CYBR-1200 Security+ Certification

Week 2 Playbook Entry: Fundamentals of Cryptography and Advanced Cryptography

Summary of Key Concepts

Cryptography is used as a mitigation technique to protect information and to harden systems making them more resilient to attacks. It provides security protections for the base CIA triad as well as adding two other security characteristics, non-repudiation and obfuscation. Note: obfuscation pertaining to specifically data; not as a part of network security.

Digital Keys and the Public Key Infrastructure provide a way for us to have secure communications within many things including email, voip, web servers, blockchain, vpn, and ssh.

Key Takeaways

- Different algorithms accomplish different tasks.
- Asymmetric cryptography uses a pair of related keys.
- A digital certificate is a technology used to associate a user's identity to a public key and has been digitally signed by a trusted third party. This third party verifies the owner and that the public key belongs to that owner.
- .pem is the file extension for PKI .. further research shows it stands for Privacy Enhanced Mail. I have always used .key or something.

Tools and Techniques Used

"cipher"
"openssl" command in linux
"certutil" command in windows
Alma linux itself was used – which is a new one to me.. meaning that CentOS has gone to pasture and RHEL has changed their ways.

Lab Summary

Lab 3-1: Data Protection Strategies
- **Objective:**
  To encrypt, hash and obfuscate data
- **Steps Performed:**
  We used commands to encrypt and hash files, and a website to obfuscate data
- **Results:**
  Discovered that the more complex the hash algorithm, the longer the output is
- **Reflection:**
  Learned to encrypt files on both linux and window systems and that the visual basic interpreter still ran the obfuscated program.

Real-World Application

I used OpenPGP to send emails to a group of us that managed servers and we had to share sensitive information. We didn't need admin passwords moving in the clear.

I've setup secure web servers for ecommerce and used SSH Tunneling to add encryption to VNC, used SSH keys to not have to remember passwords to my boxes.

Questions or Future Goals

I would like to become a part of CACert again
I would like to spin up Alma linux and give it a try
I would like to get back into using OpenPGP - I'm happy to hear they have a plugin for K9mail on Android