Advanced Network Security Part 1 Recap

Dr Rob Hegarty

Overview

This lab session will recap on key concepts from the first part of the Advanced Network Security unit. The emphasis of the lab is on the practical implementation of theory's and concepts covered in the revision lecture. Further independent research is required to fully understand these concepts.

Task 1 – Password Storage and Cracking

Review the lab sheet and notes on the Moodle area from week 3 on password exfiltration and cracking. Ensure you know how to search the shadow password file for hashes of different types, furthermore:

- Describe how passwords are stored using hash functions
- Research the issues around using older general-purpose hash function to hash and store passwords.
- Review the documentation on John the Ripper and describe the difference between brute force and dictionary attacks.
- Research and document the role of a salt in password storage, describe how and why it is used.

Task 2 – Wireshark Capture Analysis

Review the lab sheets and notes on the Moodle area from weeks 2 and 4. Ensure you know how to identify source and destination port numbers and IP addresses from a packet capture, furthermore:

- Practice the use of filters to identify packets that may be used to identify suspect or malicious network traffic.
- Research the TCP three-way handshake, and become familiar with its purpose, and how it may be misused.
- Review the different types of port scan and consider their benefits and drawbacks.

Task 3 – CREST Procurement Model, and Lockheed Martin Cyber Kill Chain

Research the Lockheed Martin Cyber Kill Chain, and CREST Ethical Hacking procurement process, the links below will help you get started. Ensure you understand each part step of each of the models and how they relate to other steps.

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.crest-approved.org/wp-content/uploads/2014/11/PenTest-Suppliers-Guide.pdf

Task 4 – Assignment Support

Please use the remainder of this session to work on your coursework. You should aim to have completed the following by the end of the session:

- Created a template for your work, with a brief description in each section describing what it will contain. Review the assignment brief and mark scheme for guidance.
- Deployed both Kali and DVL, and demonstrated that you can run a port scan against DVL