ELEC 567 Project Part 1

Harsimran Kaur V00879358

Maninder Singh V00879900

Mansi Lamba V00876307

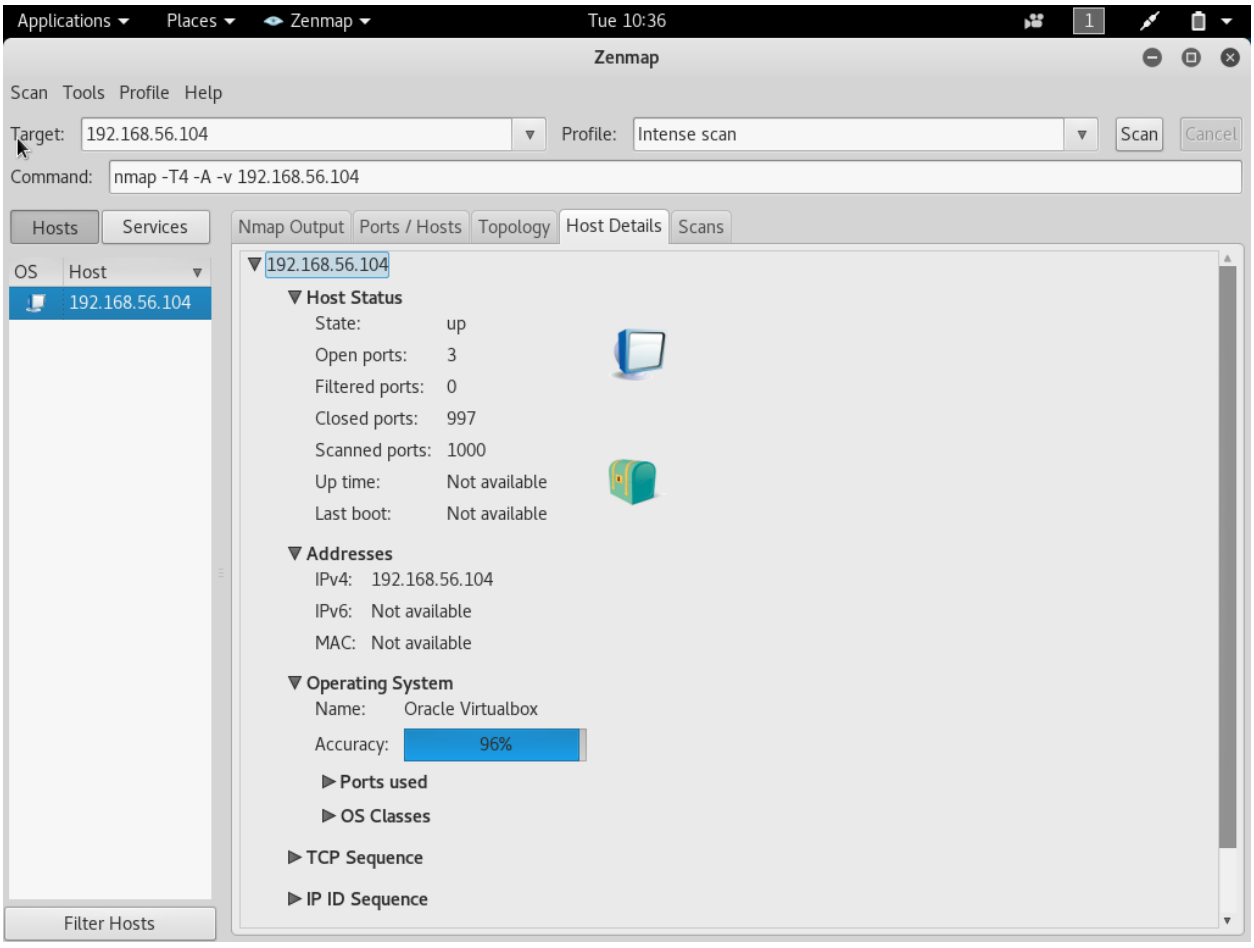
Phase 1: Information gathering (7%)

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%)

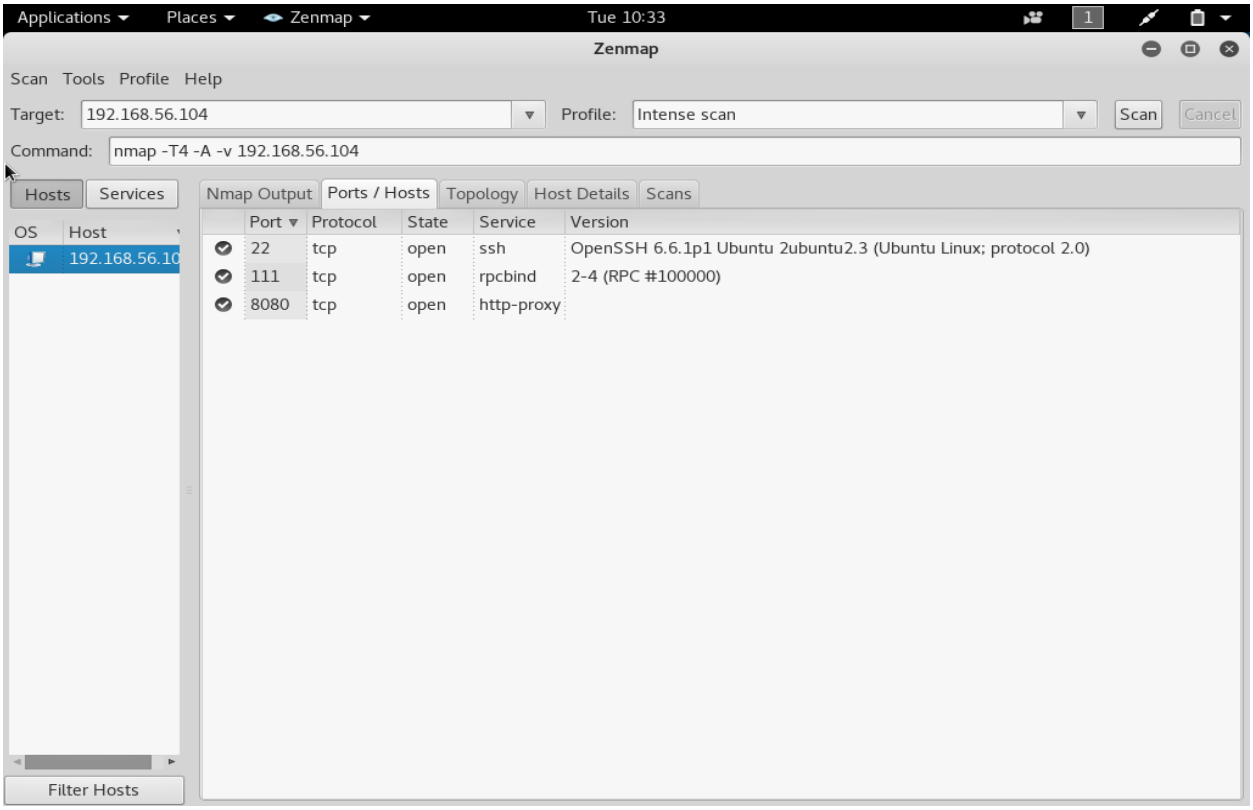
Answer:

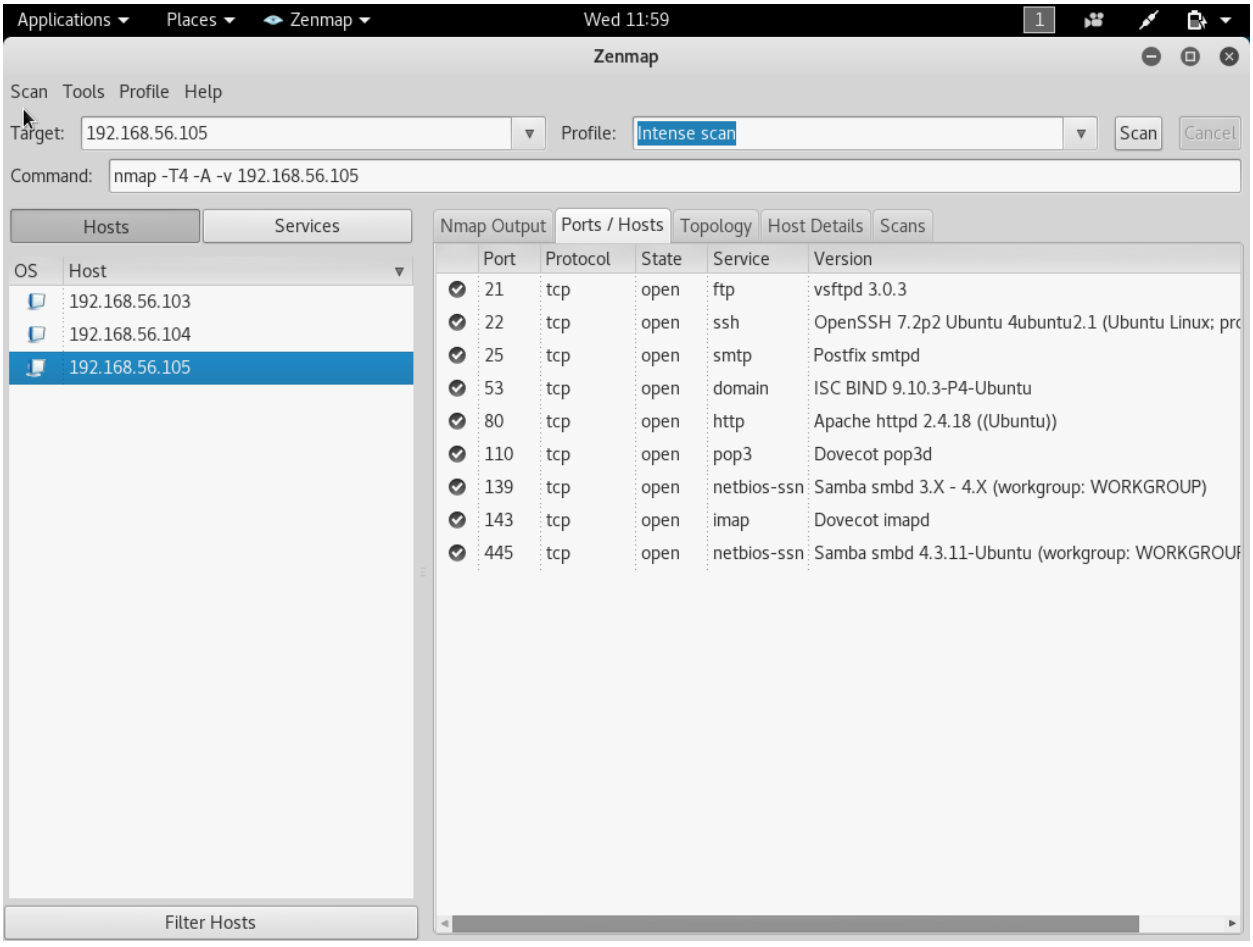
We have used ZENMAP to scan the network as it is graphical interface of NMAP and easy to use.

Step 1: The screen shot below is for 192.168.56.104

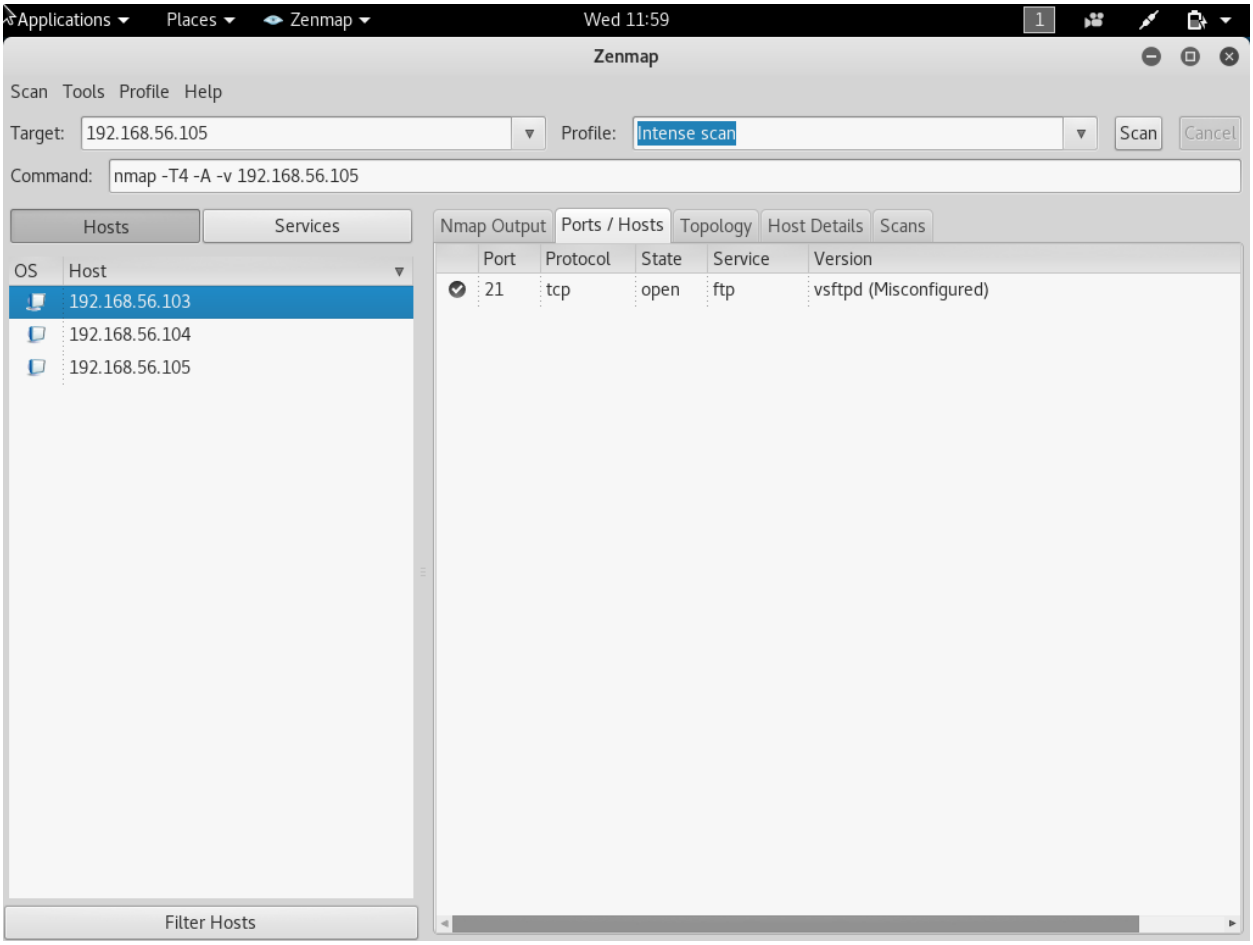


This screen shot tells us that there are 3 ports which are open. Next step is to find those ports. We can see the open ports by opening Ports/Hosts tab. As shown in the screen shots below for the hosts 192.168.56.103-105





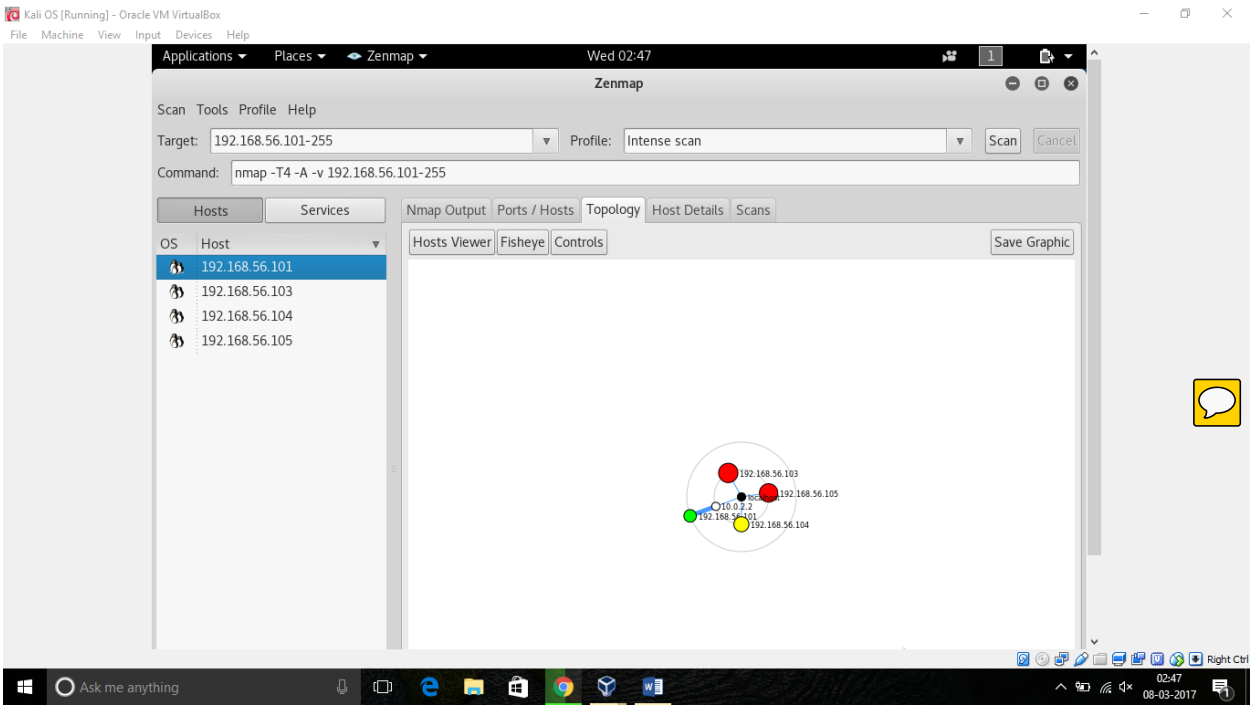
The screen shot below shows the open ports for 19.168.56.103



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

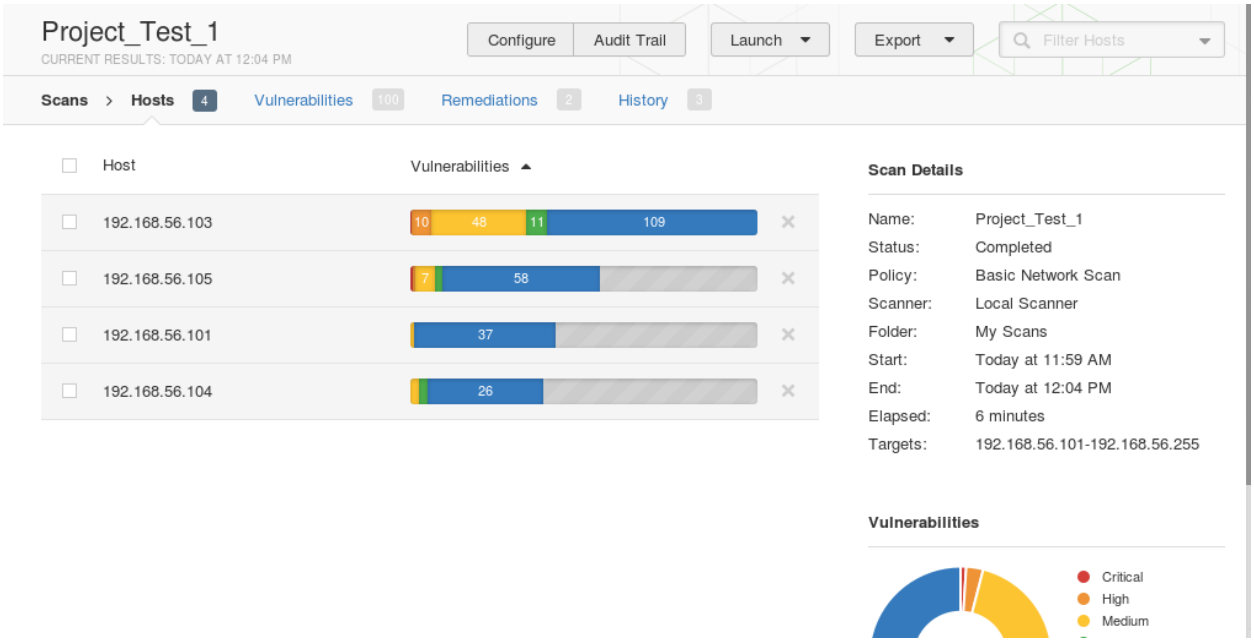
HOST NAME	IP Address	OS Type/ Version	Running Service and port number
ACME_UB14	192.168.56.104	Linux 3.2-4.4	SSH(22), RPCBIND(111), HTTP-PROXY(8080)
	192.168.56.101	Windows7	MSRPC (135), NETBIOS-SSN (139), MICROSOFT-DS (445).
UB16	192.168.56.105	Linux 3.2- 4.4	FTP(21), SSH(22), SMTP(25), DOMAIN(53),HTTP(80),POP3(110),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

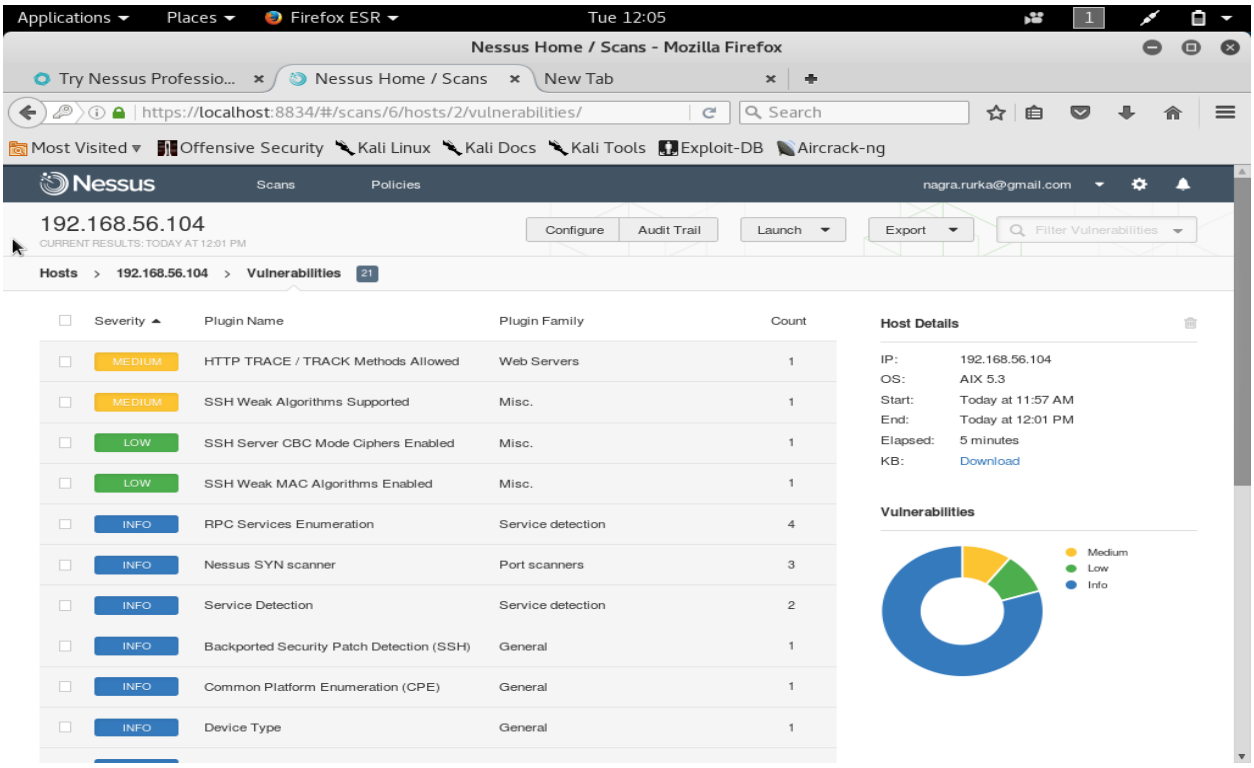


1.2 Identify vulnerable services; briefly explain why you think these services are vulnerable. (3%)

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:

a) Remote attackers can do denial of service attack.
b) The attackers can bypass security restrictions.
c) 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

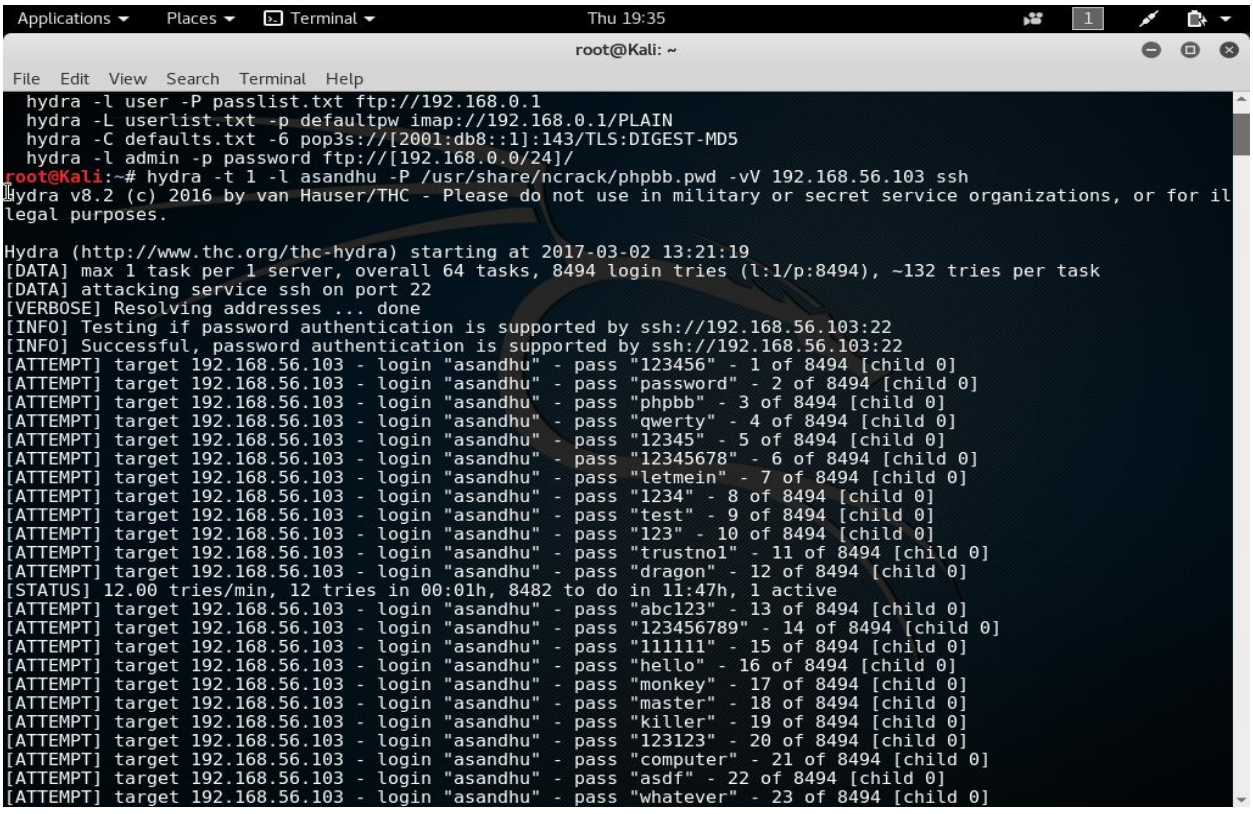
a) Remote attackers can use this port for doing DOS attacks.
b) Allows attacker to bypass security restrictions.

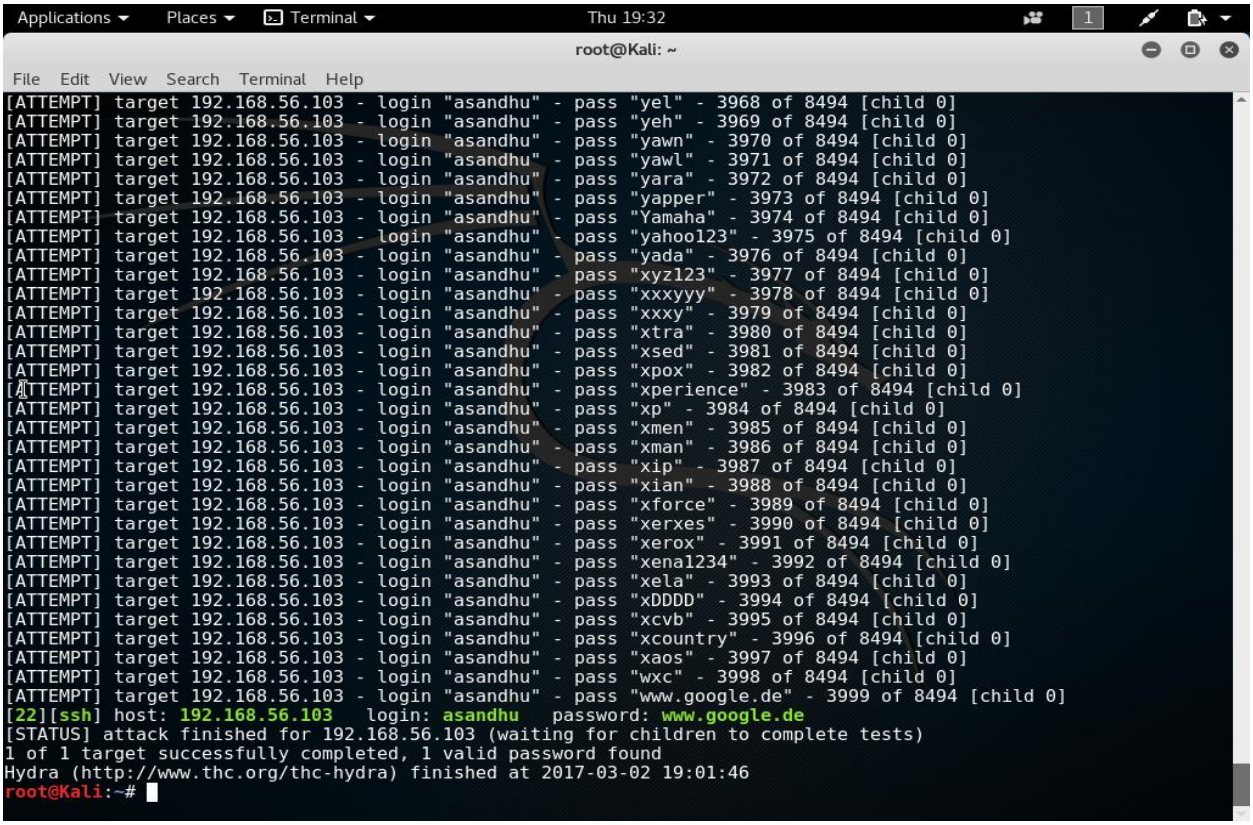
Phase 2: Exploitation (18%)

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%)

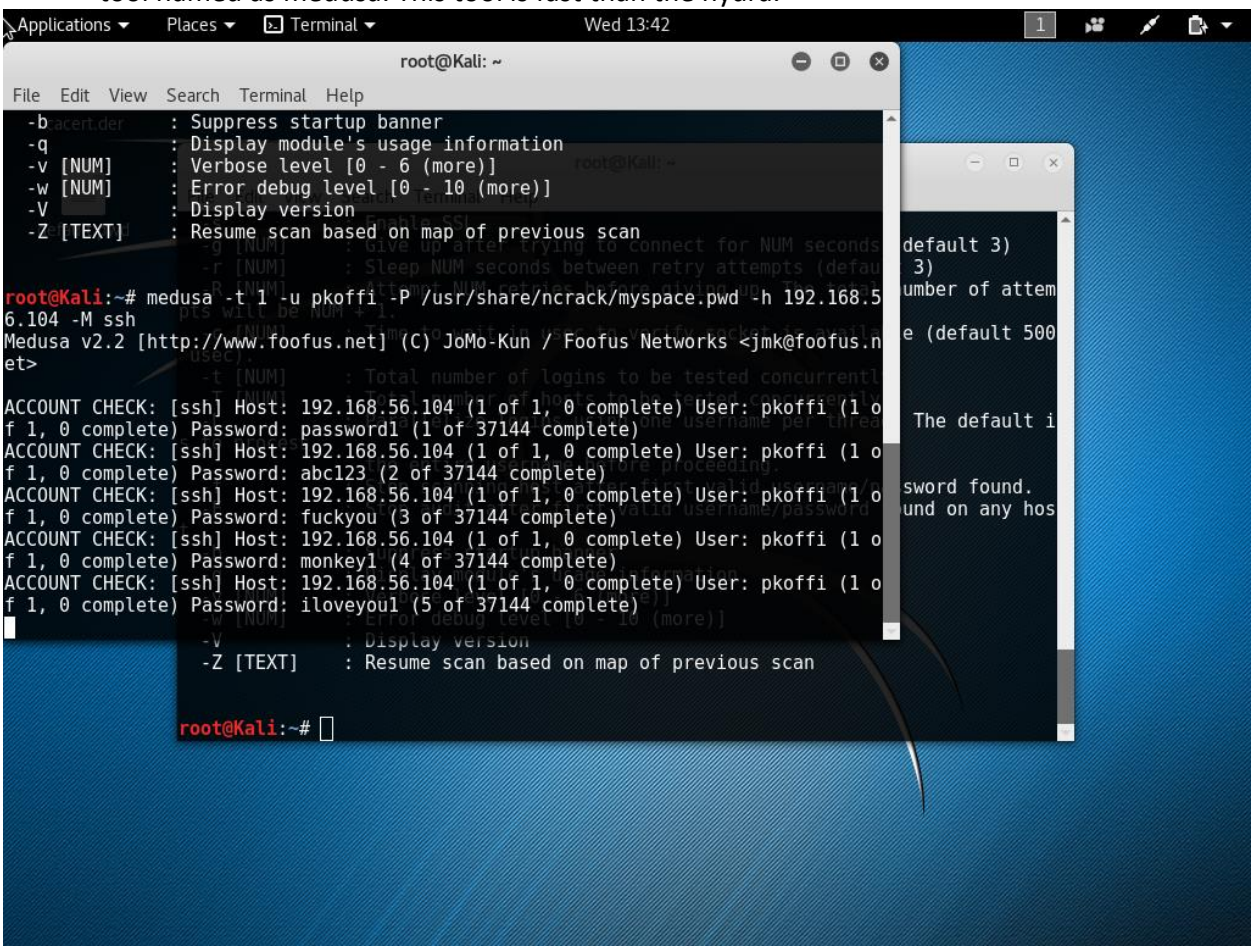
Answer: When we have used Nessus as a scanner then we have found out that SSH is vulnerable. So we use HYDRA as an online password attack tool to found the password of different users. But succeeded only in three. As explained in the screen shots below.

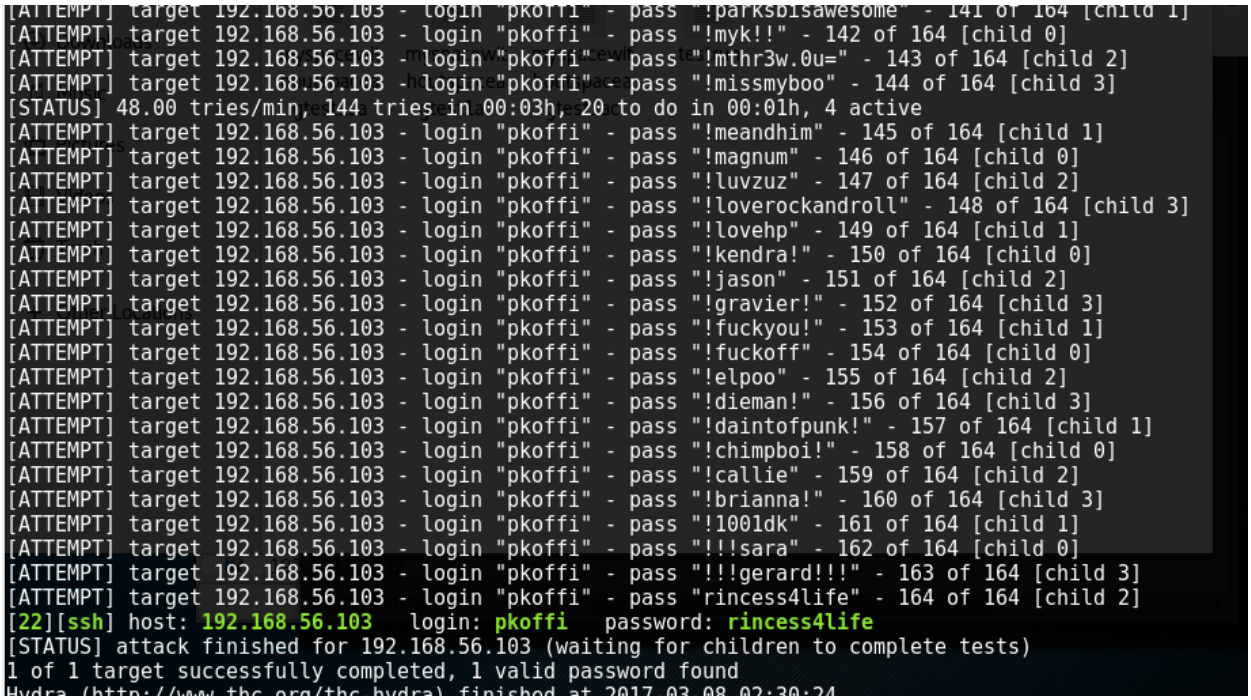
a) We targeted the username asandhu and we found the password we target him as he is Director of software development we need this as we need mobile code for GIT.





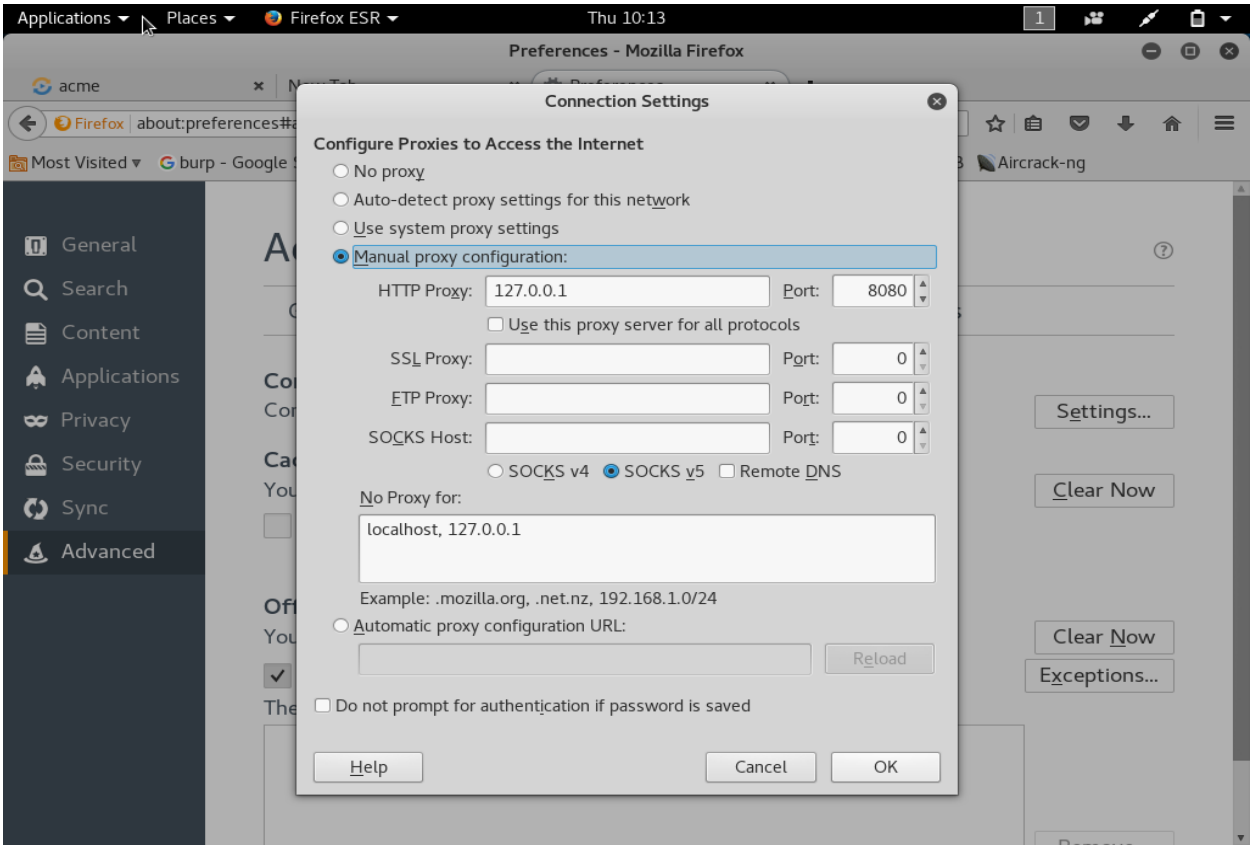
b) Then we have targeted the pkoffi as he is QA director using another online dictionary attack tool named as medusa. This tool is fast than the hydra.



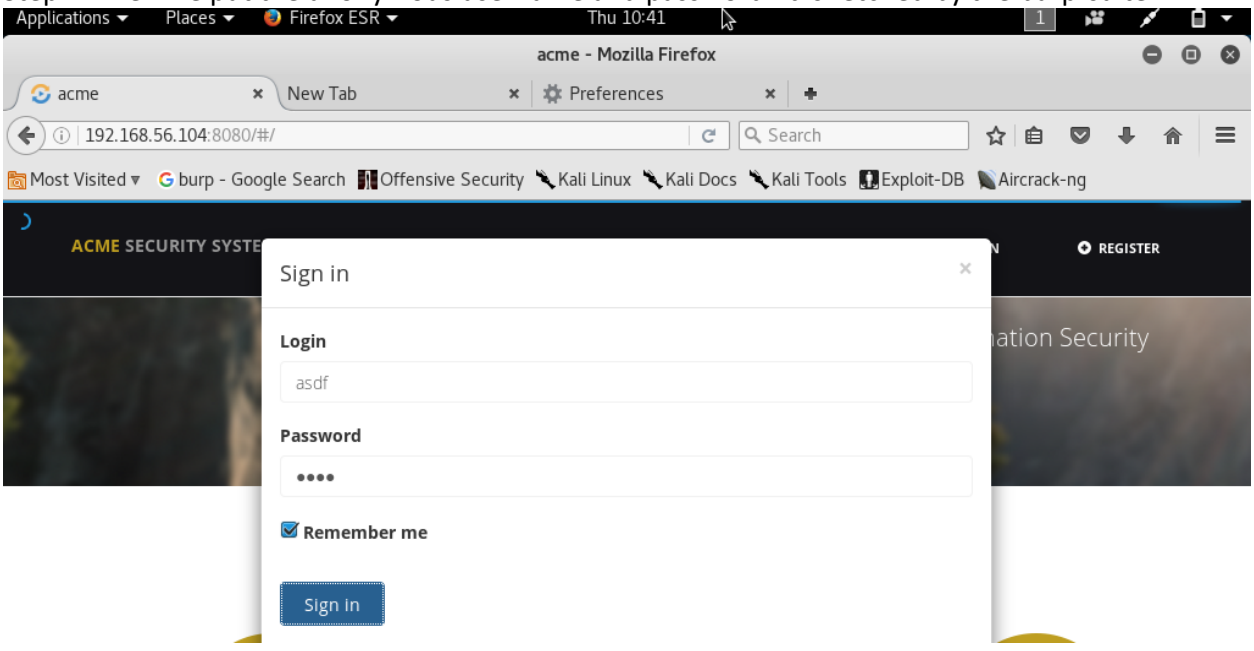


c) Then to find the password for Tom Hayes who is VP finance to get the financial history we have used Burp-suite. For running this scan I had downloaded the file default.pwd on the desktop of kali. As we need to input the whole file as password matching strings in the intruder database so that it can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

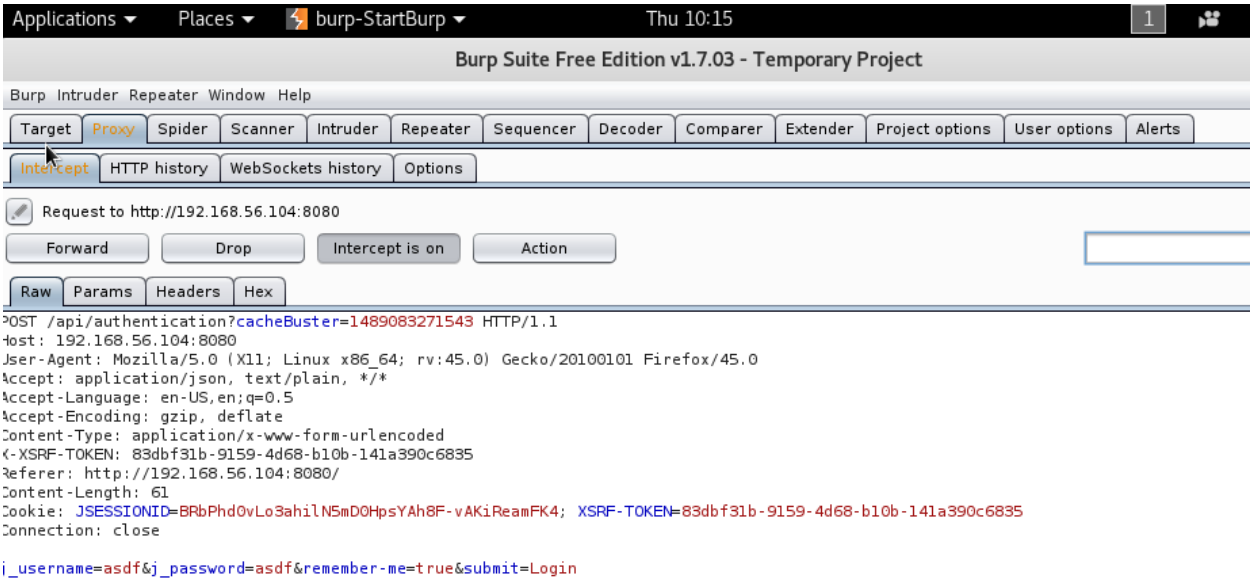
Step 1: We have to set proxy settings of Mozilla by preferences->advanced->network->settings.



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

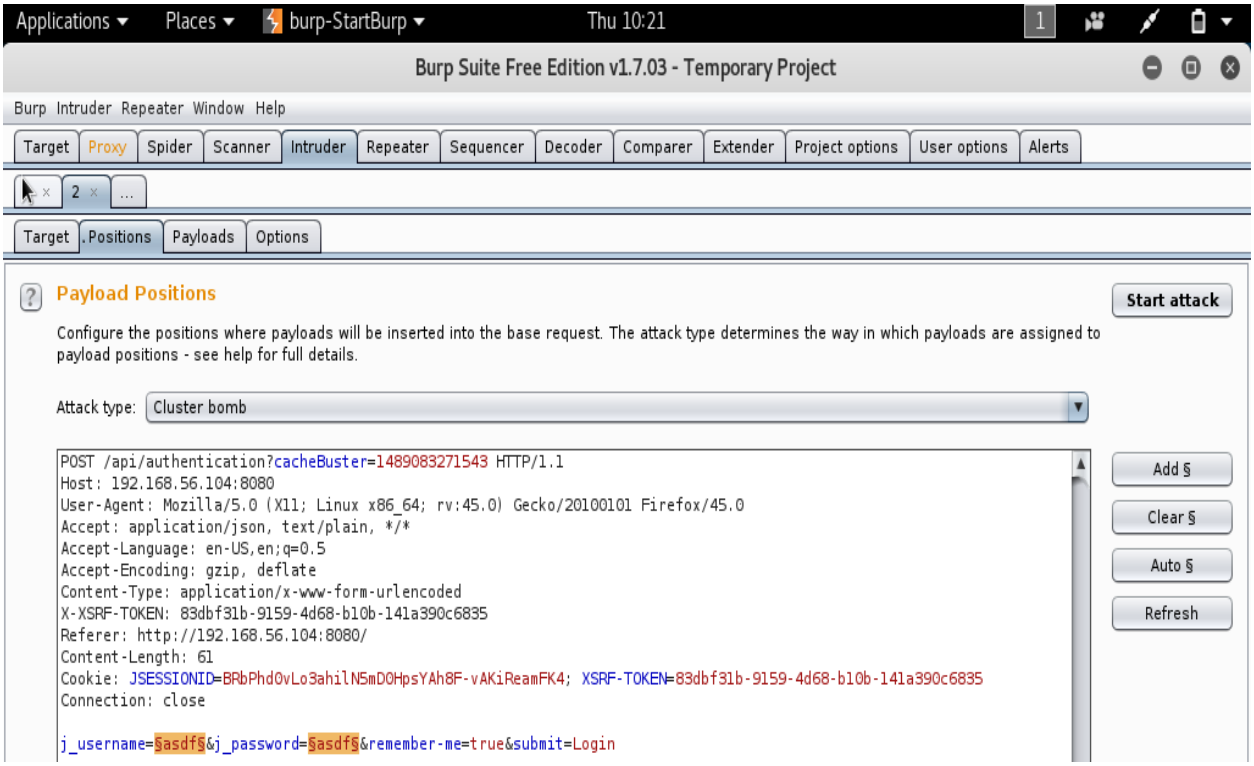


Step 4: Now we send it to intruder and then add the username and password so that it can fetch the places while we load it as payload 1 and payload 2.

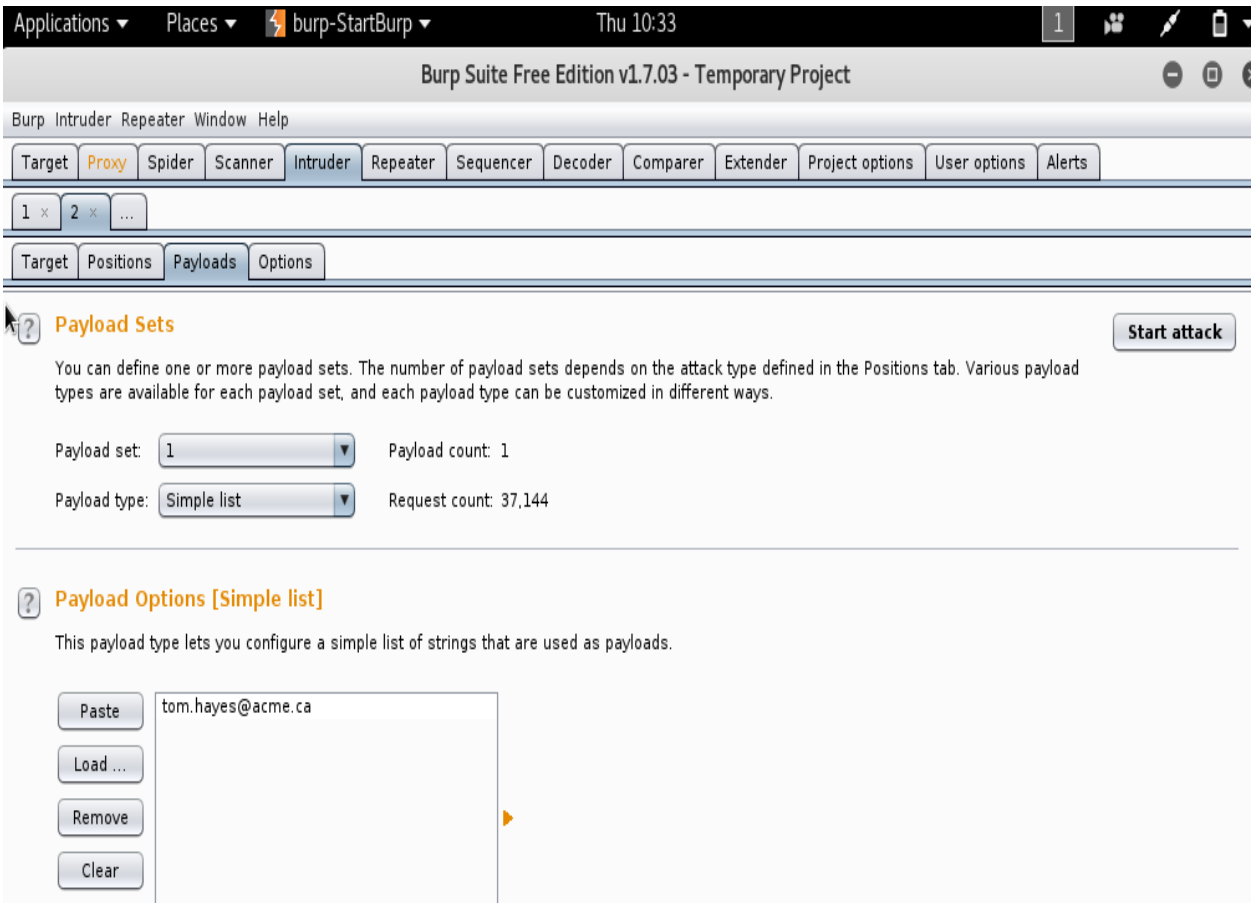
Then set the target as the IP which you want to attack.

Then,

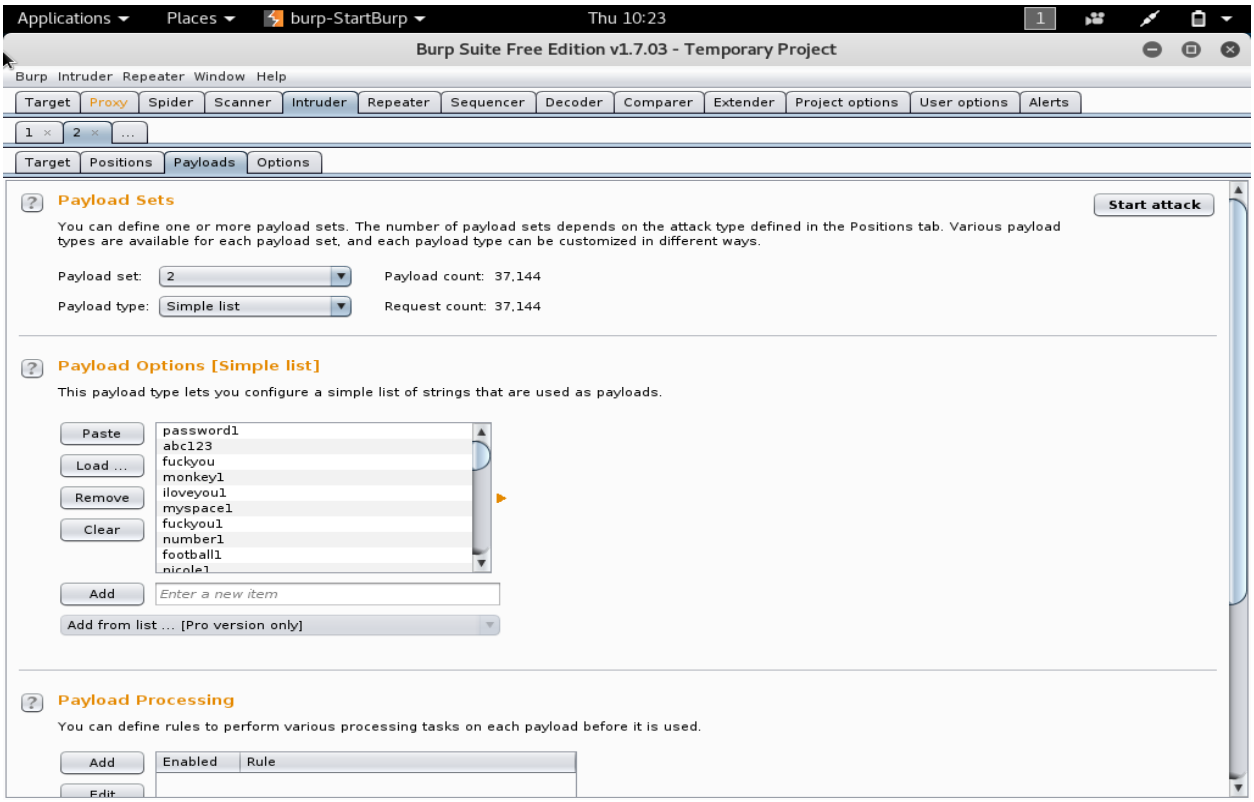
Set the attack type in positions as cluster bomb, otherwise attacker can only upload 1 payload.

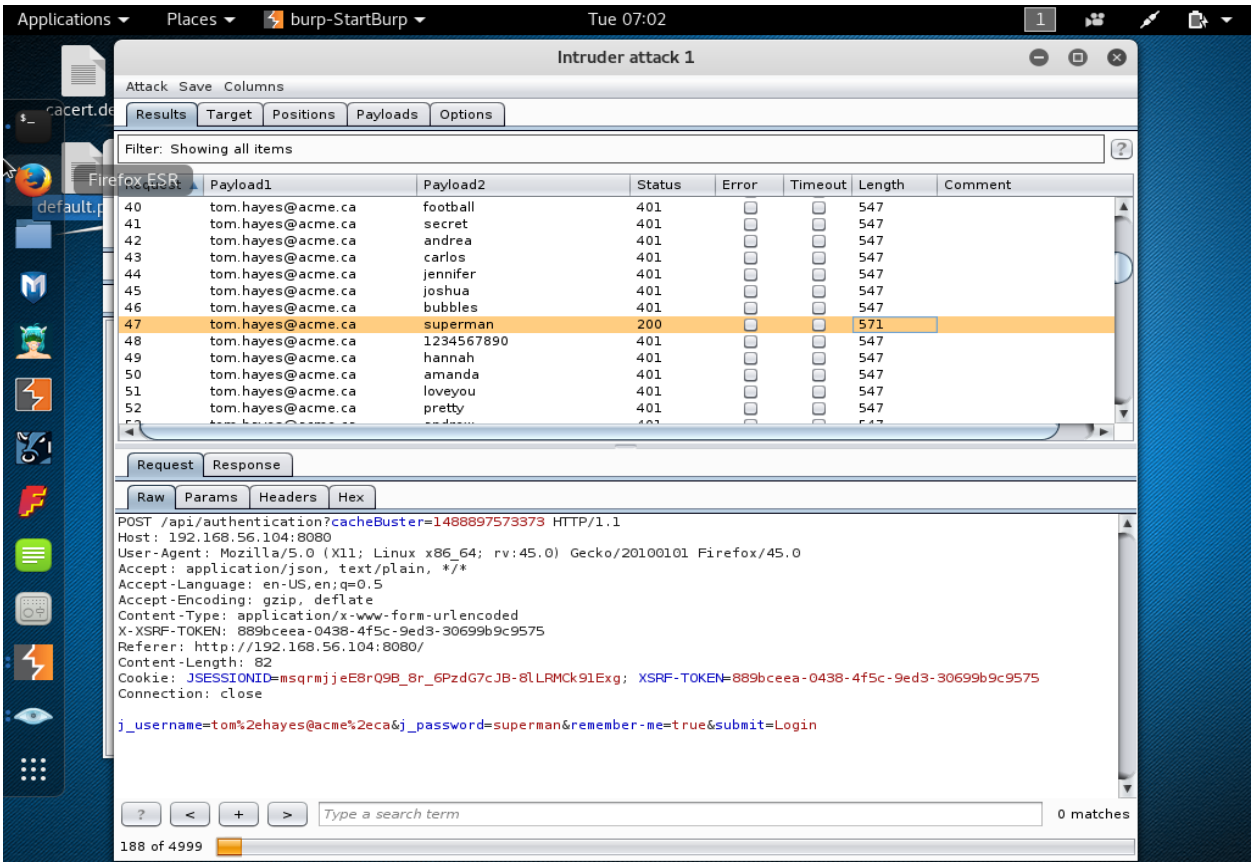


Step 5: add the username for which password has to be found.



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



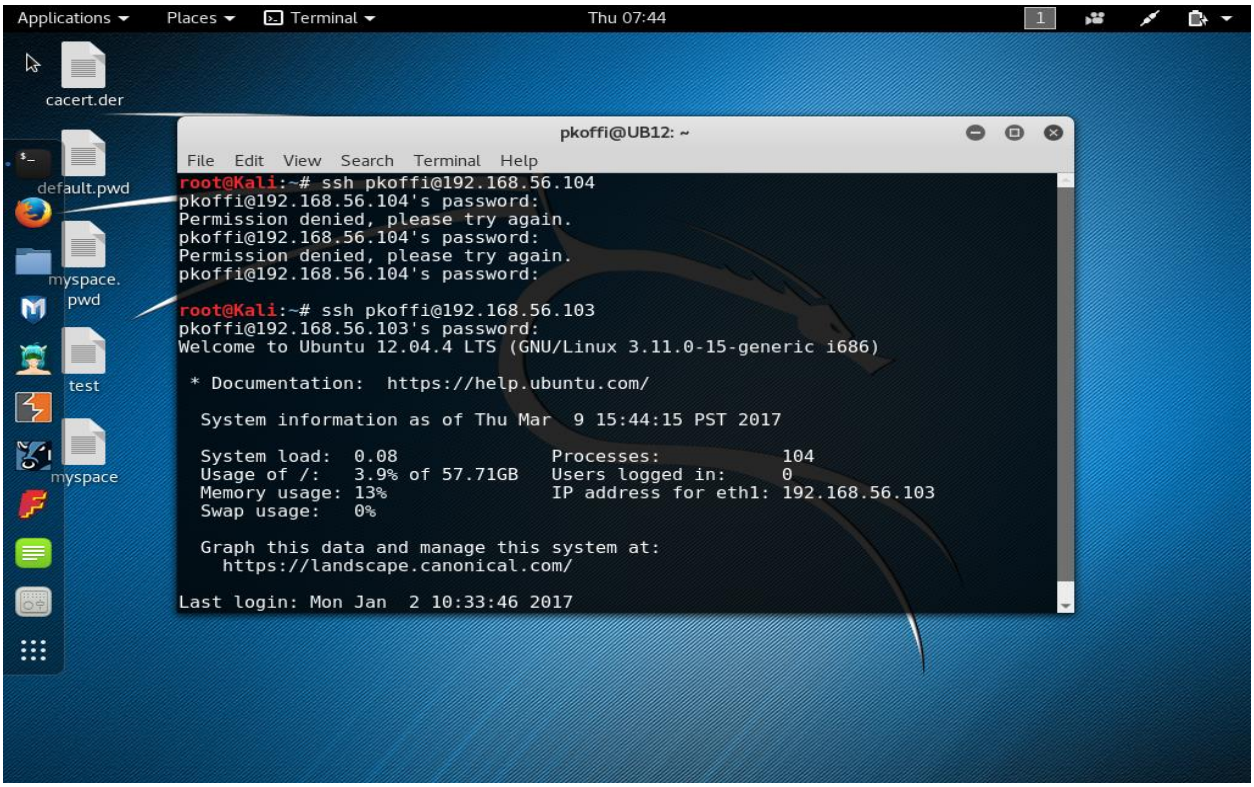


Step 7: In the above screen shot check the status code.
401- Unauthorized
200- Ok
This means if attacker carefully observes status he can easily found the correct password from the status code 200.

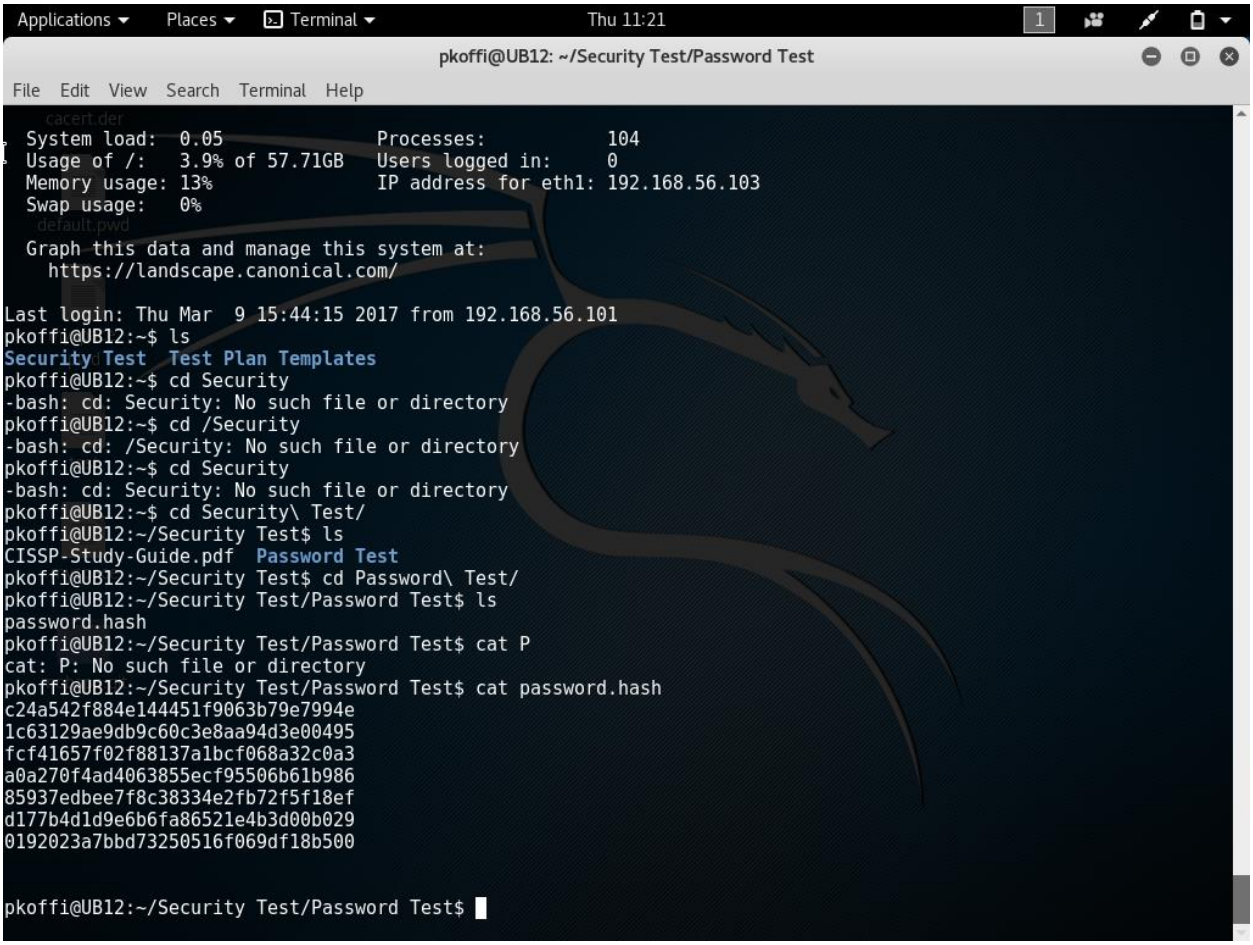
2.2 After gaining access to the private network, collect the following company confidential files (12%): (i) Employees personal records (e.g. SIN, address, bank accounts from database server) – 4%

Answer: First we had tried for logging in an ssh pkoffi@192.168.56.104. 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 and we are able to log into it.

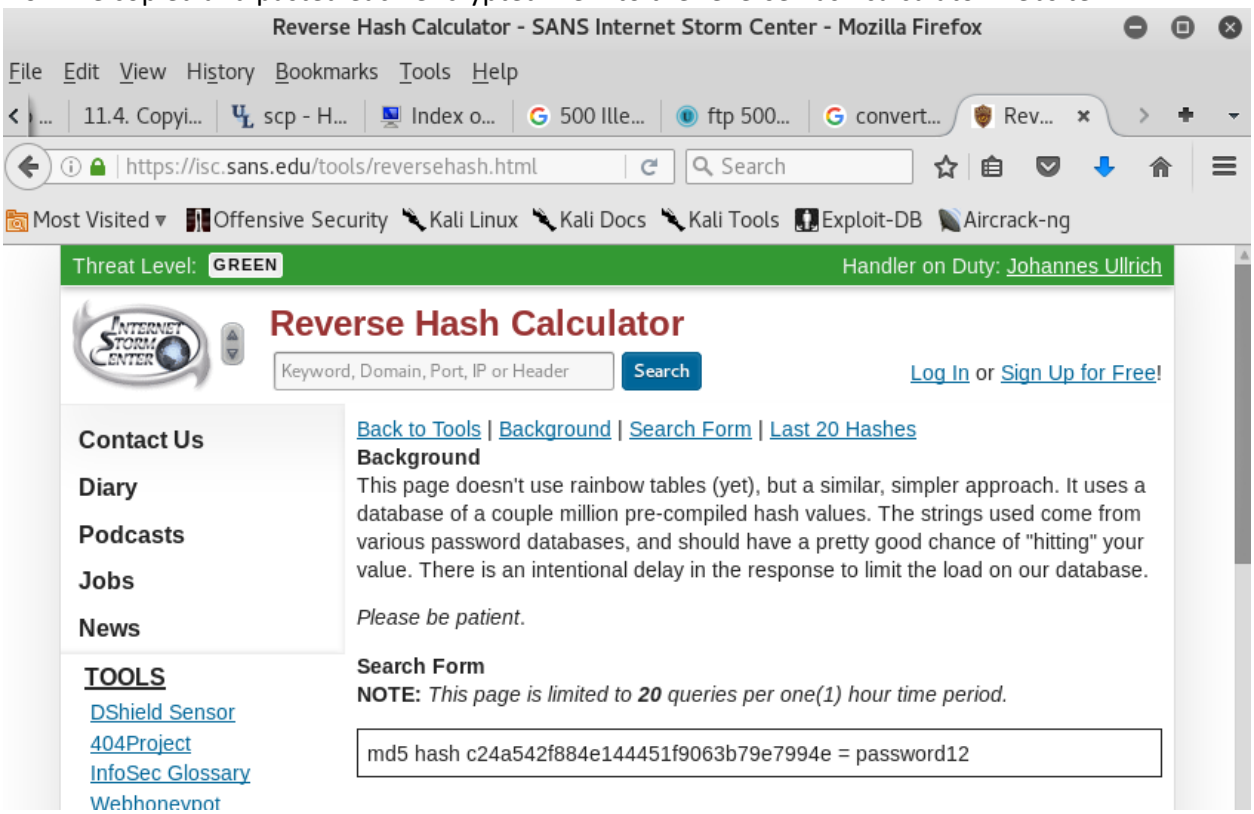
Step 1: Log into ssh pkoffi@192.168.56.103

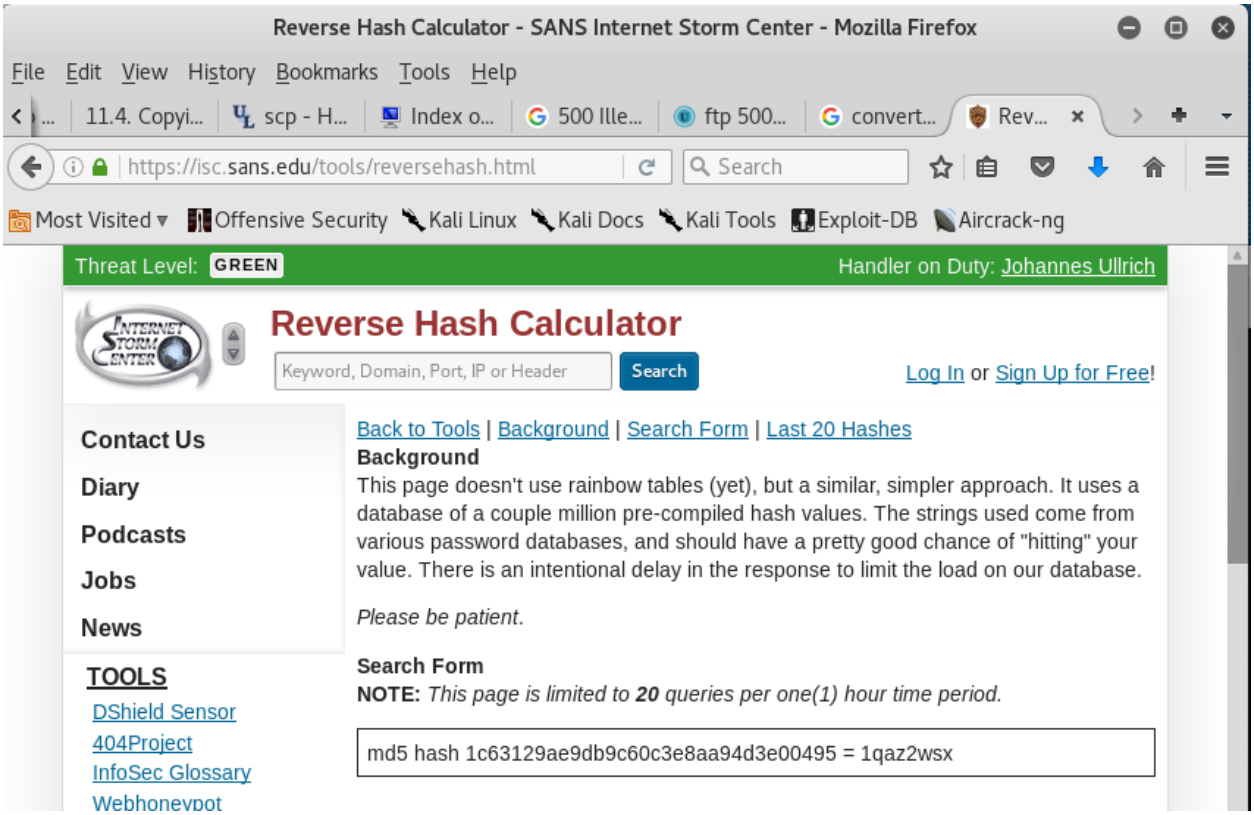


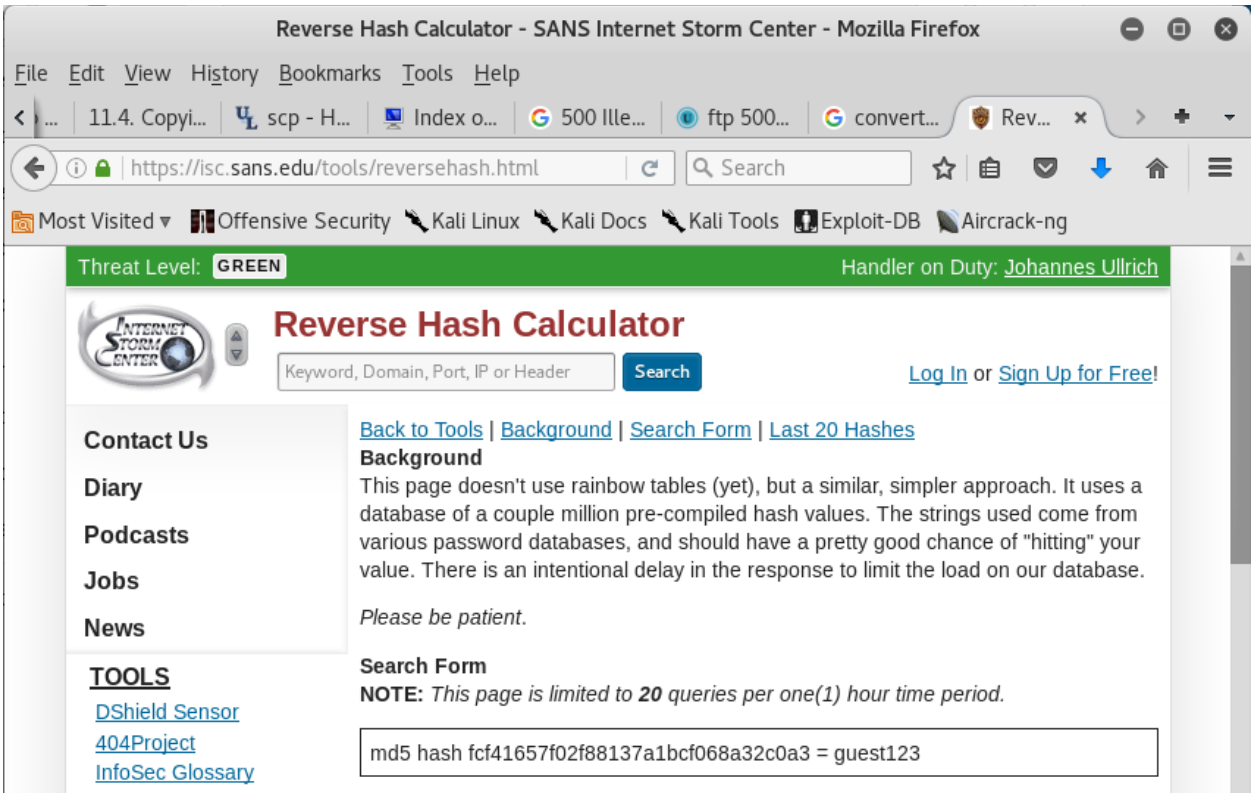
Step 2: Log into mysql –u guest –p, now we need password. So we can find the password using the following steps.
We tried using cd security and cd /security. It was not working giving us the result as bash: no such directory exists.
Then we tried cd S+tab. We got success. Then finally we get the encrypted codes as shown below.

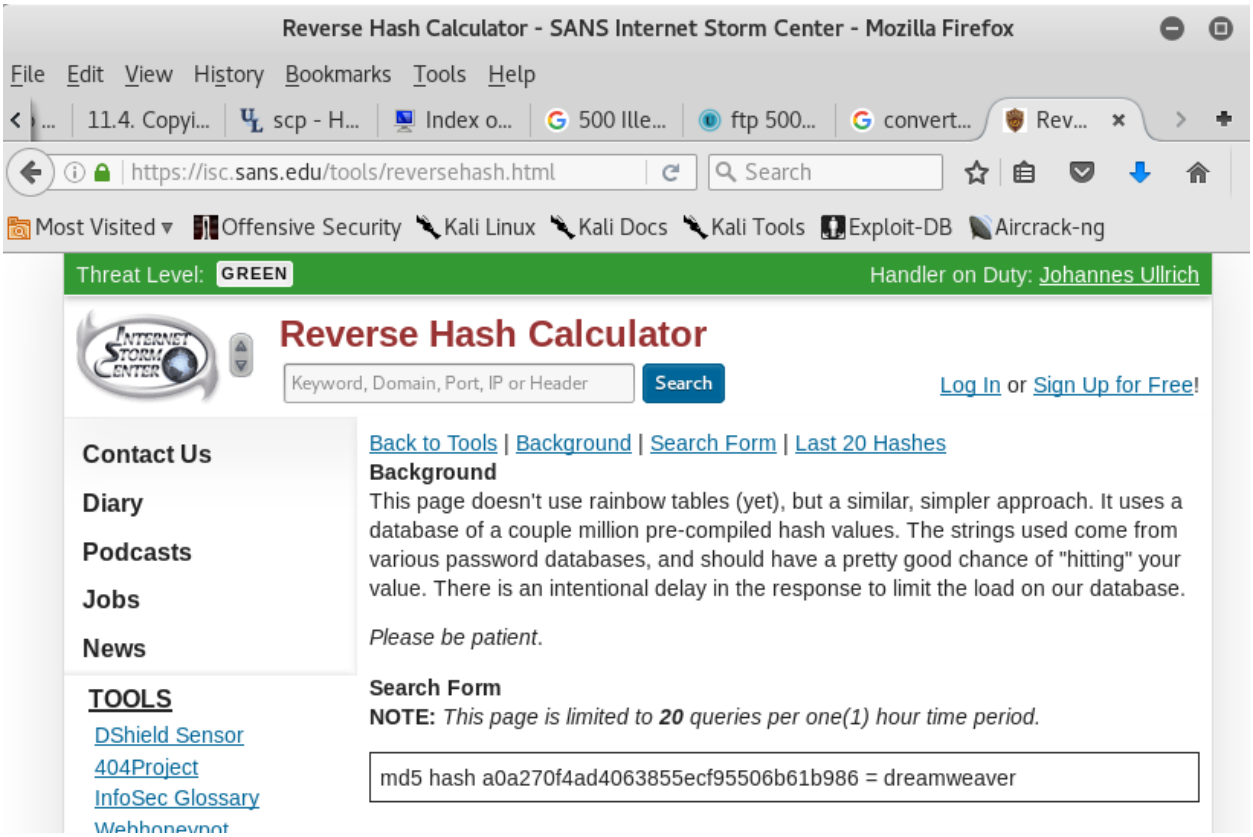


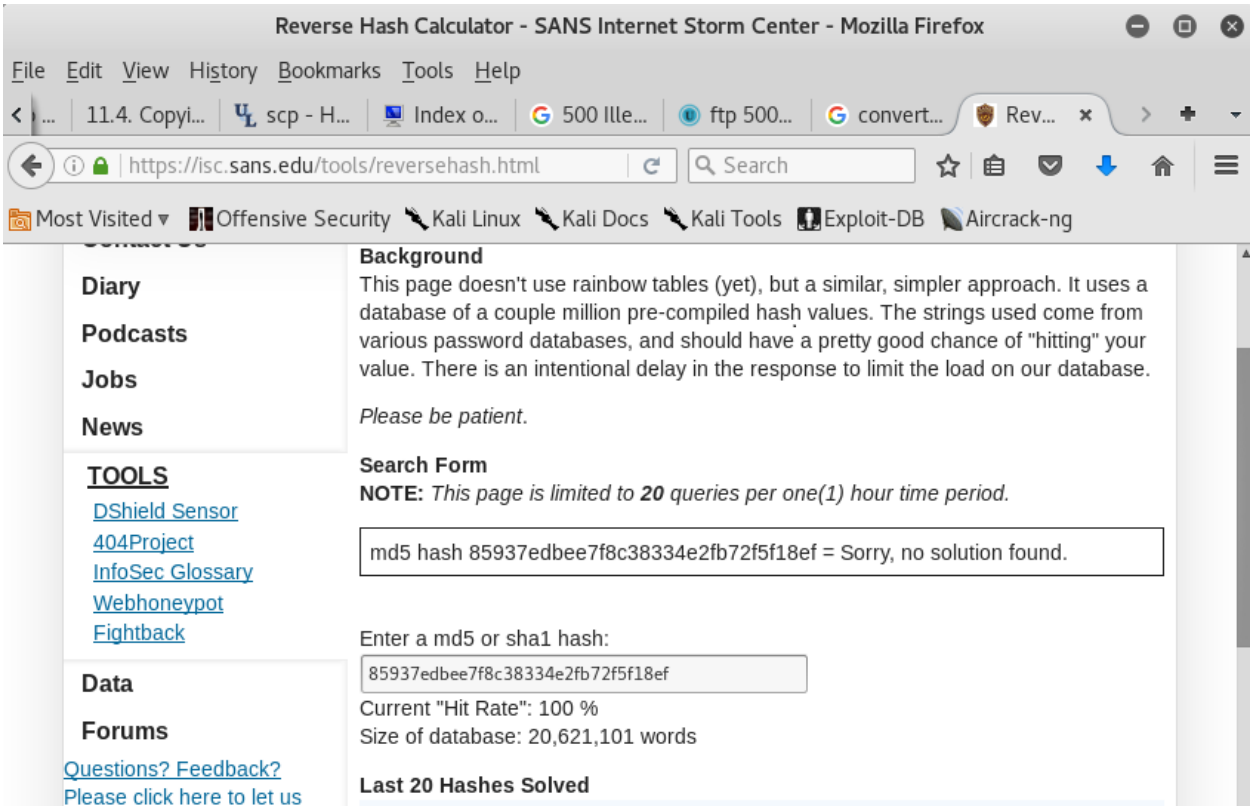
Now we copied and pasted each encrypted file into the reverse hash calculator website.



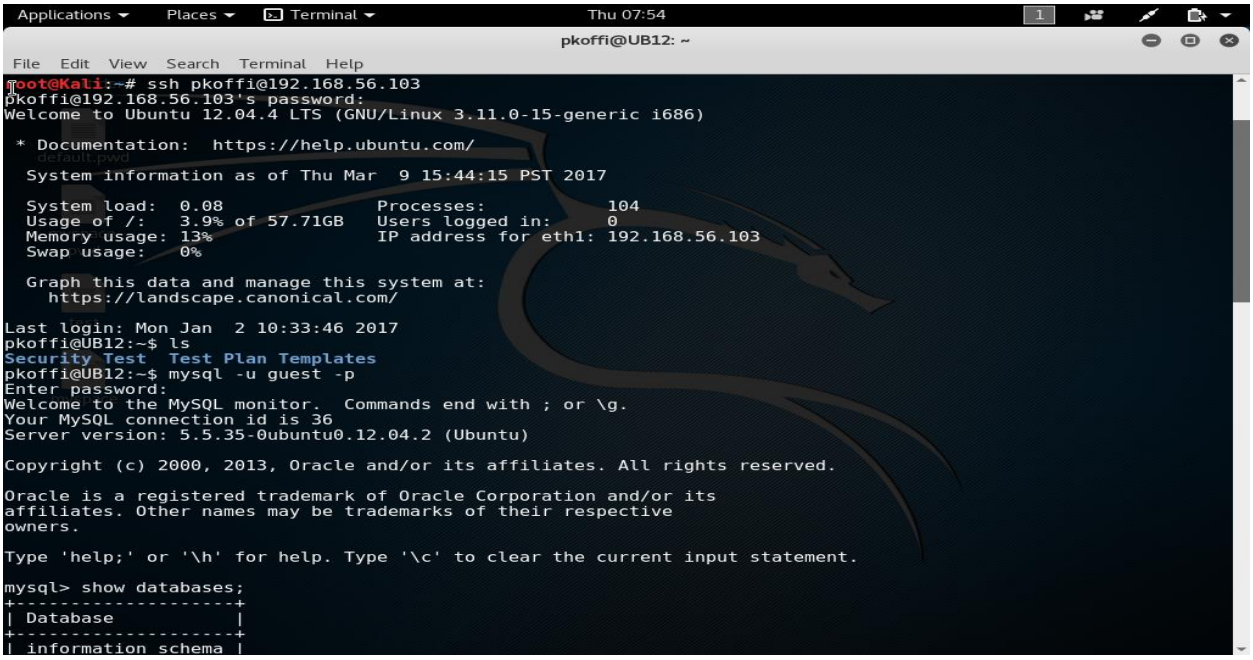

Reverse Hash Calculator - SANS Internet Storm Center - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://isc.sans.edu/tools/reversehash.html
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
Threat Level: GREEN
Handler on Duty: Johannes Ullrich
Reverse Hash Calculator
Keyword, Domain, Port, IP or Header
Search
Log In or Sign Up for Free!
Contact Us
Diary
Podcasts
Jobs
News
TOOLS
DShield Sensor
404Project
InfoSec Glossary
Webhoneypot
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
https://isc.sans.edu/tools/reversehash.html
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
Search
Log In or Sign Up for Free!
Contact Us
Diary
Podcasts
Jobs
News
TOOLS
DShield Sensor
404Project
InfoSec Glossary
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

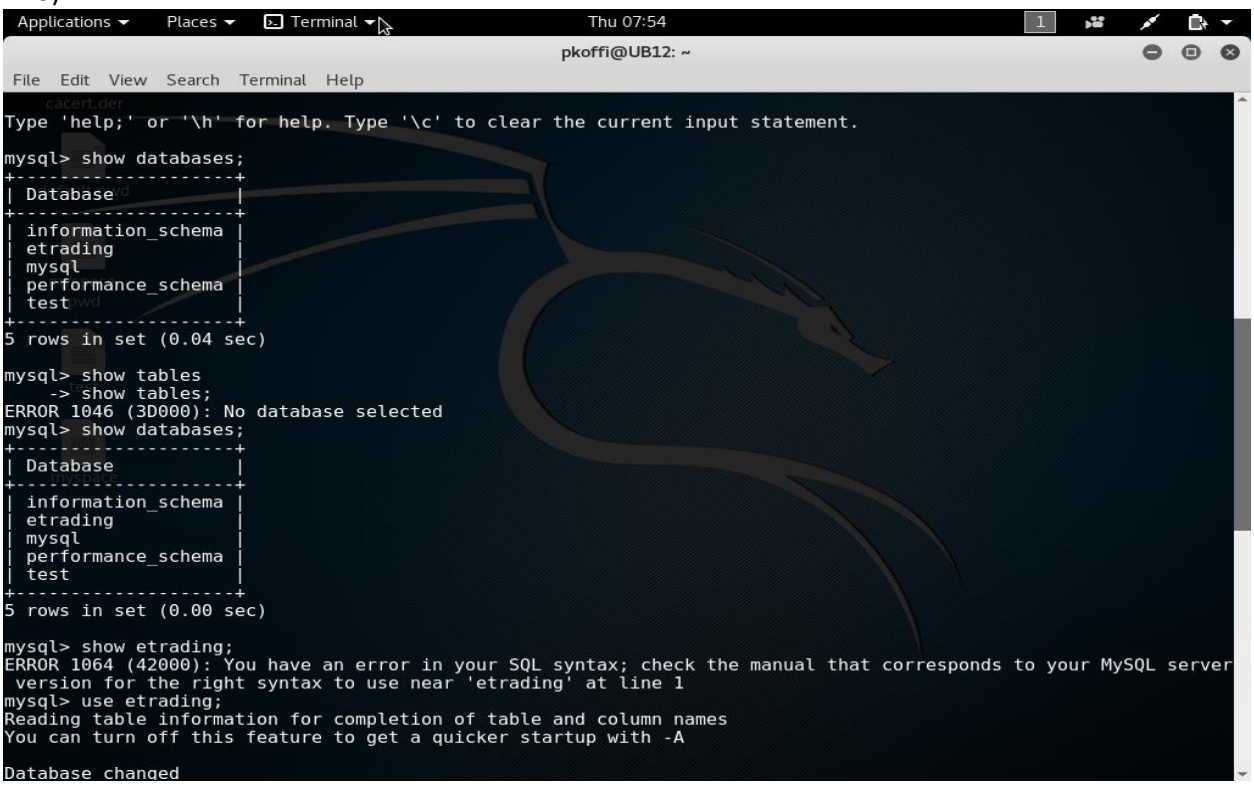




Then we tried each password while logging into the mysql database and we found the password as guest123

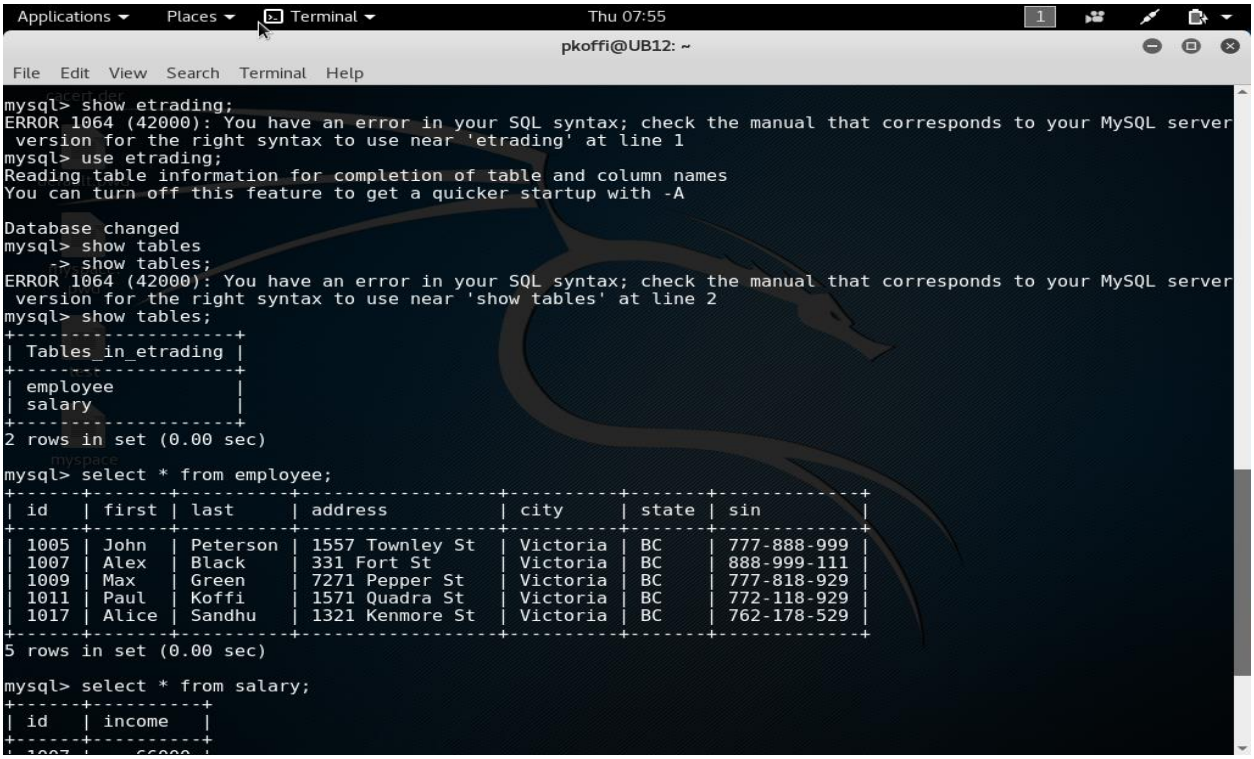


Step 3: show databases (in order to see which tables are there from which we can find the required info).



Here we tried to see etrading but received error.

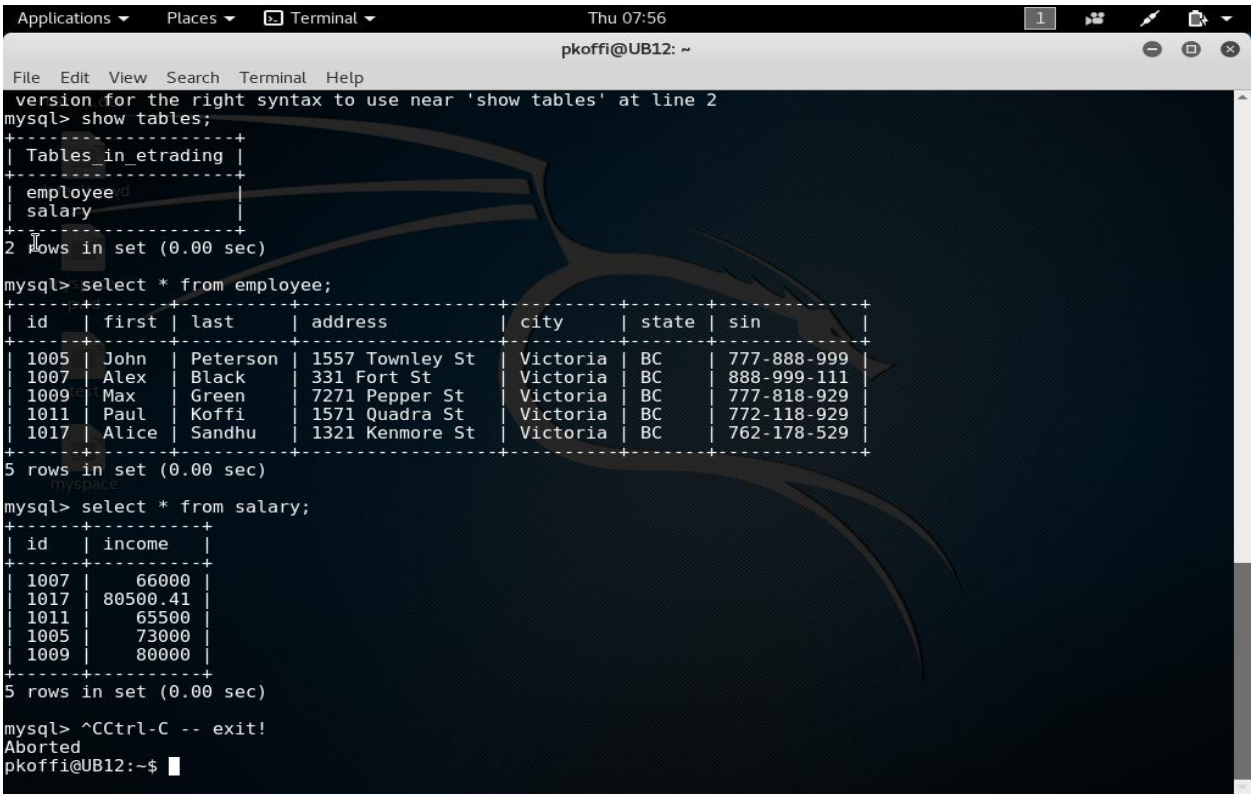
Step 4: Show tables;



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

select * from employee;

select * from salary;



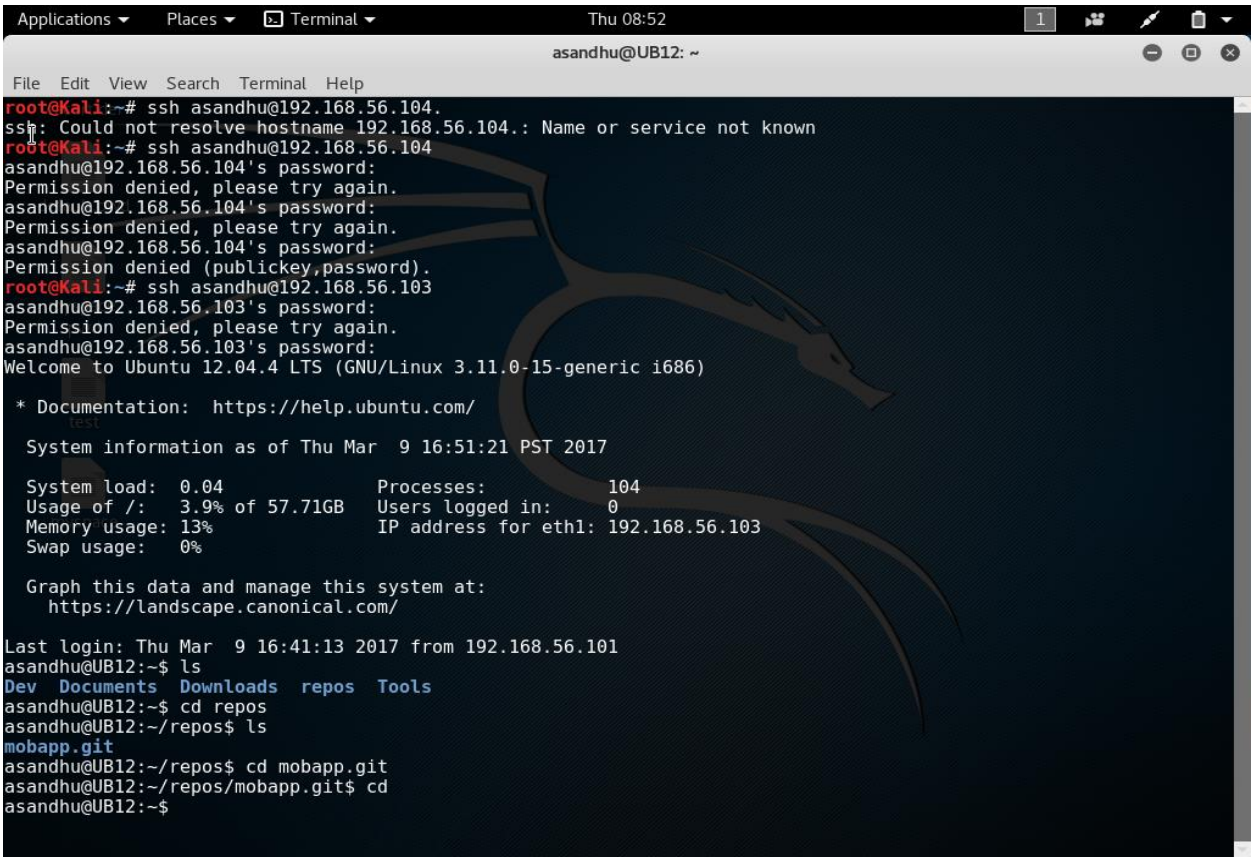
The screen shot above gives us Employees personal records (e.g. SIN, address, bank accounts from database server)

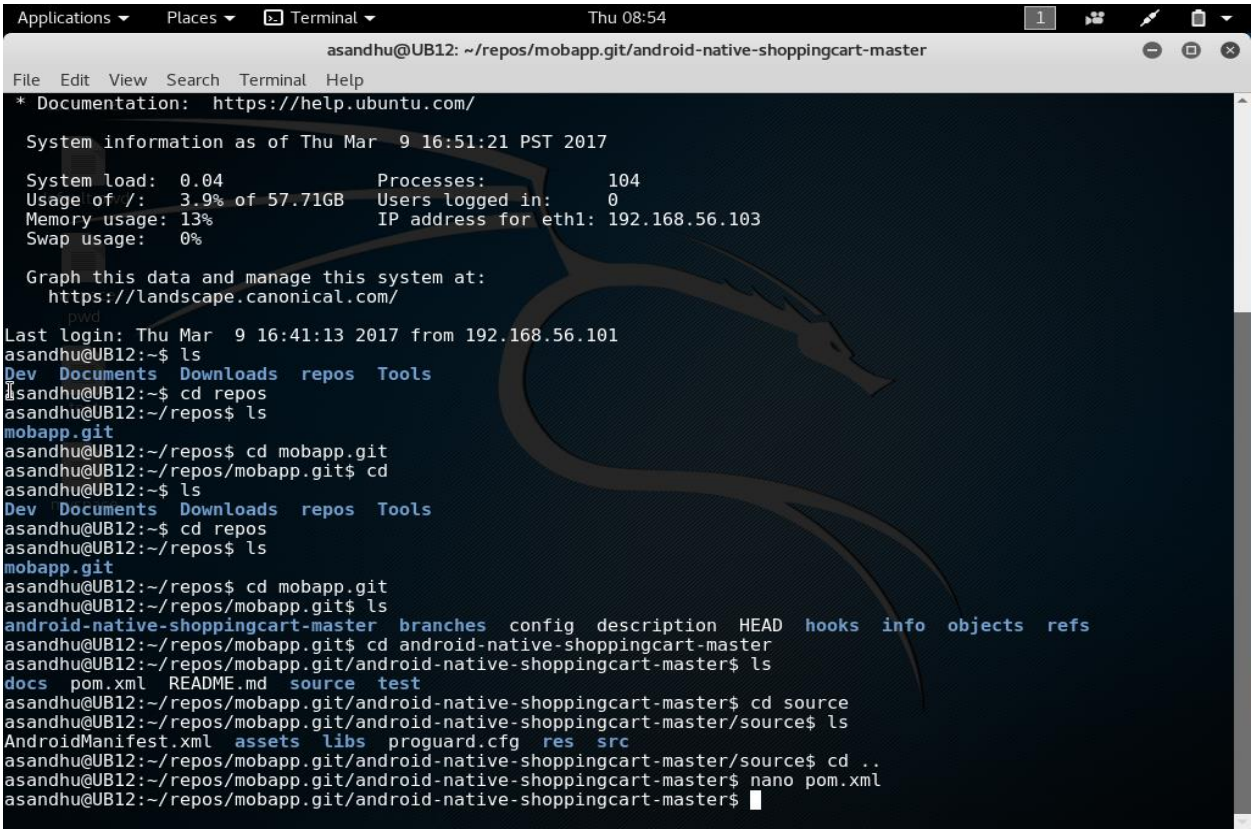
(ii) Source code of the company new mobile application (from the GIT code server) – 4%

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

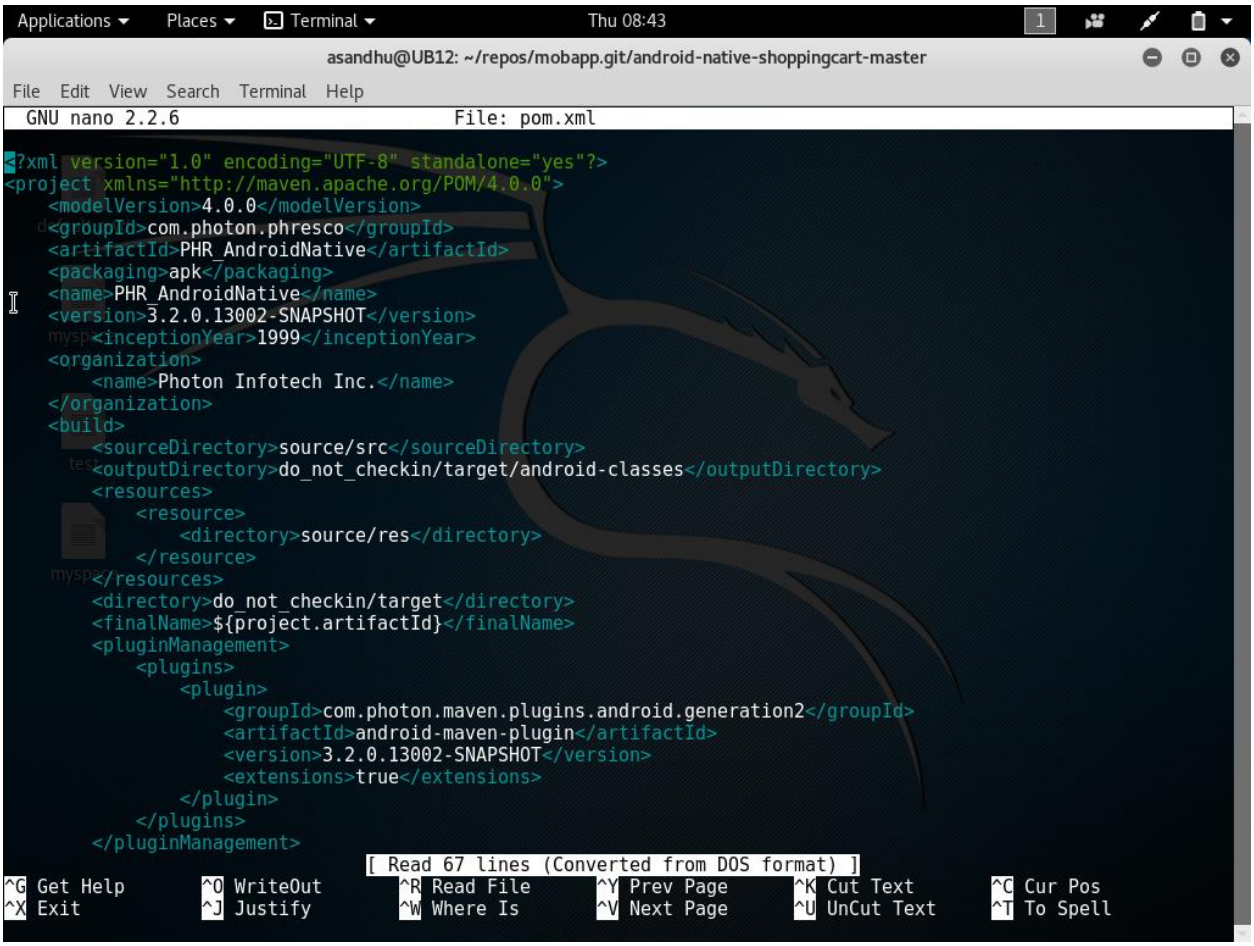
We cracked the password and run it in network interface as follows:

Step 1: login using ssh asandhu@192.168.56.103
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)

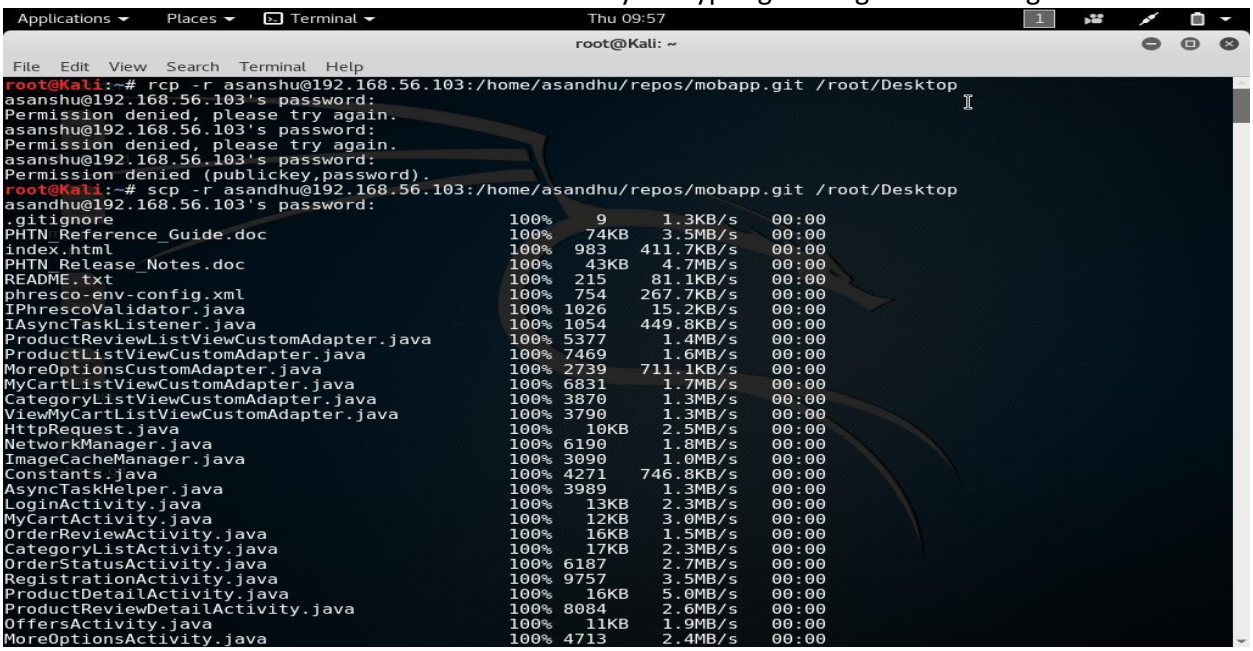




The screen shot below shows the code using nano command.

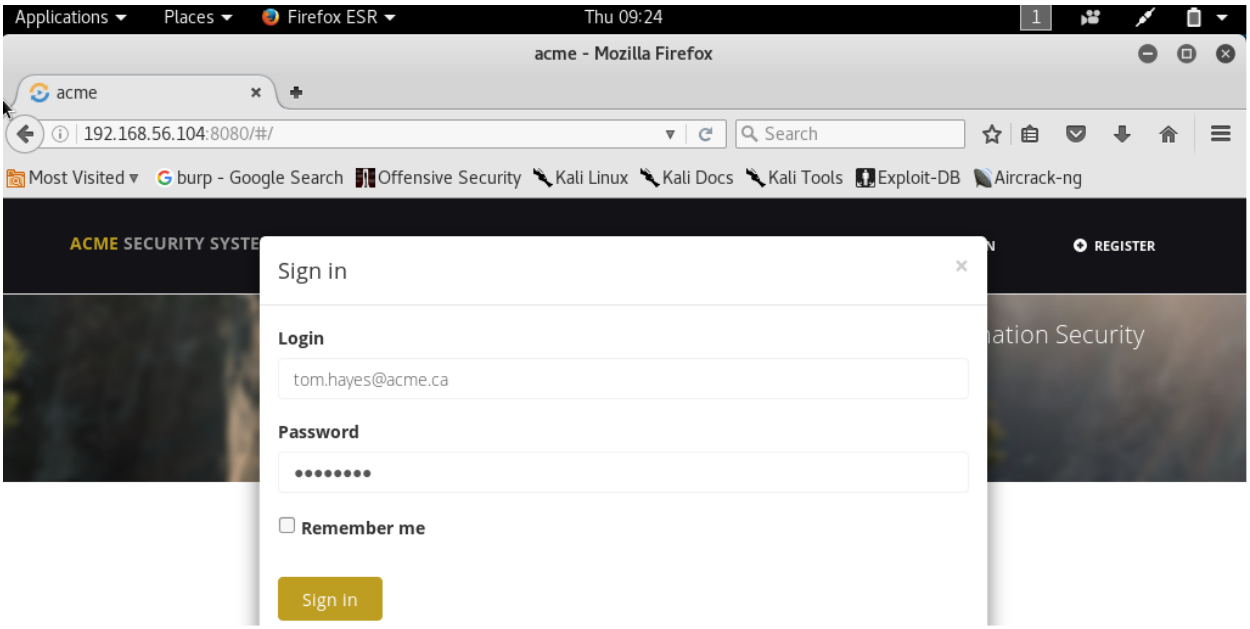


The second method is we can download the file by encrypting it using the following method:

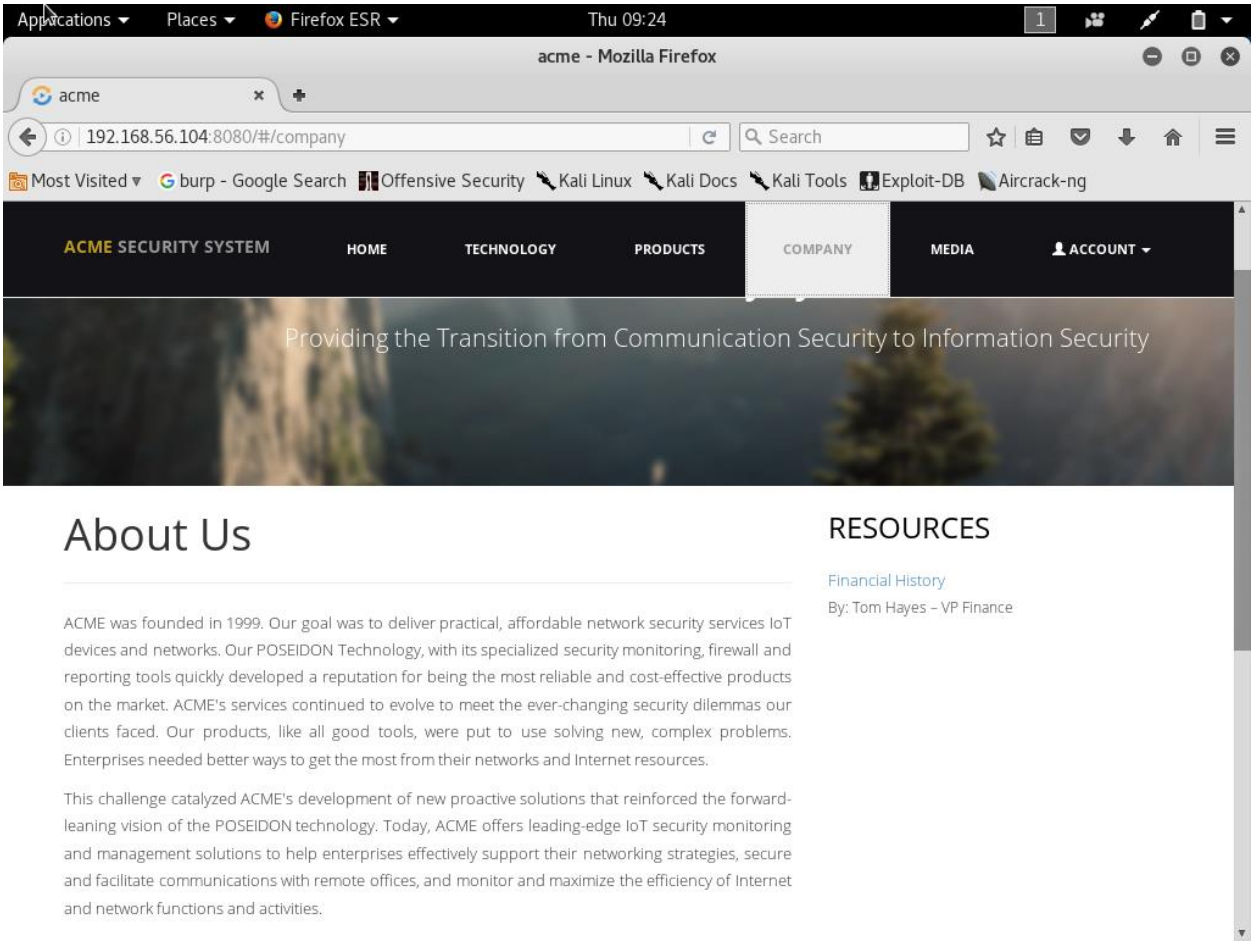


(iii) Company financial history statement – 4%

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.



Open the financial history