ETHICAL HACKING 50 hours

Ethics and Legality

- Understand ethical hacking terminology.
- Define the job role of an ethical hacker.
- Understand the different phases involved in ethical hacking.

Identify different types o f hacking technologies.

- List the five stages of ethical hacking.
- What is hacktivism?
- List different types of hacker classes.
- Define the skills required to become an ethical hacker.
- What is vulnerability research?
- Describe the ways of conducting ethical hacking.
- Understand the legal implications of hacking.
- Understand 18 U.S.C. § 1030 US Federal Law.

Footprinting

- Define the term footprinting.
- Describe information-gathering methodology.
- Describe competitive intelligence.
- Understand DNS enumeration.
- Understand Whois, ARIN lookup.
- Identify different types of DNS records.
- Understand how traceroute is used in footprinting.
- Understand how email tracking works.
- Understand how web spiders work.

Scanning

- Define the terms port scanning, network scanning, and vulnerability scanning.
- Understand the CEH scanning methodology.
- Understand ping sweep techniques.
- Understand nmap command switches.
- Understand SYN, stealth, XMAS, NULL, IDLE, and FIN scans.
- List TCP communication flag types.
- Understand war dialing techniques.
- Understand banner grabbing and OF fingerprinting techniques.
- Understand how proxy servers are used in launching an attack.
- How do anonymizers work?
- Understand HTTP tunneling techniques.
- Understand IP spoofing techniques.

Enumeration

- What is enumeration?
- What is meant by null sessions?
- What is SNMP enumeration?
- What are the steps involved in performing enumeration?

System Hacking

- Understanding password cracking techniques.
- Understanding different types of passwords.
- Identify various password cracking tools.

- Understand escalating privileges.
- Understanding keyloggers and other spyware technologies.
- Understand how to hide files.
- Understand rootkits.
- Understand steganography technologies.
- Understand how to cover your tracks and erase evidence.

Trojans and Backdoors

- What is a Trojan?
- What is meant by overt and covert channels?
- List the different types of Trojans.
- What are the indications of a Trojan attack?
- Understand how Netcat Trojan works.
- What is meant by wrapping?
- How do reverse connecting Trojans work?
- What are the countermeasure techniques in preventing Trojans?
- Understand Trojan evading techniques.

Sniffers

- Understand the protocols susceptible to sniffing.
- Understand active and passive sniffing.
- Understand ARP poisoning.
- Understand ethereal capture and display filters.
- Understand MAC flooding.
- Understand DNS spoofing techniques.
- Describe sniffing countermeasures.

Denial of Service

Understand t he types of DoS attacks.

- Understand how a DDoS attack works.
- Understand how BOTs/BOTNETs work.
- What is a Smurf attack?
- What is SYN flooding?
- Describe the DoS/DDoS countermeasures.

Social Engineering

- What is social engineering?
- What are the common types of attacks?
- Understand dumpster diving.
- Understand reverse social engineering.
- Understand insider attacks.
- Understand identity theft.
- Describe phishing attacks.
- Understand online scams.
- Understand URL obfuscation.
- Social engineering countermeasures.

Session Hijacking

- Understand spoofing vs. hijacking.
- List the types of session hijacking.
- Understand sequence prediction.
- What are the steps in performing session hijacking?
- Describe how you would prevent session hijacking.

Hacking Web Servers

- List the types of web server vulnerabilities.
- Understand the attacks against web servers.
- Understand IIS Unicode exploits.
- Understand patch management techniques.
- Understand Web Application Scanner.
- What is the Metasploit Framework?

- Describe web server hardening methods.

Web Application Vulnerabilities

Understand h
- ow a web application works.
- Objectives of web application hacking.
- Anatomy of an attack.
- Web application threats.
- Understand Google hacking.
- Understand web application countermeasures.

Web-Based Password-Cracking Techniques

- List the authentication types.
- What is a password cracker?
- How does a password cracker work?
- Understand password attacks—classification.
- Understand password cracking countermeasures.

SQL Injection

- What is SQL injection?
- Understand the steps to conduct SQL injection.
- Understand SQL Server vulnerabilities.
- Describe SQL injection countermeasures.

Wireless Hacking

- Overview of WEP, WPA authentication systems, and cracking techniques.
- Overview of wireless sniffers and SSID, MAC spoofing.
- Understand rogue access points.
- Understand wireless hacking techniques.
- Describe the methods in securing wireless networks.

Virus and Worms

- Understand the difference between a virus and a worm.
- Understand the types of viruses.
- How a virus spreads and infects the system.
- Understand antivirus evasion techniques.
- Understand virus detection methods.

Physical Security

Physical security b
- reach incidents.
- Understand physical security.
- What is the need for physical security?
- Who is accountable for physical security?
- Factors affecting physical security.

Linux Hacking

- Understand how to compile a Linux kernel.
- Understand GCC compilation commands.
- Understand how to install LKM modules.
- Understand Linux hardening methods.

Evading IDS, Honeypots, and Firewalls

- List the types of intrusion detection systems and evasion techniques.
- List firewall and honeypot evasion techniques.

Buffer Overflows

- Overview of stack based buffer overflows.
- Identify the different types of buffer overflows and methods of detection.
- Overview of buffer overflow mutation techniques.

Cryptography

- Overview of cryptography and encryption techniques.
- Describe how public and private keys are generated.
- Overview of MD5, SHA, RC4, RC5, Blowfish algorithms.

Penetration Testing Methodologies

- Overview of penetration testing methodologies.
- List the penetration testing steps.
- Overview of the Pen-Test legal framework.
- Overview of the Pen-Test deliverables.
- List the automated penetration testing too