LaboratoryNo2 of student Anastasiia Bozhko FB-73

Laboratory number: 2

Laboratory name: Scanning, Enumeration

Developers:

- Oleksii Baranovskyi
- Volodymyr Mishyn

Prerequisites: nmap, zenmap, netcat, telnet, metasploitable 2 virtual machine (https://sourceforge.net/projects/metasploitable/).

Table of Contents

Exercise 1. General scanning techniques

Purpose: understand scanning process

After the work the student must

- know: how scanning works
- be able to: conduct different types of scanning end explain results.

Tasks:

- scan scanme.nmap.org
- scan your HOME network
- extract information about services running on remote machine

Material and technical equipping of the workplace

- command console
- nmap, zenmap

References

- https://nmap.org/

TASK 1

Conduct an all types of known scans on proposed host. How many TCP ports are open on each? Are there any UDP ports open on any machine? Prove it with screenshots.

Answer:

```
UDP Scan Timing: About 79.39% done; ETC: 13:51 (0:03:27 remaining)
Stats: 0:16:03 elapsed; 1 hosts completed (3 up), 3 undergoing UDP Scan
UDP Scan Timing: About 94.82% done; ETC: 13:51 (0:00:53 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.00069s latency).
Not shown: 991 closed ports
PORT      STATE         SERVICE
53/udp    open|filtered domain
67/udp    open|filtered dhcps
1900/udp  open|filtered upnp
5351/udp  open          nat-pmp
32768/udp open|filtered omad
32770/udp open|filtered sometimes-rpc4
32772/udp open|filtered sometimes-rpc8
32773/udp open|filtered sometimes-rpc10
54321/udp open|filtered bo2k
MAC Address: B0:B2:DC:A8:F0:1C (ZyXEL Communications)

Nmap scan report for 192.168.1.35
Host is up (0.00044s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE
1900/udp open|filtered upnp
5353/udp open          zeroconf
MAC Address: 38:18:4C:35:5B:4D (Unknown)

Nmap scan report for 192.168.1.38
Host is up (0.014s latency).
Not shown: 999 closed ports
PORT     STATE         SERVICE
5353/udp open|filtered zeroconf
MAC Address: 7C:23:02:10:8D:22 (Unknown)

Nmap scan report for 192.168.1.46
Host is up (0.000033s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 5 IP addresses (4 hosts up) scanned in 1097.05 seconds
```

```
nastja@nastja-P5L-MX:~$ sudo nmap -sT 192.168.1.1,35,38,39,46
[sudo] пароль до nastja:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-10-14 13:53 EEST
Nmap scan report for 192.168.1.1
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: B0:B2:DC:A8:F0:1C (ZyXEL Communications)

Nmap scan report for 192.168.1.35
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
8008/tcp open  http
8009/tcp open  ajp13
8443/tcp open  https-alt
9000/tcp open  cslistener
MAC Address: 38:18:4C:35:5B:4D (Unknown)

Nmap scan report for 192.168.1.38
Host is up (0.032s latency).
All 1000 scanned ports on 192.168.1.38 are closed
MAC Address: 7C:23:02:10:8D:22 (Unknown)

Nmap scan report for 192.168.1.39
Host is up (0.010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync
MAC Address: 4A:A9:BD:1B:7F:CE (Unknown)

Nmap scan report for 192.168.1.46
Host is up (0.00062s latency).
All 1000 scanned ports on 192.168.1.46 are closed

Nmap done: 5 IP addresses (5 hosts up) scanned in 11.26 seconds
```

```
nastja@nastja-P5L-MX:~$ sudo nmap -sS 192.168.1.1,35,38,39,46
[sudo] пароль до nastja:

Starting Nmap 7.01 ( https://nmap.org ) at 2020-10-14 12:58 EEST
Nmap scan report for 192.168.1.1
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: B0:B2:DC:A8:F0:1C (ZyXEL Communications)

Nmap scan report for 192.168.1.35
Host is up (0.00032s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
8008/tcp open  http
8009/tcp open  ajp13
8443/tcp open  https-alt
9000/tcp open  cslistener
MAC Address: 38:18:4C:35:5B:4D (Unknown)

Nmap scan report for 192.168.1.46
Host is up (0.000026s latency).
All 1000 scanned ports on 192.168.1.46 are closed

Nmap done: 5 IP addresses (3 hosts up) scanned in 101.08 seconds
nastja@nastja-P5L-MX:~$
```

```
astja@nastja-P5L-MX:~$ sudo nmap -sA 192.168.1.1,35,38,39,46

tarting Nmap 7.01 ( https://nmap.org ) at 2020-10-14 13:24 EEST
map scan report for 192.168.1.1
ost is up (0.00053s latency).
ll 1000 scanned ports on 192.168.1.1 are unfiltered
AC Address: B0:B2:DC:A8:F0:1C (ZyXEL Communications)

map scan report for 192.168.1.35
ost is up (0.00033s latency).
ll 1000 scanned ports on 192.168.1.35 are unfiltered
AC Address: 38:18:4C:35:5B:4D (Unknown)

map scan report for 192.168.1.38
ost is up (0.0056s latency).
ll 1000 scanned ports on 192.168.1.38 are unfiltered
AC Address: 7C:23:02:10:8D:22 (Unknown)

map scan report for 192.168.1.39
ost is up (0.061s latency).
ll 1000 scanned ports on 192.168.1.39 are unfiltered
AC Address: 4A:A9:BD:1B:7F:CE (Unknown)

map scan report for 192.168.1.46
ost is up (0.000027s latency).
ll 1000 scanned ports on 192.168.1.46 are unfiltered

map done: 5 IP addresses (5 hosts up) scanned in 491.21 seconds
astja@nastja-P5L-MX:~$
```

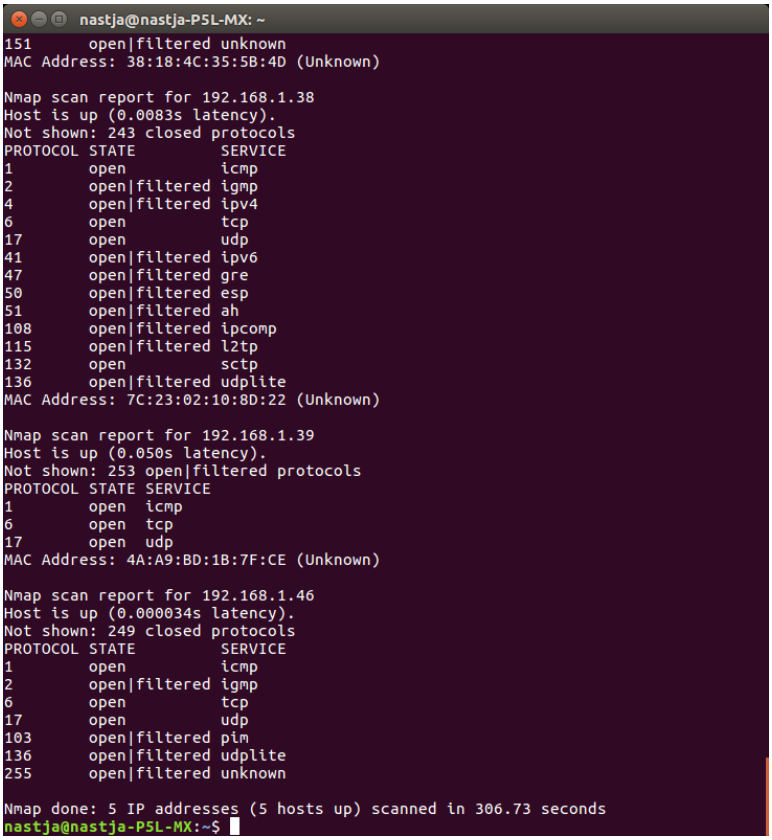
```
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$ sudo nmap -sF 192.168.1.1,35,38,39,46

Starting Nmap 7.01 ( https://nmap.org ) at 2020-10-14 14:02 EEST
Nmap scan report for 192.168.1.1
Host is up (0.00057s latency).
All 1000 scanned ports on 192.168.1.1 are open|filtered
MAC Address: B0:B2:DC:A8:F0:1C (ZyXEL Communications)

Nmap scan report for 192.168.1.35
Host is up (0.00034s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
80/tcp   open|filtered http
8008/tcp open|filtered http
8009/tcp open|filtered ajp13
8443/tcp open|filtered https-alt
9000/tcp open|filtered cslistener
MAC Address: 38:18:4C:35:5B:4D (Unknown)

Nmap scan report for 192.168.1.38
Host is up (0.0041s latency).
All 1000 scanned ports on 192.168.1.38 are closed
MAC Address: 7C:23:02:10:8D:22 (Unknown)

Nmap scan report for 192.168.1.46
Host is up (0.000026s latency).
All 1000 scanned ports on 192.168.1.46 are closed

Nmap done: 5 IP addresses (4 hosts up) scanned in 139.85 seconds
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$
```

TASK 2

Conduct an IP protocol scan (switch -sO) on host. Are the results different than that attained on previous step? Explain. Prove with screenshots.

Answer:

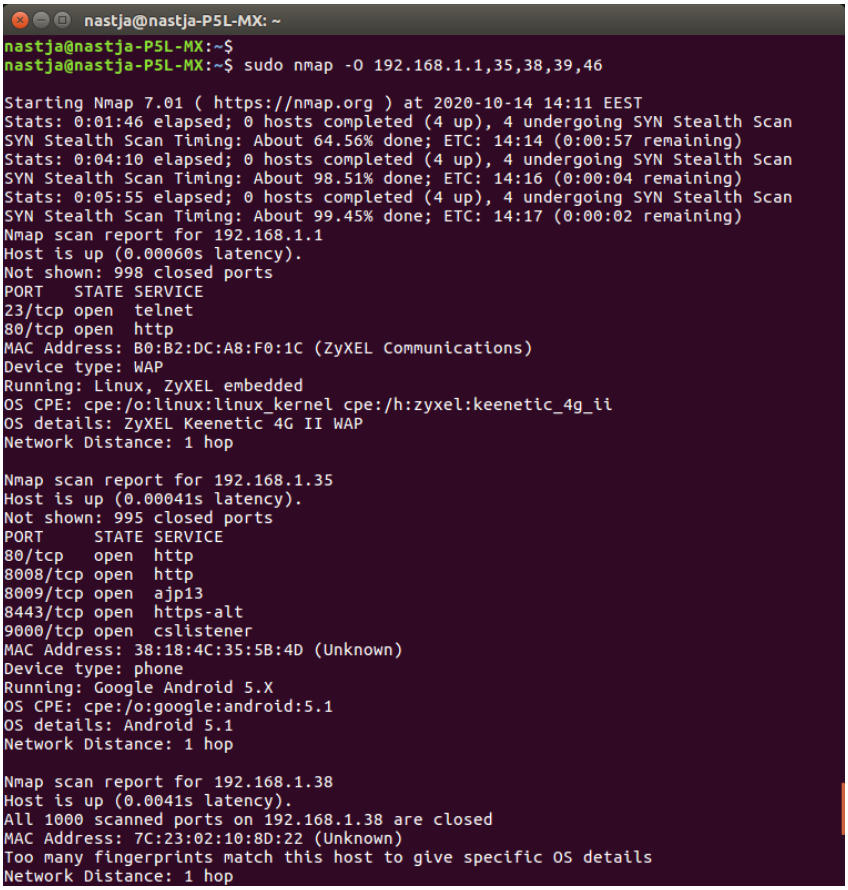
```
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$ sudo nmap -sO 192.168.1.1,35,38,39,46

Starting Nmap 7.01 ( https://nmap.org ) at 2020-10-14 13:15 EEST
Warning: 192.168.1.35 giving up on port because retransmission cap hit (10).
Warning: 192.168.1.38 giving up on port because retransmission cap hit (10).
Warning: 192.168.1.1 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.1
Host is up (0.00052s latency).
Not shown: 248 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
4        open|filtered ipv4
6        open          tcp
17       open          udp
41       open|filtered ipv6
47       open|filtered gre
136      open|filtered udplite
MAC Address: B0:B2:DC:A8:F0:1C (ZyXEL Communications)

Nmap scan report for 192.168.1.35
Host is up (0.00033s latency).
Not shown: 245 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
16       open|filtered chaos
17       open          udp
50       open|filtered esp
99       open|filtered anyencrypt
102      open|filtered pnni
108      open|filtered ipcomp
136      open|filtered udplite
151      open|filtered unknown
MAC Address: 38:18:4C:35:5B:4D (Unknown)

Nmap scan report for 192.168.1.38
Host is up (0.0083s latency).
```

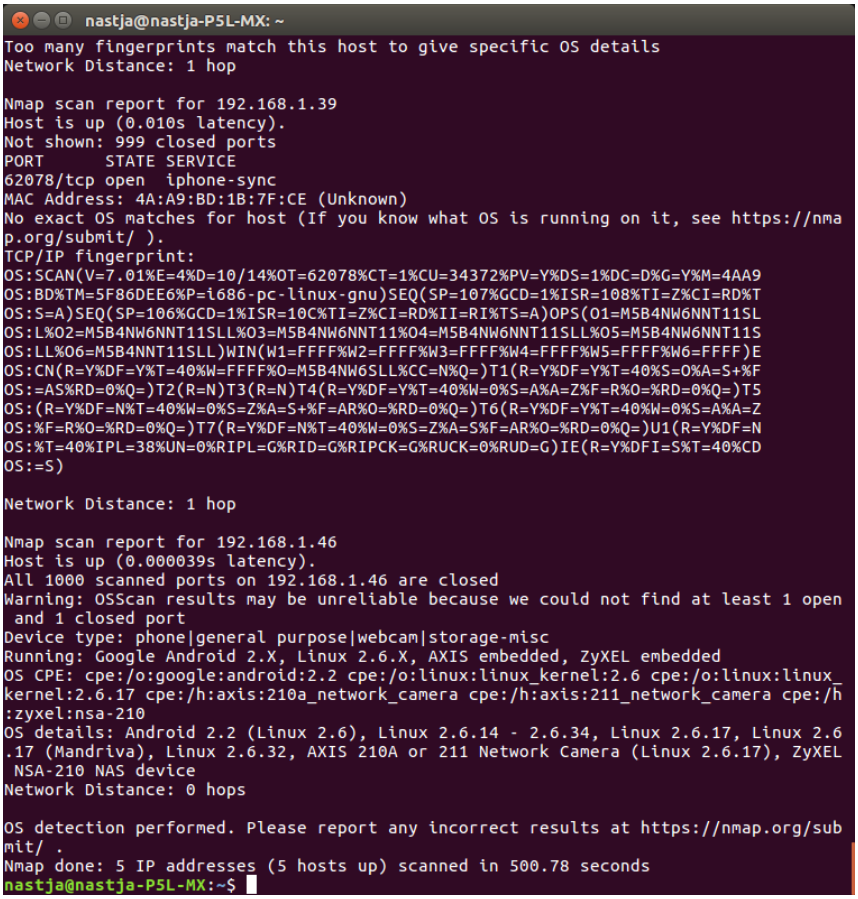


TASK 3

Conduct version detection on provided host. What operating system does nmap think host is running? What is its MAC address? How far away is it? Which hosts are located between? What operating system does nmap think host is running? Prove answers with screenshots.

Answer:





Exercise 2. Additional scanning

Purpose: understand scanning process

After the work the student must

- know: how scanning works
- be able to: conduct different types of scanning end explain results.

Tasks:

- Download and install Metasploitable 2 VM (https://sourceforge.net/projects/metasploitable/)
- scan Metasploitable
- extract information about services running on remote machine

Material and technical equipping of the workplace

- command console
- nmap, zenmap

References

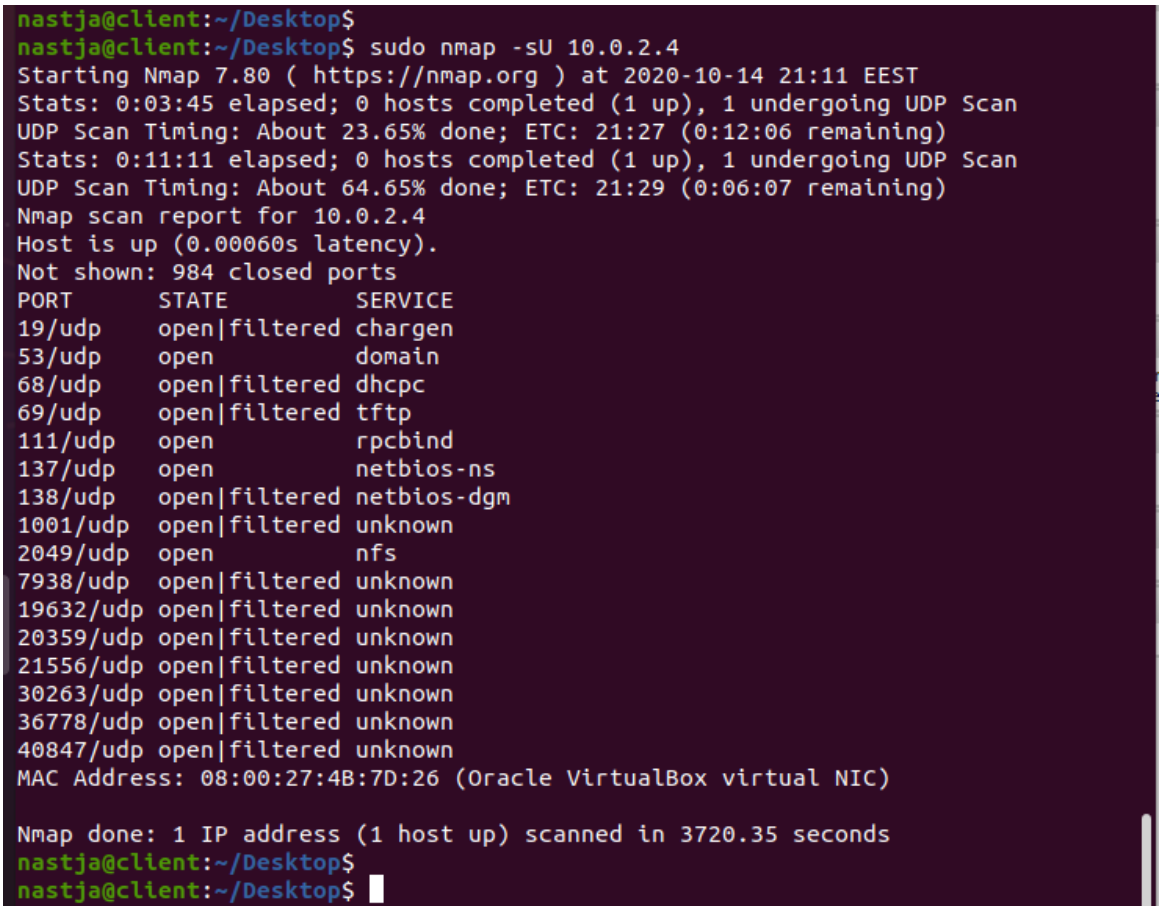
- https://nmap.org/
- https://sourceforge.net/projects/metasploitable/

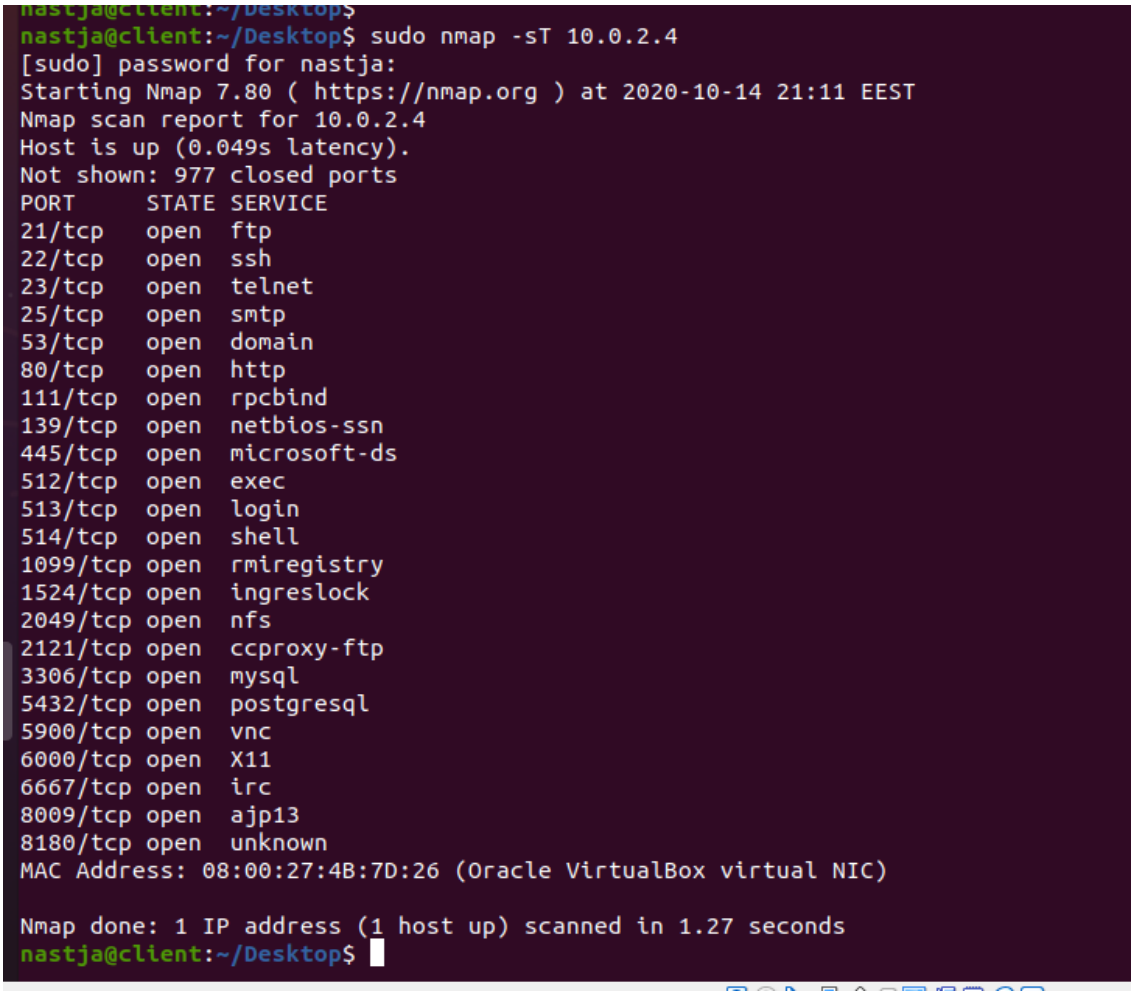
TASK 1

Conduct an all types of known scans on proposed host. How many TCP ports are open on each? Are there

any UDP ports open on any machine? Prove it with screenshots.

Answer:





'

```
nastja@client:~/Desktop$ sudo nmap -sS 10.0.2.4

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-14 20:37 EEST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 20:37 (0:00:00 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.00050s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:4B:7D:26 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
nastja@client:~/Desktop$
```

```
nastja@client:~/Desktop$
nastja@client:~/Desktop$ nmap -sA 10.0.2.4
You requested a scan type which requires root privileges.
QUITTING!
nastja@client:~/Desktop$ sudo nmap -sA 10.0.2.4
[sudo] password for nastja:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-14 22:26 EEST
Nmap scan report for 10.0.2.4
Host is up (0.00019s latency).
All 1000 scanned ports on 10.0.2.4 are unfiltered
MAC Address: 08:00:27:4B:7D:26 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.86 seconds
nastja@client:~/Desktop$
```

```
nastja@client:~/Desktop$ sudo nmap -Pn -sI 10.0.2.1 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-14 22:29 EEST
Idle scan using zombie 10.0.2.1 (10.0.2.1:80); Class: Incremental
Nmap scan report for 10.0.2.4
Host is up (0.051s latency).
Not shown: 976 closed|filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:4B:7D:26 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 46.97 seconds
nastja@client:~/Desktop$
```

TASK 2

Conduct an IP protocol scan (switch -sO) on host. Are the results different than that attained on previous step? Explain. Prove with screenshots.

Answer:

```
nastja@client:~/Desktop$
nastja@client:~/Desktop$ sudo nmap -sO 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-14 22:31 EEST
Warning: 10.0.2.4 giving up on port because retransmission cap hit (10).
Stats: 0:04:19 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 94.39% done; ETC: 22:36 (0:00:15 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.0023s latency).
Not shown: 234 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
15       open|filtered xnet
17       open          udp
21       open|filtered prm
52       open|filtered i-nlsp
55       open|filtered mobile
59       open|filtered ipv6-nonxt
68       open|filtered anydistribfs
73       open|filtered cphb
92       open|filtered mtp
102      open|filtered pnni
106      open|filtered qnx
136      open|filtered udplite
157      open|filtered unknown
168      open|filtered unknown
170      open|filtered unknown
183      open|filtered unknown
214      open|filtered unknown
231      open|filtered unknown
255      open|filtered unknown
MAC Address: 08:00:27:4B:7D:26 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 299.47 seconds
nastja@client:~/Desktop$
```

TASK 3

Conduct version detection on provided host. What operating system does nmap think host is running? What is its MAC address? What operating system does nmap think host is running? Prove answers with screenshots.

Answer:

```
nastja@client:~/Desktop$
nastja@client:~/Desktop$ sudo nmap -sV -O 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-15 16:48 EEST
Nmap scan report for 10.0.2.4
Host is up (0.00081s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:4B:7D:26 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at htt
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.68 seconds
nastja@client:~/Desktop$
```

Exercise 3. Manual and automatic enumeration

Purpose: understand enumeration process

After the work the student must

- know: how enumeration works
- be able to: conduct different types of enumeration end explain results.

Tasks:

- Download and install Metasploitable 2 VM (https://sourceforge.net/projects/metasploitable/)
- Enumerate services and users on Metasploitable

Material and technical equipping of the workplace

- command console
- nmap, zenmap, nmap scripts, metasploit, nc, telnet

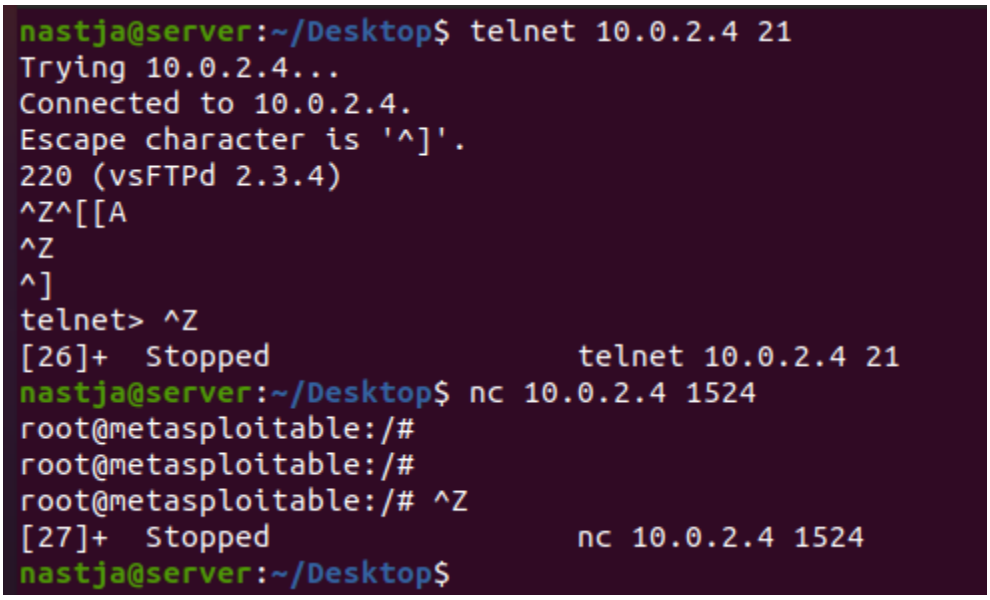
References

- https://nmap.org/
- https://sourceforge.net/projects/metasploitable/

TASK 1

Based on previous scanning results try to conduct manual enumeration on Metasploitable VM. What services are vulnerable? Prove results with screenshots.

Answer:



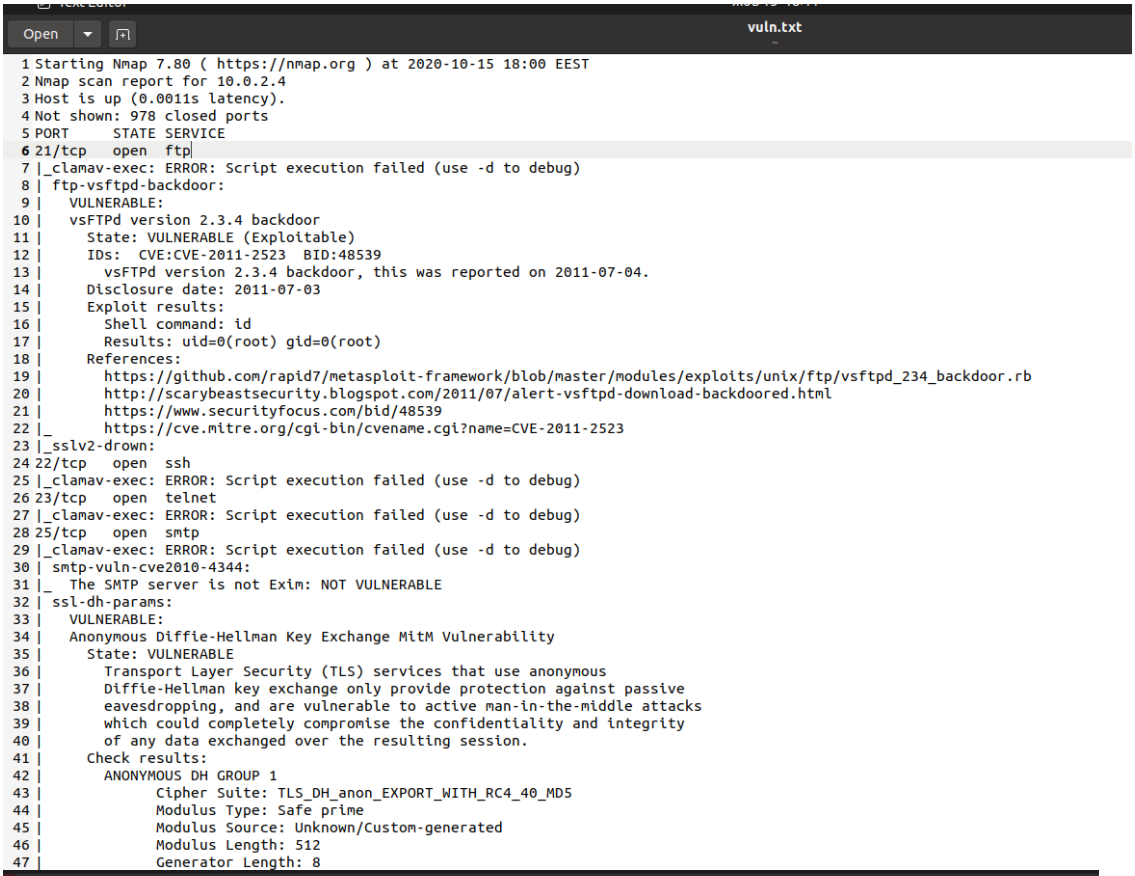
```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
id
502 5.5.2 Error: command not recognized
^Z
[7]+  Stopped                 nc 10.0.2.4 25
nastja@server:~/Desktop$ nc 10.0.2.4 53

^Z
[8]+  Stopped                 nc 10.0.2.4 53
nastja@server:~/Desktop$ nc 10.0.2.4 80
^Z
[9]+  Stopped                 nc 10.0.2.4 80
nastja@server:~/Desktop$ nc 10.0.2.4 111
^Z
[10]+  Stopped                 nc 10.0.2.4 111
nastja@server:~/Desktop$ nc 10.0.2.4 139
^Z
[11]+  Stopped                 nc 10.0.2.4 139
nastja@server:~/Desktop$ nc 10.0.2.4 445
^Z
[12]+  Stopped                 nc 10.0.2.4 445
nastja@server:~/Desktop$ nc 10.0.2.4 512
Where are you?
dasd
nastja@server:~/Desktop$ nc 10.0.2.4 513
^Z
[13]+  Stopped                 nc 10.0.2.4 513
nastja@server:~/Desktop$ nc 10.0.2.4 514
^Z
[14]+  Stopped                 nc 10.0.2.4 514
nastja@server:~/Desktop$ nc 10.0.2.4 1099
^Z
[15]+  Stopped                 nc 10.0.2.4 1099
nastja@server:~/Desktop$ nc 10.0.2.4 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin
boot
cdrom
dev
```

```
sys
tmp
usr
var
vmlinuz
root@metasploitable:/# ^Z
[16]+  Stopped                 nc 10.0.2.4 1524
nastja@server:~/Desktop$ nc 10.0.2.4 2029
nastja@server:~/Desktop$ nc 10.0.2.4 2049
^Z
[17]+  Stopped                 nc 10.0.2.4 2049
nastja@server:~/Desktop$ nc 10.0.2.4 2121
220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.4]
^Z
[18]+  Stopped                 nc 10.0.2.4 2121
nastja@server:~/Desktop$ nc 10.0.2.4 3306
>
5.0.51a-3ubuntu5
qjACkr}=,UumB@Y":=d^,^Z
[19]+  Stopped                 nc 10.0.2.4 3306
nastja@server:~/Desktop$ nc 10.0.2.4 5432
^Z
[20]+  Stopped                 nc 10.0.2.4 5432
nastja@server:~/Desktop$ nc 10.0.2.4 5900
RFB 003.003
^Z
[21]+  Stopped                 nc 10.0.2.4 5900
nastja@server:~/Desktop$ nc 10.0.2.4 6000
^Z
[22]+  Stopped                 nc 10.0.2.4 6000
nastja@server:~/Desktop$ nc 10.0.2.4 6667
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using
your IP address instead
^Z
[23]+  Stopped                 nc 10.0.2.4 6667
nastja@server:~/Desktop$ nc 10.0.2.4 8009
^Z
[24]+  Stopped                 nc 10.0.2.4 8009
nastja@server:~/Desktop$ nc 10.0.2.4 8180
^Z
[25]+  Stopped                 nc 10.0.2.4 8180
nastja@server:~/Desktop$
```

TASK 2

Based on previous scanning results try to conduct automatic enumeration on Metasploitable VM using nmap scripts. What services are vulnerable? Prove results with screenshots.

Answer:
nmap –script=vuln 10.0.2.4

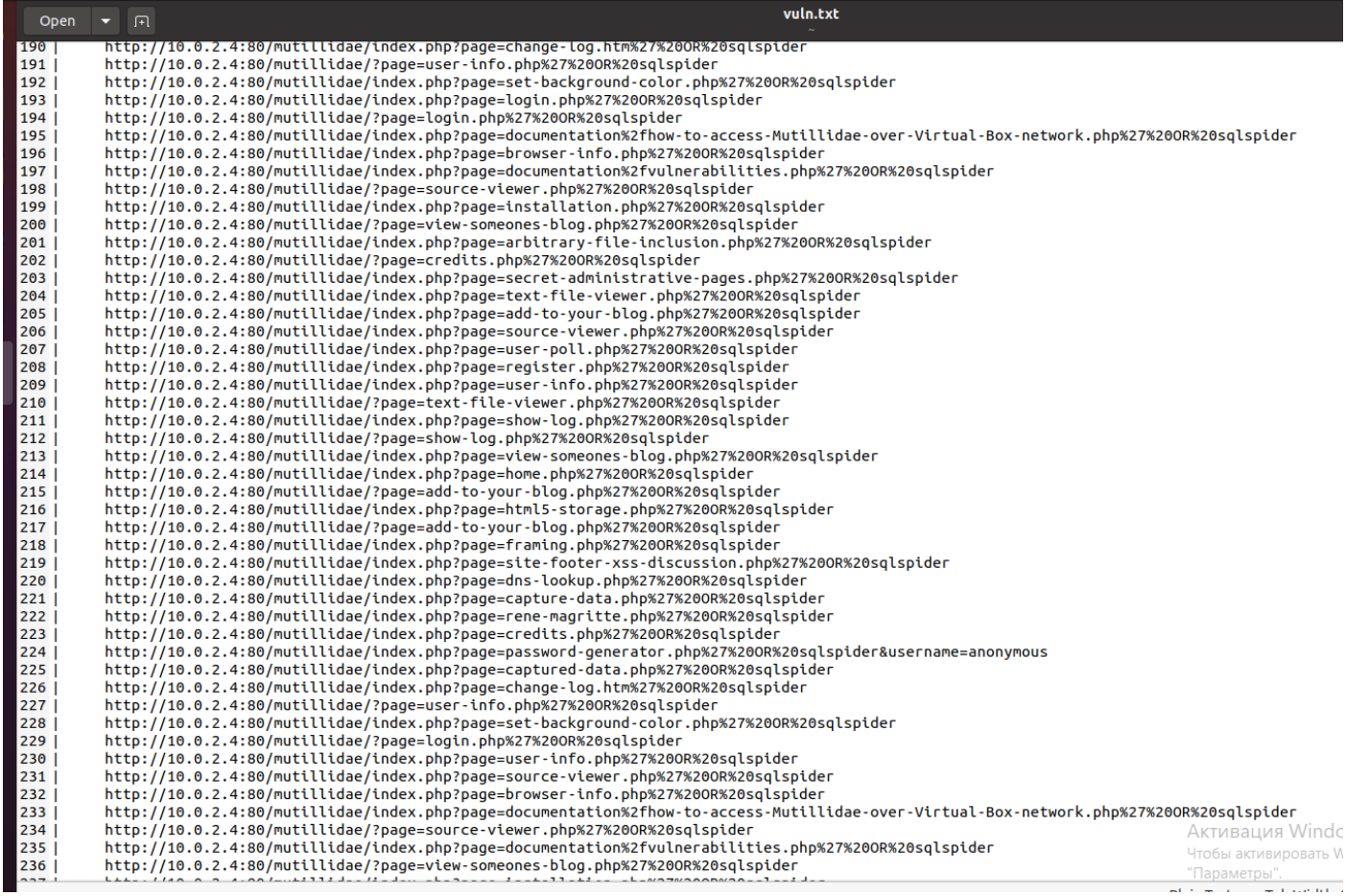


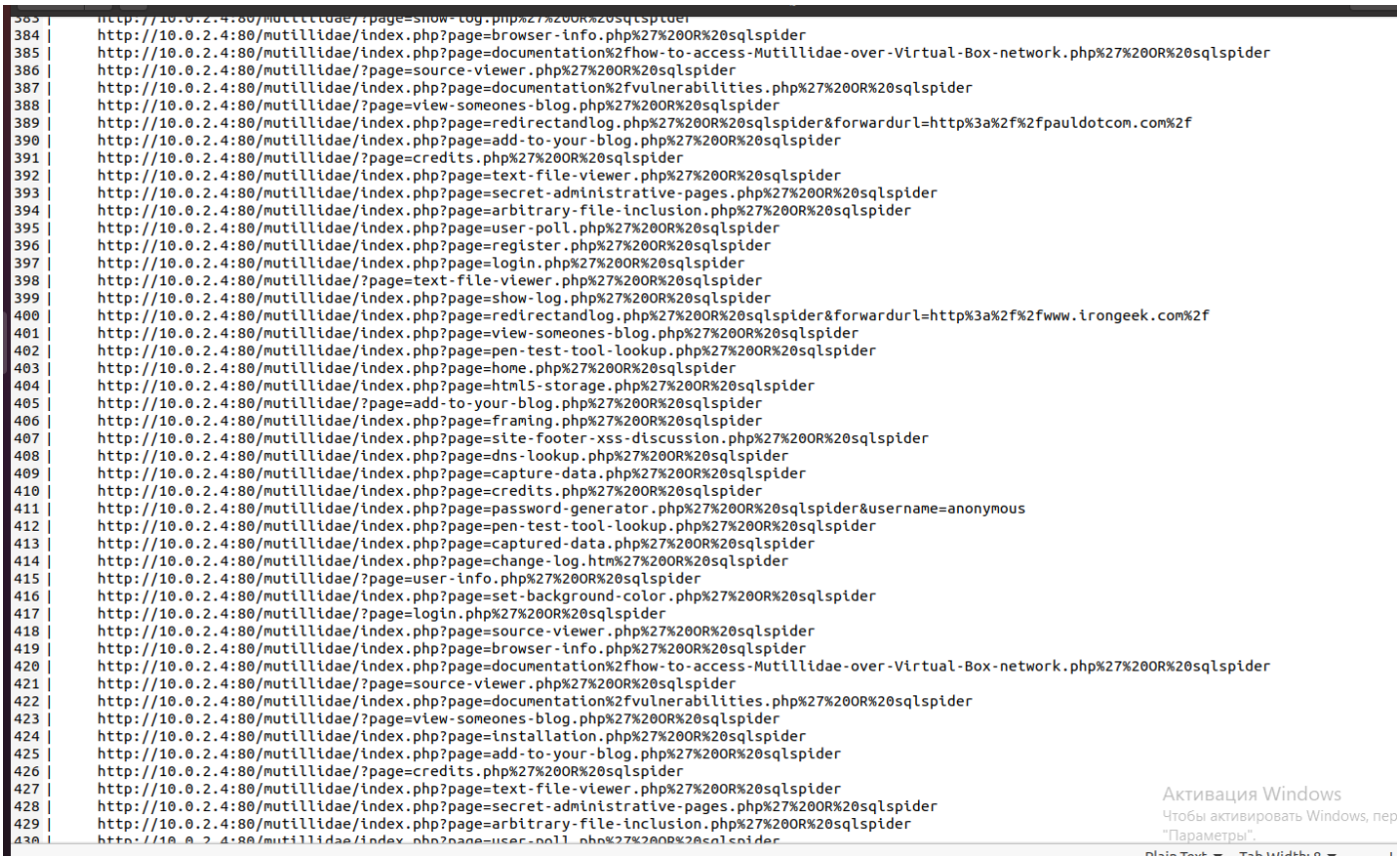
```
Open                                                    vuln.txt
 1 Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-15 18:00 EEST
 2 Nmap scan report for 10.0.2.4
 3 Host is up (0.0011s latency).
 4 Not shown: 978 closed ports
 5 PORT     STATE SERVICE
 6 21/tcp   open  ftp
 7 |_clamav-exec: ERROR: Script execution failed (use -d to debug)
 8 | ftp-vsftpd-backdoor:
 9 |   VULNERABLE:
10 |   vsFTPd version 2.3.4 backdoor
11 |     State: VULNERABLE (Exploitable)
12 |     IDs:  CVE:CVE-2011-2523  BID:48539
13 |       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
14 |     Disclosure date: 2011-07-03
15 |     Exploit results:
16 |       Shell command: id
17 |       Results: uid=0(root) gid=0(root)
18 |     References:
19 |       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
20 |       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
21 |       https://www.securityfocus.com/bid/48539
22 |_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
23 |_sslv2-drown:
24 22/tcp   open  ssh
25 |_clamav-exec: ERROR: Script execution failed (use -d to debug)
26 23/tcp   open  telnet
27 |_clamav-exec: ERROR: Script execution failed (use -d to debug)
28 25/tcp   open  smtp
29 |_clamav-exec: ERROR: Script execution failed (use -d to debug)
30 | smtp-vuln-cve2010-4344:
31 |_  The SMTP server is not Exim: NOT VULNERABLE
32 | ssl-dh-params:
33 |   VULNERABLE:
34 |   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
35 |     State: VULNERABLE
36 |       Transport Layer Security (TLS) services that use anonymous
37 |       Diffie-Hellman key exchange only provide protection against passive
38 |       eavesdropping, and are vulnerable to active man-in-the-middle attacks
39 |       which could completely compromise the confidentiality and integrity
40 |       of any data exchanged over the resulting session.
41 |     Check results:
42 |       ANONYMOUS DH GROUP 1
43 |             Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
44 |             Modulus Type: Safe prime
45 |             Modulus Source: Unknown/Custom-generated
46 |             Modulus Length: 512
47 |             Generator Length: 8
```

```
Open                                                    vuln.txt
46 |             Modulus Length: 512
47 |             Generator Length: 8
48 |             Public Key Length: 512
49 |     References:
50 |       https://www.ietf.org/rfc/rfc2246.txt
51 |
52 |   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
53 |     State: VULNERABLE
54 |     IDs:  CVE:CVE-2015-4000  BID:74733
55 |       The Transport Layer Security (TLS) protocol contains a flaw that is
56 |       triggered when handling Diffie-Hellman key exchanges defined with
57 |       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
58 |       to downgrade the security of a TLS session to 512-bit export-grade
59 |       cryptography, which is significantly weaker, allowing the attacker
60 |       to more easily break the encryption and monitor or tamper with
61 |       the encrypted stream.
62 |     Disclosure date: 2015-5-19
63 |     Check results:
64 |       EXPORT-GRADE DH GROUP 1
65 |             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
66 |             Modulus Type: Safe prime
67 |             Modulus Source: Unknown/Custom-generated
68 |             Modulus Length: 512
69 |             Generator Length: 8
70 |             Public Key Length: 512
71 |     References:
72 |       https://weakdh.org
73 |       https://www.securityfocus.com/bid/74733
74 |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
75 |
76 |   Diffie-Hellman Key Exchange Insufficient Group Strength
77 |     State: VULNERABLE
78 |       Transport Layer Security (TLS) services that use Diffie-Hellman groups
79 |       of insufficient strength, especially those using one of a few commonly
80 |       shared groups, may be susceptible to passive eavesdropping attacks.
81 |     Check results:
82 |       WEAK DH GROUP 1
83 |             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
84 |             Modulus Type: Safe prime
85 |             Modulus Source: postfix builtin
86 |             Modulus Length: 1024
87 |             Generator Length: 8
88 |             Public Key Length: 1024
89 |     References:
90 |_      https://weakdh.org
91 | ssl-poodle:
92 |   VULNERABLE:
```

```
|_      https://wiki.dh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.securityfocus.com/bid/70574
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.4
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.4:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://10.0.2.4:80/mutillidae/index.php?page=dns-lookup.php
|     Form id: iddnslookupform
|_    Form action: index.php?page=dns-lookup.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-sql-injection:
```

```
|_    Couldn't find a file-type field.
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.2.4:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://10.0.2.4:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=documentation%2fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=documentation%2fvulnerabilities.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://10.0.2.4:80/dav/?C=N%3bO%3dD%27%20OR%20sqlspider
|     http://10.0.2.4:80/dav/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://10.0.2.4:80/dav/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://10.0.2.4:80/dav/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://10.0.2.4:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
```

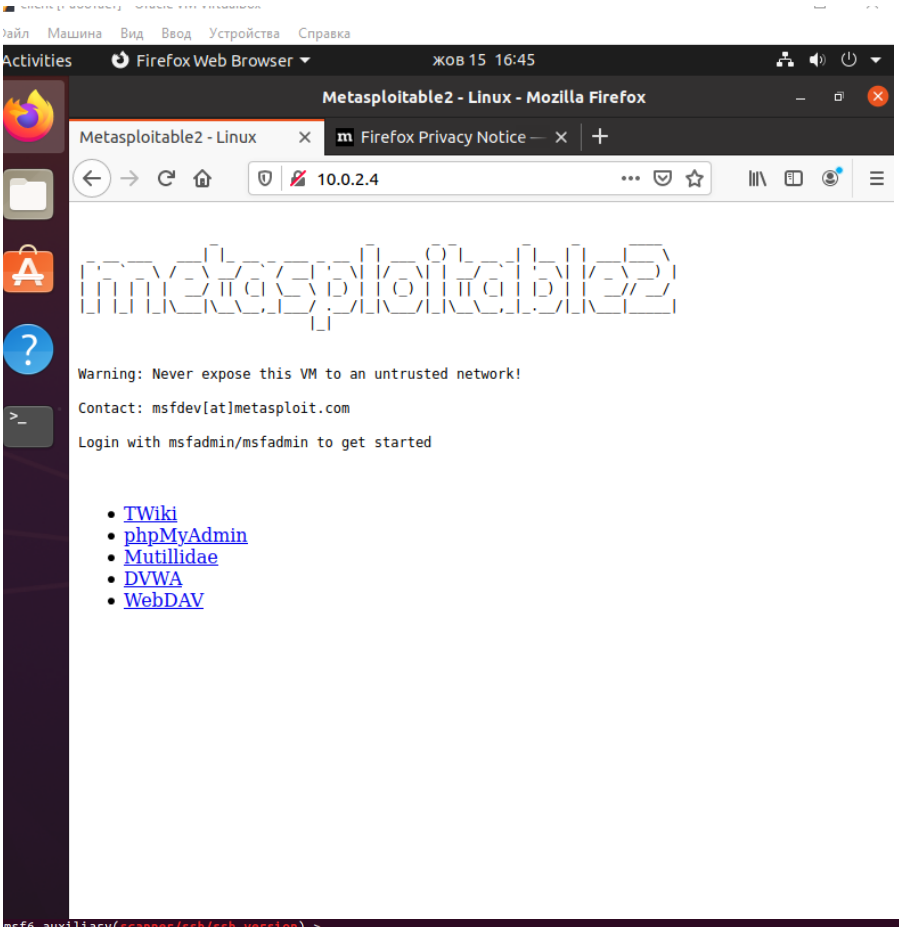




TASK 3

Based on previous scanning results try to conduct automatic enumeration on Metasploitable VM using metasploit auzillary module. Prove results with screenshots. Are any difference with results from previous steps? Explain.

Answer:




```
msf6 auxiliary(scanner/ssh/ssh_version) >
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.1.42
RHOSTS => 192.168.1.42
msf6 auxiliary(scanner/ssh/ssh_version) > run

[+] 192.168.1.42:22       - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family
=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23=cpe:/o:canonical:ubuntu_linu
x:8.04 service.protocol=ssh fingerprint_db=ssh.banner )
[*] 192.168.1.42:22       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 192.168.1.42
RHOSTS => 192.168.1.42
msf6 auxiliary(scanner/ftp/ftp_version) > run

[+] 192.168.1.42:21       - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] 192.168.1.42:21       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) > use auxiliary/scanner/smtp/smtp_version
msf6 auxiliary(scanner/smtp/smtp_version) > run
[-] Auxiliary failed: Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/smtp/smtp_version) > set RHOSTS 192.168.1.42
RHOSTS => 192.168.1.42
msf6 auxiliary(scanner/smtp/smtp_version) > run

[+] 192.168.1.42:25       - 192.168.1.42:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.168.1.42:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_version) > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.1.42
RHOSTS => 192.168.1.42
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.42:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.42
RHOSTS => 192.168.1.42
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.42:23       - 192.168.1.42:23 TELNET                                                  \x0a _ __ ___  ___| |_ ___ _ __ | | ___(_) |_ __ _| |__ | | ___|
___ \ \x0a| '_ ` _ \ / _ \ __/ _ \ / __| '_ \| |/ _ \ | |/ _ \ __| |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|___
|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                                |_|                                                \x0a\x0a\x0aWarning: Never expose this VM to
 an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.42:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > use auxiliary/scanner/mysql/mysql_version
msf6 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 192.168.1.42
RHOSTS => 192.168.1.42
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.1.42:3306     - 192.168.1.42:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 192.168.1.42:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) >
msf6 auxiliary(scanner/mysql/mysql_version) >
[2]+  Зупинено        msfconsole
nastja@nastja-P5L-MX:~$
nastja@nastja-P5L-MX:~$
```