Intro to Cybersecurity - Course Map

Course Notes:

- 1 day is ~ a 42-45 minute lesson that meets 5 days per week
- Lessons have several types of learning outside of lecture. These abbreviations are used as a reference:
  (G) Group activity) (L) Lab online (D) Discussion (A) Activity

UNIT 1 FOUNDATIONS & THREATS

0.1 First Day Info & Ethics Agreement – 1 day

1. Careers – introduction to reasons for pursuing cybersecurity career and motivations such as job demand, protect society, income, etc.
2. Review what will be covered in class – objectives handout to determine what students find most and least interesting
3. Ethics agreement – (G) group work to create a Code of Behavior. Present and discuss why we need one. Review real Ethics Agreement for understanding of expectations and consequences.

1.1 CIA Triad and Authentication – 7 days

1. Cybersecurity goal is to protect CIA of data at rest, in transit and in use.
2. Define Authentication as a key tool - explore methods including strong passwords, tokens, MFA and biometrics
3. Identify attacks on passwords and use of salted hashes as defense.

Activities: (L) Testing passwords, (L) Have You Been Pwned (L) CyberChef tool to hash & salt with CyberChef Intro Video (A) Create safe password poster, (G) Which Authentication project.

1.2 Identifying Security Threats – 6 days

1. Define types of malware and the complexity of threats
2. Examine impact on systems and on people.
3. Summarize the best practices for protecting against malicious software

Activities: (A/G) Historic Malware Research/Presentation , (L) Rapper or Malware online game

1.3 Intro to Command Line – 6 days

1. Define difference between GUI and CLI
2. Learn basic terminal commands in Linux
3. Introduce Virtualization and how to use the course VMs

Activities: (L) Terminus game part 1, (L) Try It follow along with PPT

UNIT 2 HUMAN FACTOR

2.1 Social Engineering – 2 days

1. Define steps hackers take in an attack
2. Define and explore social engineering as the human risk

Activities: (G or L) 7 Steps of an Attack – sorting, (L) CS Interactive: Social Engineering (L) Social Engineering Toolkit on Ubuntu

2.2 Phishing & OSINT – 6 days

1. Define phishing, characteristics and specialized types.
2. Define Open Source Intelligence (OSINT) and explore the tools used in OSINT.
3. How to mitigate human risk – policies, awareness training, etc.

Activities: (L) Phishing test, (A) OSINT on Tony Stark, (L/A) Phishing Myself project, (L/G) Clean Desk Policy Mistakes

UNIT 3 DATA SAFETY & BEST PRACTICES

3.1 Securing the System – 7 days

1. Define Vulnerability and Exploit – use Darknet Diaries podcast (abbreviated) for story on these topics.
2. Examine how the Common Vulnerability and Exposure database can be used as a research tool.
3. Review and apply the recommended Best Practices configurations for typical PCs.

Activities: (G) Product Analysis with CVE (L) CIS-CAT Scan + Hardening, (A) Bingo Securing the System, (L) Hardening Backups, Users & Applications, (A) CyberPatriot Demo system.

3.2 Threat Modeling & IOT – 2 days

1. Understand Threat Modeling to determine what risk you are wiling to take and what effort you are willing to put in to secure against threats.
2. Examine vulnerabilities of home Internet of Things (IOT) – Smart devices such as voice assistants, baby monitors, home routers, etc.

Activities: (G) Home IOT SPOONS Game (A) My IOT Threat Model worksheet

UNIT 4 CRYPTOGRAPHY & LINUX

4.1 Bits, Binary, & Encoding – 7 days

1. Define bits, bytes and binary number system as computer language
2. Define hexadecimal numbers, use in computing
3. Define encoding and differences from encryption
4. Introduce using Capture The Flag challenges for practice.

Activities: (L) online Binary game; (A) Convert between Decimal, Binary and Hex numbers; (L) Decoding with CTF challenges. Resource set of ways to learn binary and hex numbers.

4.2 Basic Cryptography Concepts – 6 days

1. Define terminology for cryptography
2. Define key methods of encryption and examine classic algorithms including Caesar, Transposition and Vigenere
3. Define Steganography and tools to find hidden data – hex editor, steghide, Cyberchef, Exifdata, binwalk

Activities: (G) Breaking Ciphers , (A) Vigenere Try It – AL will improve flow (G) Scavenger Hunt, (L) Steganography CTF

4.3 Advanced Linux CLI – 5 days

1. Review basic terminal commands in Linux and Windows
2. Advanced terminal commands in Linux
3. Create simple bash scripts that demo cybersecurity impact on device

Activities: (L) Terminus game part 2, (L) Try It follow along with PPT, (L) Searching with Grep (L) Shell scripting in Linux

4.5 Privacy vs Security – 4 days

1. Define difference between privacy and security
2. Review facts of case where FBI demanded access to encrypted iPhone
3. Watch excerpts from debate on the privacy vs security concepts – Fareed Zakaria (NY Times) and Edward Snowden (NSA hacker)
4. Student teams debate same topic: Government should have lawful access to any encrypted message or device

Activities: (G) Class debate

UNIT 5 DEVICES AND NETWORKS

5.1 Computer Components – 2 days

1. Device key components – Input, Memory, CPU, Output plus Motherboard. What can go wrong?

Activities: (L) Virtual Desktop Build a PC.

5.2 Networking Fundamentals – 6 days

1. Networking devices and topologies – WAN, LAN, routers, switches.
2. Define network naming – Mac vs IP addresses (basic formatting of IP addressing and subnetting) , IPv4 & IPv6

Activities: (L) ARP with Wireshark, (A) Network Puzzles (L) CS Interactives: Pizza Party (review of Mac/IP addressing).

5.3 Protocols and Packets & Getting to the Internet – 4 days

1. Define packet switching as network method of communication.
2. Define protocols, TCP/IP Suite, ports, 3-way handshake

3. Analyze network packet traffic

Activities: (G) Mobster Net (L) Wireshark Packet Analysis

END OF PART 1 PROJECTS

1. Which Authentication – Sales Pitch of Biometric Technology
2. Social Engineering PSA video
3. Benchmark Selections for OS Hardening
4. Making an Impact with Cybersecurity Technology
5. Ethics - pending

UNIT 6 – LAW & ETHICS

6.1 Law & Ethics – 3 days

1. Explore ethical issues associated with information security.
2. Examine the laws and rules concerning digital data and online activities.

Activity: (G) Cyber Crime & Punishment posters

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. Define Swatting & Doxing and recognize these are 'real-life' attacks that involve cyber tools.
2. Examine information required to get a domain/website on the Internet.
3. Examine characteristics of the Whois database and its use for Recon.
4. Identify mitigation steps for Whois Recon and threats of Doxing/Swatting.
5. Review the characteristics of the Domain Name System.
6. Examine the nslookup tool for retrieving name/ip address information.

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 of network scanning as a recon technique.
4. Interpret scan results to identify system OS, open ports and services.
5. Identify methods for securing against network scanning recon.

Activities: (G) Infection Detention (L) Nmap in CLI and Zenmap,

UNIT 8 – NETWORK & SYSTEM THREATS

8.1 Denial of Service (DoS) – 3 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 Adversary in the Middle (AiTM) attacks.
4. Define spoofing based attacks including ARP Poisoning, IP Spoofing and DNS Spoofing.
5. Review methods of protecting against IP spoofing and sniffing attacks.

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

8.3 Wireless, Mobile & VPNs – 3 days

1. Review 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.

Activities: (L) Securing Messages with Encryption

8.4 Pentesting & Exploits – 6.5 days

1. Define Pentesting and the characteristics of digital exploits.
2. Examine types of attacks that can be executed using networked systems.
3. Explore Metasploit as both a pentesting and an attack tool.
4. Define exfiltration, privilege escalation and persistence steps in an attack.
5. Understand the source of exploit tools.
6. Examine how threat hunting tools can be applied to find and kill malware.

Activities: (L) Exploring Metasploit, (L) Exfiltration with Mimikatz, (L) Post-Exploitation, (L) Hunting a Backdoor.

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.

UNIT 9 – SECURING ONLINE COMPONENTS

9.1 Web Basics – 1 day

1. Define the key components to make a website work.
2. Review and apply tools to investigate a website..

Activities: (L) Exploring Developer Tools

9.2 Web Vulnerabilities – 4 days

1. Define concept of stateless vs stateful web design.
2. Examine session management methods including cookies.
3. Identify methods of cookie theft and the possible consequences.
4. Define user input as a key source of web vulnerabilities.
5. Identify the characteristics of command injection attacks and script injection attacks.
6. Define input validation as a means of mitigation for web code attacks.

Activities: (L) Cookie Manipulation, (L) Command Injection & XSS, (L) CTF example challenges.

9.3 Databases & SQL Injection– 2 days

1. Define databases and SQL (Structured Query Language).
2. Identify the steps in a SQL injection attack.
3. Define mitigation techniques for SQL Injections Attacks

Activities: (L) SQL Injection

UNIT 10 – ENCRYPTION SECURITY TOOLS

10.1 Symmetric & Asymmetric Encryption – 4 days

1. Define vocabulary terms and methods of symmetric encryption.
2. Examine components to create strong encryption algorithms and symmetric encryption functions.
3. Understand how asymmetric encryption solves the issue of key exchange.
4. Examine Asymmetric cryptographic components including keypairs.
5. Identify cryptography software tools to secure data in transfer, in storage and at rest.

Activities: (G) Creating a Key Exchange Method (A) Investigating RSA Keypairs

10.2 SSL for Online Security – 2.5 days

1. Define creation and use of digital certificates
2. Examine how SSL/TLS and digital certificates are used to ensure secure web communications
3. Identify vulnerabilities in secure web transactions using SSL or TLS

Activities: (L) Decrypt SSL