Module 1:Ethical Hacking Introduction

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

Module 2: The architecture, design, and management of the security of organization

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Module 3: Digital Forensics Course

1,Digital Forensics Categories

2,Cybercrime Types

3,Violatile Memory

4,Non-violatile Memory

5,Installing FTK Imager

6,Installing Kaine OS

7,Storage Acquisition

8,Hashing Evidence

9,Windows Ram Acquisition with FTK Imager

10, Windows Ram Acquisition with Magnet

11,Windows Ram Analysis

12,Cridex malware Analysis

13,Metadata Fundamentals

14,Autospy Storage Analysis

15,Browser Forensics

16,Mobile Forensics

17,Lock screen cracking without data loss

18,Android Forensics

19,Digital Forensics Pattrens

Module 4:Basic Pentesting

Getting Comfortable with Kali Linux

The Linux Filesystem

Basic Linux Commands

Finding Files in Kali Linux

SSH Service

HTTP Service

Searching, Installing, and Removing Tools

- apt update
- apt upgrade
- apt-cache search and apt show
- apt install
- apt remove –purge
- dpkg

The Bash Environment

- Environment Variables
- Tab Completion
- Bash History Tricks

- Piping and Redirection
  - Redirecting to a New File
  - Redirecting to an Existing File
  - Redirecting from a File
  - Redirecting STDERR
  - Piping
- Text Searching and Manipulation
  - grep
  - sed
  - cut
  - awk
- Editing Files from the Command Line
  - nano
  - vi
- Comparing Files
  - comm
  - diff
  - vimdiff
- Managing Processes
  - Backgrounding Processes (bg)
  - Jobs Control: jobs and fg
  - Process Control: ps and kill

- File and Command Monitoring
  - tail
  - watch
- Downloading Files
  - wget
  - curl
  - axel
- Customizing the Bash Environment
  - Bash History Customization
  - Alias
  - Persistent Bash Customization
- Netcat
  - Connecting to a TCP/UDP Port
  - Listening on a TCP/UDP Port
  - Transferring Files with Netcat
  - Remote Administration with Netcat
- Socat
  - Netcat vs Socat
  - Socat File Transfers
  - Socat Reverse Shells
  - Socat Encrypted Bind Shells
- PowerShell and Powercat
  - PowerShell File Transfers
  - PowerShell Reverse Shells
  - PowerShell Bind Shells
  - Powercat
  - Powercat File Transfers
  - Powercat Reverse Shells
  - Powercat Bind Shells
  - Powercat Stand-Alone Payloads

Wireshark

- Wireshark Basics
- Launching Wireshark
- Capture Filters
- Display Filters
- Following TCP Streams

Tcpdump

- Filtering Traffic
- Advanced Header Filtering

Bash Scripting

Intro to Bash Scripting

Variables

- Arguments
- Reading User Input

If, Else, Elif Statements

Boolean Logical Operations

Loops

- For Loops
- While Loops

Functions

Taking Notes

Website Recon

Whois Enumeration

Google Hacking

Netcraft

Recon-ng

Open-Source Code

Shodan

Security Headers Scanner

SSL Server Test

Pastebin

Email Harvesting

Password Dumps

Site-Specific Tools

Stack Overflow

Information Gathering Frameworks

OSINT Framework

Maltego

DNS Enumeration

- Interacting with a DNS Server
- Automating Lookups
- Forward Lookup Brute Force
- Reverse Lookup Brute Force
- DNS Zone Transfers
- Relevant Tools in Kali Linux

- Port Scanning
  - TCP / UDP Scanning
  - Port Scanning with Nmap
  - Masscan
- SMB Enumeration
  - Scanning for the NetBIOS Service
  - Nmap SMB NSE Scripts
- NFS Enumeration
  - Scanning for NFS Shares
  - Nmap NFS NSE Scripts
- SMTP Enumeration
- SNMP Enumeration
  - The SNMP MIB Tree
  - Scanning for SNMP
  - Windows SNMP Enumeration Example
- Vulnerability Scanning Overview and Considerations
  - How Vulnerability Scanners Work
  - Manual vs. Automated Scanning
  - Internet Scanning vs Internal Scanning
  - Authenticated vs Unauthenticated Scanning
- Vulnerability Scanning with Nessus
  - Installing Nessus
  - Defining Targets
  - Configuring Scan Definitions
  - Unauthenticated Scanning With Nessus
  - Authenticated Scanning With Nessus
  - Scanning with Individual Nessus Plugins
- Vulnerability Scanning with Nmap

Web Application Assessment Methodology

Web Application Enumeration

- Inspecting URLs
- Inspecting Page Content
- Viewing Response Headers
- Inspecting Sitemaps
- Locating Administration Consoles

Web Application Assessment Tools

- DIRB
- Burp Suite
- Nikto

Exploiting Web-based Vulnerabilities

- Exploiting Admin Consoles
- Cross-Site Scripting (XSS)
- Directory Traversal Vulnerabilities
- File Inclusion Vulnerabilities
- SQL Injection

Extra Miles

Introduction to Buffer Overflows

Introduction to the x Architecture

- Program Memory
- CPU Registers

Buffer Overflow Walkthrough

Sample Vulnerable Code

Introducing the Immunity Debugger

Navigating Code

Understanding Windows Privileges and Integrity Levels
Introduction to User Account Control (UAC)
User Account Control (UAC) Bypass: fodhelper.exe Case Study
Insecure File Permissions: Serviio Case Study
Leveraging Unquoted Service Paths
Windows Kernel Vulnerabilities: USBPcap Case Study

Understanding Linux Privileges
Insecure File Permissions: Cron Case Study
Insecure File Permissions: /etc/passwd Case Study
Kernel Vulnerabilities: CVE-7-2 Case Study

Password Attacks

Wordlists

Standard Wordlists

Brute Force Wordlists
Common Network Service Attack Methods

HTTP htaccess Attack with Medusa
Remote Desktop Protocol Attack with Crowbar
SSH Attack with THC-Hydra
HTTP POST Attack with THC-Hydra

Leveraging Password Hashes

Retrieving Password Hashes
Passing the Hash in Windows
Password Cracking

Port Redirection and Tunneling
Port Forwarding

RINETD

SSH Tunneling

SSH Local Port Forwarding
SSH Remote Port Forwarding
SSH Dynamic Port Forwarding

PLINK.exe
NETSH
HTTPTunnel-ing Through Deep Packet Inspection

Active Directory Attacks
- Active Directory Theory
- Active Directory Enumeration

Traditional Approach
A Modern Approach
Resolving Nested Groups
Currently Logged on Users
Enumeration Through Service Principal Names

Active Directory Authentication

NTLM Authentication

Kerberos Authentication
Cached Credential Storage and Retrieval
Service Account Attacks
Low and Slow Password Guessing

Active Directory Lateral Movement

Core Post-Exploitation Features
Migrating Processes
Post-Exploitation Modules
Pivoting with the Metasploit Framework

Metasploit Automation

PowerShell Empire
Installation, Setup, and Usage

PowerShell Empire Syntax
Listeners and Stagers
The Empire Agent

PowerShell Modules

Situational Awareness
Credentials and Privilege Escalation
Lateral Movement

Switching Between Empire and Metasploit

Assembling the Pieces: Penetration Test Breakdown

Public Network Enumeration
Targeting the Web Application

Web Application Enumeration
SQL Injection Exploitation
Cracking the Password
Enumerating the Admin Interface
Obtaining a Shell
Post-Exploitation Enumeration
Creating a Stable Pivot Point

Targeting the Database

- Enumeration
- Attempting to Exploit the Database

Deeper Enumeration of the Web Application Server

- More Thorough Post Exploitation
- Privilege Escalation
- Searching for DB Credentials

Targeting the Database Again

- Exploitation
- Post-Exploitation Enumeration
- Creating a Stable Reverse Tunnel

Targeting Poultry

- Enumeration
- Exploitation (Or Just Logging In)
- Post-Exploitation Enumeration
- Unquoted Search Path Exploitation
- Post-Exploitation Enumeration

- Internal Network Enumeration

Targeting the Jenkins Server

Application Enumeration

Exploiting Jenkins

Post Exploitation Enumeration

Privilege Escalation

Post Exploitation Enumeration

Targeting the Domain Controller

Exploiting the Domain Controller

Module 5:Advanced Pentesting

Operating System and Programming Theory

Programming Theory

- Programming Language Level
- Programming Concepts

Windows Concepts

- Windows On Windows
- Win32 APIs
- Windows Registry

Client Side Code Execution With Office

Staged vs Non-staged Payloads

Building Our Droppers

HTML Smuggling

Jscript and C#

- Introduction to Visual Studio
- DotNetToJscript
- Win32 API Calls From C#
- Shellcode Runner in C#
- Jscript Shellcode Runner
- SharpShooter

In-memory PowerShell Revisited

Reflective Load

Process Injection and Migration Theory

Process Injection in C#

DLL Injection Theory

DLL Injection with C#

Reflective DLL Injection Theory

Reflective DLL Injection in PowerShell

Process Hollowing Theory

Process Hollowing in C#

Antivirus Software Overview

Simulating the Target Environment

Locating Signatures in Files

Bypassing Antivirus with Metasploit

Metasploit Encoders

Metasploit Encryptors

Bypassing Antivirus with C#

- C# Shellcode Runner vs Antivirus
- Encrypting the C# Shellcode Runner

- Application Whitelisting Theory and Setup
  - Application Whitelisting Theory
  - AppLocker Setup and Rules
- Basic Bypasses
  - Trusted Folders
  - Bypass With DLLs
  - Alternate Data Streams
  - Third Party Execution
- Bypassing AppLocker with PowerShell
  - PowerShell Constrained Language Mode
  - Custom Runspaces
  - PowerShell CLM Bypass
- Reflective Injection Returns
- Bypassing AppLocker with C#
  - Locating a Target
  - Reverse Engineering for Load
  - Give Me Code Exec
  - Invoking the Target Part 1
  - Invoking the Target Part 2
- Bypassing AppLocker with JScript
  - JScript and MSHTA
  - XSL Transform
- Bypassing Network Filters

Command Execution

Exploring the Filesystem
Leveraging Firefox Profiles
Enumerating System Information
Scratching the Surface

Post-Exploitation

Simulating an Interactive Shell

Privilege Escalation

Thinking Outside the Box
Root Shell at the Top of the Hour
Getting Root Terminal Access

Windows Kiosk Breakout Techniques

Windows Credentials
Local Windows Credentials

SAM Database
Hardening the Local Administrator Account

Access Tokens

Access Token Theory
Elevation with Impersonation
Fun with Incognito

Kerberos and Domain Credentials

Kerberos Authentication
Mimikatz

Processing Credentials Offline

Memory Dump
MiniDumpWriteDump

Windows Lateral Movement
Remote Desktop Protocol

Lateral Movement with RDP
Reverse RDP Proxying with Metasploit
Reverse RDP Proxying with Chisel
RDP as a Console
Stealing Clear Text Credentials from RDP

Fileless Lateral Movement

Authentication and Execution Theory
Implementing Fileless Lateral Movement in C#

Linux Lateral Movement
Lateral Movement with SSH

SSH Keys
SSH Persistence
SSH Hijacking with ControlMaster
SSH Hijacking Using SSH-Agent and SSH Agent Forwarding

DevOps

Introduction to Ansible
Enumerating Ansible
Ad-hoc Commands
Ansible Playbooks
Exploiting Playbooks for Ansible Credentials
Weak Permissions on Ansible Playbooks
Sensitive Data Leakage via Ansible Modules
Introduction to Artifactory
Artifactory Enumeration
Compromising Artifactory Backups
Compromising Artifactory's Database
Adding a Secondary Artifactory Admin Account

Kerberos on Linux

General Introduction to Kerberos on Linux
Stealing Keytab Files
Attacking Using Credential Cache Files
Using Kerberos with Impacket

Microsoft SQL Attacks
    MS SQL in Active Directory

MS SQL Enumeration
MS SQL Authentication
UNC Path Injection
Relay My Hash

MS SQL Escalation

Privilege Escalation
Getting Code Execution
Custom Assemblies

Linked SQL Servers

Active Directory Exploitation

AD Object Security Permissions

Object Permission Theory

Abusing GenericAll

Abusing WriteDACL

Kerberos Delegation

Unconstrained Delegation

I Am a Domain Controller

Constrained Delegation

Resource-Based Constrained Delegation

Active Directory Forest Theory

Active Directory Trust in a Forest

Enumeration in the Forest

Burning Down the Forest

-

Owning the Forest with Extra SIDs

Owning the Forest with Printers

Going Beyond the Forest

Active Directory Trust Between Forests

Enumeration Beyond the Forest

Compromising an Additional Forest

Linked SQL Servers in the Forest

Combining the Pieces

Enumeration and Shell

Initial Enumeration

Gaining an Initial Foothold

Post Exploitation Enumeration

Attacking Delegation

Privilege Escalation on web01

Getting the Hash

Delegate My Ticket

Owning the Domain

Lateral Movement

Becoming Domain Admin

Module 6:Advanced Web Pentesting

Web Traffic Inspection

- Authentication Bypass Discovery
  - Discovering the SQL Injection
- Authentication Bypass Exploitation
  - Obtaining Admin User Information
  - Resetting the Admin Password
- SSTI Vulnerability Discovery
  - Introduction to Templating Engines
  - Discovering The Rendering Function
  - SSTI Vulnerability Filter Evasion
- SSTI Vulnerability Exploitation
  - Finding a Method for Remote Command Execution
  - Gaining Remote Command Execution

openCRX Authentication Bypass and Remote Code Execution

- Password Reset Vulnerability Discovery
  - When Random Isn't
  - Account Determination
  - Timing the Reset Request
  - Generate Token List
  - Automating Resets

XML External Entity Vulnerability Discovery

- Introduction to XML
- XML Parsing
- XML Entities
- Understanding XML External Entity Processing Vulnerabilities
- Finding the Attack Vector
- CDATA
- Updating the XXE Exploit
- Gaining Remote Access to HSQLDB
- Java Language Routines

Remote Code Execution

- Finding the Write Location
- Writing Web Shells

openITCOCKPIT XSS and OS Command Injection - Blackbox

- Getting Started
- Black Box Testing in openITCOCKPIT
- Application Discovery

Building a Sitemap

Targeted Discovery

Intro To DOM-based XSS

XSS Hunting

Advanced XSS Exploitation

Module 7: Windows Exploit Development

WinDbg and x86 Architecture

Introduction to x86 Architecture
- Program Memory
- CPU Registers

Introduction to Windows Debugger
- What is a Debugger?
- WinDbg Interface
- Understanding the Workspace
- Debugging Symbols

Accessing and Manipulating Memory from WinDbg
- Unassemble from Memory
- Reading from Memory
- Dumping Structures from Memory
- Writing to Memory
- Searching the Memory Space

- Inspecting and Editing CPU Registers in WinDbg

Controlling the Program Execution in WinDbg
- Software Breakpoints
- Unresolved Function Breakpoint
- Breakpoint-Based Actions
- Hardware Breakpoints
- Stepping Through the Code

Additional WinDbg Features
- Listing Modules and Symbols in WinDbg
- Using WinDbg as a Calculator
- Data Output Format
- Pseudo Registers

Exploiting Stack Overflows

- Stack Oveflows Introduction
- Installing the Sync Breeze Application
- Crashing the Sync Breeze Application
- Win32 Buffer Overflow Exploitation

- A Word About DEP, ASLR, and CFG
- Controlling EIP
- Locating Space for Our Shellcode
- Checking for Bad Characters
- Redirecting the Execution Flow
- Finding a Return Address
- Generating Shellcode with Metasploit
- Getting a Shell
- Improving the Exploit

Exploiting SEH Overflows

- Installing the Sync Breeze Application
- Crashing Sync Breeze
- Analyzing the Crash in WinDbg
- Introduction to Structured Exception Handling

- Understanding SEH
- SEH Validation

Structured Exception Handler Overflows

- Gaining Code Execution
- Detecting Bad Characters
- Finding a P/P/R Instruction Sequence
- Island-Hopping in Assembly
- Obtaining a Shell

Introduction to IDA Pro