Peter the Great St.Petersburg Polytechnic University

Institute of Computer Science & Technologys

Department of Computer Systems & Software Engineering

**Laboratory №2 Report Discipline:** Information Security

**Theme:** Nmap utility

Made by student of group. 13541/1 Smirnov M.I.

(signature)

Lecturer Bogach N.V.

(signature)

“ ” 2017 г.

Saint-Petersburg

2017

Contents

|  |  |  |  |
| --- | --- | --- | --- |
| 1 Nmap (”Network Mapper”) – a free and open source utility for network discovery and | | |  |
|  | security auditing | | 2 |
|  | 1.1 | Objectives . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 2 |
|  | 1.2 | Task . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 2 |
| 2 | Work Progress | | 3 |
|  | 2.1 | Preparing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
|  | 2.2 | List targets to scan . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
|  | 2.3 | Probe open ports to determine service/version info . . . . . . . . . . . . . . . . | 6 |
|  | 2.4 | Study nmap-services, nmap-os-db, nmap-service-probes . . . . . . . . . . . . . | 8 |
|  | 2.5 | Add new service to nmap-service-probes (create a minimal tcp server, get its |  |
|  |  | name and version by nmap) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 11 |
|  | 2.6 | Output to xml-format file . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 13 |
|  | 2.7 | Study nmap stages and modes using Wireshark . . . . . . . . . . . . . . . . . . | 14 |
|  | 2.8 | Perform VM Metasploitable2 scanning using db\_nmap from metasploit frame- |  |
|  |  | work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 17 |
|  | 2.9 | Get 5 records from nmap-service-probes and describe them. . . . . . . . . . . . | 19 |
|  | 2.10 | Choose one Nmap Script and describe it . . . . . . . . . . . . . . . . . . . . . . . | 20 |
| 3 | Conclusion | | 22 |

1

Nmap (”Network Mapper”) – a free and open source utility for network discovery and se-curity auditing

1.1 Objectives

After completing this module you will be able to:

1. perform network discovery with various TARGET SPECIFICATION (hostnames, IP ad-dresses, networks, etc.);
2. perform HOST DISCOVERY;
3. apply a variety of SCAN TECHNIQUES;
4. perform PORT SPECIFICATION AND set SCAN ORDER;
5. perform SERVICE/VERSION DETECTION;
6. perform SCRIPT SCAN;
7. perform OS DETECTION;
8. manage TIMING AND PERFORMANCE.

1.2 Task

1. List targets to scan;
2. Probe open ports to determine service/version info;
3. Study nmap-services, nmap-os-db, nmap-service-probes;
4. (OPTIONAL) Add new service to nmap-service-probes (create a minimal tcp server, get its name and version by nmap);
5. Output to xml-format file;
6. Study nmap stages and modes using Wireshark.

Perform VM Metasploitable2 scanning using db\_nmap from metasploitframework.

Get 5 records from nmap-service-probes and describe them. Choose one Nmap Script and describe it

2

Work Progress

2.1 Preparing

1. Download last kali linux and metasploitable2 distributions;
2. Install it in VMware Workstation;
3. Setting up common network;
4. Define the IP addresses of virtual machines;
5. Check ping request’s in both ways.

As common network choosed - VMnet8.

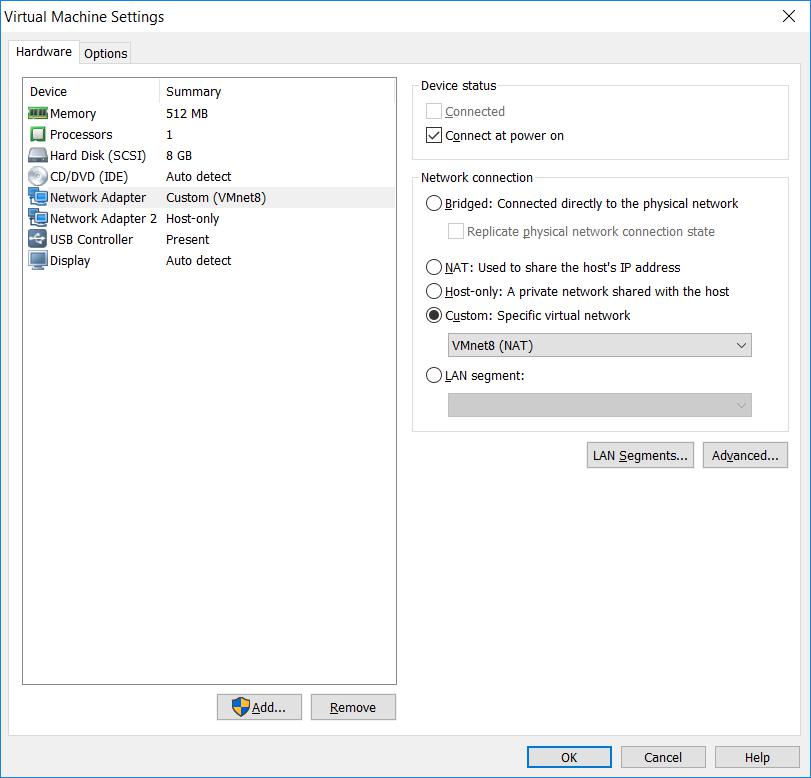


Figure 2.1: Metasploitable2 settings

3

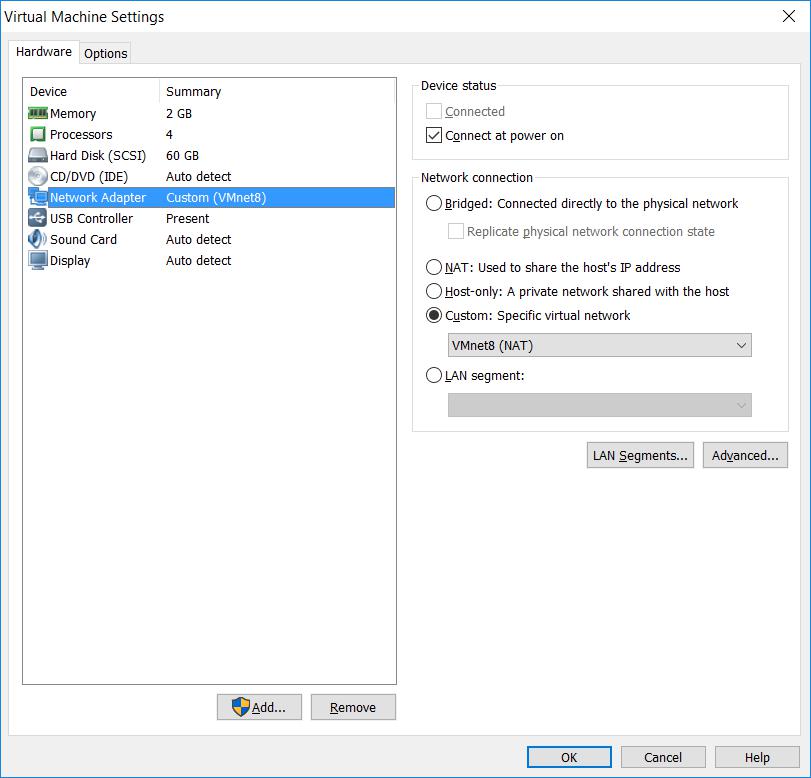
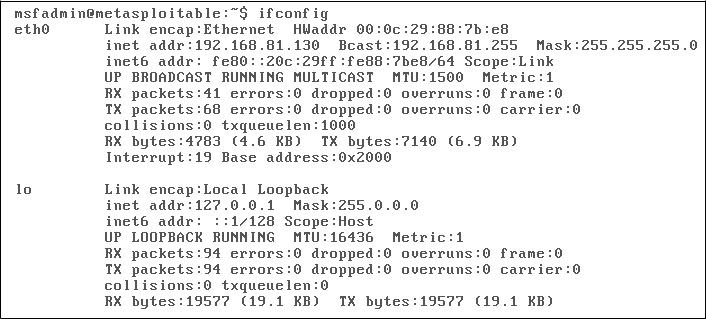


Figure 2.2: Kali settings

Now power on VM’s and define their IP addresses.



|  |  |  |  |
| --- | --- | --- | --- |
|  | Figure 2.3: Metasploitable2 ifconfig |  |  |
|  |  |  |  |
| 1 | r o o t @ k a l i : ~# i f c o n f i g |  |  |
| 2 | eth0 : f l a g s =4163<UP , BROADCAST , RUNNING , MULTICAST> | | mtu 1500 |
| 3 | i n e t 1 9 2 . 1 6 8 . 8 1 . 1 2 9 netmask 2 5 5 . 2 5 5 . 2 | 5 5 . 0 | broadcast |
|  | *,!* 1 9 2 . 1 6 8 . 8 1 . 2 5 5 |  |  |

4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | i n e t 6 | | fe80 : : 2 0 c : 2 9 f f : feed : c99e | | | | | | | p r e f i x l e n | | 64 | scopeid 0x20 | |
|  | *,!* < l i n k > | |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | e t h e r | | 0 0 : 0 c : 2 9 : ed : c9 : 9 e | | | | |  | t x q u e u e l e n | | 1000 | ( E t h e r n e t ) | |  |
| 6 | RX | packets | |  | 69 | b y t e s | 7784 | | ( 7 . 6 | KiB ) |  |  |  |  |
| 7 | RX | e r r o r s | | 0 | dropped | | 0 | o v e r r u n s 0 | | | frame | 0 |  |  |
| 8 | TX | packets | |  | 36 | b y t e s | 3002 | | ( 2 . 9 | KiB ) |  |  |  |  |
| 9 | TX | e r r o r s | | 0 | dropped | | 0 | o v e r r u n s | | 0 c a r r i e r | | 0 | c o l l i s i o n s | 0 |
| 10 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 | l o : f l a g s =73<UP , LOOPBACK , RUNNING> | | | | | | | | mtu | 65536 |  |  |  |  |
| 12 | i n e t 1 2 7 . 0 . 0 . 1 | | | | | netmask | | 2 5 5 . 0 . 0 . 0 | | |  |  |  |  |
| 13 | i n e t 6 | | : : 1 |  | p r e f i x l e n | | 128 | | scopeid 0x10 < host > | | | |  |  |
| 14 | l o o p | | t x q u e u e l e n 1000 | | | |  | ( L o c a l Loopback ) | | | |  |  |  |
| 15 | RX | packets | |  | 26 | b y t e s | 1518 | | ( 1 . 4 | KiB ) |  |  |  |  |
| 16 | RX | e r r o r s | | 0 | dropped | | 0 | o v e r r u n s 0 | | | frame | 0 |  |  |
| 17 | TX | packets | |  | 26 | b y t e s | 1518 | | ( 1 . 4 | KiB ) |  |  |  |  |
| 18 | TX | e r r o r s | | 0 | dropped | | 0 | o v e r r u n s | | 0 c a r r i e r | | 0 | c o l l i s i o n s | 0 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

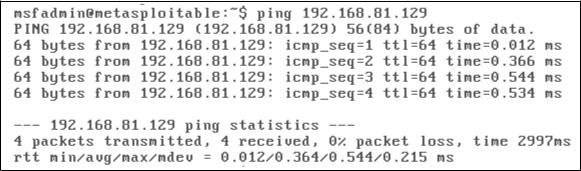
Listing 2.1: Kali ifconfig

Using ifconfig command, i defined IP addresses:

Metasploitable2 IP - 192.168.81.130

Kali IP - 192.168.81.129

To test that VM see each other, use the ping command.



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Figure 2.4: Metasploitable2 ping | | | |  |  |  |
|  |  | | |  |  |  |  |  |
| 1 | r o o t @ k a l i : ~# p i n g 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | |  |  |  |  |  |
| 2 | PING 1 9 2 . 1 6 8 . 8 1 . 1 3 0 ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 ) 5 6 ( | | | | 8 4 ) b y t e s | | o f data . |  |
| 3 | 64 | b y t e s from 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : icmp\_seq=1 | | | t t l =64 | time =2.08 | | ms |
| 4 | 64 | b y t e s from 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : icmp\_seq=2 | | | t t l =64 | time =0.542 | | ms |
| 5 | 64 | b y t e s from 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : icmp\_seq=3 | | | t t l =64 | time =0.579 | | ms |
| 6 | 64 | b y t e s from 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : icmp\_seq=4 | | | t t l =64 | time =0.669 | | ms |
| 7 | ^C |  |  |  |  |  |  |  |
| 8 | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 p i n g | | s t a t i s t i c s |  |  |  |  |
| 9 | 4 packets t r a n s m i t t e d , | | 4 r e c e i v e d , | 0% packet l o s s , | | | time 3061ms | |
| 10 | r t t | min / avg /max/mdev = | 0 . 5 4 2 / 0 . 9 6 8 / 2 . 0 8 5 / 0 . 6 4 7 ms | | | |  |  |
|  |  |  |  |  |  |  |  |  |

Listing 2.2: Kali ping

Ping requests were successfully completed, which means that the network is working suc-cessfully.

5

2.2 List targets to scan

The following command will be used to scan the network:

nmap -sn 192.168.81.0-255

Key sn means only ping scan, without port scan. 0-255 means in what range nmap should find target’s.

* r o o t @ k a l i : ~# nmap sn 192.168.81.0 255

2

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3 | S t a r t i n g Nmap | | | 7. 6 0 ( | | h t t p s : / / nmap . org ) a t 2017 11 04 06:13 EDT |
| 4 | Nmap | scan | r e p o r t | | f o r | 1 9 2 . 1 6 8 . 8 1 . 1 |
| 5 | Host | i s up | ( 0 . 0 0 0 5 0 s | | | l a t e n c y ) . |
| 6 | MAC | Address : | | 0 0 : 5 0 : 5 6 : C0 : 0 0 : 0 8 ( VMware ) | | |
| 7 | Nmap | scan | r e p o r t | | f o r | 1 9 2 . 1 6 8 . 8 1 . 2 |
| 8 | Host | i s up | ( 0 . 0 0 0 3 3 s | | | l a t e n c y ) . |
| 9 | MAC | Address : | | 0 0 : 5 0 : 5 6 : EF : 0 6 : 7 B ( VMware ) | | |
| 10 | Nmap | scan | r e p o r t | | f o r | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 11 | Host | i s up | ( 0.10 s l a t e n c y ) . | | | |
| 12 | MAC | Address : | | 0 0 : 0C : 2 9 : 8 8 : 7 B : E8 ( VMware ) | | |
| 13 | Nmap | scan | r e p o r t | | f o r | 1 9 2 . 1 6 8 . 8 1 . 2 5 4 |
| 14 | Host | i s up | ( 0.12 s l a t e n c y ) . | | | |
| 15 | MAC | Address : | | 0 0 : 5 0 : 5 6 : E1 : C6 : C7 ( VMware ) | | |
| 16 | Nmap | scan | r e p o r t | | f o r | 1 9 2 . 1 6 8 . 8 1 . 1 2 9 |

1. Host i s up .
2. Nmap done : 256 I P addresses ( 5 hosts up ) scanned i n 3. 2 3 seconds

Listing 2.3: NMAP scanning result

Metasploitable2 was successfully found.

2.3 Probe open ports to determine service/version info

Now scan 10 most popular ports at Metasploitable2 IP address.

* r o o t @ k a l i : ~# nmap top p o r t s 10 1 9 2 . 1 6 8 . 8 1 . 1 3 0

2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3 | S t a r t i n g | | Nmap 7. 6 0 ( h t t p s : / / nmap . org ) a t 2017 11 04 08:37 EDT | |
| 4 | Nmap | scan | r e p o r t | f o r 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 5 | Host | i s up ( 0 . 0 0 0 4 5 s l a t e n c y ) . | | |
| 6 | PORT |  | STATE | SERVICE |
| 7 | 21/ t c p | | open | f t p |
| 8 | 22/ t c p | | open | ssh |
| 9 | 23/ t c p | | open | t e l n e t |
| 10 | 25/ t c p | | open | smtp |
| 11 | 80/ t c p | | open | h t t p |
| 12 | 110/ t c p | | c l o s e d pop3 | |
| 13 | 139/ t c p | | open | n e t b i o s ssn |
| 14 | 443/ t c p | | c l o s e d | h t t p s |
| 15 | 445/ t c p | | open | m i c r o s o f t ds |

6

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 16 | 3389/ t c p c l o s e d | | ms wbt s e r v e r |  |
| 17 | MAC Address : | 0 0 : 0C : 2 9 : 8 8 : 7 B : E8 | | ( VMware ) |
| 18 |  |  |  |  |
| 19 | Nmap done : 1 | I P | address ( 1 host | up ) scanned i n 0 . 71 seconds |
|  |  |  |  |  |

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

Listing 2.4: NMAP scanning ports

Now determine service and version info with the sV key.

r o o t @ k a l i : ~# nmap sV 1 9 2 . 1 6 8 . 8 1 . 1 3 0

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S t a r t i n g | | Nmap 7. 6 0 ( | | | h t t p s : / / nmap . org ) a t 2017 11 04 08:40 EDT | | | | | | | | | | |
| Nmap | scan | | r e p o r t f o r | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | | | | | | | |
| Host | i s | up | ( 0 . 0 0 0 3 3 s | | l a t e n c y ) . | | | | | | | | | | |
| Not shown : 977 c l o s e d p o r t s | | | | | |  |  |  |  |  |  |  |  |  |  | |
| PORT | | STATE SERVICE | | | | VERSION |  |  |  |  |  |  |  |  |  | |
| 21/ t c p | | open | | f t p | | v s f t p d | 2 . 3 . 4 | | |  |  |  |  |  |  | |
| 22/ t c p | | open | | ssh | | OpenSSH | 4 . 7 p1 | | | Debian | | | 8ubuntu1 | | ( p r o t o c o l | |
| *,!*2 . 0 ) | | | |  | |  |  |  |  |  |  |  |  |  |  | |
| 23/ t c p | | open | | t e l n e t | | L i n u x t e l n e t d | | | |  |  |  |  |  |  | |
| 25/ t c p | | open | | smtp | | P o s t f i x | smtpd | | |  |  |  |  |  |  | |
| 53/ t c p | | open | | domain | | ISC BIND 9 . 4 . 2 | | | |  |  |  |  |  |  | |
| 80/ t c p | | open | | h t t p | | Apache | h t t p d 2 . 2 . 8 | | | | | ( ( Ubuntu ) | | | DAV / 2 ) | |
| 111/ t c p | | open | | r p c b i n d | | 2 ( RPC | #100000) | | | |  |  |  |  |  | |
| 139/ t c p | | open | | n e t b i o s ssn | | Samba smbd | | | 3 . X 4 . X | | | | ( workgroup : | | | |
| *,!* WORKGROUP) | | | | | |  |  |  | 3 . X 4 . X | | | |  |  |  | |
| 445/ t c p | | open | | n e t b i o s ssn | | Samba smbd | | | ( workgroup : | | | |
| *,!* WORKGROUP) | | | | | | n e t k i t r s h | | |  |  |  |  |  |  |  | |
| 512/ t c p | | open | | exec | | rexecd | | |  |  |  |  | |
| 513/ t c p | | open | | l o g i n | | OpenBSD | o r S o l a r i s | | | | | r l o g i n d | | |  | |
| 514/ t c p | | open | | tcpwrapped | |  |  |  |  |  |  |  |  |  |  | |
| 1099/ t c p | | open | | r m i r e g i s t r y | | GNU C l a s s p a t h | | | | g r m i r e g i s t r y | | | | |  | |
| 1524/ t c p | | open | | s h e l l | | M e t a s p l o i t a b l e | | | | r o o t | |  | s h e l l | |  | |
| 2049/ t c p | | open | | n f s | | 2 4 ( RPC #100003) | | | | | |  |  |  |  | |
| 2121/ t c p | | open | | f t p | | ProFTPD 1 . 3 . 1 | | | |  |  |  |  |  |  | |
| 3306/ t c p | | open | | mysql | | MySQL 5 . 0 . 5 1 a 3ubuntu5 | | | | | | | |  |  | |
| 5432/ t c p | | open | | p o s t g r e s q l | | PostgreSQL DB 8 . 3 . 08 . 3 . 7 | | | | | | | | |  | |
| 5900/ t c p | | open | | vnc | | VNC ( p r o t o c o l | | | | 3 . 3 ) | |  |  |  |  | |
| 6000/ t c p | | open | | X11 | | ( access | denied ) | | | |  |  |  |  |  | |
| 6667/ t c p | | open | | i r c | | UnrealIRCd | | |  |  |  |  |  |  |  | |
| 8009/ t c p | | open | | ajp13 | | Apache | J s e r v ( P r o t o c o l | | | | | | | v1 . 3 ) |  | |
| 8180/ t c p | | open | | h t t p | | Apache | Tomcat / Coyote | | | | | | JSP engine 1 . 1 | | | |
| MAC Address : | | | | 0 0 : 0C : 2 9 : 8 8 : 7 B : E8 ( VMware ) | | | | | |  |  |  |  |  |  | |
| S e r v i c e | | I n f o : | | Hosts : m e t a s p l o i t a b l e . localdomain , | | | | | | | | | | l o c a l h o s t , i r c . | | |
| *,!* M e t a s p l o i t a b l e . LAN ; OSs : Unix , | | | | | | | | L i n u x ; | | | CPE : cpe : / o : l i n u x : | | | | | |
| *,!* l i n u x \_ k e r n e l | | | | | |  |  |  |  |  |  |  |  |  |  | |
| S e r v i c e | | d e t e c t i o n performed . Please | | | | | | r e p o r t | | | any |  | i n c o r r e c t | | r e s u l t s | |
| *,!* a t | | h t t p s : / / nmap . org / submit / . | | | | | |  |  |  |  |  |  |  |  | |
| Nmap done : 1 | | | | I P address ( 1 | | host up ) | | scanned | | | i n |  | 14.48 seconds | | | |

Listing 2.5: NMAP version info

7

2.4 Study nmap-services, nmap-os-db, nmap-service-probes

Theese files can be found in the directory /usr/share/nmap.

The nmap-services file is a registry of port names to their corresponding number and pro-tocol. Each entry has a number representing how likely that port is to be found open. Most lines have a comment as well.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | tcpmux | 1/ t c p | | 0.001995 | |  | # TCP |  | P o r t S e r v i c e | | | M u l t i p l e x e r [ r f c |
|  | *,!*1078] | | | | TCP P o r t S e r v i c e M u l t i p l e x e r | | | | | | |  |  |
| 2 | tcpmux | 1/ udp | | 0.001236 | |  | # TCP |  | P o r t S e r v i c e | | | M u l t i p l e x e r |
| 3 | compressnet | | 2/ t c p | | 0.000013 | | # |  | Management | | U t i l i t y | |
| 4 | compressnet | | 2/ udp | | 0.001845 | | # |  | Management | | U t i l i t y | |
| 5 | compressnet | | 3/ t c p | | 0.001242 | | # |  | Compression | |  | Process |
| 6 | compressnet | | 3/ udp | | 0.001532 | | # |  | Compression | |  | Process |
| 7 | unknown | 4/ t c p | | 0.000477 | |  |  |  |  |  |  |  |
| 8 | r j e 5/ t c p | | 0.000000 | | # | Remote | | Job | | E n t r y |  |  |
| 9 | r j e 5/ udp | | 0.000593 | | # | Remote | | Job | | E n t r y |  |  |
| 10 | unknown | 6/ t c p | | 0.000502 | |  |  |  |  |  |  |  |
| 11 | echo | 7/ s c t p | | 0.000000 | |  |  |  |  |  |  |  |
| 12 | echo | 7/ t c p | | 0.004855 | |  |  |  |  |  |  |  |
| 13 | echo | 7/ udp | | 0.024679 | |  |  |  |  |  |  |  |
| 14 | unknown | 8/ t c p | | 0.000013 | |  |  |  |  |  |  |  |
| 15 | d i s c a r d | 9/ s c t p | | 0.000000 | |  | # s i n k | | n u l l | |  |  |
| 16 | d i s c a r d | 9/ t c p | | 0.003764 | |  | # s i n k | | n u l l | |  |  |
| 17 | d i s c a r d | 9/ udp | | 0.015733 | |  | # s i n k | | n u l l | |  |  |
| 18 | unknown | 10/ t c p | | 0.000063 | |  |  |  |  |  |  |  |
| 19 | s y s t a t | 11/ t c p | | 0.000075 | |  | # A c t i v e | | | Users |  |  |
| 20 | s y s t a t | 11/ udp | | 0.000577 | |  | # A c t i v e | | | Users |  |  |
| 21 | unknown | 12/ t c p | | 0.000063 | |  |  |  |  |  |  |  |
| 22 | daytime | 13/ t c p | | 0.003927 | |  |  |  |  |  |  |  |
| 23 | daytime | 13/ udp | | 0.004827 | |  |  |  |  |  |  |  |
| 24 | unknown | 14/ t c p | | 0.000038 | |  |  |  |  |  |  |  |
| 25 | n e t s t a t | 15/ t c p | | 0.000038 | |  |  |  |  |  |  |  |
| 26 | unknown | 16/ t c p | | 0.000050 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

Listing 2.6: Some lines of nmap-services

The nmap-os-db data file contains hundreds of examples of how different operating systems respond to Nmap’s specialized OS detection probes. It is divided into blocks known as finger-prints, with each fingerprint containing an operating system’s name.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 53775 | # | L i n u x 3.5.0 17 g e n e r i c | | | | | #28 Ubuntu SMP Tue Oct 9 1 9 : 3 1 : 2 3 UTC | | |
|  |  | *,!* 2012 x86\_64 x86\_64 | | | | | x86\_64 | | GNU/ Linux , L i n u x Mint 14 |
| 53776 | # | Google | Chromecast | | |  |  |  |  |
| 53777 | # | M i k r o T i k RouterOS 6 . 0 | | | | | r c | 14 |  |
| 53778 | # A a s t r a SIP DECT 4 . 0 SP1 | | | | | |  |  |  |
| 53779 | # | Andr oid | v e r s i o n | | 4 . 1 . 2 , | | K e r n e l | | 3 . 4 . 0 |
| 53780 | # | Amazon | F i r e S t i c k | | and | F i r e T V | | |  |
| 53781 | F i n g e r p r i n t | | | L i n u x | 2 . 6 . 3 2 | | 3. 1 0 | |  |
| 53782 | Class L i n u x | L i n u x | | | | | | 2 . 6 . X | | | g e n e r a l purpose | |
| 53783 | CPE cpe : / o : l i n u x : l i n u x \_ k e r n e l : 2 . 6 auto | | | | | | | | |
| 53784 | Class L i n u x | | | | L i n u x | | | 3 . X | | | g e n e r a l purpose | |
|  |  |  |  |  |  |  |  |  |  |

8

|  |  |  |
| --- | --- | --- |
| 53785 | CPE cpe : / o : l i n u x : l i n u x \_ k e r n e l : 3 auto | |
| 53786 | SEQ ( SP=ED 10B%GCD=1 6%ISR =F0 114%T I =Z%CI =Z% I I = I%TS = 7 | 8 | 9 | A | B ) | |
| 53787 | OPS ( O1=M5B4ST11NW1 | M5B4ST11NW2 | M5B4ST11NW3 | M5B4ST11NW4 | M5B4ST11NW5 | |
|  |  | *,!* | M5B4ST11NW6 | M5B4ST11NW7 | M5B4ST11NW8 | M5B4ST11NW9 | M5B4ST11NWA |
|  |  | *,!* %O2=M5B4ST11NW1 | M5B4ST11NW2 | M5B4ST11NW3 | M5B4ST11NW4 | |
|  |  | *,!* M5B4ST11NW5 | M5B4ST11NW6 | M5B4ST11NW7 | M5B4ST11NW8 | M5B4ST11NW9 | |
|  |  | *,!* M5B4ST11NWA%O3=M5B4NNT11NW1 | M5B4NNT11NW2 | M5B4NNT11NW3 | |
|  |  | *,!* M5B4NNT11NW4 | M5B4NNT11NW5 | M5B4NNT11NW6 | M5B4NNT11NW7 | |
|  |  | *,!* M5B4NNT11NW8 | M5B4NNT11NW9 | M5B4NNT11NWA%O4=M5B4ST11NW1 | |
|  |  | *,!* M5B4ST11NW2 | M5B4ST11NW3 | M5B4ST11NW4 | M5B4ST11NW5 | M5B4ST11NW6 | |
|  |  | *,!* M5B4ST11NW7 | M5B4ST11NW8 | M5B4ST11NW9 | M5B4ST11NWA%O5= |
|  |  | *,!* M5B4ST11NW1 | M5B4ST11NW2 | M5B4ST11NW3 | M5B4ST11NW4 | M5B4ST11NW5 | |
|  |  | *,!* M5B4ST11NW6 | M5B4ST11NW7 | M5B4ST11NW8 | M5B4ST11NW9 | M5B4ST11NWA% |
|  |  | *,!* O6=M5B4ST11 ) |
| 53788 | WIN (W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890) | |
| 53789 | ECN ( R=Y%DF=Y%T=3B 45%TG=40%W=3908%O=M5B4NNSNW1 | M5B4NNSNW2 | | |
|  |  | *,!* M5B4NNSNW3 | M5B4NNSNW4 | M5B4NNSNW5 | M5B4NNSNW6 | M5B4NNSNW7 | |
|  |  | *,!* M5B4NNSNW8 | M5B4NNSNW9 | M5B4NNSNWA%CC=N | Y ) |
| 53790 | T1 | ( R=Y%DF=Y%T=3B 45%TG=40%S=O%A=S+%F=AS%RD=0) |
| 53791 | T2 | ( R=N) |
| 53792 | T3 | ( R=N) |
| 53793 | T4 | ( R=Y%DF=Y%T=3B 45%TG=40%W=0%S=A%A=Z%F=R%RD=0) |
| 53794 | T5 | ( R=Y%DF=Y%T=3B 45%TG=40%W=0%S=Z%A=S+%F=AR%RD=0) |
| 53795 | T6 | ( R=Y%DF=Y%T=3B 45%TG=40%W=0%S=A%A=Z%F=R%RD=0) |
| 53796 | T7 | ( R=Y%DF=Y%T=3B 45%TG=40%W=0%S=Z%A=S+%F=AR%RD=0) |
| 53797 | U1 | ( DF=N%T=3B 45%TG=40%IPL =164%UN=0%RIPL=G%RID=G%RIPCK=G | I%RUCK=G% |
|  |  | *,!* RUD=G) |
| 53798 | I E ( DFI =N%T=3B 45%TG=40%CD=S ) | |

Listing 2.7: One of many fingerprint’s

nmap-service-probes file contains the probes that the Nmap service/version detection sys-tem (-sV or -A options) uses during port interrogation to determine what program is listening on a port.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12975 | ##############################NEXT PROBE | | | | | |  |  |  |
|  |  | *,!* ############################## | | | | |  |  |  |
| 12976 | # | SSLv3 | C l i e n t H e l l o | probe . | W i l l be a b l e t o | | r e l i a b l y i d e n t i f y | | t h e |
|  |  | *,!* SSL v e r s i o n | |  |  |  |  |  |  |
| 12977 | # | used , | u n l e s s t h e | s e r v e r | i s | r u n n i n g SSLv2 | o n l y . | Note t h a t i t | w i l l |
|  |  | *,!*a l s o d e t e c t | |  |  |  |  |  |  |
| 12978 | # | TLSv1 o n l y s e r v e r s , based | | | | on a f a i l e d handshake | | a l e r t . |  |
| 12979 | Probe TCP SSLSessionReq q | \ x16 \ x03 \ 0 \ 0 S \ x01 \ 0 \ 0O\ x03 \ 0?G\ xd7 \ x f 7 \ | | | | | | | | |
|  |  | *,!* xba , \ xee \ xea \ xb2 ‘ ~\ x f 3 \ 0 \ x f d \ x82 { \ xb9 \ xd5 \ x96 \ xc8w \ x9b \ xe6 \ | | | | | | | |
|  |  | *,!* xc4 \ xdb <=\ xdbo \ x e f \ x10n \ 0 \ 0 ( \ 0 \ x16 \ 0 \ x13 \ 0 \ x0a \0 f \ 0 \ x05 \ 0 \ | | | | | | | |
|  |  | *,!* x04 \0 e \0 d \0 c \0 b \0 a \ 0 ‘ \ 0 \ x15 \ 0 \ x12 \ 0 \ x09 \ 0 \ x14 \ 0 \ x11 \ 0 \ x08 \ 0 \ | | | | | | | |
|  |  | *,!* x06 \ 0 \ x03 \ x01 \ 0 | | | |  |  |  |  |  |
| 12980 | r a r i t y | | 1 |  |  |  |  |  |  |
| 12981 | p o r t s 3 2 2 , 4 4 3 , 4 4 4 , 4 6 5 , 5 4 8 , 6 3 6 , 9 8 9 , 9 9 0 , 9 9 2 , 9 9 3 , 9 9 4 , 9 9 5 , 1 2 4 1 , 1 3 1 1 , | | | | | | | | |
|  |  | *,!* 1443 ,2000 ,2252 ,2443 ,3443 ,4433 ,4443 ,4444 ,4911 ,5061 ,5443 ,5550 , | | | | | | | |
|  |  | *,!* |  |  |  |  |  |  |  |

*,!* 6443 ,6679 ,6697 ,7000 ,7210 ,7272 ,7443 ,8009 ,8181 ,8194 ,8443 ,8531 ,

9

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | *,!*8883 ,9001 ,9443 ,10443 ,14443 ,44443 ,60443 | | | | | | | |  |  |  |  |  |
| 12982 | f a l l b a c k GetRequest | | | |  |  |  |  |  |  |  |  |  |
| 12983 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12984 | # OpenSSL / 0 . 9 . 7 aa , | | | | 0 . 9 . 8 e |  |  |  |  |  |  |  |  |
| 12985 | match | s s l | m| ^ \ x16 \ x03 \ 0 \ 0 J \ x02 \ 0 \ 0 F \ x03 \ 0 | p / OpenSSL / | | | | | | | i / SSLv3 / | | | cpe |
| 12986 | *,!* : / a : openssl : openssl / | | | | |  |  |  |  |  |  |  |  |
| # M i c r o s o f t I I S / 5 . 0 | | | | note |  |  |  |  |  |  |  |  |
| 12987 | t h a t OpenSSL must go above | | | | t h i s | one | |  |
|  | *,!* because t h i s | | | | i s more | g e n e r a l |  |  |  |  |  |  |  |
| 12988 | match | s s l | m| ^ \ x16 \ x03 \ 0 . . \ x02 \ 0 \ 0 F \ x03 \ 0 | s p / M i c r o s o f t | | | | | | | I I S | SSL / | | o / |
|  | *,!* Windows / cpe : / a : m i c r o s o f t : i i s / | | | | | | | cpe : / o : m i c r o s o f t : windows / a | | | | |  |
| 12989 | # N o v e l l | | Netware | 6 | E n t e r p r i s e Web | | s e r v e r 5 . 1 | | h t t p s |  |  |  |  |
| 12990 | # N o v e l l | | Netware | Ldap o v e r | | SSL o r | e n t e r p r i s e | | web s e r v e r 5 . 1 | |  | o v e r | |
|  | *,!* SSL | |  |  |  |  |  |  |  |  |  |  |  |
| 12991 | match | s s l | m| ^ \ x16 \ x03 \ 0 \ 0 : \ x02 \ 0 \ x006 \ x03 \ 0 | | | | | | | p / N o v e l l | NetWare SSL / | | | |
|  | *,!* | o / NetWare / | | cpe : / o : n o v e l l : netware / a | | | | |  |  |  |  |  |
| 12992 | # Cisco IDS 4 . 1 A p p l i a n c e | | | | |  |  |  |  |  |  |  |  |
| 12993 | match | s s l | m| ^ \ x16 \ x03 \ 0 \ 0 \ \*\ x02 \0\0 &\ x03 \ 0 \ xd10 : \ xbd \ \ \ x8e \ xe3 \ x15 | | | | | | | | | | |
|  | *,!* \ x1c \ x0fZ \ xe4 \ x04 \ x87 \ x07 \ xc0 \ x82 \ xa9 \ xd4 \ x0e \ x9c1LXk \ xd1 \ | | | | | | | | | | | | |
|  | *,!* xd2 \ x0b \ x1a \ xc6 / p \ 0 \ 0 \ n \ 0 \ x16 \ x03 \ 0 \ x026 \ x0b \ 0 \ x022 \ 0 | | | | | | | | | | | | p / |  |
|  | *,!* Cisco IDS SSL / d / f i r e w a l l / | | | | | |  |  |  |  |  |  |  |
| 12994 | # PGP | C o r p o r a t i o n | | K e y s e r v e r | | Web Console 7 . 0custom Apache | | | | |  | 1 . 3 |  |
| 12995 | # PGP LDAPS K e y s e r v e r 8 . X | | | | |  |  |  |  |  |  |  |  |
| 12996 | match | s s l | m| ^ \ x16 \ x03 \ 0 \ 0 \ + \ x02 \ 0 \ 0 ’ \ x03 \ 0 . . . \ ? | s p /PGP | | | | | | | |  |  |  |
|  | *,!* C o r p o r a t i o n p r o d u c t SSL / | | | | | |  |  |  |  |  |  |  |
| 12997 | # U n r e a l IRCd SSL | | |  |  |  |  |  |  |  |  |  |  |
| 12998 | # RemotelyAnywhere | | | |  |  |  |  |  |  |  |  |  |
| 12999 | match | s s l | m| ^ \ x16 \ x03 \ 0 \ 0 \ \*\ x02 \0\0 &\ x03 \ 0 \ ? | | | | | | |  | Secure P o r t | | | |
| 13000 | # Tumbleweed S e c u r e T r a n s p o r t 4 . 1 . 1 | | | | | | T r a n s a c t i o n Manager | | |
|  | *,!* | on | S o l a r i s |  |  |  |  |  |  |  |  |  |  |
| 13001 | # D e l l | Openmanage | |  |  |  |  |  | p / m u l t i vendor | | |  |  |
| 13002 | match | s s l | m| ^ \ x15 \ x03 [ \ x01 \ x00 ] \ 0 \ x02 \ x01 \0 $ | | | | | | | SSL / | |
| 13003 | # P r o b a b l y O r a c l e | | | h t t p s ? | |  |  |  |  |  |  |  |  |
| 13004 | match | s s l | m| ^ } \ 0 \ x02 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 | p / O r a c l e h t t p s / | | | | | | | | | |  |
| 13005 | match | s s l | m| ^ \ x15 \ x03 \ 0 \ 0 \ x02 \ x02 \ ( 3 1 6 6 6 : e r r o r :1408A0C1 : SSL | | | | | | | |  |  |  |
|  | *,!* r o u t i n e s : SSL3\_GET\_CLIENT\_HELLO : no shared c i p h e r : s 3 \_ s r v r \ . c | | | | | | | | | | | | |
|  | *,!* : 8 8 1 : \ n | p /Webmin SSL | | | | | C o n t r o l | | Panel / |  |  |  |  |  |
| 13006 | match | s s l | m| ^ 2 0 9 2 8 : e r r o r :140760FC : SSL r o u t i n e s : | | | | | | |  |  |  |  |
|  | *,!* SSL23\_GET\_CLIENT\_HELLO : unknown | | | | | | | p r o t o c o l : s 2 3 \_ s r v r \ . c : 5 6 5 : \ n | | | | | | |
|  | *,!* p / qmail pop3d | | | | behind | s t u n n e l / | | cpe : / a : d j b : qmail / | |  |  |  |  |

Listing 2.8: Some lines of nmap-service-probes

The Probe directive tells Nmap what string to send to recognize various services. All of the directives discussed later operate on the most recent Probe statement. The arguments are as follows:

1. <protocol>
   * This must be either TCP or UDP.
2. <probename>

10

* + Plain English name for the probe.

1. <probestring>
   * Tells Nmap what to send. It must start with a q, then a delimiter character which begins and ends the string. Between the delimiter characters is the string that is actually sent.

2.5 Add new service to nmap-service-probes (create a mini-mal tcp server, get its name and version by nmap)

|  |  |
| --- | --- |
|  | The source code of echo-server is shown below. |
|  |  |
| 1 | package s e r v e r ; |
| 2 |  |
| 3 | import j a v a . n e t . \* ; |

* import j a v a . i o . \* ;

5

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | p u b l i c c l a s s S e r v e r { | | |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |
| 8 | p r i v a t e | s t a t i c | i n t SERVER\_PORT=8090; | | | |  |  |
| 9 | p r i v a t e | s t a t i c | S t r i n g | SERVER\_IP= ” 1 2 7 . 0 . 0 . 1 ” ; | | | |  |
| 10 |  |  |  |  |  |  |  |  |
| 11 | p r i v a t e | s t a t i c | S t r i n g | VERSION | = | ” 1 . 0 ” ; |  |  |
| 12 |  |  |  |  |  |  |  |  |
| 13 | p u b l i c s t a t i c | | void main ( S t r i n g [ ] | | | args ) | { |  |
| 14 | t r y | { |  |  |  |  |  |  |
| 15 |  | S e r v e r S o c k e t | | s e r v e r S o c k e t = new | | | S e r v e r S o c k e t ( | |
|  | *,!* SERVER\_PORT , 0 , I n e t A d d r e s s . getByName ( SERVER\_IP ) ) ; | | | | | | |  |
| 16 |  | System . out . p r i n t l n ( ” S e r v e r s t a r t e d . ” ) ; | | | | | |  |
| 17 |  | Socket | c l i e n t S o c k e t = | | s e r v e r S o c k e t . accept ( ) ; | | | |
| 18 |  | P r i n t W r i t e r out = new | | | P r i n t W r i t e r ( c l i e n t S o c k e t . | | | |
|  | *,!* getOutputStream ( ) , | | | t r u e ) ; |  |  |  |  |
| 19 |  | B u f f e r e d R e a d e r i n = new | | | | B u f f e r e d R e a d e r ( new | | |
| 20 | *,!* InputStreamReader ( c l i e n t S o c k e t . g e t I n p u t S t r e a m ( ) ) ) ; | | | | | | | |
|  |  |  |  |  |  |  |  |
| 21 |  | S t r i n g i n p u t L i n e ; | | |  |  |  |  |
| 22 |  | w h i l e ( t r u e ) { | | |  |  |  |  |
| 23 |  | i n p u t L i n e = i n . r e a d L i n e ( ) ; | | | | |  |  |
| 24 |  | i f ( i n p u t L i n e ! = n u l l ) { | | | | |  |  |
| 25 |  |  | i f ( i n p u t L i n e . e q u a l s ( ” v e r s i o n ” ) ) | | | | |  |
| 26 |  |  | out . p r i n t l n ( VERSION ) ; | | | |  |  |
| 27 |  |  | e l s e |  |  |  |  |  |
| 28 |  |  | out . p r i n t l n ( i n p u t L i n e ) ; | | | | |  |
| 29 |  | } |  |  |  |  |  |  |
| 30 |  | } |  |  |  |  |  |  |
| 31 | } catch ( I O E x c e p t i o n e ) { | | | |  |  |  |  |
| 32 | *,!* l i s t e n | System . out . p r i n t l n ( ” E x c e p t i o n caught when | | | | | | t r y i n g t o |
|  | on p o r t ” + SERVER\_PORT | | | | + ” o r | l i s t e n i n g | f o r a |
|  | *,!* c o n n e c t i o n ” ) ; | | |  |  |  |  |  |

11

|  |  |
| --- | --- |
| 33 | System . out . p r i n t l n ( e . getMessage ( ) ) ; |

1. }
2. }
3. }

Listing 2.9: Server.java

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | r o o t @ k a l i : ~/ Desktop / t c p S e r v e r # | j a v a c | s e r v e r / S e r v e r . j a v a |
| 2 | r o o t @ k a l i : ~/ Desktop / t c p S e r v e r # | j a v a | s e r v e r / S e r v e r |
| 3 | S e r v e r s t a r t e d . |  |  |
|  |  |  |  |

Listing 2.10: Compiling and starting server

Echo server was successfully detected, but nmap did not determine what it is, not even that this is echo-server.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | r o o t @ k a l i : ~# nmap sV p 8090 | | | | | | | 1 2 7 . 0 . 0 . 1 | |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  | 2017 11 04 | | |  |  |
| 3 | S t a r t i n g | | Nmap | | 7. 6 0 ( | h t t p s : / / nmap . org ) | | | | a t | 12:55 | EDT |
| 4 | Nmap | scan | | r e p o r t f o r | | l o c a l h o s t ( 1 2 7 . 0 . 0 . 1 ) | | | | |  |  |  |  |  |
| 5 | Host | i s | up | (0.000045 s | |  | l a t e n c y ) . | |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | PORT |  | STATE SERVICE | | | |  | VERSION |  |  |  |  |  |  |  |
| 8 | 8090/ t c p | | open | | opsmessaging ? | | |  |  |  |  |  |  |  |  |
| 9 | 1 s e r v i c e | | | unrecognized | | | d e s p i t e r e t u r n i n g | | | data . | | I f | you | know | t h e |
|  | *,!* s e r v i c e / v e r s i o n , | | | | | | p l e a s e | submit | t h e | f o l l o w i n g | | | f i n g e r p r i n t a t | | |
|  | *,!* h t t p s : / / nmap . org / c g i b i n / submit . c g i ?new s e r v i c e | | | | | | | | | | | | | : |  |
| 10 | SF Port8090 TCP : V=7.60% I =7%D=11/4%Time=59FDF102%P=x86\_64 pc l i n u x | | | | | | | | | | | | | | |
|  | *,!* gnu%r ( s i | | | | |  |  |  |  |  |  |  |  |  |  |
| 11 | SF : mple tcp s e r v e r ver , 8 , ” v e r s i o n \ n ” ) ; | | | | | | | | |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13 | S e r v i c e | | d e t e c t i o n performed . | | | | | Please | r e p o r t | | any | i n c o r r e c t r e s u l t s | | | |
|  | *,!* a t | | h t t p s : / / nmap . org / submit / . | | | | | |  |  |  |  |  |  |  |
| 14 | Nmap done : | | | 1 | I P address ( 1 host up ) | | | | scanned | | i n | 11.61 | | seconds | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Listing 2.11: Nmap scanning(unsuccessful)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Now add the server description to the nmap-service-probes. | | | | |
|  |  | | | | |
| 1 | r o o t @ k a l i : ~# t a i l n 7 / u s r / share /nmap/nmap s e r v i c e probes | | | | |
| 2 | ##############################NEXT PROBE | | | |  |
|  | *,!* ############################## | | | |  |
| 3 | # Echo | TSP | s e r v e r . |  |  |
| 4 | Probe | TCP | echo tcp s e r v e r v e r | q | v e r s i o n \ r \ n | | |
| 5 | r a r i t y | 9 |  |  |  |
| 6 | p o r t s 8090 | |  |  |  |
| 7 | match | s tc ps m| ^ 1 \ . 0 $ | p / Echo | | TCP S e r v e r / | v / 1 . 0 / |
|  |  | | |  |  |
|  | Listing 2.12: Adding description | | |  |  |
|  |  | | |  |  |
|  | And scan with nmap again. | | |  |  |
|  |  | | |  |  |
| 1 | r o o t @ k a l i : ~# nmap sV p 8090 | | | 1 2 7 . 0 . 0 . 1 |  |
| 2 |  |  |  |  | a t 2017 11 04 13:02 EDT |
| 3 | S t a r t i n g Nmap 7. 6 0 ( h t t p s : / / nmap . org ) | | | |

12

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4 | Nmap | scan | | r e p o r t f o r | l o c a l h o s t ( 1 2 7 . 0 . 0 . 1 ) | |
| 5 | Host | i s | up | (0.000065 s | l a t e n c y ) . | |
| 6 |  |  |  |  |  |  |
| 7 | PORT |  | STATE SERVICE VERSION | | | |
| 8 | 8090/ t c p | | open st cp s | | Echo | TCP S e r v e r 1 . 0 |
| 9 |  |  |  |  |  |  |
| 10 | S e r v i c e | | d e t e c t i o n performed . | | | Please r e p o r t any i n c o r r e c t r e s u l t s |
|  | *,!* a t | | h t t p s : / / nmap . org / submit / . | | | |

1. Nmap done : 1 I P address ( 1 host up ) scanned i n 6 . 54 seconds

Listing 2.13: Nmap scanning(successful)

As expected, nmap successfully determined my echo server.

2.6 Output to xml-format file

Adding oX key for output to xml file.

root@kali: # nmap -sV -p 8090 -oX myOutput.xml 127.0.0.1

1 <? xml v e r s i o n = ” 1 . 0 ” encoding = ” UTF 8”? >

* < !DOCTYPE nmaprun>

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3 | <?xml s t y l e s h e e t | | | | h r e f = ” f i l e : / / / u s r / b i n / . . / share /nmap/nmap . x s l ” | | | | | | | | | | | | |
|  | *,!* t y p e = ” t e x t / x s l ” ? > | | | | | |  |  |  |  |  |  |  |  |  |  | nmap |
| 4 | <!Nmap | | 7 . 6 0 scan | | | i n i t i a t e d Sat | | | | Nov | 4 1 3 : 2 6 : 0 7 | | | 2017 as : | | |
|  | *,!* sVp 8090 oX | | | | | myOutput . xml | | | | 1 2 7 . 0 . 0 . 1> | | |  |  |  |  |  |
| 5 | <nmaprun | | scanner = ”nmap ” | | | | args = ”nmap sV p 8090 oX | | | | | | | myOutput . xml | | | |
|  | *,!* 1 2 7 . 0 . 0 . 1 ” | | | | s t a r t =”1509816367” s t a r t s t r = ” Sat | | | | | | | | Nov | | 4 | 1 3 : 2 6 : 0 7 | |
|  | *,!* 2017” v e r s i o n = ” 7 . 6 0 ” | | | | | | | x m l o u t p u t v e r s i o n = ” 1 . 0 4 ” > | | | | | | |  |  |  |
| 6 | < s c a n i n f o | | t y p e = ” syn ” | | | p r o t o c o l = ” t c p ” numservices = ” 1 ” s e r v i c e s | | | | | | | | | | | |
|  | *,!* = ” 8 0 9 0 ” / > | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | < verbose | | l e v e l = ” 0 ” / > | | |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | < debugging l e v e l = ” 0 ” / > | | | | | |  |  |  |  |  |  |  |  |  |  |  |
| 9 | < host | s t a r t t i m e =”1509816367” endtime =”1509816373” > < s t a t u s | | | | | | | | | | | | | | | s t a t e = ” |
|  | *,!* up ” | | reason = ” l o c a l h o s t response ” | | | | | | | | r e a s o n \_ t t l = ” 0 ” / > | | | |  |  |  |
| 10 | < address | | addr = ” 1 2 7 . 0 . 0 . 1 ” a d d r t y p e = ” i p v 4 ” / > | | | | | | | | |  |  |  |  |  |  |
| 11 | <hostnames > | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 | <hostname | | name= ” l o c a l h o s t ” | | | | | t y p e = ” PTR ” / > | | | |  |  |  |  |  |  |
| 13 | </ hostnames > | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 | < p o r t s >< p o r t p r o t o c o l = ” t c p ” | | | | | | | p o r t i d =”8090” > < s t a t e | | | | | s t a t e = ” open ” | | | | |
|  | *,!* reason = ” syn ack ” | | | | | | r e a s o n \_ t t l = ” 6 4 ” / > < s e r v i c e | | | | | | name= ” st cp s ” | | | | |
|  | *,!* p r o d u c t = ” Echo TCP | | | | | | S e r v e r ” | | v e r s i o n = ” 1 . 0 ” | | | method = ” probed ” conf | | | | | |
|  | *,!* = ” 1 0 ” / > < / p o r t > | | | | |  |  |  |  |  |  |  |  |  |  |  |  |
| 15 | </ p o r t s > | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 | < times | s r t t = ” 4 8 ” | | | r t t v a r = ” 5 0 0 0 ” | | | | t o =”100000”/ > | | |  |  |  |  |  |  |
| 17 | </ host > | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 18 | < r u n s t a t s >< f i n i s h e d | | | | | time =”1509816373” | | | | | t i m e s t r = ” Sat | | | Nov | | 4 | 1 3 : 2 6 : 1 3 |
|  | *,!* | 2017” elapsed = ” 6 . 5 7 ” | | | | | | summary = ”Nmap done a t | | | | | Sat | | Nov | | 4 |
|  | *,!* 1 3 : 2 6 : 1 3 | | | 2017; | | 1 | I P address | | | ( 1 host up ) | | scanned | | | i n | 6. 5 7 | |
|  | *,!* seconds ” | | | e x i t = ” success ”/ > < hosts | | | | | | | up = ” 1 ” | down = ” 0 ” | | | t o t a l = ” 1 ” / > | | |

13

1. </ r u n s t a t s >
2. </nmaprun>

Listing 2.14: myOutput.xml

2.7 Study nmap stages and modes using Wireshark

Scanning port 22

* r o o t @ k a l i : ~# nmap sV 1 9 2 . 1 6 8 . 8 1 . 1 3 0 p 22

2

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3 | S t a r t i n g Nmap | | | | 7. 6 0 ( h t t p s : / / nmap . org ) a t | | | | 2017 11 04 14:23 | EDT |
| 4 | Nmap | scan | | r e p o r t | | f o r 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |  |  |  |
| 5 | Host | i s | up | ( 0 . 0 0 0 4 1 s l a t e n c y ) . | | | |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |
| 7 | PORT |  | STATE SERVICE VERSION | | | |  |  |  |  |
| 8 | 22/ t c p | | open | | ssh | OpenSSH | 4 . 7 p1 | Debian | 8ubuntu1 ( p r o t o c o l | 2 . 0 ) |
| 9 | MAC | Address : | | | 0 0 : 0C : 2 9 : 8 8 : 7 B : E8 ( VMware ) | | | |  |  |
| 10 | S e r v i c e | | I n f o : | | OS : | L i n u x ; CPE : | cpe : / o : l i n u x : l i n u x \_ k e r n e l | | |  |
| 11 |  |  |  |  |  |  |  |  |  |  |
| 12 | S e r v i c e | | d e t e c t i o n | | | performed . | Please | r e p o r t | any i n c o r r e c t r e s u l t s | |
|  | *,!* a t h t t p s : / / nmap . org / submit / . | | | | | | |  |  |  |

1. Nmap done : 1 I P address ( 1 host up ) scanned i n 0 . 97 seconds

Listing 2.15: Scanning port 22

Let’s see what is in the packets, that captured with wireshark.

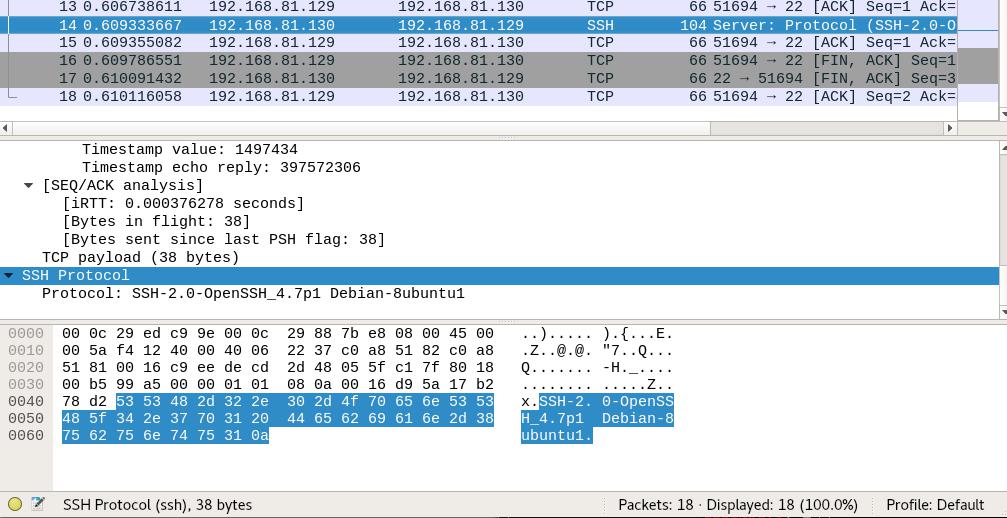


Figure 2.5: Wireshark packets

In response message, we see name of service at this port.

Now let’s see what happens when the command below is used.

14

* r o o t @ k a l i : ~# nmap top p o r t s 10 1 9 2 . 1 6 8 . 8 1 . 1 3 0

2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3 | S t a r t i n g | | Nmap 7. 6 0 ( h t t p s : / / nmap . org ) a t 2017 11 04 14:57 EDT | |
| 4 | Nmap | scan | r e p o r t | f o r 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 5 | Host | i s up ( 0 . 0 0 0 8 0 s l a t e n c y ) . | | |
| 6 |  |  |  |  |
| 7 | PORT |  | STATE | SERVICE |
| 8 | 21/ t c p | | open | f t p |
| 9 | 22/ t c p | | open | ssh |
| 10 | 23/ t c p | | open | t e l n e t |
| 11 | 25/ t c p | | open | smtp |
| 12 | 80/ t c p | | open | h t t p |
| 13 | 110/ t c p | | c l o s e d pop3 | |
| 14 | 139/ t c p | | open | n e t b i o s ssn |
| 15 | 443/ t c p | | c l o s e d | h t t p s |
| 16 | 445/ t c p | | open | m i c r o s o f t ds |
| 17 | 3389/ t c p | | c l o s e d ms wbt s e r v e r | |
| 18 | MAC | Address : 0 0 : 0C : 2 9 : 8 8 : 7 B : E8 ( VMware ) | | |
| 19 |  |  |  |  |

1. Nmap done : 1 I P address ( 1 host up ) scanned i n 0 . 57 seconds

Listing 2.16: 10 most popular ports

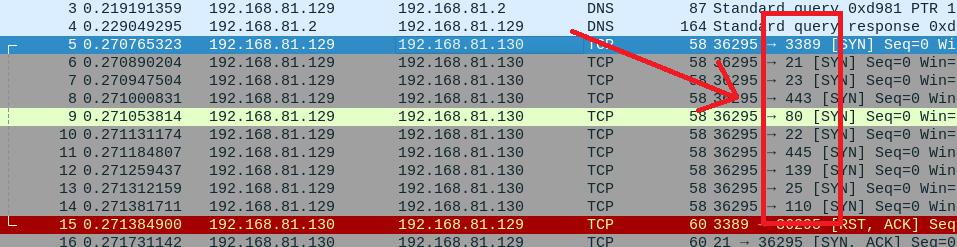


Figure 2.6: Wireshark packets

The screenshot highlights that 10 requests were sent to the most popular ports.

15

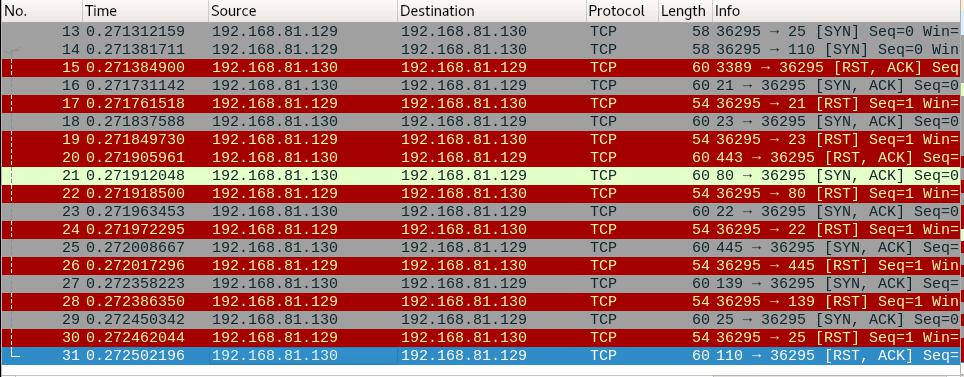


Figure 2.7: Wireshark packets

As result wireshark got 10 answers. Now let’s how nmap understand that port state is open or closed.

For example port 110 in state closed.

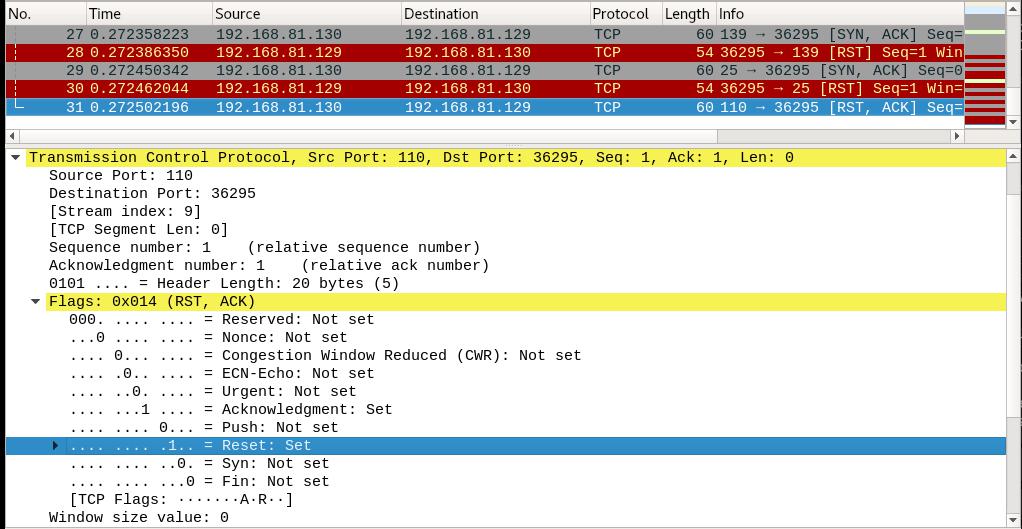


Figure 2.8: TCP flag RST

This porst is closed, because in response messege we got RST flag, which means, accord-ing to the tcp methodology, that there is no connection.

Port 25(Open) don’t have this flag.

16

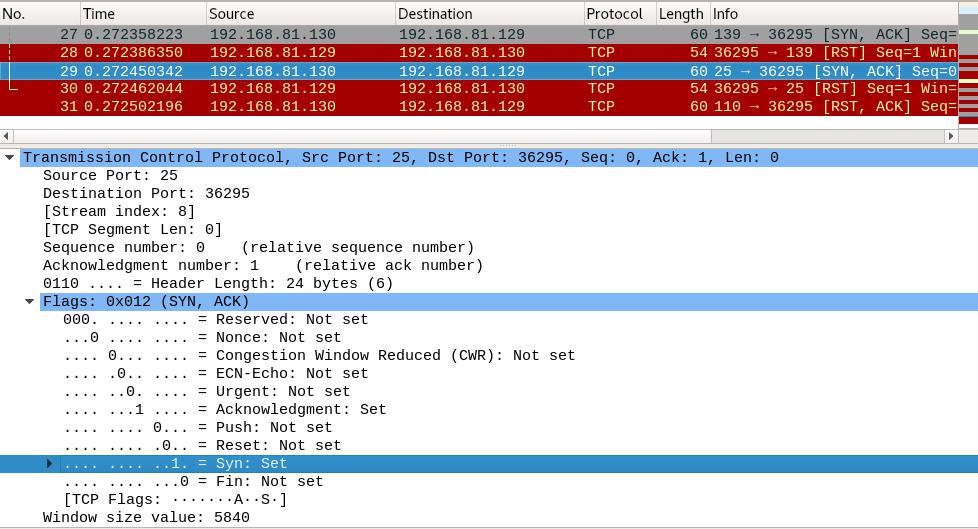


Figure 2.9: RST flag not setted

2.8 Perform VM Metasploitable2 scanning using db\_nmap from metasploit framework

To use db\_nmap, need to perform steps below:

1. start posgresql server;
2. initialize the database with the msfdb init command;
3. start the console of the msfconsole.

Then use db\_nmap, which has same functionality as nmap, but all results will be stored in the database.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > db\_nmap v sV | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | |  |  |  |  | a t 2017 11 04 | |
| 2 | [ \* ] | Nmap : | S t a r t i n g Nmap | | 7 . 60 | ( | h t t p s : / / nmap . org | | | | | ) |
|  | *,!* 22:24 EDT | | |  |  |  |  |  |  |  |  |  |  |  |
| 3 | [ \* ] | Nmap : | NSE : Loaded 42 | | s c r i p t s | | | f o r | scanning . | | |  |  |  |
| 4 | [ \* ] | Nmap : | I n i t i a t i n g | ARP Ping Scan a t 22:24 | | | | | | |  |  |  |  |
| 5 | [ \* ] | Nmap : | Scanning 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | | [ 1 | p o r t ] | |  |  |  |  |
| 6 | [ \* ] | Nmap : | Completed | ARP | Ping | Scan | | a t | 2 2 : 2 4 , | | 0 .2 6 s | | elapsed | ( 1 t o t a l |
|  | *,!*hosts ) | | |  |  |  |  |  |  |  |  |  |  |  |
| 7 | [ \* ] | Nmap : | I n i t i a t i n g | P a r a l l e l | |  | DNS | r e s o l u t i o n | | | o f | 1 | host . a t 22:24 | |
| 8 | [ \* ] | Nmap : | Completed | P a r a l l e l | | DNS | | r e s o l u t i o n | | | o f | 1 | host . a t | 2 2 : 2 4 , |
|  | *,!* 0. 0 0 s elapsed | | |  |  |  |  |  |  |  |  |  |  |  |
| 9 | [ \* ] | Nmap : | I n i t i a t i n g | SYN | S t e a l t h | | | Scan | a t | 22:24 | |  |  |  |
| 10 | [ \* ] | Nmap : | Scanning 1 9 2 . 1 6 8 . 1 1 9 . 1 2 8 [1000 | | | | | | | p o r t s ] | |  |  |  |
| 11 | [ \* ] | Nmap : | D i s c o v e r e d | open p o r t | | | 25/ t c p | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | |  |
| 12 | [ \* ] | Nmap : | D i s c o v e r e d | open p o r t | | | 53/ t c p | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | |  |
| 13 | [ \* ] | Nmap : | D i s c o v e r e d | open p o r t | | | 139/ t c p on | | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

17

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 23/ t c p | | on | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 15 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 21/ t c p | | on | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 16 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 445/ t c p | | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |
| 17 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 22/ t c p | | on | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 18 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 5900/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 19 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 111/ t c p | | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |
| 20 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 3306/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 21 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 80/ t c p | | on | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 22 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 8180/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 23 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 6667/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 24 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 2049/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 25 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 8009/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 26 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 514/ t c p | | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |
| 27 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 6000/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 28 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 513/ t c p | | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |
| 29 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 1524/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 30 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 512/ t c p | | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |
| 31 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 2121/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 32 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 5432/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 33 | [ \* ] | Nmap : | D i s c o v e r e d | | |  | open p o r t | | | 1099/ t c p | | |  | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 34 | [ \* ] | Nmap : | Completed | |  | SYN | | S t e a l t h | | Scan | | a t |  | 2 2 : 2 4 , 9 .4 5 s elapsed (1000 |
|  |  | *,!*t o t a l p o r t s ) | | |  |  |  |  |  |  |  |  |  |  |
| 35 | [ \* ] | Nmap : | I n i t i a t i n g | | |  | S e r v i c e scan | | | | a t | 22:24 | | |
| 36 | [ \* ] | Nmap : | Scanning | | 23 | | s e r v i c e s | | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | |
| 37 | [ \* ] | Nmap : | Completed | |  | S e r v i c e | | | scan | | a t 2 2 : 2 4 , 14.22 s elapsed (23 | | | |
|  |  | *,!* s e r v i c e s | | on 1 | host ) | | | |  |  |  |  |  |  |
| 38 | [ \* ] | Nmap : | NSE : S c r i p t | | | | scanning | | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 . | | | | |
| 39 | [ \* ] | Nmap : | I n i t i a t i n g | | |  | NSE | a t | 22:24 | |  |  |  |  |
| 40 | [ \* ] | Nmap : | Completed | |  | NSE | | a t | 2 2 : 2 4 , | | 0 .9 2 s | |  | elapsed |
| 41 | [ \* ] | Nmap : | I n i t i a t i n g | | |  | NSE | a t | 22:24 | |  |  |  |  |
| 42 | [ \* ] | Nmap : | Completed | |  | NSE | | a t | 2 2 : 2 4 , | | 0 .0 9 s | |  | elapsed |
| 43 | [ \* ] | Nmap : | Nmap | scan |  | r e p o r t | | | f o r | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | |
| 44 | [ \* ] | Nmap : | Host | i s up | |  | ( 0 . 0 0 0 8 9 s | | | l a t e n c y ) . | | | |  |

1. [ \* ] Nmap : Not shown : 977 c l o s e d p o r t s
2. [ \* ] Nmap : PORT STATE SERVICE VERSION

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 47 | [ \* ] | Nmap : | 21/ t c p | open | f t p | v s f t p d 2 . 3 . 4 | | |  |  |  |
| 48 | [ \* ] | Nmap : | 22/ t c p | open | ssh | OpenSSH | | 4 . 7 p1 | Debian | 8ubuntu1 | ( p r o t o c o l |
|  |  | *,!* 2 . 0 ) |  |  |  |  |  |  |  |  |  |
| 49 | [ \* ] | Nmap : | 23/ t c p | open | t e l n e t | | L i n u x | t e l n e t d | |  |  |
| 50 | [ \* ] | Nmap : | 25/ t c p | open | smtp | P o s t f i x | | smtpd | |  |  |
| 51 | [ \* ] | Nmap : | 53/ t c p | open | domain | | ISC BIND 9 . 4 . 2 | | |  |  |
| 52 | [ \* ] | Nmap : | 80/ t c p | open | h t t p Apache | | | h t t p d | 2 . 2 . 8 | ( ( Ubuntu ) | DAV / 2 ) |
| 53 | [ \* ] | Nmap : | 111/ t c p | open | r p c b i n d 2 ( RPC #100000) | | | | | 3 . X 4 . X |  |
| 54 | [ \* ] | Nmap : | 139/ t c p | open | n e t b i o s ssn | | | Samba smbd | | ( workgroup |
|  |  | *,!* : WORKGROUP) | | | n e t b i o s ssn | | |  |  | 3 . X 4 . X |  |
| 55 | [ \* ] | Nmap : | 445/ t c p | open | Samba smbd | | ( workgroup |
|  |  | *,!* : WORKGROUP) | | |  |  | n e t k i t r s h | |  |  |  |
| 56 | [ \* ] | Nmap : | 512/ t c p | open | exec | | rexecd |  |  |
| 57 | [ \* ] | Nmap : | 513/ t c p | open | l o g i n | | OpenBSD o r | | S o l a r i s r l o g i n d | |  |
| 58 | [ \* ] | Nmap : | 514/ t c p | open | tcpwrapped | | |  |  |  |  |

18

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 59 | [ \* ] | Nmap : | 1099/ t c p | open | r m i r e g i s t r y GNU C l a s s p a t h | | | | | g r m i r e g i s t r y | | |
| 60 | [ \* ] | Nmap : | 1524/ t c p | open | s h e l l M e t a s p l o i t a b l e | | | | r o o t | s h e l l | |  |
| 61 | [ \* ] | Nmap : | 2049/ t c p | open | n f s | 2 4 ( RPC #100003) | | |  |  |  |  |
| 62 | [ \* ] | Nmap : | 2121/ t c p | open | f t p | ProFTPD 1 . 3 . 1 | | |  |  |  |  |
| 63 | [ \* ] | Nmap : | 3306/ t c p | open | mysql MySQL | | | 5 . 0 . 5 1 a 3ubuntu5 | | |  |  |
| 64 | [ \* ] | Nmap : | 5432/ t c p | open | p o s t g r e s q l PostgreSQL DB 8 . 3 . 08 . 3 . 7 | | | | | | | |
| 65 | [ \* ] | Nmap : | 5900/ t c p | open | vnc | VNC ( p r o t o c o l 3 . 3 ) | | | |  |  |  |
| 66 | [ \* ] | Nmap : | 6000/ t c p | open | X11 | ( access | | denied ) |  |  |  |  |
| 67 | [ \* ] | Nmap : | 6667/ t c p | open | i r c | UnrealIRCd | | |  |  |  |  |
| 68 | [ \* ] | Nmap : | 8009/ t c p | open | ajp13 Apache | | | J s e r v ( P r o t o c o l | | | v1 . 3 ) | |
| 69 | [ \* ] | Nmap : | 8180/ t c p | open | h t t p | Apache | | Tomcat / Coyote | | JSP | engine 1 . 1 | |
| 70 | [ \* ] | Nmap : | MAC Address : | | 0 0 : 0C : 2 9 : 8 8 : 7 b : e8 ( VMware ) | | | | |  |  |  |
| 71 | [ \* ] | Nmap : | S e r v i c e | I n f o : | Hosts : m e t a s p l o i t a b l e . localdomain , | | | | | | | |
|  | *,!* l o c a l h o s t ,i r c . M e t a s p l o i t a b l e . LAN ; OSs : | | | | | | | | Unix , L i n u x ; | | | |
| 72 | CPE : | cpe : / o : l i n u x : l i n u x \_ k e r n e l | | | | |  |  |  |  |  |  |
| 73 | [ \* ] | Nmap : | Read data f i l e s from : / u s r / b i n / . . / share /nmap | | | | | | | | |  |
| 74 | [ \* ] | Nmap : | S e r v i c e d e t e c t i o n | | | performed . Please | | | r e p o r t | | any | i n c o r r e c t |
|  | *,!*r e s u l t s a t | | | h t t p s : / / nmap . org / submit / . | | | | |  |  |  |  |
| 75 | [ \* ] | Nmap : Nmap done : 1 | | | I P address | | ( 1 | host up ) | scanned | | i n | 32.19 |
|  | *,!* seconds | | |  |  |  |  |  |  |  |  |  |
| 76 | [ \* ] | Nmap : Raw packets s e n t : | | | | 1411 | ( 6 1 . 8 2 1KB ) | | | Rcvd : 1411 | | | ( 5 5 . 5 4 2KB |
|  | *,!* ) | |  |  |  |  |  |  |  |  |  |  |
|  | Listing 2.17: db\_nmap output | | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

2.9 Get 5 records from nmap-service-probes and describe them.

Let’s analyze a Listing 2.8. It describes the behavior of various services that work with the SIP protocol.

Line 12975 separates one set of rules from another.

Line 12979 contains the probe directive. It is used to indicate which data is sent during the service definition process. The command already analyzed at page 10.

In the line 12980, the rarity parameter is set to 1. The higher its value (maximum 9), the fewer chances to expect results from this test.

The line 12981 indicates the port number to which data will be sent from the probe direc-tive. In our case, we use array of ports (then they are separated by commas), but in general there can be one single port. Also, if needed to install an encrypted connection over SSL (then the sslports directive is used instead of the ports).

Now let’s analyze 12988, 12991, 12993 lines. All theese lines had the match directive that tells nmap how to accurately determine the service using the received response to the re-quest sent by the previous probe directive. This directive is used in the case when the received response completely coincides with the template. In this case, the testing of the port is con-sidered complete, and with the help of additional specifiers, nmap builds a report on the name of the application, the version number and additional information received during the test.

The syntax of the match:

match <service> <pattern> [<versioninfo>]

where

19

* service - This is simply the service name that the pattern matches. Examples would be ssh, smtp, http, or snmp. As a special case, you can prefix the service name with ssl/, as in ssl/vmware-auth. In that case, the service would be stored as vmware-auth tunneled by SSL.
* pattern - This pattern is used to determine whether the response received matches the service given in the previous parameter. The format is like Perl, with the syntax being m/[regex]/[opts]. The “m” tells Nmap that a match string is beginning. The forward slash

(/) is a delimiter, which can be substituted by almost any printable character as long as the second slash is also replaced to match.

* versioninfo - The <versioninfo> section actually contains several optional fields. Each field begins with an identifying letter (such as h for “hostname”). Next comes a delimiter character which the signature writer chooses. The preferred delimiter is slash (‘/’) un-less that is used in the field itself. Next comes the field value, followed by the delimiter character.

2.10 Choose one Nmap Script and describe it

Let’s describe script named as unittest.nse.

|  |  |  |
| --- | --- | --- |
| 1 | l o c a l stdnse = r e q u i r e | ” stdnse ” |
| 2 | l o c a l u n i t t e s t = r e q u i r e ” u n i t t e s t ” | |
| 3 |  |  |
| 4 | d e s c r i p t i o n = [ [ |  |
| 5 | Runs u n i t t e s t s on a l l | NSE l i b r a r i e s . |

* ] ]

7

8

|  |  |  |
| --- | --- | --- |
| 9 | @args u n i t t e s t . run | Run t e s t s . Causes <code > u n i t t e s t . t e s t i n g ( ) </ |
| 10 | *,!* code > t o | r e t u r n t r u e . |
|  |

12 @args u n i t t e s t . t e s t s Run t e s t s from o n l y these l i b r a r i e s ( *,!* d e f a u l t s t o a l l )

1. @usage

15 nmap s c r i p t u n i t t e s t s c r i p t args u n i t t e s t . run

1. @output

|  |  |
| --- | --- |
| 18 | Pre scan s c r i p t r e s u l t s : |
| 19 | | u n i t t e s t : |
| 20 | | \_ A l l t e s t s passed |
| 21 |  |
| 22 | a u t h o r = ” D a n i e l M i l l e r ” |
| 23 | l i c e n s e = ” Same as Nmap See h t t p s : / / nmap . org / book /man l e g a l . html ” |
| 24 |
| 25 |  |
| 26 | c a t e g o r i e s = { ” s a f e ” } |
| 27 |  |

20

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 28 |  |  |  |  |
| 29 | p r e r u l e = u n i t t e s t . t e s t i n g | | | |
| 30 |  |  |  |  |
| 31 | a c t i o n = f u n c t i o n ( ) | | | |
| 32 | l o c a l l i b s = | | | stdnse . g e t \_ s c r i p t \_ a r g s ( ” u n i t t e s t . t e s t s ” ) |
| 33 | l o c a l r e s u l t | | |  |
| 34 | i f | l i b s | then |  |
| 35 |  | r e s u l t = u n i t t e s t . r u n \_ t e s t s ( l i b s ) | | |
| 36 | e l s e | |  |  |
| 37 |  | r e s u l t = u n i t t e s t . r u n \_ t e s t s ( ) | | |
| 38 | end | |  |  |
| 39 | i f | # r e s u l t == | | 0 then |
| 40 |  | r e t u r n | ” A l l | t e s t s passed ” |
| 41 | e l s e | |  |  |
| 42 |  | r e t u r n r e s u l t | | |

1. end
2. end

Listing 2.18: unittest.nse

In first two lines, variables stdnse and unittest are declared for later use in the script.

In line 4 describes the purpose of this module - run unit tests on all NSE libraries.

In line’s from 9 to 20 we see comment’s, what arguments must be passed, example of usage and output of result.

In the line 22 the author is indicated, in the 24th line the type of license.

Line 26 defines the categories of the script. There are 10 categories in total. The safe cat-egory says that the script is safe, and his work will not lead to incorrect operation or stopping of any service.

In the remaining lines, the main logic of the script is presented. In the parameter, you can specify libraries and only for them will be held a unittest’s. If you do not specify a parameter, the unittests will be run for all libraries. To perform tests, the unittest.run\_tests() function is calling, and if its return result 0 then this means that all tests were successful.

21

Conclusion

As result in this report i learned how to use nmap tool - a powerful tool for researching a new network or studying the effects of external penetration.

Nmap features include:

* Host discovery – Identifying hosts on a network. For example, listing the hosts that re-spond to TCP and/or ICMP requests or have a particular port open.
* Port scanning – Enumerating the open ports on target hosts.
* Version detection – Interrogating network services on remote devices to determine ap-plication name and version number.
* OS detection – Determining the operating system and hardware characteristics of net-work devices.

Also results can be saved in external XML file or into database, using db\_nmap.

22