Handling Wireless Network Security Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what wireless network security incidents are.

Explain what the different types of wireless access control attacks (confidentiality, integrity and availability) that IH&R team members may detect during an investigation are.

Identify what steps the IH&R team should take to contain and eradicate wireless network security incidents.

Define what the steps that the IH&R team should take to ensure recovery from wireless network security incidents.

External Resources:

Handling Wireless Network Security Incidents

What are Wireless access control attacks? -

Aim is to penetrate a network by evading wireless LAN access control measures, such as AP MAC filters and Wi-Fi port access controls.

There are several types of access control attacks, including:

```
▪ War Driving - wireless LANS are detected either by sending probe requests
over a connection or by listening to web beacons. Some of the tools that the
attacker may use to perform wardriving attacks are KisMAC and NetStumbler.

▪ Rogue Access Points - A wireless access point is termed as a rogue access
point when it is installed on a trusted network without authorization. In order
to create a backdoor into a trusted network, an attacker may install an
unsecured AP or fake AP inside a firewall.

▪ MAC Spoofing - An attacker can reconfigure a MAC address to appear as an
authorized AP to a host on a trusted network. The attacker may use tools such
as SMAC to perform this kind of attack.

▪ AP Misconfiguration - Improper configuration of any of the critical security
settings at any of the APs can expose the entire network to vulnerabilities
and attacks.

▪ Ad Hoc Associations - connecting directly to an unsecured client, avoiding
AP security.

▪ Promiscuous Client - Exploiting the behavior of 802.11 wireless cards, as
they always try to find a stronger signal with which to connect. An attacker
places an AP near the target Wi-Fi network and gives it a common SSID name,
and then offers an irresistibly stronger signal and higher speed than the
target Wi-Fi network. The intent is to lure the client to connect to the
attacker's AP rather than legitimate Wi-Fi network. Promiscuous clients allow
an attacker to transmit target network traffic through a fake AP. Very similar
to the evil twin threat on a wireless network, in which an attacker launches
an AP that poses as an authorized AP by beaconing the WLAN's SSID.
```

What are Wireless Integrity Attacks? -

Changing or altering data during transmission, via the sending of forged control, management, or data frames to misdirect wireless devices in order to perform another type of attack (e.g., DoS).

```
▪ Data Frame Injection - Constructing and sending forged 802.11 frames;
(Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject)

▪ WEP Injection - Constructing and sending forged WEP encryption keys.

▪ Bit-Flipping Attacks - Capturing the frame and flipping random bits in the
data payload, modifying ICV, and sending to the user.

▪ Extensible AP Replay - Capturing 802.1X Extensible Authentication
Protocols (e.g., EAP Identity, Success, and Failure) for later replay.

▪ Data Replay - Capturing 802.11 data frames for later (modified) replay.

▪ Initialization Vector Replay Attacks - Deriving the key stream by sending
plain-text message.

▪ RADIUS Replay - Capturing RADIUS Access-Accept or Reject messages for later
replay

▪ Wireless Network Viruses
```

What are Wireless Confidentiality Attacks? -

Attempt to intercept confidential information, regardless of whether the system transmits data in clear text or encrypted format. Confidentiality attacks on wireless networks Include:

```
▪ Eavesdropping
▪ Traffic Analysis
▪ Cracking WEP Key
▪ Evil Twin AP - Posing as an authorized AP by beaconing the WLAN's SSID to
lure users.
▪ Honeypot AP
▪ Session Hijacking
▪ Masquerading
▪ MITM Attack
```

What are Wireless Availability Attacks? -

Obstructing the delivery of services to legitimate users, either by crippling those resources or by denying them access to WLAN resources. Availability attacks include:

```
▪ AP Theft

▪ Disassociation Attacks

▪ EAP-Failure - Observing a valid 802.1X EAP exchange, and then sending the
client a forged EAP-Failure message.

▪ Beacon Flood - Generating thousands of counterfeit 802.11 beacons to make
it hard for clients to find a legitimate AP.

▪ Denial-of-Service

▪ De-authenticate Flood - Flooding client(s) with forged de-authenticates or
disassociates to disconnect users from an AP.

▪ Routing Attacks

▪ Authenticate Flood - Sending forged authenticates or associates from random
MACs to fill a target AP's association table.

▪ ARP Cache Poisoning Attack

▪ Power Saving Attacks - Transmitting a spoofed Traffic Indication
Map (TIM) and/or Delivery Traffic Indication Map (DTIM) to the client while
in power saving mode

    The TIM information element advertises if any associated stations have
    buffered UNICAST frames

    The DTIM information element advertises if any associated stations have
    buffered broadcast / multicast traffic frames.


▪ TKIP MIC Exploit - Generating invalid TKIP data to exceed the target AP's
MIC error threshold.
```

What are Wireless Authentication Attacks? -

Steal the identity of Wi-Fi clients, their personal information and login credentials to gain unauthorized access to network resources. Authentication attacks include:

- Preshared Key (PSK) Cracking - Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.

- LEAP Cracking - Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.

- VPN Login Cracking = Gaining user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by using brute force attacks on VPN authentication protocols.

- Domain Login Cracking - Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute force or dictionary attack tool.

- Identity Theft - Capturing user identities from cleartext 802.1X Identity Response packets.

- Shared Key Guessing - Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.

- Password Speculation - Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.

- Application Login Theft - Capturing user credentials (e.g., email address and password) from cleartext application protocols.

- Key Reinstallation Attack - Exploiting the 4-way handshake of the WPA2 protocol.

How do we prepare for handling Wireless Network Security Incidents? -

- Create an up to date inventory of all the wireless networking devices along with their MAC and IP addresses, authentication details, credentials, strength, and points of placement

- Enable all the wireless devices to log the incoming and outgoing traffic and save it to a centralized server

- Audit the wireless devices present in the organization and store the details in an easily accessible system

- Create forms and checklists to help incident responders handle any type of wireless network security incident

- Install wireless network monitoring and traffic monitoring tools, firewalls, IDS, and vulnerability management tools

What about containment of Wireless Network Security Incidents? -

Containment is a crucial step in the incident management process that focuses on preventing additional damage. Organizations can contain wireless network security incidents by following the below mentioned steps:

- Disable wireless access once detection of an intrusion has occurred

- Check ALL devices connected to the victim access points for traces of compromise

- Change the passwords of all devices across the organization

- Identify the attacker details such as IP address and MAC address, and block the devices used for attack

- Whitelist the authorized user devices so that no other devices are able to connect to the access points

What about eradication of Wireless Network Security Incidents? -

The following steps can be used for wireless network security threat eradication:

```
▪ Use complex passphrases of a minimum of 20 characters in length and change
them at regular intervals

▪ Use WPA2 Enterprise with AES/CCMP encryption

▪ Implement a Network Access Control (NAC) or Network Access Protection (NAP)
solution for additional control over end-user connectivity

▪ Turn On auto updates for all wireless devices and patch the device firmware

▪ Train users to avoid the use of public Wi-Fi networks

▪ Train users to avoid accessing sensitive resource when devices are connected
to an unprotected network

▪ In the case of IoT devices, perform audits of devices and avoid connection
to insecure Wi-Fi routers

▪ Enable HTTPS Everywhere extension and two factor authentication
```

https://www.eff.org/https-everywhere

What about recovery after Wireless Network Security Incidents? -

Recovering a system depends on the extent of the security breach.

When a wireless network security incident occurs, the incident response team will decide whether to restore the system(s) or completely replace them.

The following steps can be used for wireless network security recovery:

```
▪ Properly set the client settings (e.g., validate the server, specify server
    address, do not prompt for new servers)

▪ Update all the routers and Wi-Fi devices with the latest security patches

▪ Disable SSID broadcasts

▪ Change the default SSID after WLAN configuration

▪ Use SSID cloaking to keep certain default wireless messages from broadcasting
the ID to everyone

▪ Place a firewall or packet filter in between the AP and the corporate Intranet

▪ Disable remote router login and wireless administration

▪ Enable MAC Address filtering on your access point or router

▪ Enable encryption on access point and change passphrase often

▪ Limit the strength of the wireless network so it cannot be detected outside
the bounds of your organization

▪ Check the wireless devices for configuration or setup problems regularly

▪ Implement WPA2 Enterprise wherever possible

▪ Disable the network when not required

▪ Place wireless access points in a secured location

▪ Keep drivers on all wireless equipment updated

▪ Use a centralized server for authentication

▪ Keep Bluetooth in the disabled state, enable it only when needed and disable
immediately after the intended task is completed

▪ Use Link Encryption for all Bluetooth connections
```