DLE COURSE ON ETHICAL HACKING

Table of Contents

Course Contents of Ethical Hacking

Background:

This course provides the foundational knowledge needed to ethically and effectively discover and exploit vulnerabilities in systems by assuming both the mindset and toolset of an attacker. The objective of conducting this course is not to create hackers but to protect the system from the perpetrators. It is taken for granted that without having the proper expertise of how hackers do hack, it is obvious that orchestrating remedial measures will be an unrealistic dream. Hence, to protect individual's system and improve organization's security, this course will work as a foundation. It will not be realistic to take that by doing a 4 (four) week course all the techniques and tools of hacking will be discovered. The motto of the course should not be over emphasized. Realistically, it is undeniable that by attending the course and following the assignments and contents the participants will have the interest and the confidence to understand and face the threat from preliminary level of hacking. Moreover, the course will arouse the interest in the participants to move forward and attend more advanced courses on ethical hacking.

What you will learn?

- To start thinking and looking at your network through the eyes of malicious attackers.
- To understand the motivation of an attacker.

- To protect infrastructure from not only outside attackers but also attackers within your company. The terminology used by attackers
- The difference between "hacking" and "ethical hacking"
- The phases of hacking
- The types of attacks on a system, what skills an Ethical Hacker needs to obtain
- Types of security policies
- Why Ethical Hacking is essential
- How to roam around the hacking world
- To know who is a "hacker" and what are the biggest security attack vectors
- How to identify vulnerable
- How to defend attacks
- How to apply ethical hacking

Pre-requisites:

- Primary knowledge of IT, software, website, web hosting, Computer and Networking Hardwares
- Understanding TCP/IP
- Understanding Operating Systems (Windows and Linux)
- At least one year experience on Computer Networking
- No experience needed on Hacking

Course Details:

Class 1: Introduction to Ethical Hacking & Cyber Law

Topic Title	Content
Information Security Terminology	○Hack Value: Notion among hackers that something is worth doing or interesting ○Vulnerability: Existence of a weakness, design, or implementation error that can lead to an expected event compromising the security of the system ○Exploit: A breach of IT system security through vulnerabilities ○Payload: Part of an exploit code that perform the intended malicious action ○Zero-Day Attack: An attack that exploits computer app vulnerabilities before the software developer releases a patch for the vulnerability ○Daisy Chaining: Gaining access to one network and/or computer and then using the same info to gain access to multiple networks and computer that contains desirable info ○Doxing: Publishing personally identifiable information ○Bot: software app that can be controlled remotely to execute or automate pre-defined tasks
Elements of Information Security	○Non-Repudiation: Sender of a message cannot later deny having sent the message ○Confidentiality: Only authorized users able to view content ○Integrity: Trustworthiness of data or resource in prevention of unauthorized changes

Topic Title	Content
	○Availability: assurance systems are accessible ○Authenticity: The quality of being genuine
Information Security Threats and Attack Vectors	●Cloud computing: is an on-demand delivery of IT capabilities, and stores data. Must be secure ●Advanced Persistent Threats: APT focus on stealing info from victim machine w/o user aware ●Viruses and Worms: Capable of infecting a network within seconds ●Mobile Threats: Many attackers see mobile phone as a way to gain access ●Botnet: huge network of compromised systems ●Insider Attack: an attack performed on a corporate network by an entrusted person w/ access ●Threat categories: Network Threats, Host Threats, App Threats ●Types of Attacks: OS Attacks, Mis-Config attacks, App Level Attacks, Shrink Wrap Code Attacks
Hacking Concepts, Types, and Phases	●Hacking: Exploiting system vulnerabilities and compromising se curity ●Five Phases of Hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks ●Reconnaissance: Preparation phase when an attacker seeks to gather information. Does not directly interact with the system, and relies on social engineering and public info ●Scanning: Identify specific vulnerabilities (in-depth probing). Using Port scanners to detect listening ports (companies should shut down ports that are not required) ●Gaining Access: Using vulnerabilities identified during r econnaissance [DoS, Logic/Time Exploit, reconfiguring/crashing system] ●Maintaining Access: Keeping a low profile, keeping system as a launch pad, etc. ●Clearing Tracks: Hiding malicious acts while continuing to have access, avoiding suspici
Information Security Controls	●Information Assurance: Assurance for integrity, availability,confidentiality, and authenticity of info ●Threat Modeling: Risk Assessment approach for analyzing security. 1) Identify Security Objectives 2) Application overview 3) Decompose Application 4) Identify Threats 5) Identify Vulnerabilities ●Network Security Zoning (High to Low): Internet Zone -Internet DMZ Production Network Zone-Intranet Zone -Management Network Zone ●Security Policies are the foundation of security infrastructure ●Info security policy defines basic requirements and rules to be implemented in order to protect and secure organizations information systems ●4 types of security policies ○Promiscuous Policy ○Permissive Policy

Topic Title	Content
	○Prudent Policy ○Paranoid Policy ●Incident Management: set of defined processes to identify, analyze, prioritize, and resolve security incidents ●Types of Vulnerability Assessments: ○Active Assessments ○Passive Assessments ○Host-Based assessment ○Internal Assessment ○External Assessment ○Application Assessments ○Network Assessments ○Wireless Network Assessments ●Methodology of Assessment: -Acquisition -Identification -Analyzing -Evaluation -Reports ●Penetration Testing: Simulating an attack to find out vulnerabilities ●Blue Team: Detect and Mitigate ○Red Team: Attack w/ limited access w/ or w/o warning ●Types of Pen Test: ○black-box (no prior knowledge) ○white-box (complete knowledge) ○grey-box(limited knowledge) ●Lots of open source security testing methodologies (OWASP, NIST , etc)
Information Security Laws & Standards	●Payment card Industry Data Security Standard (PCI-DSS) -Payment Systems ●Sarbanes Oxley Act (SOX) -Protect investors and public by increasing reliability of corporate disclosures

Class 2: Hacking Web Servers

Objectives: Understanding web server concepts, understanding web server attacks, understanding webserver attack methodology, webserver attack tools, countermeasures against web server attacks, overview of patch management, webserver security tools, overview of web server penetration testing

Topic	Detail Description
Web server Concepts	●A web server is a program that hosts websites, attackers usually target software vulnerabilities and config errors to compromise the servers ○Nowadays, network and OS level attacks can be well defended using proper network security measures such

Topic	Detail Description
	as firewalls, IDS, etc. Web servers are more vulnerable to attack since they are available on the web ●Why are web servers compromised ○Improper file/directory permissions ○Installing the server with default settings ○Unnecessary services enabled ○Security conflicts ○Lack of proper security policy ○Improper Authentication ○Default Accounts ○Misconfigs ○Bugs in OS ○Misconfigured SSL certificates ○Use of self-signed certs ●IIS (internet information service) is a webserver application developed by Microsoft for Windows.
Webserver Attacks	●DoS/DDoS Attacks: Attackers may send numerous fake requests to the web server which results in the web server crash or become unavailable ○May target high-profile web servers ●DNS Server Hijacking: Attacker compromises DNS server and changes the DNS settings so that all requests coming towards the target web server is redirected to another malicious server ●DNS Amplification Attack: Attacker takes advantage of DNS recursive method of DNS redirection to perform DNS amplification attack ○Attacker uses compromised PCs with spoofed IPs to amplify the DDoS attack by exploiting the DNS recursive method ●Directory Traversal Attack: Attackers use ../ to sequence to access restricted directories outside of the web server root directory (trial and error) ●Man-in-the middle Sniffing Attack: MITM attacks allow an attacker to access sensitive info by intercepting and altering communications ●Phishing Attacks: Attacker tricks user to submit login details for website that looks legit but it's not. Attempts to steal credentials ●Website Defacement: intruder maliciously alters visual appearance of a web page by inserting offending d

Topic	Detail Description
	ata. Variety of methods such as MYSQL injection ●Web Server Configuration: Refers configuration weaknesses in infrastructure such as directory traversal ●HTTP Responses Splitting Attack: involves adding header data into the input field so that the server split the response into two responses. The attack can control the second response to redirect user to malicious website whereas the other response will be discarded by browser ●Web Cache Poisoning: An attacker forces the web server's cache to flush its actual cache content and sends a specially crafted requests, which will be stored in cache ●SSH Bruteforce Attack: SSH protocols are used to create encrypted S SH Tunnel between two hosts. Attackers can brute force the SSH login credentials ●Webserver Password Cracking: An attacker tries to exploit the weaknesses to hack well-chosen passwords (social engineering, spoofing, phishing,etc). ●Web Application Attacks: Vulnerabilities in web apps running on a webserver provide a broad attack path for webserver compromise ○SQL Injection, Directory Traversal, DoS, Cookie Tampering, XSS Attack, Buffer Overflow, CSRF attack,
Attack Methodology:	Information Gathering, Webserver Footprinting, Mirroring Website, Vulnerability Scanning, Session hijacking, Hacking webserver passwords ●Information Gathering: Robots.txt file contains list of web server directory and files that website owner wants to hide from web crawlers ●Use tools such as burp suite to automate session hijacking
Webserver Attack Tools	●Metasploit: Encapsulates an exploit. ○Payload module: carries a backpack into the system to unload ○Metasploit Aux Module: Performing arbitrary, one-off actions such as port scanning, DoS, and fuzzing ○NOPS module: generate a no-operation instructions used for blocking out buffers ●Password Cracking: THC Hydra, Cain & Abel

Topic	Detail Description
Countermeasures	●An ideal web hosting network should be designed with at least three segments namely: The internet segment, secure server security segment (DMZ), internal network ○Placed the web server in DMZ of the network isolated from the public network as well as internal network ○Firewalls should be placed for internal network as well as internet traffic going towards DMZ ●Patches and Updates: Ensure service packs, hotfixes, and security patch levels are consistent on all domain controllers ●Protocols: block all unnecessa ry ports, ICMPs, and unnecessary protocols such as NetBIOS and SMB. Disable WebDav if not used ●Files and Directories: delete unnecessary files, disable serving of directory listings, disable serving certain file types , avoid virtual directories ●Detecting Hacking Attempts: Run scripts on the server that detects any changes made in the existing executable file. Compare hash values of files on server to detect changes in codebase. Alert user upon any change in detection ●Secure the SAM (stand-alone servers only) ●Defending against DNS hijacking: choose ICANN accredited registrar. Install anti-virus
Patch Management	●Hotfixes are an update to fix a specific customer issue ●A patch is a small piece of software designed to fix problems ○Hotfixes and Patches are sometimes combined for server packs ●Patch Management is a process used to ensure that the appropriate patches are installed on a system to help fix known vulnerabilities ○Before installing a patch, verify the source. ●Patch Management Tools: MBSA (Microsoft baseline Security Analyzer) -checks for available updates to OS, SQL Server, .NET framework etc
Webserver Security Tools	●Syhunt helps automate web app security testing and guards. N Stalker is a scanner to search vulnerabilities
Webserver Pen Testing	●Used to identify, analyze, and report vulnerabilities

Class 3: Designing Secure Web Application

Topics:

- Architecture and Design Issues for Web Applications
- Top issues need to address with secure design practices
- Web Application Vulnerabilities due to Bad design
- Input Validation
- Authentication
- Authorization
- Configuration Management
- Sensitive Data
- Session Management
- Cryptography
- Parameter Manipulation
- Exception Management
- Auditing and Logging

Class 4: Hacking Web Applications

Module Objectives: Understanding Web Application concepts, understanding web app threats, understanding web app hacking methodology, web app hacking tools, understanding web app countermeasures, web app security tools, overview of web app pen testing .

Topic	Detail Description
Web App Concepts	●Web apps provide an interface between end users and web servers through a set of pages ●Web tech such as Web 2.0 support critical business functions such as CRM, SCM
Web App Threats	●Cookie Poisoning: by changing info in a cookie, attackers can bypass authentication process ●Directory Traversal: Gives access to unrestricted directories ●Unvalidated Input: Tempering http request s, form field, hidden fields, query strings, so on. Example of these attacks include SQL injection, XSS, buffer overflows ●Cross Site Scripting: Bypassing client-ID mechanisms to gain privileges, injecting malicious scripts into web pages ●Injection Flaws: Injecting malicious code, commands, scripts into input gates of flawed apps ●SQL Injection: type of attack where attackers inject SQL commands via input data, and then tamper with the data ○LDAP Injection to obtain direct access to databases behind LDAP tree

Topic	Detail Description
	●Parameter/Form tampering: Manipulates the parameters exchanged between client and server to modify app data such as user cred and permissions. ●DoS: intended to terminate operations ●Broken Access Control: method in which attacker identifies a flaw related to access control and bypasses the authentication, then compromises the network ●Cross-Site Request Forgery: attack in which an authenticated user in made to perform certain tasks on the web app that an attacker chooses. ●Information Leakage: can cause great losses to company. ●Improper Error Handling : important to define how a system or network should behave when an error occurs. Otherwise, error may provide a chance for an attacker to break into the system. Improper error can lead to DoS attack ●Log Tampering: Attackers can inject, delete, or tamper with app logs to hide their identities ●Buffer Overflow: Occurs when app fails to guard its buffer property and allows writing beyond its maximum size ●Broken Session management: When credentials such as passwords are not properly secured ●Security Misconfigurations ●Broken Account Management: account update, forgotten/lost password recovery/reset ●Insecure Storage: Users must maintain the proper security of their storage locations ●Platform Exploits: Each platform (BEA WEBLOGIC, COLD FUSION) has its own various vulnerabilities ●Insecure Direct Object References: When developers expose objects such as files, records, result is insecure direct object reference ●Insecure Cryptographic Storage: Sensitive data should be p roperly encrypted using cryptographic. Some cryptographic techniques have inherent weaknesses however ●Authentication Hijacking: Once an attacker compromises a system, user impersonation can occur ●Network Access attacks: can allow levels of access that stan dard HTTP app methods could not grant ●Cookie Snooping ●Web Services Attack: Web services are based on XML protocols such SOAP (simple object access protocol) for communication between web services ●Insufficient Transport layer protection ●Hidden Manipulation ●DMZ protocol attacks ●Unvalidated redirects and forwards ●Failure to restrict URL access ●Obfuscation Application ●Security Management Exploits

Topic	Detail Description
	●Session Fixation Attack: Attacker tricks user to access a genuine web server using an explicit session ID value. Attacker assumes identity of the victim and exploits credentials on the server ●Malicious File Execution
Hacking Methodology	●Hackers first footprint the web infrastructure ○Server discovery, location ●Service Discovery: Scan Ports ●Banner grabbing: footprinting technique to obtain sensitive info about target. They can analyze the server response to certain requests (server identifi cation) ●Detecting Web App Firewalls and Proxies on target site ○Use Trace method for proxy, and cookie response for a firewall ●Hidden Content discovery: Web spidering automatically finds hidden content ●Launch web server attack to exploit identified vulner abilities, launch DoS ●Attacking authentication mechanism ○Username enumeration ■Verbose failure messages. Predictable user names ○Cookie Exploitation ■Poisoning(tampering), Sniffing Replay ○Session Attack ■Session prediction, brute forcing, poisoning ○Password Attack: ■Guessing, brute force ●Authorization attack: finds legitimate accounts then slowly escalates privileges ●Attack Session Management Mechanism: involves exchanging sensitive info between server and clients. If session management is insecure, attacker c an take advantage of flawed session management session ○Bypassing authentication controls ●Perform injection attacks: exploiting vulnerable input validation mechanism implement ●Attack Data connectivity: attacking database connection that forms link between a database server and its client software ○ Connection string injection: attacker injects parameters in a connection string. CSPP attacks (Connection String Parameter Attacks). ○Connection Pool DoS: Attacker examines connection pooling settings and constructs large SQL query, and runs multiple queries simultaneously to consume all connections
Countermeasures	●Encoding Schemes: employing encoding schemes for data to safely handle

Topic	Detail Description
	unusual characters and binary data in the way you intent ○Ex. unicode editing ●How to defend against SQL Injection Attacks ○Limit length of user input ○Perform input validation ●How to defend against xss ○Validate all headers, cookies, strings, form fields. Use firewall ●How to configure against DoS ○Configure firewall to deny ICMP traffic access ○Perform thorough input validation ●How to defend against web services attack ○Multiple layer protection
Tools	●N-Stalker is effective suite of web security assessment tools
Pen Testing	1.Info Gathering 2.Config Management Testing 3.Authentication Testing 4.Session Management testing 5.Authorization Testings 6.Data Validation Testing 7.DoS Testing 8.Web Services Testing 9.AJAX Testing 10.Use Kali Linux tools a.Metasploit

Class 5: SQL Injection

Module Objective: Understanding SQL injection concepts, understanding various types of SQL injection attacks, understanding SQL injection methodology, SQL injection tools, understanding different IDS evasion techniques, SQL injection countermeasures, SQL injection detection tools.

Topic	Detail Description
SQL Injection Concepts	●SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web app for execution by the backend database ○Usually to retrieve information ○This is a flaw in web apps ●Attacker can deface a web page with this attack ●They can add info to your website, extract data, and insert new data

Topic	Detail Description
Types of SQL Injection	●Error based SQL Injection: Attacker puts intentional bad input into app to see the database-level error messages. Uses this to create carefully designed SQL Injections ●Blind SQL Injection: Attacker has no error messages from the system with which to work. Instead, attack simply sends a malicious SQL query to the database ●Whenever you see SELECT, it is probably a SQL command ●Union SQL command, joining a forged query to the original query ●Time-Based SQL Injection: evaluates time delay in response to true-false queries
SQL Injection Methodology	●Information gathering and SQL vulnerability detection ○Attackers analyze web GET and POST requests to identify all input fields ○Afterwards, launch attack ○Advanced SQL injections ●SQL Injection Black Box Pen Testing ○Send single quotes and input data to see where the user input is not sanitized ○Send long strings of junk data to detect buffer overruns ○Used right square bracket as input data
Evasion Techniques	●Evading IDS ○Obscure input strings ○Hex Encoding ○Manipulating whitespace ○Inline Comment ○Char encoding
Countermeasures	●Use Firewalls on SQL server ●Make no assumptions about size, type, or content of the data that is received by the application ●Avoid constructing dynamic SQL with concatenated input values

Class 6: Penetration testing

Material : Book & Slide

Objectives: This Metasploit training class will teach you to utilize the deep capabilities of Metasploit for penetration testing and help you to prepare to run vulnerability assessments for organizations of any size.

- Module 1 - Introduction & Kali Installation
- Module 2 - Metasploit Fundamentals
- Module 3 - Information Gathering
- Module 4 - Vulnerability Scanning

Class 7: Penetration testing

Objectives: This Metasploit training class will teach you to utilize the deep capabilities of Metasploit for penetration testing and help you to prepare to run vulnerability assessments for organizations of any size.

Topics:

- Module 5 - Client Side Attacks
- Module 6 - Post Exploitation
- Module 7 - Maintaining Access
- Module 8 - Metasploit Extended Usage
- Module 9 - Using the Metasploit GUIs

Class 8: Sniffing

Topics:

- Using Wireshark and conclusions
- **Objectives:** Overview of sniffing concepts, understanding MAC attacks, Understanding DHCP attacks, understanding ARP poisoning, Understanding MAC spoofing attacks, Understanding DNS poisoning, Sniffing tools, Sniffing countermeasures, Understanding various techniques to detect sniffing, overview of sniffing pen testing

- **Sniffing Concepts**
  - Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools (form of wire tap)
  - Many enterprises switch ports are open
  - Anyone in same physical location can plug into network with ethernet
  - How a sniffer works
  - Sniffer turns on the NIC of a system to the promiscuous mode that it listens to all the data transmitted on its segment
  - Each computer has a MAC address and an IP address
  - Passive sniffing means through a hub (involves sending no packets), on a hub traffic is sent to all ports
  - Most modern networks use switches
  - Active Sniffing: Searches for traffic on a switched LAN by actively injecting traffic into the LAN. Involves injecting address resolution packets (ARP) into the network
  - Protocols vulnerable to sniffing:
    - HTTP, Telnet and Rlogin, POP, IMAP, SMTP and NNTP
  - Sniffers operate at the Data Link layer of the OSI model

Assignment

1. Theory: Cyber crime, virus, hacking techniques, software and hardware
2. Installation of centos on VMware
3. Solve all Levels of DVWA: Practical
4. Report Using Metasploit ,BURP SUITE, Wireshark