Week 1:

Introduction to Cybersecurity: Realities of work, analysis, Attack frameworks (mitre, etc), job aspects.

Phishing/Spam: Fake logins, banking “Your computer has been hacked”, etc.

Malware: Trojans, spyware, adware, PUM/PUP (Potentialy unwanted (malware/programs)), worms, CVE, What is a vulnerability.

Week 2:

Attack: Information Gathering and Fuzzing

NMAP, NESSUS, Openvas, Dig, Fierce, enum4linux,etc. This is 90% of any threat hunt, Pen test, forensics, etc. Interpreting results. (Scanning laws in different countries, public v private). Open source intelligence should be mentioned.

Week (3): Attack: Web Application Analysis

Burp suite, Nikito, OWASP, PHP, ASPX, more CVES

Week (4): Attack: SQL Injections

SQLmap, SQLninja,

Week 5: Attack: ~~Distributed~~ Denial of Service

Low orbit ion cannon, Slowloris, Sockstress, etc. Types of dos, Network, memory, processor, DNS reflection. Etc. Many newly discovered exploits are first tested as a POC with DOS payloads to crash the machine, or process.

Week 6: Defense: Monitoring and Analytics Packages

Take a look at Security onion, it is an excellent OS that contains tons of open source monitoring and IPS/IPS software. Additionally Graylog is a great logging tool.

Week 7: Defense: Hard Drive Forensic Tools, Wireshark I

photorec, sleuthkit, etc.

Wire shark should focus on analyzing simple things: ICMP (Packet size, amount), http requests. Port and host filtering.

Week 8: Defense: Wireshark II, Encryption

possibly more complex wireshark, DNS, https, UDP etc.

Asymmetric, vs symmetric vs Hash. DO NOT EMPHASIZE MATHEMATICS, If math is to be mentioned, mention prime numbers and primitive roots. Matrix multiplication can be confusing.

Week 9: Attack: Pen Testing Suites and Kali Linux

Metasploit, basic commands, running nmap from Metasploit. Possibly adding more modules,(Reminder that linux is not more secure than windows.) Metasploit is tool used by good and bad actors. It is a powerful tool, that CAN get you in trouble at your place of work. Do not use in public areas.

Week 10: Group Project I, Compliance

PCI-DSS, Hippa/hitta, Mitre ,etc.

Password strength, Patch management, (if you haven’t already go over the 4th amendment)

Week 11: Group Project II

Week 12: Group Project Presentations

Notes there is to much to go over in 12 weeks, Focus either on lots of stuff in general or half as much in depth. It’s good to mention that cybersecurity professionals need to be proficient in many aspects of tech. Additionally cyber security requires CONSTANT studying to stay up to date, however a deep understanding of how computers work can compensate. For example, Understanding how the memory stack and heap work can greatly help in the understanding of Buffer overflow and Heap spray attacks. Because these are Memory based attacks additional studying is rarely needed.

it’s also good to mention how fucking stressful cybersecurity is. If needed I can come in a few times to talk about my experiences. Or do guest lecturing. Hell if time permits I can come by for weeks 10 through 12 and help with group projects.

If you’d like we can schedule a time and we can go over more ideas and hammer our more details for each week.