Week 6

Lecture 1

In contrast to how deep into the inner workings of a computer we got last week, this time we are taking a big step back away from the computer entirely and focusing on network security. Network security poses an interesting challenge because it has to act as a first line of defense against a lot of different kinds of threats without being too overbearing to be inconvenient to the user.

Network security is used for many different reasons. It creates “safe spaces” where data going in and out of a network can be filtered, it inhibits attacks such as DDos or slow down malicious Recon, and it can slow down threats that snuck into the network by performing damage control against worms and botnets. A lot of network security revolves around the “robustness Principle”, which advises to “be liberal in what you accept, and conservative in what you send”.

Whitelisting is a common policy designed to limit an infinite amount of threats by only allowing a finite amount of approved sources, but be careful the filtering isn’t too specific or nothing will get done. A firewall helps a network admin define zones in network policy and provide protection to the outside and inner zones of a network, similar to a medieval castle. The lecturer went in depth about the similarities between the two but for the sake of brevity I will continue steaming ahead into Web Gateways, which are proxy web connections to apply policy to and often paired with “the cloud”. These gateways behave similar to a dns server but more involved and actively analyze in and out-going traffic for malicious items. Intrusion detection such as IDS and IPS use signatures/anomaly detection to detect attacks and can be very quick + efficient, however are susceptible to day zero attacks and false positives. Honeynets are used to learn more about attackers and waste their time by pretending to be a valid target. Reputation and Quarantine protections are also valid methods of protecting your network, but have similar shortcomings as IDS/IPS.

Next we talked about MITM, which We have already learned about a million times HOWEVER it turns out you can use it for good as well by having a TCP proxy jump in between you and a dangerous host like a protagonist in an action film, taking the bullet in slow motion. This proxy detects malicious scripts and can get you out of there safely. Next we talked about hashes and protecting against man in the middle using shared secret but That’s already been done to death so I Won’t repeat all of it.

Lecture 2

Reconnaissance is the first phase a malicious agent goes through while attacking a target, and it involves reconning their target to learn more about habits, software, schedules, hardware, and basically everything they can. It can range from physical recon (watching the corporate office) to digital recon, which is typically done through nmap and very slow pings against the firewall. There are two types of Recon,

Active – Attacker wants to attack vulnerable machines on network and needs to find addresses for attackable services

Passive – Attacker is able to see data passing by on network (wireshark) and learns about how the people on the network use the service and what kind of traffic goes by.

Next up is Spoofing, where the attacker masquerades as another network entity in order to gain an advantage over the network defenses of the target. IP and ARP spoofing can be used for MITM attacks, certain DoS attacks rely on spoofing (LAND) and all kinds of other things can be spoofed like IP, MAC, HTTP fields, and more. Speaking of DoS, what is it?

DoS stands for Denial of Service, and involves consuming target resources for an extended period of time so that the targeted service is degraded or unusable. A DDoS is similar but is a Distributed DoS, and usually involves large numbers of computers performing exhaustion attacks against a target so that it is overwhelmed and cannot perform its function. An example of this would be thousands of computers all asking Github to display the entirety of it’s database, thousands of times. It would add up quick and soon Github would be unable to process all the queries and shut down.

Next we went oer VPN, IPSEC, NAT, NGFW, Packet filtering, deep inspection, and packet filtering…

Eventually we got to database poisoning, which is an interesting attack where the attacker inserts invalid data into a database causing clients to aid them with the attack. ARP poisoning is very effective and so is DNS poisoning, which tries to confuse targets into accepting invalid certs or connecting to wrong services.

Overall this was an interesting albiet unfocused lecture that covered a very wide range of topics.