Writeup

Kevin Turkington

I. Lecture Overview

In Ram Venugopalan and Geoffery Coopers lectures they describe basics of netowrking, networking attacks, and network security. The primary subjects of these lectures where to highlight the different known attacks capable of interfering with a users communication with the internet. While also providing examples of illegal (black hat) and legal (white hat) variants of these intrusive attacks.

II. Networking Overview

To understand the threats in the world of networking and how to protect against them, secturity analyst need to know the basics of how networking works. For example on a high level most protocols are wrappers of the known tcp and udp protocols like smtp (mail). While on the highest most level these concepts are based off of the 'Robustness Principle' created by Jon Postel. His expanded principle focuses on "being liberal in what you accept, and conservative in what you send" with the addition of assuming anything you accept is malevolent.

III. Attacks

There are two types of attacks and inspection of network traffic that are highlighted in this weeks lectures. Mainly 'Man in the Middle' (MITM), Denial Of Service (DDOS), and actice/passive reconnaissance. To begin Denial Of Service attacks are simply a method of sending multiple requests from a collection of computers intended to clog up a targets processing power to deny others access to the site. This can be done by both CPU and memory usuage of resources. As well as targeting a servers packet acknoledgement queue to overflow with first in sequence packets instead of sequential handshakes between client and server. For Man In The Middle attacks, the attacker will most commonly sniff out traffic on a local network and do one of two things. Read the data of packets contained inside to capture usernames and passwords. Or act as a proxy between the client and server creating the handshakes themselves. This can be beneficial for the attacker because during the hand off of acknowledgements and requests to the server and client the attacker can modify data being handed off. As for reconnaissance the attacker either actively sends packets to different ports connected to an address to map out and find vulnerabilities connected to known ports. Or passively gathers data over months by tapping network closets or watching traffic move on the network.

IV. Security

Although all of these attacks seem like methods that would only be used by black hat hackers, they can also be utilized by white hat hackers too. For example DDOS attacks can be used to test load on a server in preparation to move content to production. And Man in the middle attacks or reconnaissance can take up for form of proxy's to monitor traffic in a corporate setting to defend against internal leaks of information or network bugs scanning for exploits themselves.

for a more detailed list of network protections:

- Proxies
- Firewalls
- network policys
- Intrusion detection

Firewalls being the most prominent network security, it defines zones of policy throughout a network. Often scanning and denying packets if they meet a known definition for an exploit. Firewalls are commonly used in settings like testing labs, data centers, user stations, and many more. Intrustion detection on the other hand doesnt focus as much on filtering outside traffic but invites it in. For example Honey pots are a form of intrusion detection that notifys users if attackers are sniffing around a part of the network that is meant to be dead or filled with dummy data to begin wtih. Network policys act as a yara signatures matching with incoming or outgoing traffic to find and detect possible security threats. And finally proxies act as an in between quarantine zone for a mixture of these protection methods to be held.

V. Conclusion

This weeks lectures gave me an indepth answer to how interception and monitoring of packets over a networks is done. Particularly it has peaked my interest in creating my own demo of a man in the middle attack using an old router as a wifi pineapple / simple packet sniffing using the scapy python package (on my own network).