Lesson Proper for Week 8

WIRELESS AND WI-FI SECURITY

Wireless network security

The process of designing, implementing and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.

Also known as wireless security. Wi-Fi security is the protection of devices and networks connected in a wireless environment. Without Wi-Fi security, a networking device such as a wireless access point or a router can be accessed by anyone using a computer or mobile device within range of the router's wireless signal.

WI-FI NETWORK SECURITY METHODS

1. Media Access Control (MAC) addresses

Restrict access to a Wi-Fi network. (A MAC address is a unique code or number used to identify individual devices on a network.) While this tactic provides a higher measure of security than an open network, it is still susceptible to attack by adversaries using "spoofed" or modified addresses.

2. Encryption

A more common method of protecting Wi-Fi networks and devices is the use of security protocols that utilize encryption. Encryption in digital communications encodes data and then decodes it only for authorized recipients.

There are several types of encryption standards in use today, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). See the section "Types of wireless security protocols" on this page for more details about these and other standards related to Wi-Fi security.

Most newer network devices, such as access points and Wi-Fi routers, feature built-in wireless-security encryption protocols that provide Wi-Fi protection.

3. Virtual private networks (VPNs)

VPNs are another source of Wi-Fi network security. They allow users to create secure, identity-protected tunnels between unprotected Wi-Fi networks and the internet.

A VPN can encrypt a user's internet connection. It also can conceal a user's IP address by using a virtual IP address it assigns to the user's traffic as it passes through the VPN server.

4. Security software

There are many types of consumer and enterprise software that also can provide Wi-Fi security. Some Wi-Fi protection software is bundled with related products, such as antivirus software.

TYPES OF WIRELESS SECURITY PROTOCOLS

There are four main wireless-security protocols. These protocols were developed by the Wi-Fi Alliance, an organization that promotes wireless technologies and interoperability. The group introduced three of the protocols, described below, in the late 1990s. Since then, the protocols have been improved with stronger encryption. The fourth protocol was released in 2018.

a. WEP (Wired Equivalent Privacy). A security protocol for Wi-Fi networks. Since wireless networks transmit data over radio waves, it is easy to intercept data or "eavesdrop" on wireless data transmissions. The goal of WEP is to make wireless networks as secure as wired networks, such as those connected by Ethernet cables.

b. WPA (Wi-Fi Protected Access). A security protocol designed to create secure wireless (Wi-Fi) networks. It is similar to the WEP protocol, but offers improvements in the way it handles security keys and the way users are authorized.

c. WPA2 (Wi-Fi Protected Access II). It is the second version of WPA, a technology used for secure Wi-Fi connections. Both WPA and WPA2 provide encrypted data transfers over a Wi-Fi connection. Both require a password with a minimum length of 8 characters. The technologies differ in the way they encrypt the data.

WPA uses the Temporal Key Integrity Protocol (TKIP) to dynamically vary the encryption key shared between the access point and connected clients. The continually changing key provides more secure authentication than the earlier WEP wireless encryption standard.

d. **WPA3 (Wi-Fi Protected Access III).** Makes further security improvements that make it harder to break into networks by guessing passwords; it also makes it impossible to decrypt data captured in the past i.e., before the key (password) was cracked.

THE MAIN THREATS TO WI-FI SECURITY

v **MAN-IN-THE-MIDDLE ATTACKS**

A man-in-the-middle (MITM) attack is an incredibly dangerous type of cyber-attack that involves a hacker infiltrating a private network by impersonating a rogue access point and acquiring login credentials.

The attacker sets up hardware pretending to be a trusted network, namely Wi-Fi, in order to trick unsuspecting victims into connecting to it and sending over their credentials. MITM attacks can happen anywhere, as devices connect to the network with the strongest signal, and will connect to any SSID name they remember.

v **CRACKING AND DECRYPTING PASSWORDS**

Cracking and decrypting passwords is an old method that consists of what is known as “A brute force attack.” This attack consists of using a trial and error approach and hoping to eventually guess correctly. However, there are many tools that hackers can use to expedite the process.

v **PACKET SNIFFERS**

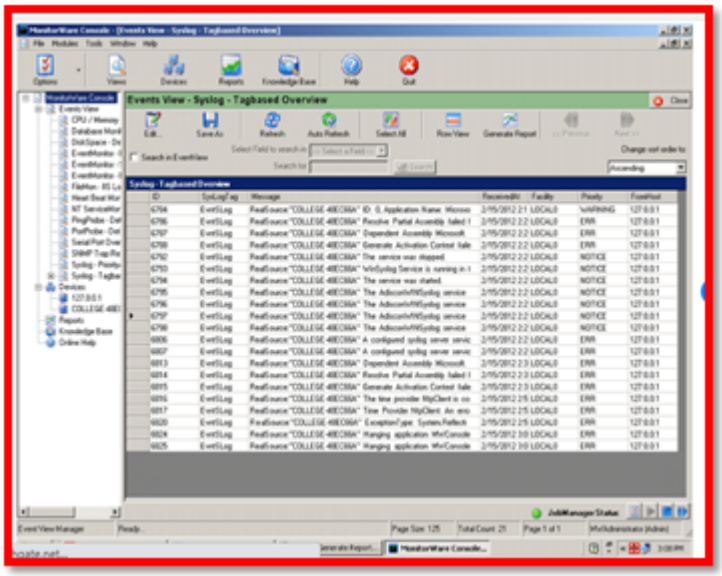
Packet sniffers are computer programs that can monitor traffic on a wireless network. They can also intercept some data packages and provide a user with their contents. They can be used to harmlessly gather data about traffic, but in the wrong hands can introduce errors and break down a network.

NETWORK MONITORING TOOLS

- System Logging Protocol (Syslog)

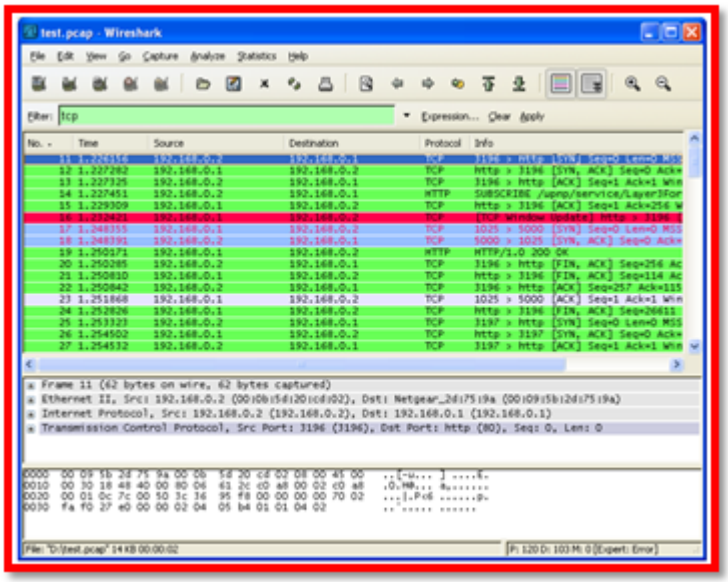
A way network devices can use a standard message format to communicate with a logging server. It was designed specifically to make it easy to monitor network devices. Devices can use a Syslog agent to send out notification messages under a wide range of specific conditions.

The syslog server receives, categorizes, and stores log messages for analysis, maintaining a comprehensive view of what is going on everywhere on the network. Without this view, devices can malfunction unexpectedly, and outages can be hard to trace.



- Wireshark

A network protocol analyser, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.



Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

Packet Capture: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

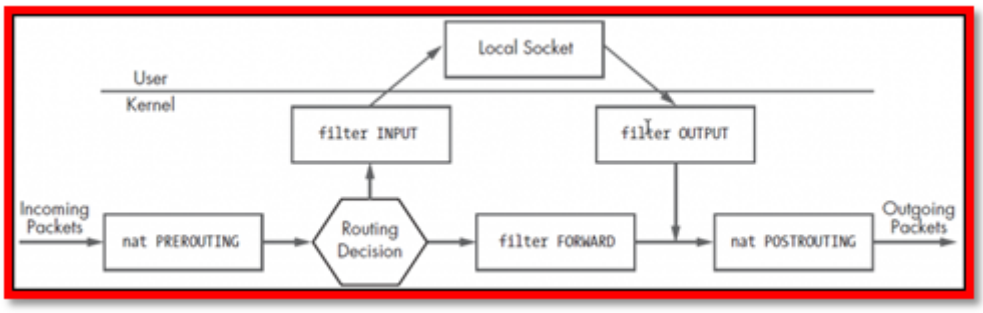
Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

- Tcpdump

A command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.

- Iptables

A chain for packets that come to the server, exit the server, and that the server routes. These chains are called INPUT, OUTPUT and FORWARD respectively. iptables allows the user to add rules to these chains and take certain actions when the inspected package complies with one of these rules. The package leaves that chain with the first rule it matches in a chain. When the packet matches, it either jumps to another user-defined chain or is DROP or ACCEPT.



INPUT: It is checked whether an incoming package matches the rules in this chain structure during its entry to the user. If they match, the target option is applied.

OUTPUT: During the exit of a packet from the user, it is checked whether it matches the rules in this chain structure. If they match, the target option is applied.

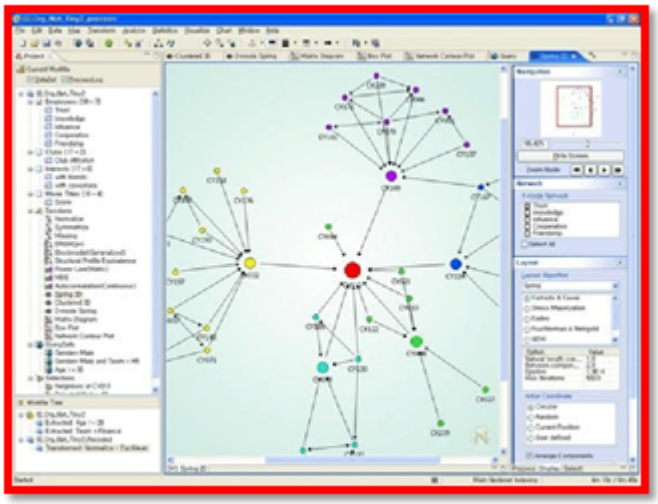
FORWARD: If the packet is to be forwarded correctly to a new address, it is checked whether it matches the rules in this chain structure. If they match, the target option is applied.

PREROUTING: Pre-routing package header information is checked to see if it matches the rules in this chain structure. If they match, the target option is applied.

POSTROUTING: After routing, it is checked if it matches the rules in this chain structure in order to organize the package header information. If they match, the target option is applied.

- NetMiner

An application software for exploratory analysis and visualization of large network data based on SNA (Social Network Analysis). It can be used for general research and teaching in social networks. This tool allows researchers to explore their network data visually and interactively, helps them to detect underlying patterns and structures of the network. It features data transformation, network analysis, statistics, and visualization of network data, chart, and a programming language based on the Python script language.



Navigation

Fair Warning

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

- Assignments
- Forums
- Quizzes
- Resources