Week 2 PlayBook Entry- Common Security Threats, Vulnerabilities and Cryptography

Key Components

-Phishing attacks- A social engineering tactic where attackers send misleading emails or messages to trick users into revealing sensitive information.

-**DDoS (Distributed Denial of Service) attacks-** Overwhelming a network or server with traffic, making it inaccessible to legitimate users.

Key Takeaways

- **Distributed Denial of Service (DDoS)-** is an attack of one form of cybercrime where a website or server is overloaded with excessive internet traffic, rendering it inaccessible. DDoS attacks are a more massive version of Denial of Service (DoS) attacks.
- **Phishing attacks-** Is a specious method where attackers send convincing emails, texts, or other messages to deceive users into disclosing sensitive information such as passwords, credit card numbers, or personal details by pretending to be a trusted source. The goal is typically to steal money or gain unauthorized access to systems.
- **Authentication-** Is a process that verifies a user's identity before they can access a system or network. It's a key step in protecting systems from unauthorized access.

Tools

TryHackMe

Virtual Lab Environment

Lab Summary

Lab 3-1 Data Protection Strategies- I learned important concepts and techniques for securing data in a virtualized environment. The focus is on the 3-2-1 backup strategy which recommends creating at least three copies of data, two stored on different types of media and one kept off site. This approach helps protect against data loss due to hardware failures, system crashes, or disasters.

lab 4-1 cryptographic solutions- I Learned a cryptographic solution is a practical application of cryptography to a security goal. Cryptographic solutions are often computer programs that use cryptographic protocols and cryptosystems.

Real World scenario

An online banking platform where a user's login credentials are compromised through a scam email, allowing an attacker to access their account due to weak password practices, which could then lead to unauthorized transactions if the bank doesn't implement strong protection of sensitive financial data.

Goals

KEEP LEARNING !