Operating System Commands

What command can be used to find printable characters within a file (NOTE: typically used on binary or non-text files)?

“Cat -v” or “od -c”

Networking

Last week you researched proxies, this week the question is: what are two different ways proxies manage IP addresses of their clients?

- Forward and reverse proxies

Security Principles

Last week you determined the difference between vulnerability assessments and penetration tests. This week let’s look at a third: red teaming. From an assessment/engagement aspect, what’s the difference between a red team exercise and a penetration test?

 Penetration testing seeks to identify application layer flaws, network and system level

flaws and opportunities to compromise physical security barriers too. While, red team operation involve more people, resources and time as they dig deep to fully understand the realistic level of risk and vulnerabilities against an organizations technology, human and physical assets.

Cyber Threat Intelligence

Identify and define the 4 points of the Diamond Model of Intrusion Analysis.

Adversary- BadGuy persona:email addresses, handles, phone #’s, network assets

Capabilities- Malware, Exploits, Hacker Tools, Stolen Certs

Victim- Personas, Network Assets, Email Addresses

Infrastructure- IP addresses, domain names, email addresses