Week 6 Write Up

This week we discussed multiple ways to defend and attack a network. In specific, we discussed the following protection strategies:

* Having a policy for both positive and negative movement within the network. This includes applications, HTTP traffic and more
* Having a firewall designated as the network’s DMZ. Network segmentation within the DMZ/firewall is critical.
* Have a layered defense. This includes not only having a firewall, but having a intrusion detection system, a security information and event management system (i.e. LogRythm) and ensuring that these system can talk to each other via functioning API’s. This is important since most of these systems may come from different applications and vendors.
* Intrusion detection which is the searching and monitoring for things you DON’T want to happen on your network. However, this does have its limitation. In example, does may not help you in your efforts to detect attacks involving zero day vulnerabilities.
* Quarantine hosts that may be infected so the infection does not spread across the network to other hosts. This could also include a blacklist component.

Other examples of strategies include honeypots/honeynet’s and reputation.

Other topics also discussed in the lecture were attacks against networks. One in particular I found interesting was Man In the Middle Attacks (MITM).

Having worked as a fraud investigator, I investigated various cases of fraud in which bank users/clients were victims of online banking and wire fraud. Most of which was perpetrated via MITM attacks. This mounted to large losses for the financial institutions who paid out such claims to the clients who losses were not reimbursed by the same banks.

In our investigations, our immediate source for review was the online banking session logs. Most often than not, we would find various session log in and activity from multiple IP addresses in concurrency with the legitimate user’s activity (i.e. while the bank client was performing a balance inquiry via an IP address in Venezuela, another user was performing a wire transfer request via an IP address in Russia, both using the same session ID). These investigations proved frustrating but I was interested how these attacks could be carried out against sophisticated online banking platforms. Most often than not, the client’s devices were unpatched and poorly secured.

One part of the lecture that interested me regarding man in the middle attacks was SSL renegotiation attacks. Renegotiation is required when no client-server authentication is initially required while making an SSL connection but is required later. Thus instead of dropping and creating a new SSL connection, renegotiation adds authentication details to the current connection.

However renegotiation is vulnerable to attacks. Two worries are:

1. A man in the middle attacker can inject data into an HTTPS session and execute requests on behalf of the victim
2. Denial of Service (DoS), by establishing a secure SSL connection requires more processing power on the server, an attacker can exploit this processing power property with renegotiation to trigger hundreds of handshakes in the same TCP connection.

There are ways to mitigate these threats. Some are:

* Renegotiation is not required by the majority of the sites. Disable SSL renegotiation support on the server
* Limit the number of SSL handshakes, or upgrade server resources by adding an SSL accelerator

Below is a link to a proof of concept for TLS renegotiation and its vulnerability in which an attacker can perform a DoS attack.