ETHICAL HACKING AND PENETRATION TESTING CURRICULUM

INTRODUCTION

- Course Introduction & Overview
- What Is Ethical Hacking and Penetration Testing & Why Learn It?

SETTING UP A HACKING LAB

- Initial Preparation
- Virtual Box Overview
- Installing Kali Linux as a Virtual Machine

LINUX BASICS

- Overview of Kali Linux
- The Terminal & Linux Commands

NETWORK HACKING

- Introduction to Network Hacking / Penetration Testing
- Networks Basics
- Connecting a Wireless Adapter to Kali
- What is MAC Address & How to Change It
- Spoofing Mac Address Manually
- Wireless Modes (Managed & Monitor)

NETWORK HACKING – PRECONNECTION ATTACKS

- Packet Sniffing Basics
- WiFi Bands - 2.4Ghz & 5Ghz Frequencies
- Targeted Packet Sniffing
- Discovering Hidden Networks
- Deauthenticating a Client from Protected WiFi Networks
- Deauthenticating Multiple Clients from Protected WiFi Networks
- Deauthenticating All Clients from Protected WiFi Network

NETWORK HACKING – GAINING ACCESS – WPA &WPA2 NETWORK

- Introduction to WPA and WPA2 Cracking
- Hacking WPA & WPA2 Without a Wordlist
- Capturing WPA2 Handshake

- Creating a Wordlist
- Cracking WPA & WPA2 Using a Wordlist Attack

GAINING ACCESS CAPTIVE PORTAL ATTACKS

- Sniffing Captive Portal Login Information in Monitor Mode
- Creating a Fake Captive Portal - Introduction
- Creating Login Page - Cloning a Login Page
- Creating Login Page - Fixing Relative Links
- Creating Login Page - Adding Form Tag
- Creating Login Page - Adding Submit Button
- Preparing Computer to Run Fake Captive Portal
- Starting the Fake Captive Portal
- Redirecting Requests to Captive Portal Login Page
- Generating Fake SSL Certificate Enabling SSL/HTTPS on Webserver
- Sniffing & Analysing Login Credentials

NETWORK HACKING – SECURING YOUR NETWORK

- Securing Your Network from Hackers
- Configuring Wireless Settings for Maximum Security

NETWORK HACKING - POST CONNECTION ATTACKS – INFORMATION GATHERING

- Installing Windows as a Virtual Machine
- Discovering Devices Connected to the Same Network
- Gathering Sensitive Info About Connected Devices (Device Name, Ports, etc.)
- Gathering More Sensitive Info (Running Services, Operating System, etc.)

NETWORK HACKING – POST CONNECTION ATTACKS MITM

- What is ARP Poisoning?
- ARP Request & Arp Response
- Intercepting Network Traffic (Dsniff)
- Bettercap Basics
- ARP Spoofing Using Bettercap
- Spying on Network Devices (Capturing Passwords, Visited Websites...etc.)
- Creating Custom Spoofing Script
- Bypassing HTTPS
- DNS Spoofing - Controlling DNS Requests on The Network
- Injecting JavaScript Code

- BeEF Overview & Basic Hook Method
- BeEF - Hooking Targets Using Bettercap
- BeEF - Running Basic Commands on Target
- BeEF - Stealing Passwords Using A Fake Login Prompt
- BeEF - Hacking Windows 10 Using a Fake Update Prompt
- Doing All of The Above Using a Graphical Interface
- Wireshark - Basic Overview & How to Use It with MITM Attacks
- Wireshark - Sniffing & Analyzing Data
- Wireshark - Using Filters, Tracing & Dissecting Packets
- Wireshark - Capturing Passwords & Anything Sent by Any Device in The Network
- Ettercap - Basic Overview
- Ettercap - ARP Spoofing & Sniffing Sensitive Data Such as Usernames & Passwords
- Automatically ARP Poisoning New Clients
- Bypassing Router-Side Security & Poisoning Target Without Triggering Alarms

POST CONNECTION ATTACKS ANALYSING DATA FLOW & RUNNING CUSTOM ATTACKS

- Introduction to MITMproxy
- Using MITMproxy In Explicit Mode
- Analysing (Filtering & Highlighting) Flows
- Intercepting Network Flows
- Modifying Responses & Injecting JavaScript Manually
- Intercepting & Modifying Responses in Transparent Mode
- Editing Responses & Injecting BeEF's Code on The Fly
- Editing Responses Automatically Based on Regex
- Introduction to MITM Scripts?
- Configuring the Trojan Factory's MITMproxy Script
- Converting Downloads to Trojans On the Fly

NETWORK HACKING - DETECTION AND SECURITY

- Detecting ARP Poisoning Attacks
- Detecting suspicious Activities in The Network
- Preventing MITM Attacks - Method 1
- Preventing MITM Attacks - Method 2

GAINING ACCES – CLIENT-SIDE ATTACKS

- Introduction to Client-Side Attacks
- Introduction to msfpayload
- Installing Veil Framework

- Veil Overview & Payloads Basics
- Generating Undetectable Backdoor
- Listening for Incoming Connections
- Hacking Windows 10

GAINING ACCES – CLIENT-SIDE ATTACKS – SOCIAL ENGENERRING

- Introduction to Social Engineering
- Maltego Basics
- Discovering Websites, Links & Social Accounts Associated with Target
- Discovering Twitter Friends & Associated Accounts
- Discovering Emails of The Target's Friends
- Analysing the Gathered Info & Building an Attack Strategy
- Intro to Trojans - Backdooring Any File Type (images, PDF's, etc.)
- Compiling & Changing Trojan's Icon
- Spoofing .exe Extension to Any Extension (jpg, pdf ...etc)
- Spoofing Emails - Setting Up an SMTP Server
- Email Spoofing - Sending Emails as Any Email Account
- Email Spoofing - Method 2
- How to Protect Yourself from The Discussed Delivery Methods
- Detecting Trojans Manually
- Detecting Trojans Using a Virus Total
- Detecting Trojans Using a Sandbox

GAINING ACCES – SERVER-SIDE ATTACKS

- Installing Metasploitable As a Virtual Machine
- Introduction to Server-Side Attacks
- Information Gathering (Nmap)
- Hacking a Remote Server Using a Basic Metasploit Exploit
- Exploiting a Code Execution Vulnerability to Hack Remote Server
- Nexpose - Installing Nexpose
- Nexpose - Scanning a Target Server for Vulnerabilities
- Nexpose - Analysing Scan Results & Generating Reports
- Server-Side Attacks Conclusion

WEBSITE HACKING & PENETRATION TESTING

- What is a Website?
- How to Hack a Website?

WEBSITE HACKING – INFORMATION GATHERING

- Gathering Information Using Whois Lookup
- Discovering Technologies Used on The Website
- Gathering Comprehensive DNS Information
- Discovering Subdomains
- Discovering Sensitive Files
- Analysing Discovered Files
- Maltego - Discovering Servers, Domains & Files
- Maltego - Discovering Websites, Hosting Provider & Emails

CODE EXECUTION VULNERABILITY

- How to Discover & Exploit Basic Code Execution Vulnerabilities to Hack Websites
- Exploiting Advanced Code Execution Vulnerabilities
- [Security] - Fixing Code Execution Vulnerabilities

FILE UPLOAD VULNERABILITY

- How to Discover & Exploit Basic File Upload Vulnerabilities to Hack Websites
- GET & POST Requests
- Intercepting Requests
- Exploiting Advanced File Upload Vulnerabilities to Hack Websites
- [Security] Fixing File Upload Vulnerabilities

LOCAL FILE INCLUSION VULNERABILITY (L.F.I)

- What are they? And How to Discover & Exploit Them
- Gaining Shell Access from LFI Vulnerabilities

REMOTE FILE INCLUSION

- Remote File Inclusion Vulnerabilities - Configuring PHP Settings
- Remote File Inclusion Vulnerabilities - Discovery & Exploitation
- Exploiting Advanced Remote File Inclusion Vulnerabilities to Hack Websites
- [Security] Fixing File Inclusion Vulnerabilities

SQL INJECTION VULNERABILITIES

- What is SQL?
- Dangers of SQL Injections

SQL IN LOGIN PAGE

- Discovering SQL Injections In POST
- Bypassing Logins Using SQL Injection Vulnerability
- Bypassing More Secure Logins Using SQL Injections
- [Security] Preventing SQL Injections in Login Pages

EXTRACTING DATA FROM DATABASE

- Discovering SQL Injections in GET
- Reading Database Information
- Finding Database Tables
- Extracting Sensitive Data Such as Passwords

ADVANCE SQL INJECTION

- Discovering & Exploiting Blind SQL Injections
- Discovering Complex SQL Injection Vulnerabilities
- Exploiting an advanced SQL Injection Vulnerability to Extract Passwords
- Bypassing Filters
- Bypassing Security & Accessing All Records
- [Security] Quick Fix to Prevent SQL Injections
- Reading & Writing Files on The Server Using SQL Injections
- Getting A Shell & Controlling the Target Server Using an SQL Injection
- Discovering SQL Injections & Extracting Data Using SQLmap
- Getting a Direct SQL Shell using SQLmap
- [Security] - The Right Way to Prevent SQL Injection Vulnerabilities

XSS VULNERABILITIES

- Introduction - What is XSS or Cross Site Scripting?
- Discovering Basic Reflected XSS
- Discovering Advanced Reflected XSS
- Discovering an Even More Advanced Reflected XSS
- Discovering Stored XSS
- Discovering Advanced Stored XSS

XSS VULNERABILITIES – EXPLOITATION

- Hooking Victims to BeEF Using Reflected XSS
- Hooking Victims to BeEF Using Stored XSS

INSECURE SESSION MANAGEMENT

- Logging in As Admin Without a Password by Manipulating Cookies
- Discovering Cross Site Request Forgery Vulnerabilities (CSRF)
- Exploiting CSRF To Change Admin Password Using a HTML File
- Exploiting CSRF Vulnerabilities to Change Admin Password Using Link
- [Security] The Right Way to Prevent CSRF Vulnerabilities

BRUTE FORCE / DICTIONARY ATTACKS

- Introduction to Brute Force & Dictionary Attacks?
- Guessing Login Password Using a Wordlist Attack with Hydra

DISCOVERING VULNERABILITIES AUTOMATICALLY USING Owasp ZAP

- Scanning Target Website for Vulnerabilities
- Analysing Scan Results
- Conclusion
- Writing a Pentest Report
- Ways to Secure Websites