

Incident Response Procedures, Forensics and Forensics Analysis Lab

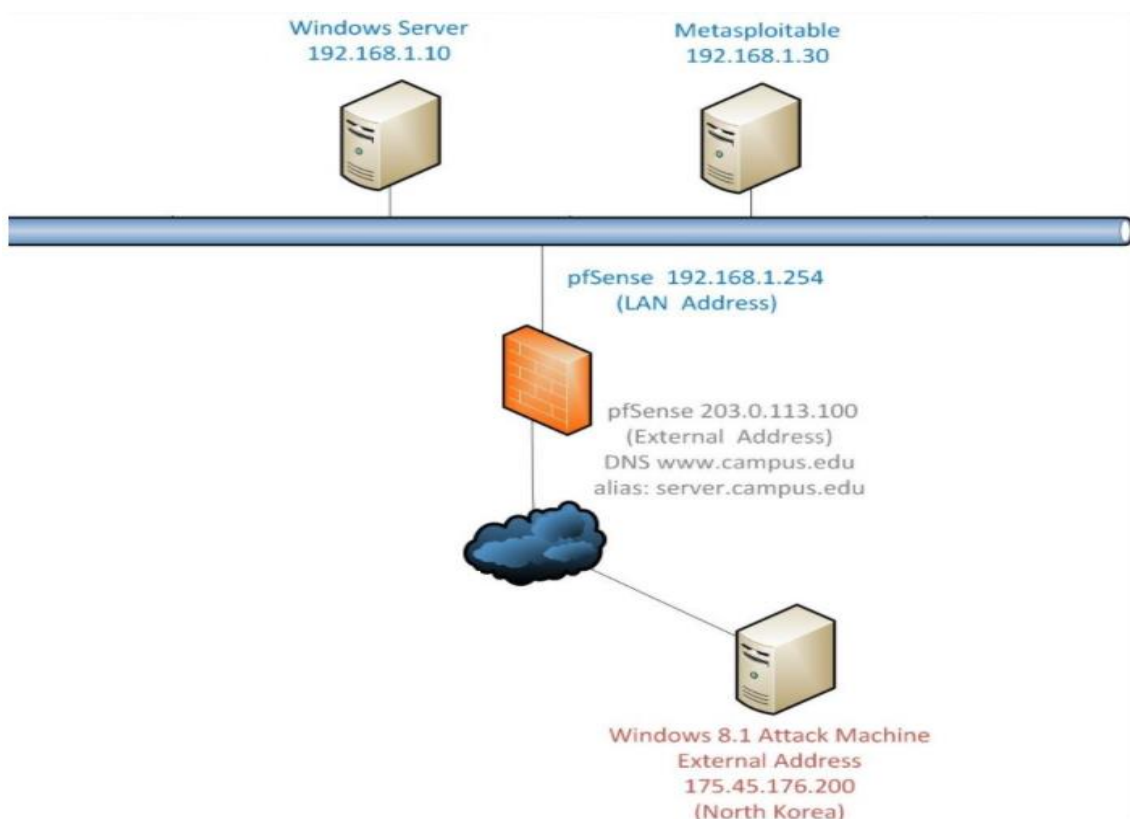


Figure 1.1

In this lab, the main aim is to find out the artifacts which are present in the Victim Machine. We will exploit the remote system first and analyse web logs and at last perform incident response on the compromised host.

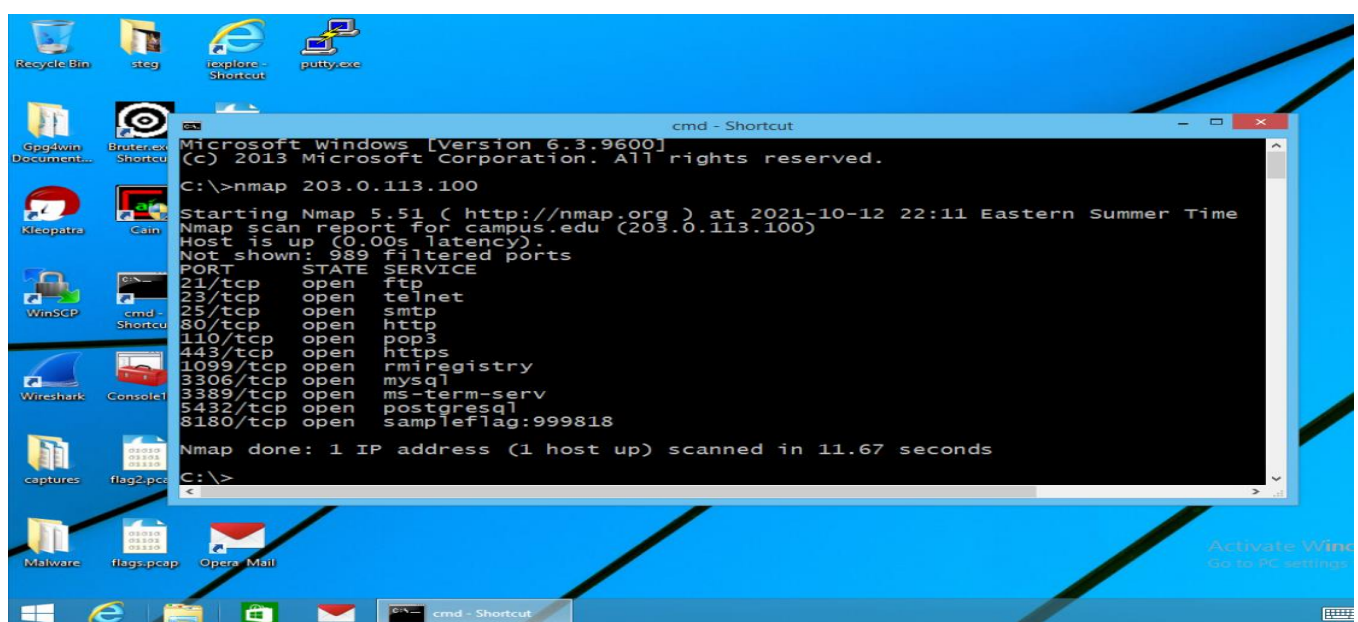


Figure 1.2

Logging into the Windows 8.1 machine and accessing cmd, we are going to find the open ports on the firewall using nmap as seen in **figure 1.2**.

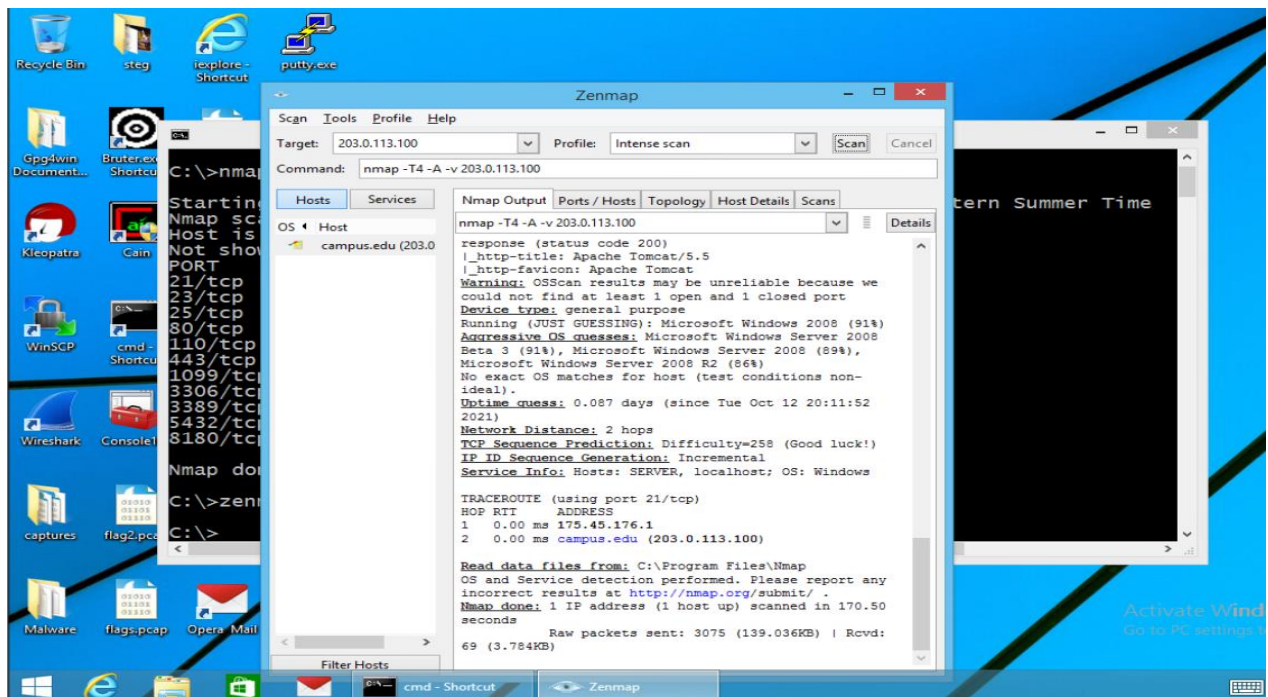


Figure 1.3

Using Zenmap, the target id – 203.0.113.100 is entered and the command – **nmap -T4 -A -v 203.0.113.100** is used for the intense scan

T4 - Aggressive (4) speeds scans, assumes reasonably fast and reliable network

A - Enables OS detection, version detection, script scanning, and traceroute

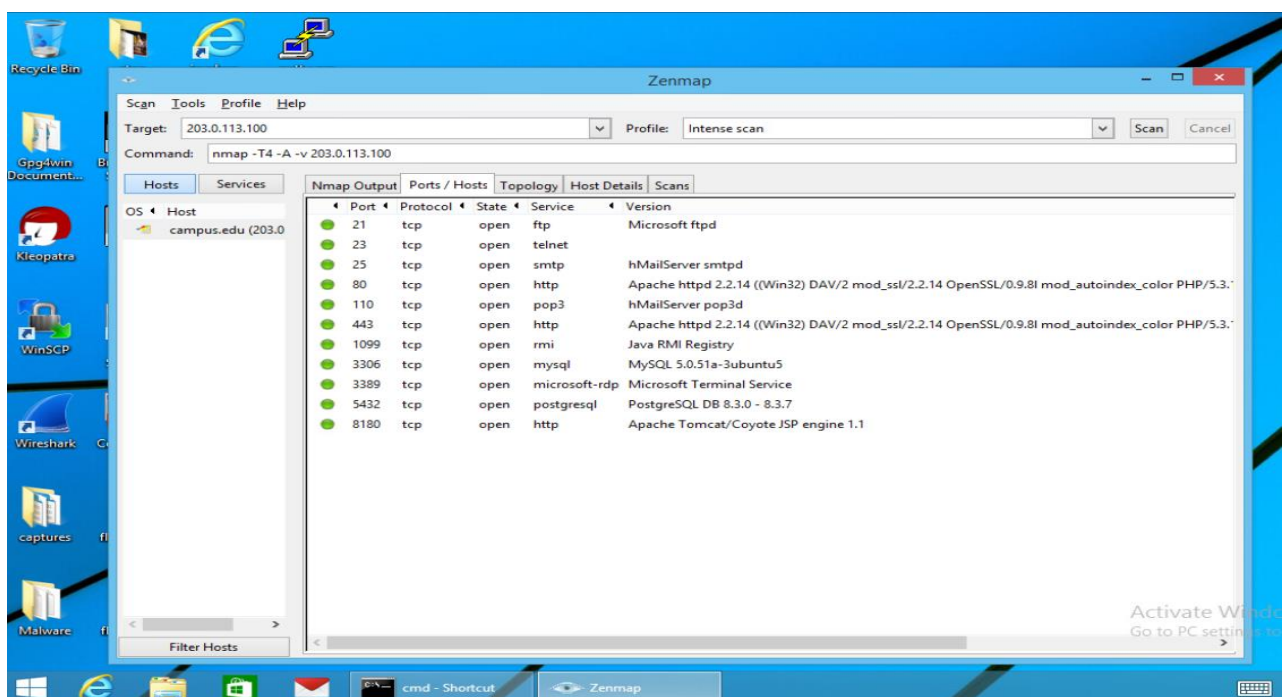


Figure 1.4

Once the scan is completed, we found the open ports and in figure 1.4, we can see that FTP is a Microsoft Service.

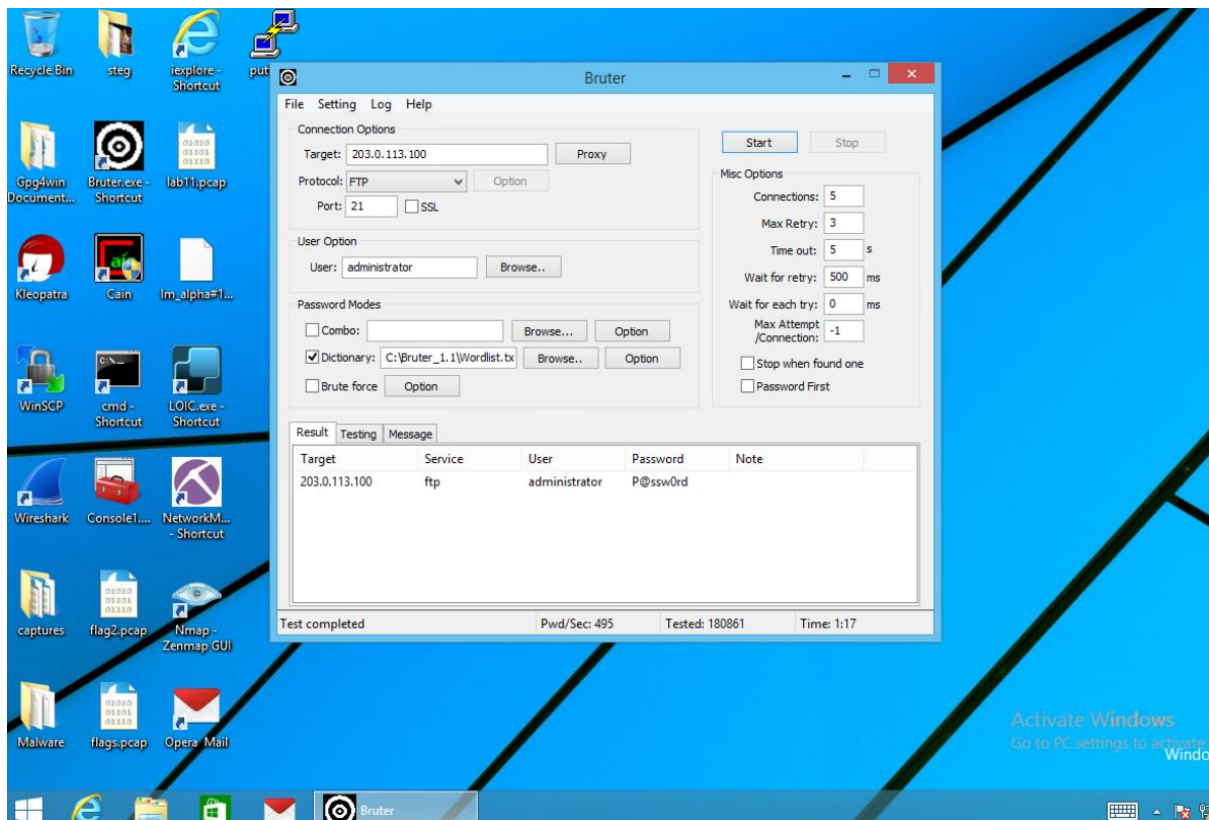


Figure 1.5

Using Bruter, we are going to find the password of FTP service. The target id is 203.0.113.000 and the port is 21. As we can see the password is found out using the dictionary combination.

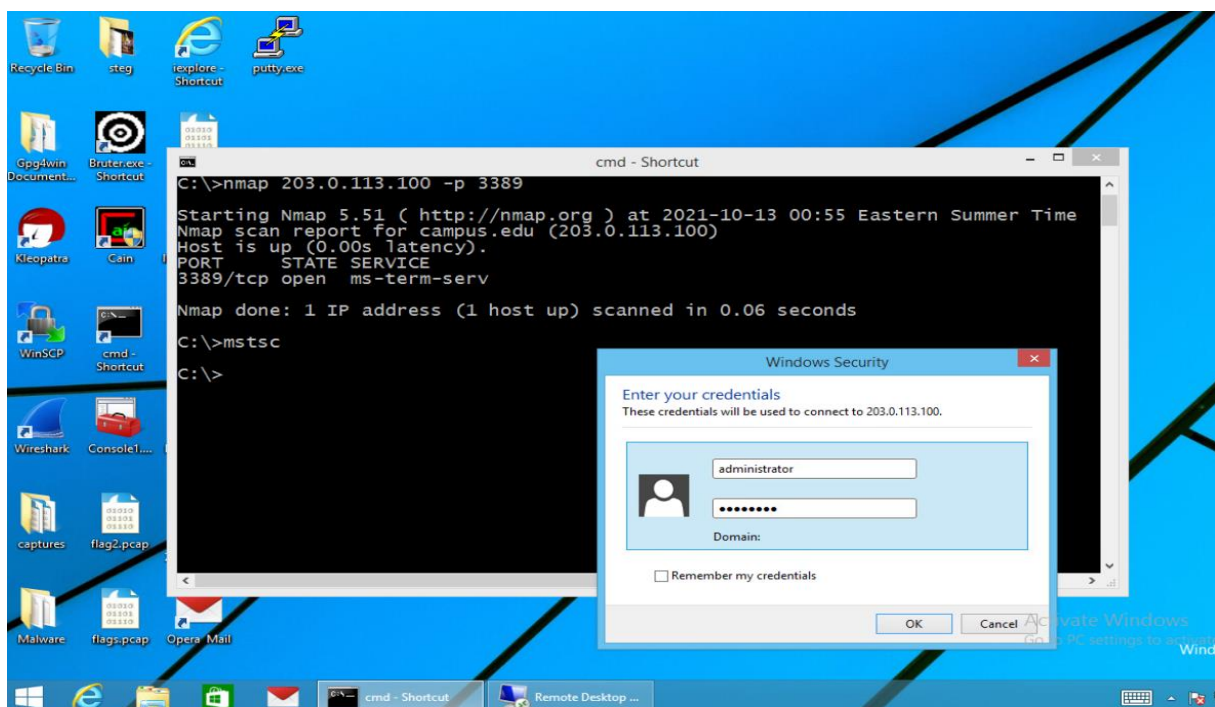


Figure 1.6

To find the RDP is open, nmap is opened and the following command is used:

nmap 203.0.113.100 -p 3389



Figure 1.7

The Microsoft Terminal Service is opened using mstsc. The RDP is opened.

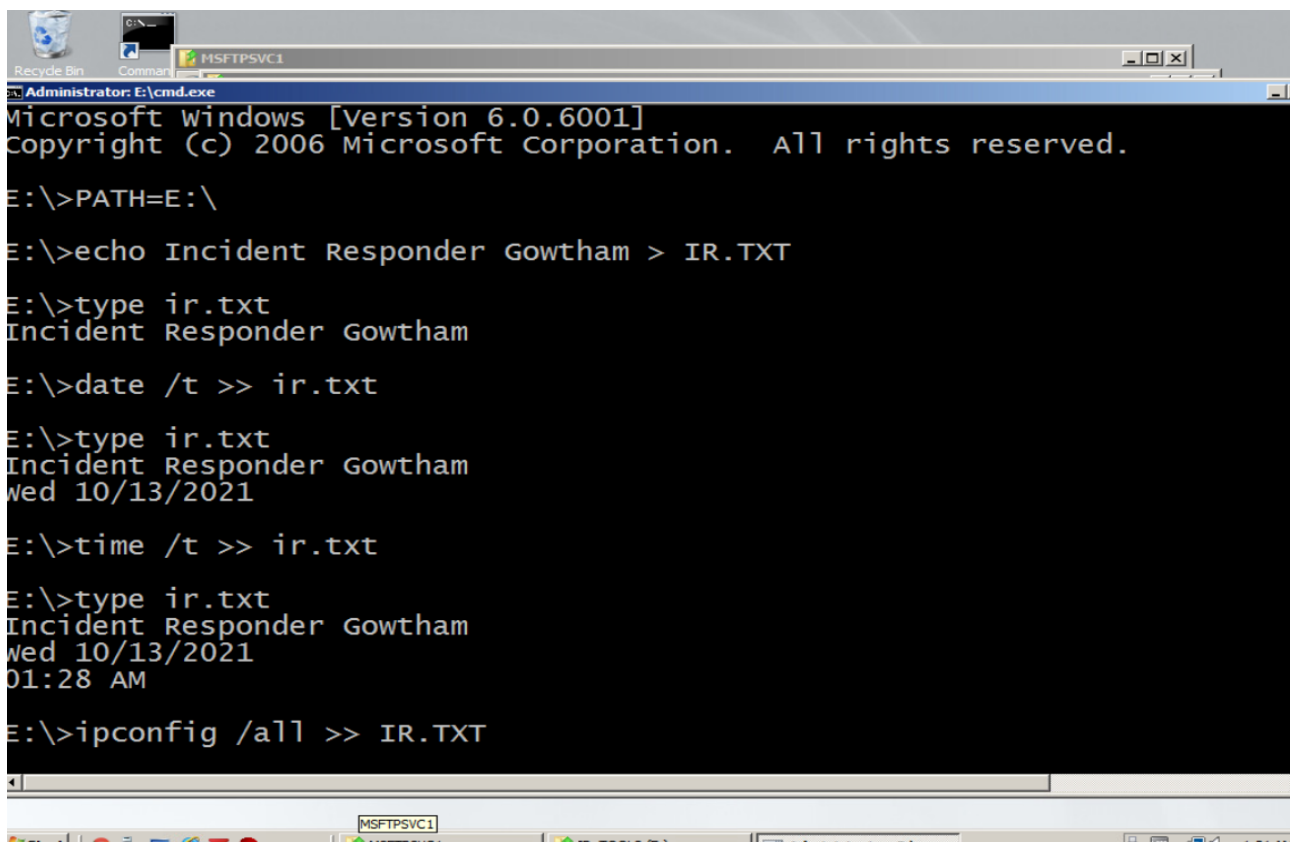
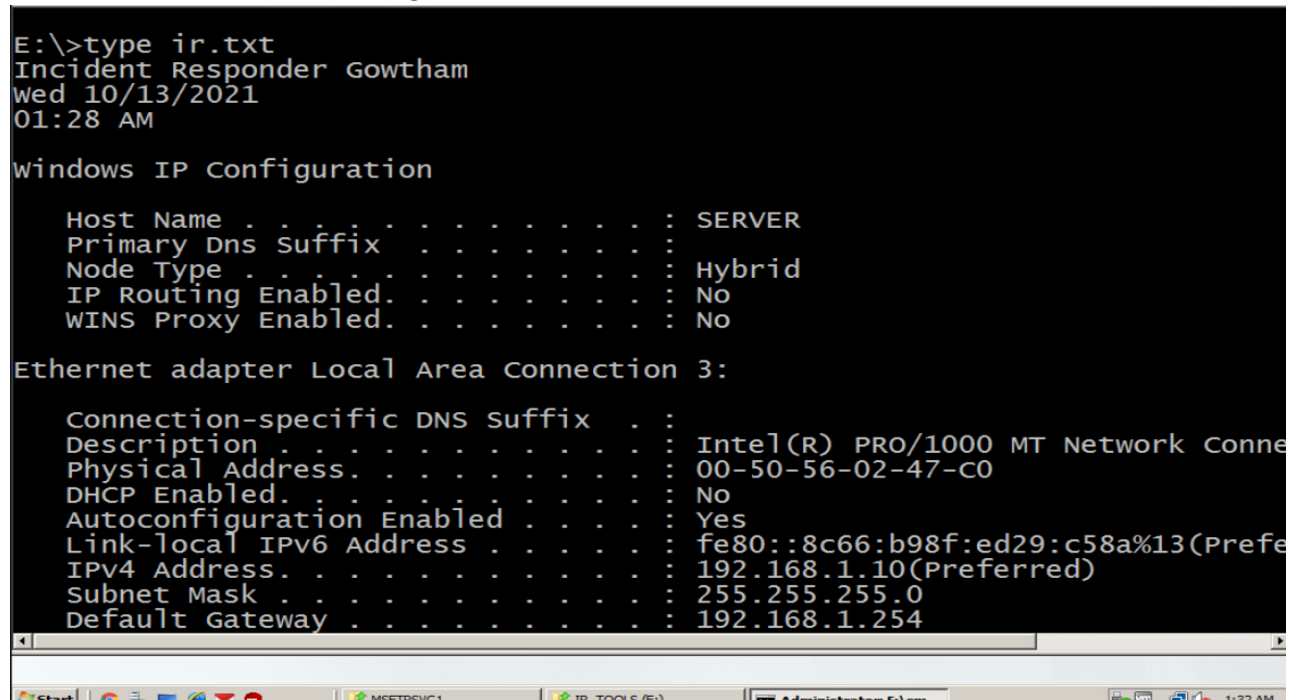


Figure 1.8

Logging into 192.168.1.10 server, the following command is used to add the incident responder to the IR.txt file: **echo Incident Responder Gowtham > IR.TXT**

The date and time command are used to add date to the IR.txt file. It is checked by using the type command.

Ipconfig /all >> IR.TXT command is used to add ip address information to the IR.txt file. To add the connection information to the incident response text file, the following command is used : **netstat -ano >> ir.txt** as seen in **figure 1.10**.



```
E:\>type ir.txt
Incident Responder Gowtham
Wed 10/13/2021
01:28 AM

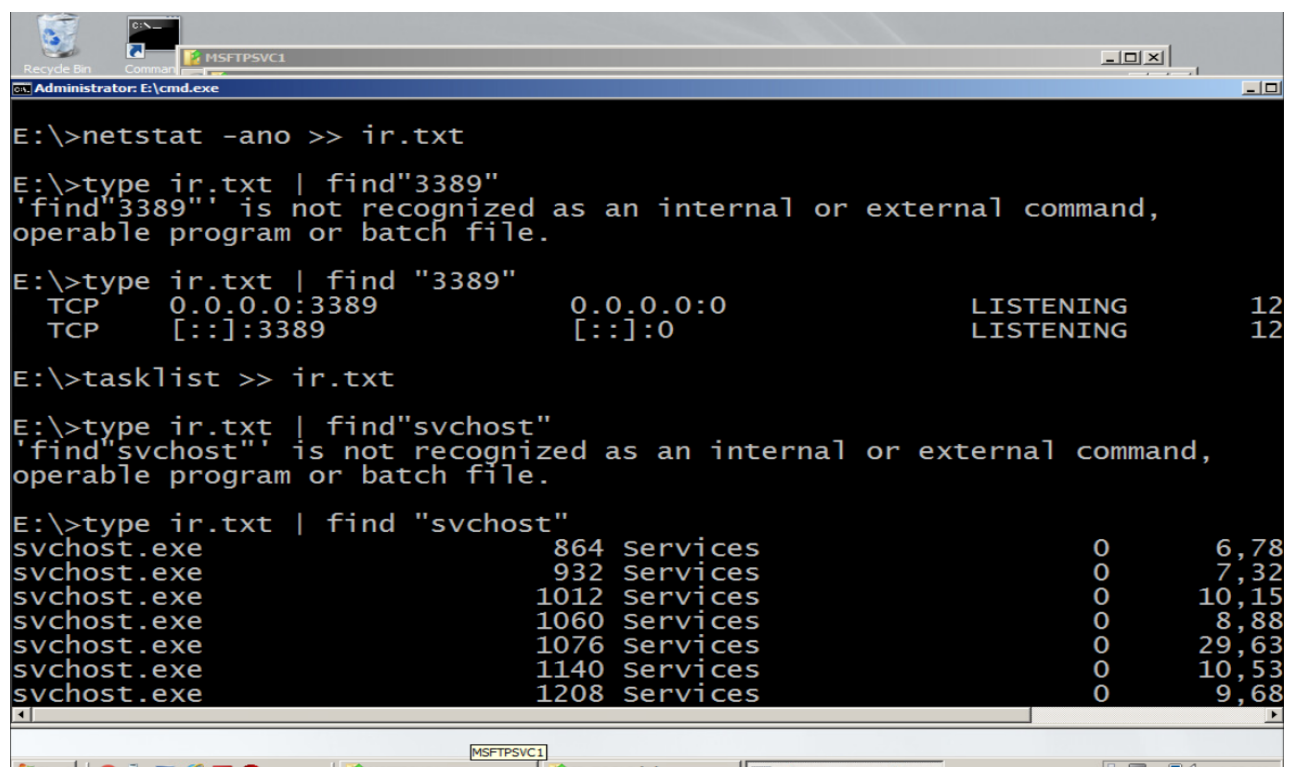
Windows IP Configuration

Host Name . . . . . : SERVER
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Conne
Physical Address. . . . . : 00-50-56-02-47-C0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8c66:b98f:ed29:c58a%13(Prefe
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
```

Figure 1.9



```
E:\>netstat -ano >> ir.txt

E:\>type ir.txt | find "3389"
'find"3389"' is not recognized as an internal or external command,
operable program or batch file.

E:\>type ir.txt | find "3389"
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 12
TCP [::]:3389 [::]:0 LISTENING 12

E:\>tasklist >> ir.txt

E:\>type ir.txt | find "svchost"
'find"svchost"' is not recognized as an internal or external command,
operable program or batch file.

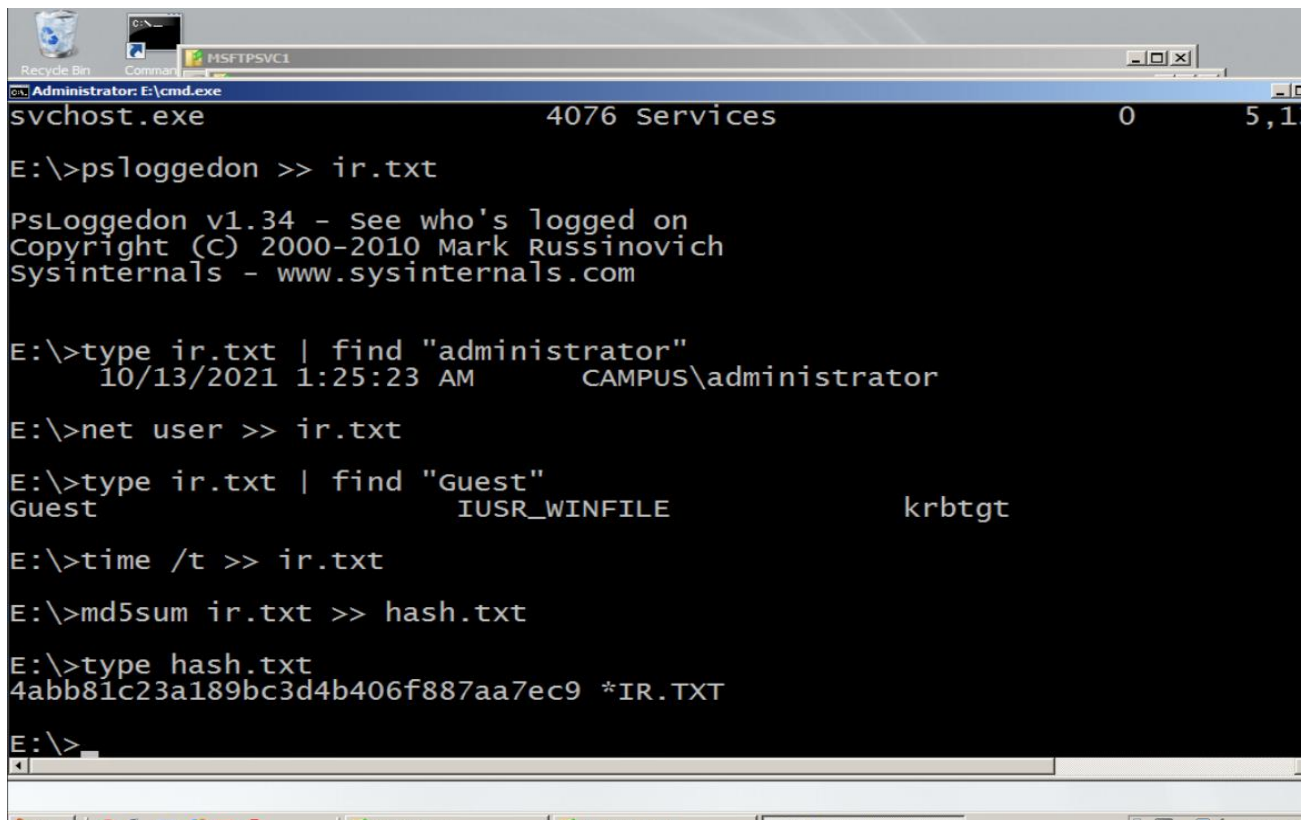
E:\>type ir.txt | find "svchost"
svchost.exe 864 Services 0 6,78
svchost.exe 932 Services 0 7,32
svchost.exe 1012 Services 0 10,15
svchost.exe 1060 Services 0 8,88
svchost.exe 1076 Services 0 29,63
svchost.exe 1140 Services 0 10,53
svchost.exe 1208 Services 0 9,68
```

Figure 1.10

The following command is used to add the process information to the IR.txt file : **tasklist >> ir.txt**

To view the svchost processes in the incident response text file, the following command is used:

type ir.txt | find "svchost"



```
Administrator: E:\cmd.exe
svchost.exe 4076 Services 0 5,1

E:\>psloggedon >> ir.txt

PsLoggedon v1.34 - See who's logged on
Copyright (C) 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

E:\>type ir.txt | find "administrator"
10/13/2021 1:25:23 AM CAMPUS\administrator

E:\>net user >> ir.txt

E:\>type ir.txt | find "Guest"
Guest IUSR_WINFILE krbtgt

E:\>time /t >> ir.txt

E:\>md5sum ir.txt >> hash.txt

E:\>type hash.txt
4abb81c23a189bc3d4b406f887aa7ec9 *IR.TXT

E:\>
```

Figure 1.11

To add information about the logged-on users to the incident response text file, the following command is used : **psloggedon >> ir.txt**

To view the administrator account in the IR.txt file, the following command is used :

type ir.txt | find "administrator"

The user account information is added to the IR.txt file and the guest account are viewed. To hash the incident respond file and send the output to the hash.txt file, the following command is used :

md5sum ir.txt >> hash.txt

The file is checked by using **type hash.txt** command.