Overview

Network attacks vary in objective:

- Steal sensitive information
- Disrupt communication/operations
- Modify records or data on servers
- Inject malicious content into legitimate traffic
- Gain a foothold for future attack
- Leverage less valuable systems for future attacks

Cyber attackers share at least one thing in common. They can't do squat without access to a target resource or its dependencies. But access is an interesting concept. Good attackers have mastered the art of gaining a tiny foothold in a system that can be exploited to accomplish a larger goal.

To properly address network security, we need to change the way we think about the components of the network. Everything we talk about in this class is a useful and often necessary tool (for connecting and communicating). BUT IT'S ALL A TARGET AS WELL. AND IT'S ALL A WEAPON.

Examples:

- ARP poisoning
- Controlling network configuration with rogue DHCP servers
- Deploying rogue access points to fool clients
- Poisoning DNS caches for a network
- Monitoring DNS queries and spoofing responses
- Generating spurious traffic
- Hijacking clients/servers and network capacity to avoid detection or carry out attacks on availability, e.g., botnets
- Using broadcasts and spoofed traffic to amplify attacks on availability
- Aggregating DNS query statistics to analyze user or organization behavior

If we have any hope to maintain security of the system, we should learn how to use these components to construct our defense.

Access Control and Network Security

If we want to prevent an attack on our system, we need to limit access to its components. The task of preventative network security is to reduce attack surface much as possible throughout the system without placing undue burden on the users, applications, and devices that rely on the network to communicate.

This job is incredibly difficult given the complexity of most networks and the variety of techniques attackers have at their disposal.

- Break in or get hired and use physical access to gain a presence on a wired network
- Exploit weaknesses in wireless network security to establish a presence
- Leverage a browser weakness hijack a client and gain an internal foothold
- Take over a public-facing server by exploiting a vulnerability in the software
- Compromise the perimeter router/firewall of a network by exploiting configuration weaknesses or unpatched software vulnerabilities

It's not enough to protect the system at any single layer of the OSI model. We should layer our defenses to maintain integrity of the system at all points where communication is taking place. In the spirit of access control, we also aim to construct the network in a way to reduce the scope of the defensive task.

- Restrict access to physical network infrastructure (data centers, network closets, ports, and SSIDs), to minimize the presence of unauthorized devices.
- Segment Layer-1/2 architecture, i.e., 1) using switches to separate collision domains to prevent passive monitoring and 2) *pairwise* encryption of wireless associations.
- Segment Layer-2/3 architecture, i.e., 1) leveraging hardware separation and VLANs to enforce the path of communication between endpoints at the router/firewall or 2) using host isolation techniques such as private VLANs to block direct communication between devices.
- Implement layer-2 technical controls to prevent attackers from masquerading as other system components (by spoofing ARP requests or masquerading as DHCP servers).
- Filter traffic between network segments/subnets based on source/destination/ports and other traffic characteristics. Allow the conversations required to satisfy business requirements. Hide everything else. Minimize the footprint of the network perimeter. Maximize the opportunities to enforce policy between internal segments.
- Implement dynamic policies and network access control that considers identity of devices, users, etc before giving access to network fully.
- Funnel DNS through trusted resolvers. Implement a robust strategy to protect the integrity of the local and public zones associated with an organization/network.
- Implement proxies and application-layer firewalls that restrict behavior of network clients (legitimate and illegitimate).

It should be clear that these safeguards aim to interrupt attacks by placing new boundaries between discrete components of the system.

- Monitor network behavior using pattern-based or statistical intrusion detection systems that analyze actual PDUs or traffic flow patterns. Deploy intrusion prevention to

automatically block suspicious activity. Use segmentation to maximize the opportunity to expand

- Design systems with resilience, redundancy, and additional capacity to offset attacks on availability.

Don't rely on the network. Implement end-to-end controls whenever possible.

- Encrypt application data in transit to prevent attackers from capturing sensitive information or manipulating contents of the session, e.g., to inject attack code or malware that will be processed by the endpoint.
- Leverage digital certificates and/or key pinning to detect hosts that are attempting to perform active attacks (MITM) on encrypted protocols.
    - Attacks: HTTPS splitting/stripping, STRIPTLS, obtaining fraudulent certificates from trusted authorities
    - Defenses: X.509+TLS+HSTS/HPKP, DNSSEC+DANE, SSH