a map of the network

Very noisy process and a firewall is likely to deny access

Sites like scanme.nmap.org allow for practise

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

The -p argument is for choosing specific ports

A single port -p80

A list of ports -p80-100 or -p80,25,21

All of the ports -p-

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

The -s argument is the Scanning technique

TCP SYN port scan -sS

TCP connect port scan -sT

No Scan. List targets only -sL

No Scan. Host discovery only -sn

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

The -T timing argument ranges from T0-5

The most careful and least resource intensive is -T0

And the fastest scan being -T5

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

This argument is used for OS detection using TCP/IP stack fingerprinting

Remote OS detection -O

Makes Nmap guess more aggressively -O -osscan-guess

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

Service version detection

Standard detection `-sV`

Allows to set an intensity from 1-9 `-sV -version-intensity 8`

Lower chance of correctness but faster `-sV -version-light`

Opposite of light `-sV -version-all`

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

The -A enables OS detection, version detection, script scanning, and traceroute

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

This is for single IPs 192.168.0.1

Multiple Specific IPs 192.168.0.1 192.168.1.1

A range of IPs 192.168.0.1-254

Scan a domain scanme.nmap.org

Scan using CIDR 192.168.0.0/24

Other Useful NMap Arguments

Time before timing out `-host-timeout 2m`

Port scan retransmissions `-max-retries 3`

Send packets at most as fast `-max-rate 100`

Send packets at least as fast `-min-rate 100`

Key NMap Arguments

```
$ nmap -p80 -sS -T5 -O -sV -A 192.168.0.1
```

Ports -px -px-y -px,y,z -p-

Scanning modes -sS -sT -sL -sn

Timing -T0-5

OS Detection -O -O -osscan-guess

Version detection -sV -sV -version-intensity x -sV -version-light -sV -version-all

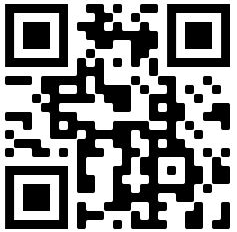
Address scanme.nmap.org 192.168.0.1-254 192.168.0.0/24

NMap - Resources

Test out nmap using challenges on Hack the box

Or just practise with scanme.nmap.org

Use the data on shodan.io or censys.io for passive reconnaissance.



Crackchester

Put yourself in the running for our new PR Officer position here!

Here’s a link to our link tree where you can find all our socials and our discord!


crackchester crackchester
chester
Demonstration