UNIT 9 – Securing Online Components

9.1 Interactive Web Vulnerabilities – 4 days
1. Contrast old stateless websites versus current stateful sites that provide interactive features.
2. Define how interactive features in websites create vectors for attacks.
3. Identify vulnerabilities in session management tools including cookies, URLs, and form fields.
4. Investigate proxy software as a tool for both security professionals and threat actors.

Activities: (L) Using Burp Suite, (L) Spoofing a Cookie, (L) Gruyere Cookie Manipulation, (L) CTF challenges

UNIT 8 – Network & System Threats

8.1 Denial of Service (DoS) – 2 days
1. Apply CLI commands to troubleshoot network connections.
2. Define Denial of Service attacks and techniques/tools.
3. Evaluate methods and tools to identify and secure against DoS attacks.

Activities: (A) Paper balls DDoS, (L) SYN Flood DoS Attack

8.2 Spoofing & Sniffing – 3 days
1. Define IP spoofing and identify limitations of this attack technique.
2. Examine methods of sniffing on a Local Area Network.
3. Define Man in the Middle (MITM) attacks.
4. Review methods of protecting against IP spoofing and sniffing attacks.

Activities: (A) Paper ball Smurf attack; (L) ARP Spoofing for MITM Attack

8.3 Wireless, Mobile & VPNS – 5 days
1. Define wireless technologies of WiFi, Bluetooth, and Cellular.
2. Identify vulnerabilities of wireless devices and common threats.
3. Define and apply best practices to secure wireless transmissions including VPNs.
4. Review methods of protecting against IP spoofing and sniffing attacks.
5. Identify methods for securing against Web Search reconnaissance.
6. Explore Metasploit as both a pentesting and an attack tool.

Activities: (L) Recon with WHOIS & Nslookup tools

8.4 Pentesting & Exploits – 5 days
1. Define Pentesting and the characteristics of digital exploits.
2. Examine types of attacks that can be executed using networked systems.
3. Identify how pivoting in a network can provide transitive access.
4. Explore Metasploit as both a pentesting and an attack tool.
5. Define Metasploit and Armitage based attacks, (A) Google Dorking using Metasploit – circle back (L) Password Cracking & Capture

8.5 Cyber War – 4 days
1. Examine definitions of Cyberwarfare.
2. Review and compare the use of cyber tools by nation states.
3. Analyze the facts of how EternalBlue, an NSA tool, was stolen and the global impact of this event.
4. Students use courtroom roleplay to determine who is to blame for the damage caused by EternalBlue.

Activities: (G) Trial of EternalBlue

UNIT 7 – Reconnaissance

7.1 Recon Intro and Google Dorking – 3 days
1. Define techniques for reconnaissance of digital targets.
2. Identify and apply advanced operators for Google searches.
3. Investigate the Google Hacking Database (GHDB).
4. Define use of robots.txt files for websites and for reconnaissance.
5. Identify method for securing against Web Search reconnaissance.

Activity: (L) Recon with Google worksheet

7.2 WHOIS and Nslookup – 4 days
1. Understand organizations that support the Internet addressing structure.
2. Examine the characteristics of the WHOIS databases.
3. Identify how the WHOIS database information can be used for Recon.
4. Review the characteristics of the Domain Name System.
5. Examine the nslookup tool for retrieving name/ip address information.
6. Identify how DNS information can be used for Recon.

Activity: (L) Recon with WHOIS & Nslookup tools

7.3 Network Scanning – 6 days
1. Examine how a subnet mask identifies to which network an IP address belongs and how subnetting can provide network segmentation.
2. Identify the IP addresses that are reserved for special functions.
3. Examine the characteristics and goals of network scanning as a recon technique.
4. Interpret scan results to identify operating systems, open ports and running services on a system.
5. Identify methods for securing against network scanning recon.

Activities: (G) Infection Detention (L) Nmap in CLI and Zenmap,
UNIT 10 – Security Tools & Techniques

10.1 Network Defense – 4 days
1. Examine and compare Defense in Depth vs Zero Trust theories...
2. Identify and configure tools for network segmentation including VLANS, DMZ and airgap.
3. Define characteristics of email defensive controls - SPF, DKIM and DMARC.
Activities: (A) Verizon Data Breach Investigation, (L) Applying CIS Controls, (L) Packet Tracer Network Configuration, (A) Who’s got Mail Controls?

10.2 Monitors and Alarms – 3 days
1. Evaluate tools for monitoring and access control including Firewalls, IDS and ACLs.
2. Examine how honeypots can be used to detect and analyze attacks.
Activities: (L) Configure ACL on Firewall, (L) Build a Honeypot

10.3 Encryption for Online Security – 6 days
1. Define symmetric encryption and characteristics of strong encryption including entropy and publicly published algorithms.
2. Examine asymmetric encryption and impact on key exchange security.
3. Identify how SSL / Internet use both symmetric and asymmetric to secure data in transfer.
4. Define Digital Signatures and examine impact of cryptocurrency on threat actors and cybersecurity.
Activities: (G) Invent method to exchange secret keys (A) Using Prime numbers to prove KeyPairs, (L) NDG Lab Connecting to Remote computer, (G) Bitcoin Insecurity.