CYBR-1200 Security+ Certification

Week 1 Playbook Entry: Introduction to Security and Malware Attacks

Summary of Key Concepts

Cybersecurity is the practice of protecting digital assets from cyberattacks. Information Security is a high-level plan an organization uses to make sure it's data is protected.

Information Security relies on three crucial components: confidentiality, integrity and availability. These basic tenets are lovingly referred to as the "CIA Triad" and form the platform of a strong Information Security strategy.

Key Takeaways

- Threat vectors are targets to be attacked and threat actors are the attackers
- Frameworks provide guidelines for organizations to outline and implement their own policies and procedures
- A very popular threat vector is humans, it is easy to take advantage of our naivety and emotion
- A list of threat actors includes: unskilled attackers, Shadow IT, Organized Crime, Insider Threats, Hacktivists, Nation-State Actors, Competitors, Brokers, and Cyberterrorists

Tools and Techniques Used

Haveibeenpwned.com – for checking if our email shows up in a database that's been compromised.
Nmap – network scanner
Defender Firewall – a windows firewall

Lab Summary

Lab 3-1: Data Protection Strategies
- **Objective:**
  To discover unnecessary ports and close them using a OS native firewall
- **Steps Performed:**
  First we opened up web and mysql ports on one machine, used nmap to scan for them on another machine and then used windows firewall to close those ports
- **Results:**
  We wouldn't be able to breach any vulnerabilities on the web or mysql ports if there was a vulnerability
- **Reflection:**
  Nmap is still the tool to use for port scanning
  Windows has a native firewall, that's new to me.

There was another lab I believe where we installed an old version of Adobe Reader and tried to exploit it's vulnerability – but it's vulnerability was tied to WindowsXP and not Windows11 –so nothing malicious happened but we got to see how to breach a threat vector.

Real-World Application

IIS is a web server that's had many vulnerabilities over the years. People use those vulnerabilities to take down the webserver, or hack into it to display their own agenda on a companies website

Questions or Future Goals

It would be fun to learn what it takes to do network audits