
Lab Report - Exercise 1

Gitesh Gund
(gund@rhrk.uni-kl.de) Group 3

Ashitha Mudraje
(bud07nyc@rptu.de) Group 3

Anas Ahmad
(aahmad@rhrk.uni-kl.de) Group 3

Vinson Noronha
(noronha@rptu.de) Group 9

May 5, 2023

1 Abstract

Short summery of key findings.

1. We developed a shell script that checks for live hosts in a subnet that respond to ICMP and UDP ping sweep. We then performed a similar scan using nmap and compared the results.
2. We enumerated directories and searched for files in those directories using a provided wordlist. We compared the results of our custom script with Gobuster.
3. we successfully located the required flags for the lab and submitted them on OLAT.

2 Scanning Results

2.1 Bash script for Host Discovery

We created the following bash script to discover live hosts in the subnet.

```
1 #!/bin/bash
2
3 check_host_alive_ping()
4 {
5     ping -c 1 -W 2 192.168.59.$i > /dev/null
6     [ $? -eq 0 ] && echo "192.168.59.$i"
7 }
8
9 check_host_alive_nmap(){
10     fping -u -t 100 192.168.59.$i > /dev/null
11     [ $? -eq 0 ] && echo "192.168.59.$i"
12 }
13
14
15 ips=$(for i in {1..254}; do (check_host_alive_ping 192.168.59.$i); done))
16
17 ips+=($(for i in {1..254}; do (check_host_alive_nmap 192.168.59.$i); done))
18
19
20 sorted_unique_ips=$(echo "${ips[@]}" | tr ' ' '\n' | sort -u | tr '\n' ' ')
21
22 check_host_port(){
23     echo "nc -nvz $1"
24     nc -nvz $1 1 100 > $1.txt 2>&1
25     cat $1.txt
26     rm -rf \ $1.txt
27 }
```

```
28  
29 for i in "${sorted_unique_ips[@]}"; do ( echo "$i" >> ping_sweep_output.txt); done
```

This is the result of our script and these are IPs that we got:

```
(jetsunburst@LAP-GIGU)-[~/Infosec]  
$ cat ping_sweep_output.txt  
192.168.59.127  
192.168.59.148  
192.168.59.2  
192.168.59.22  
192.168.59.69  
192.168.59.99
```

2.2 Subnet scan using Nmap

We used the preinstalled tool nmap to find the Up hosts in the subnet.

```
(jetsunburst@LAP-GIGU)-[~]  
$ nmap -sn 192.168.59.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 23:11 CEST  
Nmap scan report for 192.168.59.22  
Host is up (0.0032s latency).  
Nmap scan report for 192.168.59.69  
Host is up (0.0039s latency).  
Nmap scan report for 192.168.59.99  
Host is up (0.0033s latency).  
Nmap scan report for 192.168.59.127  
Host is up (0.0031s latency).  
Nmap scan report for 192.168.59.148  
Host is up (0.0053s latency).  
Nmap scan report for 192.168.59.206  
Host is up (0.0045s latency).  
Nmap scan report for 192.168.59.233  
Host is up (0.0044s latency).  
Nmap done: 256 IP addresses (7 hosts up) scanned in 15.11 seconds  
  
(jetsunburst@LAP-GIGU)-[~]  
$ |
```

2.3 Comparison of results

Now we have results of both the scans, one from our bash script and the other from nmap. Following are the detailed comparison results:

1. Our bash script provided us with 6 Up hosts in the subnet, the IPs are: 192.168.59.2, 192.168.59.22, 192.168.59.69, 192.168.59.99, 192.168.59.127, 192.168.59.148

2. Nmap provided the following IPs: 192.168.59.22, 192.168.59.69, 192.168.59.99, 192.168.59.127, 192.168.59.148, 192.168.59.206, 192.168.59.237
3. Through our script we got an IP "192.168.59.2" that is not provided through the result of nmap.
4. Whereas nmap gives two additional IPs that were missing in the result of our script "192.168.59.206" and "192.168.59.237"

2.4 Service and OS Discovery

After discovering the live hosts in the subnet we performed scan using nmap to find out the services running on each host and their respective Operating Systems. We used the following nmap command "sudo nmap -p 1-65535 -sV -O 192.168.59.0/24", the result are as follows:

```

1 (jetsunburstLAP-GIGU)-[~]
2 $ sudo nmap -p 1-65535 -sV -O 192.168.59.0/24
3 [sudo] password for jetsunburst:
4 Sorry, try again.
5 [sudo] password for jetsunburst:
6 Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 18:55 CEST
7 Nmap scan report for 192.168.59.2
8 Host is up (0.0056s latency).
9 All 65535 scanned ports on 192.168.59.2 are in ignored states.
10 Not shown: 65535 filtered tcp ports (proto-unreach)
11 Too many fingerprints match this host to give specific OS details
12 Network Distance: 2 hops
13
14 Nmap scan report for 192.168.59.22
15 Host is up (0.0040s latency).
16 All 65535 scanned ports on 192.168.59.22 are in ignored states.
17 Not shown: 65535 closed tcp ports (reset)
18 Too many fingerprints match this host to give specific OS details
19 Network Distance: 2 hops
20
21 Nmap scan report for 192.168.59.69
22 Host is up (0.0041s latency).
23 Not shown: 65534 closed tcp ports (reset)
24 PORT      STATE SERVICE VERSION
25 80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
26 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
27 TCP/IP fingerprint:
28 OS: SCAN (V=7.93%E=4%D=5/5%OT=80%CT=1%CU=34360%PV=Y%DS=2%DC=I%G=Y%TM=6455352F
29 OS:%P=x86_64-pc-linux-gnu) SEQ (SP=104%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A) OPS (
30 OS:01=M551ST11NW7%02=M551ST11NW7%03=M551NNT11NW7%04=M551ST11NW7%05=M551ST11
31 OS:NW7%06=M551ST11) WIN (W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88) ECN (
32 OS:R=Y%DF=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=) T1 (R=Y%DF=Y%T=40%S=0%A=S+%F=AS
33 OS:%RD=0%Q=) T2 (R=N) T3 (R=N) T4 (R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=) T5 (R=
34 OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=) T6 (R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
35 OS:R%O=%RD=0%Q=) T7 (R=N) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%R
36 OS:UCK=G%RUD=G) IE (R=Y%DFI=N%T=40%CD=S)
37
38 Network Distance: 2 hops
39
40 Nmap scan report for 192.168.59.99
41 Host is up (0.0041s latency).
42 Not shown: 65533 closed tcp ports (reset)
43 PORT      STATE SERVICE VERSION
44 139/tcp   open  netbios-ssn Samba smbd 4.6.2
45 445/tcp   open  netbios-ssn Samba smbd 4.6.2
46 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
47 TCP/IP fingerprint:
48 OS: SCAN (V=7.93%E=4%D=5/5%OT=139%CT=1%CU=37003%PV=Y%DS=2%DC=I%G=Y%TM=6455352
49 OS:F%P=x86_64-pc-linux-gnu) SEQ (SP=106%GCD=2%ISR=110%TI=Z%CI=Z%II=I%TS=A) OPS
50 OS:(01=M551ST11NW7%02=M551ST11NW7%03=M551NNT11NW7%04=M551ST11NW7%05=M551ST1
51 OS:1NW7%06=M551ST11) WIN (W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88) ECN
52 OS:(R=Y%DF=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=) T1 (R=Y%DF=Y%T=40%S=0%A=S+%F=A
53 OS:S%RD=0%Q=) T2 (R=N) T3 (R=N) T4 (R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=) T5 (R
54 OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=) T6 (R=Y%DF=Y%T=40%W=0%S=A%A=Z%F

```

```

55 OS:=R%O=%RD=0%Q=) T7 (R=N) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
56 OS:RUCK=G%RUD=G) IE (R=Y%DFI=N%T=40%CD=S)
57
58 Network Distance: 2 hops
59
60 Nmap scan report for 192.168.59.127
61 Host is up (0.0041s latency).
62 Not shown: 65534 closed tcp ports (reset)
63 PORT      STATE SERVICE VERSION
64 22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
65 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
66 TCP/IP fingerprint:
67 OS:SCAN(V=7.93%E=4%D=5/5%OT=22%CT=1%CU=39616%PV=Y%DS=2%DC=I%G=Y%TM=64553567
68 OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS(O
69 OS:1=M551ST11NW7%02=M551ST11NW7%03=M551NNT11NW7%04=M551ST11NW7%05=M551ST11N
70 OS:W7%06=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R
71 OS:=Y%DF=Y%T=40%W=FAFO%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%
72 OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y
73 OS:%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
74 OS:%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RU
75 OS:CK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
76
77 Network Distance: 2 hops
78 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
79
80 Nmap scan report for 192.168.59.148
81 Host is up (0.0041s latency).
82 Not shown: 64510 closed tcp ports (reset), 980 filtered tcp ports (no-response), 42 filtered
   tcp ports (host-prohibited)
83 PORT      STATE SERVICE VERSION
84 22/tcp    open  ssh      OpenSSH 7.8 (protocol 2.0)
85 80/tcp    open  http     Apache httpd 2.4.38 ((Fedora) OpenSSL/1.1.1 mod_perl/2.0.10 Perl/v5
   .28.0)
86 3306/tcp  open  mysql    MariaDB (unauthorized)
87 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
88 TCP/IP fingerprint:
89 OS:SCAN(V=7.93%E=4%D=5/5%OT=22%CT=1025%CU=30173%PV=Y%DS=2%DC=I%G=Y%TM=64553
90 OS:5677%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=2%ISR=10E%TI=Z%CI=Z%II=I%TS=A)S
91 OS:EQ(SP=102%GCD=1%ISR=10E%TI=Z%CI=Z%TS=A)OPS(O1=M551ST11NW7%02=M551ST11NW7
92 OS:%03=M551NNT11NW7%04=M551ST11NW7%05=M551ST11NW7%06=M551ST11)WIN(W1=7120%W
93 OS:2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M551NN
94 OS:SNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y
95 OS:%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
96 OS:O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF
97 OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
98 OS:%CD=S)
99
100 Network Distance: 2 hops
101
102 Nmap scan report for 192.168.59.206
103 Host is up (0.0046s latency).
104 All 65535 scanned ports on 192.168.59.206 are in ignored states.
105 Not shown: 65535 closed tcp ports (reset)
106 Too many fingerprints match this host to give specific OS details
107 Network Distance: 2 hops
108
109 Nmap scan report for 192.168.59.233
110 Host is up (0.0041s latency).
111 Not shown: 65534 closed tcp ports (reset)
112 PORT      STATE SERVICE VERSION
113 21/tcp    open  ftp      vsftpd 3.0.5
114 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
115 TCP/IP fingerprint:
116 OS:SCAN(V=7.93%E=4%D=5/5%OT=21%CT=1%CU=33141%PV=Y%DS=2%DC=I%G=Y%TM=64553567
117 OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%TS=A)OPS(O1=M5
118 OS:51ST11NW7%02=M551ST11NW7%03=M551NNT11NW7%04=M551ST11NW7%05=M551ST11NW7%0
119 OS:6=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%D
120 OS:F=Y%T=40%W=FAFO%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0

```

```

121 OS:%Q=) T2(R=N) T3(R=N) T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=) T5(R=Y%DF=
122 OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=) T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
123 OS:RD=0%Q=) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
124 OS:%RUD=G) IE(R=N)
125
126 Network Distance: 2 hops
127 Service Info: OS: Unix
128
129 OS and Service detection performed. Please report any incorrect results at https://nmap.org/
    submit/ .
130 Nmap done: 256 IP addresses (8 hosts up) scanned in 121.57 seconds
131 (jetsunburstLAP-GIGU)-[~]

```

Services and OS of each host:

1. 192.168.59.22 - It does not clearly indicate either service or OS
2. 192.168.59.69 - Service running is Apache and OS is Ubuntu
3. 192.168.59.99 - Service running is Samba and OS cannot be determined
4. 192.168.59.127 - Service running is OpenSSH and OS is Ubuntu
5. 192.168.59.148 - Services running are OpenSSH, Apache and MariaDB and OS is Fedora
6. 192.168.59.206 - It does not clearly indicate either service or OS
7. 192.168.59.233 - Service running is FTP and OS cannot be determined

3 Directory Scanning

In directory scanning we performed following tasks, firstly we created a python script that enumerates all the directories and list out the files present in the root as well as in the discovered directories. Secondly, we performed the same implementation using the tool gobuster. Finally, we compared the result of the above two implementations.

3.1 Directory Scanning using custom script

This is the python script that we have created to scan all directories and files present in those directories and in root. We used the wordlist provided with the Lab.

```

1 #!/usr/bin/python
2 # -*- coding: utf-8 -*-
3 import requests
4
5 # Define the url and wordlist file path
6
7 url = 'http://192.168.59.69/'
8 wordlist_file = 'Lab1/web_directory_wordlist.txt'
9
10 # Define the file extensions to search for
11
12 file_extensions = ['.html', '.php', '.txt']
13
14 # Read the wordlist file into a list
15
16 with open(wordlist_file, 'r') as f:
17     wordlist = [line.strip() for line in f]
18
19
20 # Function to check if a directory exists
21 found_directories = []
22 def check_directory(directory):
23     response = requests.get(url + directory)
24     if response.status_code == 200:
25         found_directories.append(directory)
26         return True
27     else:

```

```

28         return False
29
30 # Loop through each directory in the wordlist and check if it exists
31
32 for directory in wordlist:
33     if check_directory(directory):
34         print ('Directory found: ' + directory)
35
36 for word in wordlist:
37     for extension in file_extensions:
38         for directory in found_directories:
39             file_url = url + directory + "/" + word + extension
40             response = requests.get(file_url)
41             if response.status_code == 200:
42                 print("File found: " + file_url)

```

This is the result that we got through our script:

```

(kali㉿kali)-[~/Desktop/ISAO Ex1]
$ python directory_scan.py
Directory found: inprogress
Directory found: sources
Directory found: test
Directory found:

File found: http://192.168.59.69//flag.php
File found: http://192.168.59.69/inprogress/hidden.txt
File found: http://192.168.59.69//index.php

(kali㉿kali)-[~/Desktop/ISAO Ex1]
$

```

3.2 Directory Scanning using Gobuster

We used the tool Gobuster in Kali Linux to enumerate the directories and find out the files present. We used the following Gobuster command

```

1 gobuster dir -e -u http://192.168.59.69 -w web_directory_wordlist.txt -x php,html,txt -t20

```

The results are as follows:

```
(jetsunburst@LAP-GIGU)~[~/Infosec/Lab1]
$ gobuster dir -u http://192.168.59.69 -w web_directory_wordlist.txt -x php,html,txt -t20
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.59.69
[+] Method: GET
[+] Threads: 20
[+] Wordlist: web_directory_wordlist.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: php,html,txt
[+] Timeout: 10s
=====
2023/05/05 19:24:15 Starting gobuster in directory enumeration mode
=====
/.htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htaccess.php (Status: 403) [Size: 278]
/.htpasswd.php (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/flag.php (Status: 200) [Size: 165]
/index.php (Status: 200) [Size: 1268]
/inprogress (Status: 301) [Size: 319] [--> http://192.168.59.69/inprogress/]
/server-status (Status: 403) [Size: 278]
/sources (Status: 301) [Size: 316] [--> http://192.168.59.69/sources/]
/test (Status: 301) [Size: 313] [--> http://192.168.59.69/test/]
/. (Status: 200) [Size: 1268]
/.php (Status: 403) [Size: 278]
=====
2023/05/05 19:24:29 Finished
=====
(jetsunburst@LAP-GIGU)~[~/Infosec/Lab1]
$
```

3.3 Comparison

Both the implementations, one with our custom python script and the other with Gobuster provided almost similar results in directory listing as well as found the similar files.