UNIT 1 FOUNDATIONS & THREATS

0 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. Define 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 willing 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

START CYBERSTART AMERICA OR PICOCTF OR ANY OTHER ONLINE CHALLENGES
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 YEAR 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