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

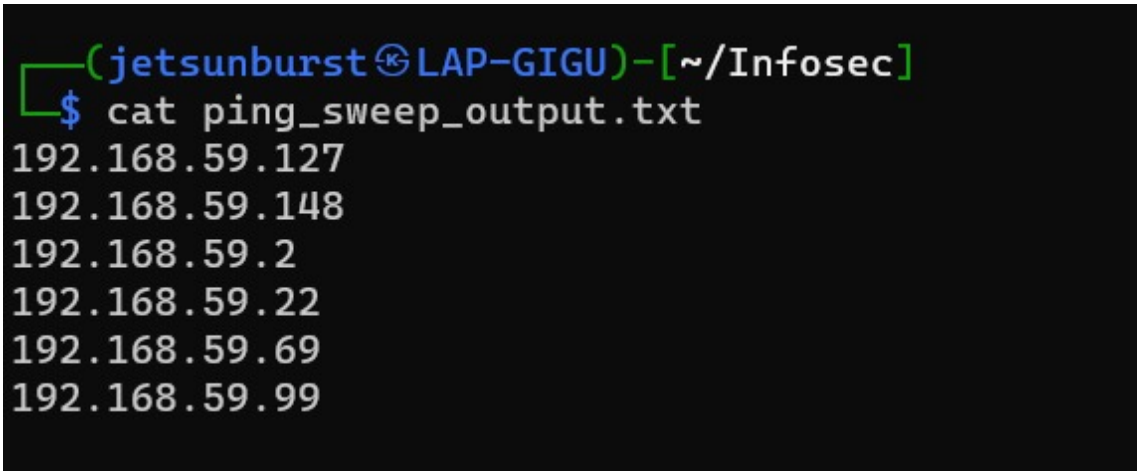
2.1 Bash script for Host Discovery

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

```
#!/bin/bash

check_host_alive_ping()
{
  ping -c 1 -W 2 192.168.59.$i > /dev/null
  [ $? -eq 0 ] && echo "192.168.59.$i"
}

check_host_alive_nmap(){
  fping -u -t 100 192.168.59.$i > /dev/null
  [ $? -eq 0 ] && echo "192.168.59.$i"

}

ips=($(for i in {1..254}; do (check_host_alive_ping 192.168.59.$i); done))

ips+=($(for i in {1..254}; do (check_host_alive_nmap 192.168.59.$i); done))


sorted_unique_ips=($(echo "${ips[@]}" | tr ' ' '\n'| sort -u | tr '\n' ' '))

check_host_port(){
 echo "nc -nvz $1"
 nc   nvz   $1 1  100   > $1.txt 2>&1
 cat $1.txt
 rm   rf   \$1.txt
}
```

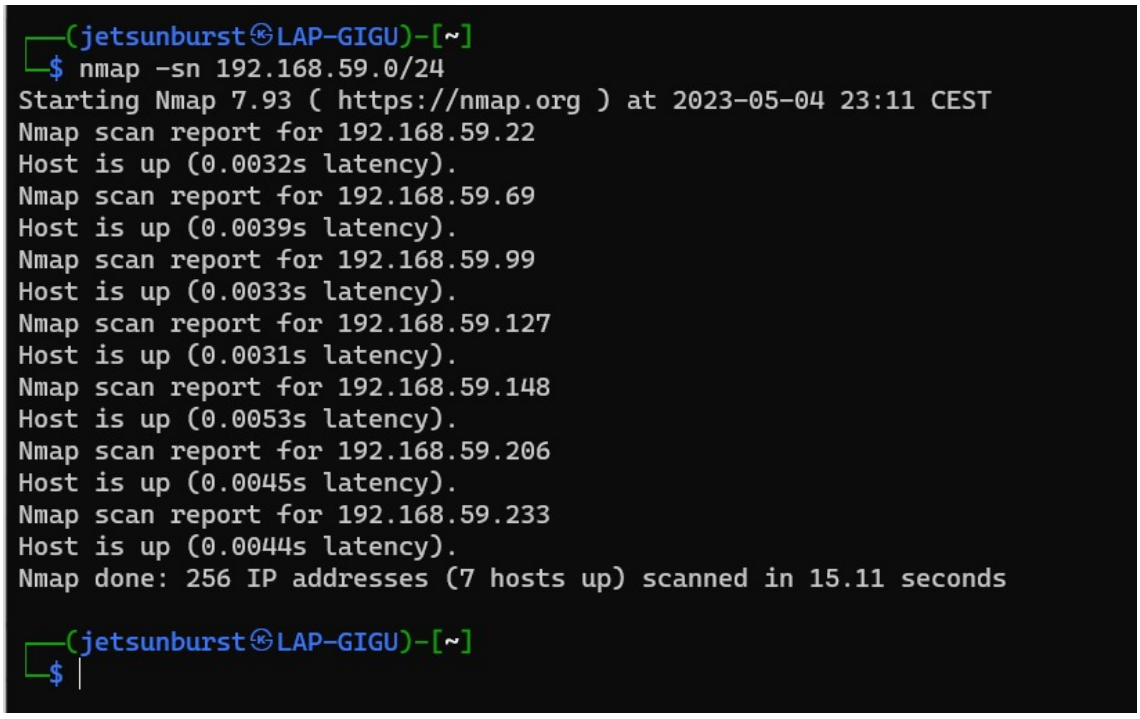
```
28
29 for i in "${sorted_unique_ips[@]}"; do ( echo "$i" >> ping_sweep_output.txt); done
```

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



2.2 Subnet scan using Nmap

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



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:

```
(jetsunburstLAP-GIGU)-[~]
$ sudo nmap -p 1-65535 -sV -O 192.168.59.0/24
[sudo] password for jetsunburst:
Sorry, try again.
[sudo] password for jetsunburst:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 18:55 CEST
Nmap scan report for 192.168.59.2
Host is up (0.0056s latency).
All 65535 scanned ports on 192.168.59.2 are in ignored states.
Not shown: 65535 filtered tcp ports (proto-unreach)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

Nmap scan report for 192.168.59.22
Host is up (0.0040s latency).
All 65535 scanned ports on 192.168.59.22 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

Nmap scan report for 192.168.59.69
Host is up (0.0041s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
    submit/ ).
TCP/IP fingerprint:
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
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M551ST11NW7%O2=M551ST11NW7%O3=M551NNT11NW7%O4=M551ST11NW7%O5=M551ST11
OS:NW7%O6=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
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=
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=
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
OS:UCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

Nmap scan report for 192.168.59.99
Host is up (0.0041s latency).
Not shown: 65533 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
    submit/ ).
TCP/IP fingerprint:
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
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=2%ISR=110%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M551ST11NW7%O2=M551ST11NW7%O3=M551NNT11NW7%O4=M551ST11NW7%O5=M551ST1
OS:1NW7%O6=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
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
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
```

```
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%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

Nmap scan report for 192.168.59.127
Host is up (0.0041s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
    submit/ ).
TCP/IP fingerprint:
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
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS(O
OS:1=M551ST11NW7%O2=M551ST11NW7%O3=M551NNT11NW7%O4=M551ST11NW7%O5=M551ST11N
OS:W7%O6=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R
OS:=Y%DF=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
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
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
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
OS:CK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.59.148
Host is up (0.0041s latency).
Not shown: 64510 closed tcp ports (reset), 980 filtered tcp ports (no-response), 42 filtered
     tcp ports (host-prohibited)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.8 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.38 ((Fedora) OpenSSL/1.1.1 mod_perl/2.0.10 Perl/v5
    .28.0)
3306/tcp open  mysql   MariaDB (unauthorized)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
    submit/ ).
TCP/IP fingerprint:
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
OS:567%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=2%ISR=10E%TI=Z%CI=Z%II=I%TS=A)S
OS:EQ(SP=102%GCD=1%ISR=10E%TI=Z%CI=Z%TS=A)OPS(O1=M551ST11NW7%O2=M551ST11NW7
OS:%O3=M551NNT11NW7%O4=M551ST11NW7%O5=M551ST11NW7%O6=M551ST11)WIN(W1=7120%W
OS:2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M551NN
OS:SNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y
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
OS:%O=%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
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
OS:%CD=S)

Network Distance: 2 hops

Nmap scan report for 192.168.59.206
Host is up (0.0046s latency).
All 65535 scanned ports on 192.168.59.206 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

Nmap scan report for 192.168.59.233
Host is up (0.0041s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/
    submit/ ).
TCP/IP fingerprint:
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
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%TS=A)OPS(O1=M5
OS:51ST11NW7%O2=M551ST11NW7%O3=M551NNT11NW7%O4=M551ST11NW7%O5=M551ST11NW7%O
OS:6=M551ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%D
OS:F=Y%T=40%W=FAF0%O=M551NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
```

```
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=
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=%
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
OS:%RUD=G)IE(R=N)

Network Distance: 2 hops
Service Info: OS: Unix

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
    submit/ .
Nmap done: 256 IP addresses (8 hosts up) scanned in 121.57 seconds
(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.

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
import requests

# Define the url and wordlist file path

url = 'http://192.168.59.69/'
wordlist_file = 'Lab1/web_directory_wordlist.txt'

# Define the file extensions to search for

file_extensions = ['.html', '.php', '.txt']

# Read the wordlist file into a list

with open(wordlist_file, 'r') as f:
    wordlist = [line.strip() for line in f]


# Function to check if a directory exists
found_directories = []
def check_directory(directory):
    response = requests.get(url + directory)
    if response.status_code == 200:
        found_directories.append(directory)
        return True
    else:
```

```
        return False

# Loop through each directory in the wordlist and check if it exists

for directory in wordlist:
    if check_directory(directory):
        print ('Directory found: ' + directory)

for word in wordlist:
    for extension in file_extensions:
        for directory in found_directories:
            file_url = url + directory + "/" + word + extension
            response = requests.get(file_url)
            if response.status_code == 200:
                print("File found: " + file_url)
```

This is the result that we got through our scipt:

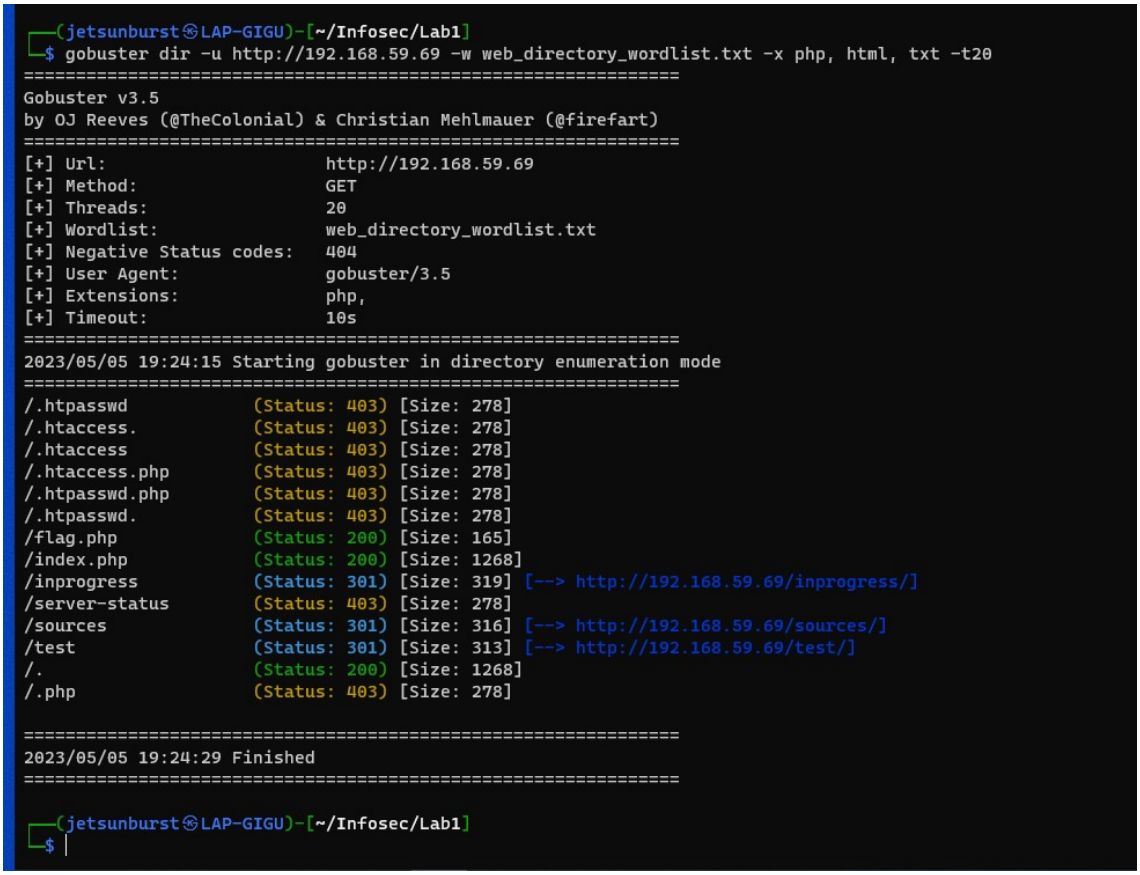
```
┌──(kali㉿kali)-[~/Desktop/ISAO Ex1]
└─$ python directory_scan.py
Directory found: inprogress
Directory found: sources
Directory found: test
Directory found:

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

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

The results are as follows:



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.