

Agenda for eight days hands on cyber security workshop– Online


Day 1 (2 hours)

- Introduction to cyber security
 - **Why** Cyber Security:
 - Types of hackers/attackers:
 - **What** is Cyber Security:
 - Explanation and demonstration of what we protect (Data & Infrastructure) and how we protect (through controls).
 - Cyber Security Controls.
 - Explanation about various security standards, laws and regulations that are being followed.
 - Explanation of cyber security domains in detail.
 - **How** attacks happen:
 - Explanation about vulnerability, types, affected platforms
 - Common Vulnerability Exposure walkthrough and other major vulnerability walkthrough
 - Cyber Security in the organization:
 - Overview of various cyber security teams and departments
 - Overview of various cyber security roles

Assessment:

1. Make research on any 5 vulnerabilities and prepare a report of the vulnerability
2. Make research on any 3 cyber-attacks and prepare a report of how the attack was performed (i.e., details of the flaws), the loss occurred and what was compromised.

There would be viva taken on the submitted reports.




Day 2 (2 hours)

- Explanation and demonstration of below protocols:
 - HTTP, HTTPS and it's certificates
 - FTP, DNS, SMTP
 - TCP, UDP
- Cryptography
- Explanation of Cyber Security Attacks
 - Eavesdropping attack demonstration: Hands on practical demonstration using Wireshark tool
 - Demonstrating Eavesdropping attack using www.testfire.net website which runs on HTTP protocol.
 - Similarly, demonstrating the same attack on a website which runs on HTTPS protocol which encrypts the data.
 - Social Engineering attack demonstration:
 - Various social engineering attacks
 - Explanation and demonstration by creating an identical website
 - Demonstration of Phishing attack by creating a fake Instagram login page

Assessment:

1. Prepare a step by step report of the Eavesdropping attack along with screenshots for each step.
2. Pick up any 5 protocols that would appear in the Wireshark tool, make a thorough research and submit the report.
3. Prepare at least 4 scenarios of any Social Engineering attacks.




Day 3 (2 hours)

- Explanation of Proxy and VPN in detail with demonstration
- Man-In-The-Middle - Hands on practical demonstration using BurpSuite tool
 - Creating a proxy server in the system and then configuring the server in the BurpSuite tool to perform the attack.
- DoS and DDoS attack
 - Types of DoS attack
 - Botnets
- Netstat command demonstration
- Working of PING command and ICMP protocol

Assessment:

1. Prepare a step by step report of the MITM attack along with screenshots for each step.
2. Make a research on the other functionalities of the BurpSuite tool.
3. Research on how to prevent and control a DDOS attack and submit the report.




Day 4 (2 hours)

- Networking:
 - Explanation of
 - Networking, IP address, IP Classes, Private & Public IP
 - Demonstration of world wide networking using the website www.submarinecablemap.com.
 - Designing and configuring a client-server based network model using Cisco Packet Tracer tool.
- Network Security
 - Demonstration of Firewall working
 - Defense in Depth
 - SIEM working
- Information Classification & it's Schema
- Steganography:
 - Explanation of Steganography concepts – Hiding a digital content into another digital content.
 - Where Steganography is used and the working of Steganography.
 - Demonstration of Steganography using OpenStego tool.

Assessment:

1. Configure a network design with 2 Desktops, 2 PC's, a web server and a DHCP Server. Assign IP address to each and bring the network up.
2. Make a research on various network security devices, its working and purpose and prepare a report.
3. Prepare a report on the different types of Firewalls.
4. Install any one open source firewall on your system.




Day 5 (2 hours)

- Ethical Hacking
 - Difference between Hacking and Ethical Hacking
 - Explanation of Section 66 of the IT ACT 2000
 - How is ethical hacking done – By explaining the different phases at a high level
- Vulnerability Assessment and Penetration Testing
 - VAPT types
 - Various cyber security testing
 - VAPT report walkthrough
- Cloud Technology and Cloud Security

Assessment:

1. Prepare a list of at least 3 tools that are used at each stage of Ethical Hacking
2. Choose any 5 sections from the IT ACT 2000 and prepare a report along with case scenarios




Day 6 (2 hours)

- Ethical Hacking Phase 1 – Reconnaissance
 - Explanation of Active and Passive reconnaissance.
 - Active Reconnaissance: Here we will be using various tools for gathering information:
 - Nmap – nmap is a tool used to collect information of a network or a host machine. Information gathered such as open ports, services running, OS, OS versions, network topology and so on
 - Who.is – who.is and there are similar other websites which provides details of the IP address, hosting provider, website update details and so on
 - Other information gathering tools such as BurpSuite, people search, Nslookup, dnsdumpster
 - Sublister tool for finding subdomains
 - DNSRecon tool to gather DNS record details
 - Theharvester tool to information from public sources
 - Passive Reconnaissance: Gathering information via human visualizing
 - Demonstration of collecting information from various sites
 - Explanation of Dumpster diving

Assessment:

1. Perform Reconnaissance on your network and prepare a report of the information gathered.
2. Perform Reconnaissance of your own profile and prepare a report of the information that is available in the public domain.




Day 7 (2 hours)

- Ethical Hacking Phase 2 – Scanning
 - Scanning refers to finding vulnerabilities in a website
 - OWASP ZAP – Tool used for finding OWASP vulnerabilities in a website
 - Vega Scanning Tool
 - Acunetix Scanning Tool
- Introduction to OWASP Top Ten
 - Overview of OWASP TOP 10 vulnerabilities:
 - Injection
 - Broken Authentication and Session Management
 - Sensitive Data Exposure
 - XML External Entity
 - Broken Access Control
 - Security Misconfiguration
 - Cross-Site Scripting (XSS)
 - Insecure deserialization
 - Using Components With Known Vulnerabilities
 - Insufficient Logging and Monitoring
- Demonstration of SQL Injection attack
- Demonstration of XSS attack

Assessment:

1. Prepare a list of various scanning tools available
2. Do a thorough study on any of the two OWASP vulnerabilities and prepare a report on exploiting the vulnerability using DVWA.



Day 8 (2 hours)

- Ethical Hacking Phase 3 & 4 – Gaining Access and Maintaining Access
 - Demonstration of Metasploit tool for creating a payload
 - Explanation of how payloads can be created and transferred for various platforms
 - Hacking into an android phone
 - Hacking Windows machine
- Ethical Hacking Phase 5 – Clearing Tracks
 - Explanation of Log management in Windows platform
 - Demonstration of Windows Log Management
- Demonstration of Social Media account takeover attack
- Bug Hunting