10.1.16 Sniffing Countermeasure and Detection Facts

This lesson covers the following topics:

- Network intrusion detection systems
- Secure network traffic
- Switched networks

Network Intrusion Detection Systems

Network intrusion detection systems (NIDSs) are used to prevent intrusion and alert network administrators of active attacks. These systems search for anomalies in network traffic. They can detect network cards running in promiscuous mode and flag MAC addresses that are not a part of the internal network. An NIDS uses promiscuous mode to capture and analyze packets. It collects data on the packets received and labels them based on their potential threat level. A notable fact about an NIDS is that it can identify both external and internal threats, reducing the potential for insider abuse.

Secure Network Traffic

Two areas that are frequently overlooked by administrators are physical security and wireless access points. The best network security won’t mean much if an attacker can walk right in and plug into a physical port. The same is true for a wireless access points. By nature, wireless traffic is more susceptible to sniffing, so you’ll want to be strategic when you determine where to put these on your network and what type of access they provide.

There are a few additional things to keep in mind when locking down your network:

- Use the more secure IPv6 instead of IPv4.
- Replace clear text protocols like FTP and Telnet with more secure options such as SSH, SSL, and IPsec.
- Use encryption for all sensitive traffic using protocols, end-to-end encryption, and VPNs.

Switched Networks

Switched networks provide a natural barrier for an attacker, so you’ll want to segment a network in a way that isolates sensitive traffic. Of course, switches alone are not going to be enough. You’ll want to enable port security on your switches to ensure that only specific MAC addresses and only a specific number of MAC addresses can access a port. Be sure to configure settings so the switch shuts down a port when the max number of MAC addresses is reached so that MAC flooding isn’t possible. DHCP snooping is another feature that can be enabled on the switch to prevent ARP poisoning and spoofing attacks. DHCP snooping is built into most switches and blocks DHCP servers, that are not under the organization’s control from assigning IP addresses to DHCP clients.