CYBR-1200 Security+ Certification

Week 2 Playbook Entry: Fundamentals of Cryptography and Advanced Cryptography

Summary of Key Concepts

Cryptography is the backbone of cybersecurity. It provides the tools and techniques used to ensure the confidentiality, integrity, and availability (CIA) triad and adds two other security characteristics, non-repudiation and obfuscation. It uses techniques like encryption, hashing, digital signatures and certificates to protect data from unauthorized access, guarantee it's authenticity and prevents tampering.

Note: obfuscation pertaining to specifically data; not as a part of network security.

Key Takeaways

- Different algorithms accomplish different tasks.
- Asymmetric cryptography uses a pair of related keys.
- Certificates and Digital signatures are noteworthy cryptographic tools
- .pem is the file extension for PKI keys .. it stands for Privacy Enhanced Mail. I have always used .key or something. And I look forward to using the proper file extension from now on.

Tools and Techniques Used

"cipher" command in windows
"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.

Lab 4-1: Cryptographic Solutions
- **Objective:**
  To get comfortable with the tools to make Digital Signatures and Certificates
- **Steps Performed:**
  Create and verify a digital signature; create and approve a certificate signing request
- **Results:**
  See the creation of signatures, their verification and failure and the creation of a certificate.
- **Reflection:**
  It is good to step away from the book and use the tools to get a better feel for these things.

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