ProLUG Security Engineering
Unit 9 Worksheet

Instructions

Fill out this sheet as you progress through the lab and discussions. Hold your worksheets until the end to turn them in as a final submission packet.

Discussion Questions:

Unit 9 Discussion Post 1: Read the Security Services section, pages 22-23 of https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf and answer the following questions.

1. How do these topics align with what you already know about system security?
2. Were any of the terms or concepts new to you?

Unit 9 Discussion Post 2: Review the TLS Overview section, pages 4-7 of https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf and answer the following questions

1. What are the three subprotocols of TLS?
2. How does TLS apply
    a. Confidentiality
    b. Integrity
    c. Authentication
    d. Anti-replay

Definitions/Terminology

- TLS
- Symmetric Keys
- Asymmetric Keys
- Non-Repudiation
- Anti-Replay
- Plaintext
- Cyphertext

- Fingerprints
- Passphrase (in key generation)

Notes During Lecture/Class:

Links:

- https://www.sans.org/information-security-policy/
- https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

Terms:

Useful tools:

- STIG Viewer 2.18
- Ansible
- Killercoda

Lab and Assignment

Unit9-Certificates and keys - To be completed outside of lecture time.

Digging Deeper

1. Finish reading about TLS in the publication and think about where you might apply it.

Reflection Questions

1. What were newer topics to you, or alternatively what was a new application of something you already had heard about?

2. What questions do you still have about this week?

3. How are you going to use what you’ve learned in your current role?