Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

Protecting Networks

- Proper network design provides us with one of the chief tools we have to protect ourselves from the variety of network threats we might face. A well-configured and patched network is the foundation of any security program. With a properly laid out network, we can prevent some attacks entirely, mitigate others, and, when we can do nothing else, fail in a graceful way.
- Tools we use to defend our networks
  - Network segmentation
  - Firewalls
  - IDS/IPS
  - Wireless Secure Protocols
  - VPNs
  - Secure Protocols
  - MDM
  - Port Scanners
  - Packet Sniffers
  - Honeypots

Network Segmentation and Firewalls

- **Network Segmentation**: is when we segment a network, we divide it into multiple smaller networks, each acting as its own small network called a subnet. We can control the flow of traffic between subnets, allowing or disallowing traffic based on a variety of factors, or even blocking the flow of traffic entirely if necessary.
- **Firewalls**: are a mechanism for maintaining control over the traffic that flows into and out of our network(s). Firewalls naturally create network segmentation when installed.

Firewalls and DMZs

- **Packet filtering**: is one of the oldest and simplest of firewall technologies. Packet filtering looks at the contents of each packet in the traffic individually and makes a gross determination, based on the source and destination IP addresses, the port number, and the protocol being used, of whether the traffic will be allowed to pass.
- **Stateful firewall**: uses what is called a state table to keep track of the connection state and will only allow traffic through that is part of a new or already established connection. Most stateful firewalls can also function as a packet filtering firewall, often combining the two forms of filtering. For example, this type of firewall can identify and track the traffic related to a particular user-initiated connection to a Web site, and knows when the connection has been closed and further traffic should not legitimately be present.
- **Deep packet inspection firewalls**: add yet another layer of intelligence to our firewall capabilities. Deep packet inspection firewalls are capable of analyzing the actual content of the traffic that is flowing through them. Although packet filtering firewalls and stateful firewalls can only look at the structure of the network traffic itself in order to filter out attacks and undesirable content, deep packet inspection firewalls can actually reassemble the contents of the traffic to look at what will be delivered to the application for which it is ultimately destined.
- **Proxy servers**: Proxy servers can serve as a choke point in order to allow us to filter traffic for attacks or undesirable content such as malware or traffic to Web sites hosting adult content.
- **DMZ, or demilitarized zone**: is generally a combination of a network design feature and a protective device such as a firewall. As we discussed earlier in the "Security in Network Design" section, we can often increase the level of security on our networks by segmenting them properly. When we look at systems that need to be exposed to external networks such as the Internet in order to function, such as mail servers, proxy servers, software as a service application, and Web servers, we need to ensure their security and the security of the devices on the network behind them.

IDS\IPS methods

- **Intrusion detection**: (IDSes) An IDS performs strictly as a monitoring and alert tool, only notifying us that an attack or undesirable activity is taking place.
- **Intrusion prevention**: (IPSes) An IPS can actually take action based on what is happening in the environment. In response to an attack over the network, an IPS might refuse traffic from the source of the attack.
- **Signature-based**: works in a very similar fashion to most antivirus systems
- **Anomaly-based**: typically work by taking a baseline of the normal traffic and activity taking place on the network

The Impact of Intercepted Data

- One of the largest concerns when we are sending sensitive data over a network is of having the data intercepted by someone that might misuse it. Given the many networks available today in offices, hotels, coffee shops, restaurants, and other places, the opportunity to accidentally expose data to an attacker is large.
- **Wireless networks security**: For the legitimate and authorized devices on our network, our chief method of protecting the traffic that flows through them is the use of encryption. The encryption used by 802.11 wireless devices, the most common of the wireless family of network devices, breaks down into three major categories: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access version 2 (WPA2). Of these, WPA2 is the most current and offers the strongest inherent security.
- **Wireless exposure**: Wireless networks, in particular, are one of the major security risks when we consider places where our data might be exposed. Free wireless Internet access is commonly provided today in a number of places.
- **VPNs**: The use of virtual private networks (VPNs) can provide us with a solution for sending sensitive traffic over unsecure networks. A VPN connection, often referred to as a tunnel, is an encrypted connection between two points.
- **Secure Protocols**: the simplest and easiest ways we can protect our data is to use secure protocols.

Mobile Devices

- **Mobile devices**: are any device that communicates via a wireless medium.
- **Mobile Device Management**: While most devices that are not running a mobile operating system, that is, Windows, OS X, Linux, etc. have a well-established seat of tools and features that allow them to be centrally managed, this may not hold true with mobile devices. We generally want to be able to mandate patching and software upgrades, force changing of passwords at some interval, regulate and track installed software, adjust settings to a standard dictated by our policies, and a number of other similar functions.
- **Bring Your Own Device (BYOD)**: is often brought up when discussing mobile device security. BYOD generally refers to an organization's strategy and policies regarding the use of personal versus corporate devices. This can range from only corporate-owned devices being allowed to interact with enterprise resources to only personal devices being used and any combination in between.

Network Tools

- **Wireless**: Attackers accessing a wireless device can potentially bypass all our carefully planned security measures. Worse yet, if we do not take steps to ensure that unauthorized wireless devices, such as rogue access points, are not put in place on our network, we could be allowing a large hole in our network security and never know it.
  - **Kismet** is commonly used to detect wireless access points and can find them even when attempts have been made to make doing so difficult.
  - **NetStumbler** exists for Windows, although it does not have as full a feature set as Kismet.
- **Port Scanners**: Scanners are one of the mainstays of the security testing and assessment industry. We can generally break these into two main categories: port scanners and vulnerability scanners. There is some overlap between the two, depending on the particular tool we are talking about.
  - **Nmap** is short for network mapper. Although Nmap is generally referred to as a port scanner, we actually do it a bit of a disservice to call it that. Although Nmap can conduct port scans, it can also search for hosts on a network, identify the operating systems those hosts are running, detect the versions of the services running on any open ports, and much more.
- **Packet Sniffers**: A network or protocol analyzer, also known as a packet sniffer, or just plain sniffer is a tool that can intercept traffic on a network, commonly referred to as sniffing. Sniffing basically amounts to listening for any traffic that the network interface of our computer or device can see, whether it was intended to be received by us or not.
  - **Wireshark:** Graphical interface tool for packet anlayzer.
  - **Tcpdump**: This command-line packet sniffing tool runs on Linux and UNIX operating systems.
- **Honeypots**: can detect, monitor, and sometimes tamper with the activities of an attacker. Honeypots are configured to deliberately display vulnerabilities or materials that would make the system attractive to an attacker.

Firewall Tools

- Firewall tools: are tools that are used to test firewall vulnerabilities.
  - **Hping3:** is a well-known and useful tool for such efforts. It is able to construct specially crafted Internet Control Message Protocol (ICMP) packets in such a way as to evade some of the normal measures that are put in place to prevent us from seeing the devices that are behind a firewall. We can also script the activities of Hping3 in order to test the responses of firewalls and IDSes, so that we can get an idea of the rules on which they are operating.