Andrew Plum

Mr. Alves-Foss

Cyb 110

10/28/21

Ch. 10 Homework

1) When working with wireless networks, the tool Kismet can be used to detect devices. Kismet runs on Linux and macOS. It can also be found on the Kali distribution. Kismet is also used by penetration testers to detect wireless access points and can find them even when their well-hidden. Another use for Kismet is that it can be used to sniff from wireless networks.

2) The idea of segmentation is taking something relatively large and breaking it down into relatively smaller partitions. Network segmentation is similar in that when you segment a network, you divide it into multiple smaller networks called subnets. When the network is segmented you can better control and manage the flow of traffic between subnets. You can do this by allowing or disallowing the traffic based on a variety of factors or even block the flow of traffic entirely if necessary. If the networks are also properly segmented, the network performance can be enhanced. This is done by having certain traffic only being contained to portions of the network that need to see it. The subnets can help you localize technical network issues. Network segmentation can also prevent unauthorized network traffic or attacks from reaching particularly sensitive portions of the network.

3) The three main types of wireless encryption are WPA, WPA2, and WPA3. The acronym WPA in each of these types stands for Wi-Fi Protected Access. WPA and WPA2 were the first two standards. WPA3 is the current standard used.

4) A tool you can use to scan for devices on a network is Nmap which is short for a network mapper. Nmap is typically considered a port scanner. It searches for hosts on a network, identifies the operating systems the hosts are running, and detects the version of the services running on any open ports.

5) Packet sniffers are tools which can intercept (or sniff) traffic on a network. A classic sniffer is Tcpdump, a command-line tool invented in the 1980s. Tcpdump only runs on UNIX-like operating systems, but Windows systems can run a version of the tool called WinDump. Wireshark is a capable packet sniffer which can intercept traffic from a great selection of wired and wireless sources. Wireshark has a graphical interface and includes many filtering, sorting, and analysis tools making it one of the more popular packet sniffers used today. Kismet can also be used to sniff wireless networks. There are also hardware forms of packet sniffers like OptiView Portable Network Analyzer from Fluke Networks. Although portable packet sniffers like this are well equipped and feature increase capture capacity and capabilities, they are often expensive.

6) You use a honeypot to attract the attention of the attackers and then study them and their tools. A honeypot is a system that can detect, monitor, and sometime tamper with the activities of an attacker. Honeypots are configured so that they intentionally display fake vulnerabilities or materials so that it might attract an attacker. The honeypots monitor the activity of the attacker when they access it without their knowledge of this occurring. Honeypots can be set up so that they serve as an early warning system for an institution. They also might be used to monitor the activities of malware to understand it so that you can better defend your system against it. When you create a network of

honeypots you create what is called a honeynet which is particularly useful in understanding malware on a large scale.

7) Even though signature-based IDS and anomaly-based IDS are both IDS's, there are a few differences between the two. A signature-based IDS works similar to most antivirus systems. A database of signatures that might signal an attack is maintained and incoming traffic is compared to those signatures. This method works well typically except if an attack is new or if the attack has been designed specifically not to match a certain attack signature. You may not see the attack at all if you don't have an existing signature. Also, if the attacker creating the traffic has access to the same IDS tools you're using and is able to test the attack against them, they may be able to specifically avoid your security measures. An anomaly-based IDS works by distinguishing normal traffic from traffic which is out of the ordinary. Anomaly-based IDS determine traffic to be normal traffic if it follows the normal patterns. This method of comparing traffic to normal patterns works very well compared to signature-based IDS at detecting new attacks as well as attacks made to avoid IDS. The drawback of anomaly-based IDS is it might produce more false positives than a signature-based IDS due to it possibly flagging legitimate activity that cause spikes in traffic or unusual traffic patterns.

8) If you need to send sensitive data over an untrusted network, you should use a VPN which stands for virtual private network. VPNs are commonly called a tunnel because a VPN connection uses an encrypted connection between two points. The connection is created using a VPN client application and a VPN concentrator. All traffic flows through an encrypted VPN tunnel once the connection has been established. VPNs are useful in that it allows remote workers to access their organization's internal resources as if they were directly connected to their organization's internal network. VPNs can also be used to protect or anonymize the traffic you're sending over untrusted connections. VPNs can be used to stop people on the same network from viewing your activity, to keep your internet service provider from logging the contents of your traffic, or obscure your geographical location and bypass location-oriented blocking. VPNs are also used sometime for malicious means like sharing pirated media.

9) DMZs are used as a layer of protection which separates a device from the rest of a network. This is accomplished by using multiple layers of firewalls. The DMZ is where a webserver would be place and the there would be an internet facing firewall between it and the internet while there would be another internal firewall between the DMZ where the web server is located and the internal servers. DMZs allow public facing servers to be accessed whilst providing some protection for them and restricting some traffic from those servers from penetrating more sensitive areas of the network. This aids in stopping an attack where the attackers compromise the public facing servers and then use them to attack the other servers behind them.

10) The difference between stateful firewalls and deep packet inspection firewalls is deep packet inspection firewalls are more advanced. Stateful firewalls function similar to packet filtering firewalls except they keep track of traffic at a very precise level, and they can watch the traffic over a given connection. Stateful firewalls can also function as packet filtering firewalls. Deep packet inspection firewalls are more complex than stateful firewalls in that they can analyze the actual content of the traffic that flows through them. Deep packet inspection firewalls can reassemble the contents of the traffic to see what it will deliver to the application for which it's destined and then decides on whether to send it based on the contents. This is a great improvement compared to the other firewalls because packet filtering firewalls and stateful firewalls can only look at the structure of the network traffic to

filter out attacks and undesirable content. Both stateful firewalls and deep packet inspection firewalls are more advanced than packet filtering firewalls.