Handling Unauthorized Access Incidents

Objectives:

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

Understand what unauthorized access incidents are.

Explain what the different methods of unauthorized access that IH&R team members may encounter during an investigation may be.

Identify different types of network attacks that can be used to gain unauthorized access.

Define what the steps that the IH&R team should carry out to contain unauthorized access incidents are.

External Resources:

Handling Unauthorized Access Incidents

What is an Unauthorized Access Incident? -

An unauthorized access incident involves gaining illegal access to resources without authorization.

Intruders involved in unauthorized access include casual hackers, security experts, professional hackers, and organizational employees.

Methods of unauthorized access include:

```
▪ Exploiting vulnerabilities in an operating system, networks, servers and
databases
▪ Exploiting vulnerabilities or misconfigurations in software applications
▪ Stealing user authentication credentials such as login names and passwords
▪ Using social engineering tricks
▪ Insider threats
```

Some of the network attacks used to gain unauthorized access include:

```
▪ Reconnaissance attacks
▪ Sniffing and spoofing attacks
    o Eavesdropping
    o DNS and ARP poisoning
▪ Firewall and IDS evasion attacks
▪ Brute force attacks
```

The following are the possible indications of unauthorized access incidents:

```
▪ Physical Intrusion
▪ Changes in System Configuration:
▪ Changes in Network Settings/Behavior
▪ Changes in Administrator Settings
▪ Unauthorized Data Modification
▪ Unauthorized Usage of a Standard User Account
▪ Unauthorized Data Access
▪ High Resource Utilization
```

How do we detect Reconnaissance Attacks? -

In reconnaissance attacks, attackers make an attempt to profile the target network, using network mapping tools such as Nmap and Network Topology Mapper to determine the vulnerabilities of the network and exploit them.

Information obtained using reconnaissance attacks includes:

```
▪ Domain and sub-domains
▪ Network blocks
▪ Whois and DNS records
▪ O/S and location of web servers
▪ IP addresses
▪ TCP and UDP services running
▪ Live hosts
▪ Open ports
▪ Running services on hosts
▪ Access Control Mechanisms and ACL’s
▪ Networking protocols
▪ VPN endpoints
▪ IDS and firewalls
▪ Employee details
▪ Web technologies used in the organization
▪ Telephone numbers
▪ Authentication mechanisms
```

What are the most common types of reconnaissance attacks? -

```
▪ Ping Sweeping: Scanning an IP range to detect live hosts
▪ Port Scanning: Scanning target for open ports
▪ DNS Footprinting: Extracting DNS information from publicly available sources
▪ Social Engineering: Tricking people to reveal sensitive information
```

Detecting Reconnaissance Attacks: PING Sweep Attempts -

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique that is employed to determine which range of IP addresses map to live hosts (computers). Although a single ping will tell the user whether one specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts. If a specified host is active, it will return an ICMP ECHO reply. It is accomplished using ICMP, TCP, or UDP. Attackers send a series of ICMP, TCP, or UDP echo requests to the specified IP range.

An incident handler can use the Wireshark tool in order to detect such ping sweep attempts on the organization’s network.

```
▪ Use the filter icmp.type==8 or icmp.type==0 to detect an ICMP ping sweep attempt
▪ Use the filter tcp.dstport==7 to detect a TCP ping sweep attempt
▪ Use the filter udp.dstport==7 to detect an UDP ping sweep attempt
```

Detecting Reconnaissance Attacks: Port Scanning Attempts -

Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a listening state.

Detecting Half Open/Stealth Scan Attempts -

The Stealth scan involves resetting the TCP connection between client and server abruptly before completion of the three-way handshake signals, hence, making the connection half open.

A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers. This type of scan sends a single frame with the expectation of a single response.

The stealth scan is also called a “SYN scan,” because it only sends the SYN packet. This prevents the service from notifying the incoming connection.

The stealth scan process is shown below:

```
▪ The client sends a single SYN packet to the server on the appropriate port.
▪ If the port is open, subsequently, the server responds with an SYN/ACK packet.
▪ If the server responds with an RST packet, then the remote port is in
the "closed” state.
▪ The client sends the RST packet to close the initiation before a connection
can ever be established.
```

Detecting Full Connect Scan Attempts -

In TCP Connect scanning, the operating system’s TCP connect() system call tries to open a connection to every interesting port on the target machine. If the port is listening, the connect() call will result in a successful connection with the host on that particular port; otherwise, it will return an error message stating that the port is not reachable.

The TCP Connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with a SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection.

Once the handshake is completed, the scanner sends a RST packet to end the connection. Making a separate connect() call for every targeted port in a linear fashion would take a long time over a slow connection. The attacker can accelerate the scan by using many sockets in parallel.

Using non-blocking, I/O allows the attacker to set a low time-out period and watch all the sockets simultaneously. The drawback of this type of scan is that it is easily detectable and filterable. The logs in the target system will disclose the connection.

```
NOTE: This type of scanning DOES NOT REQUIRE super user privileges !!!
```

The incident handler can use the Wireshark tool in order to detect a Full Connect scan using the same method that is used for detecting a stealth scan attempt.

```
▪ Check for SYN, SYN+ACK, and RST+ACK packets or ICMP type 3 packets
```

Detecting Null Scan Attempts -

In a Null port scan, an attacker sends a TCP packet without setting a flag on it.

If they receive a RST packet in response, then the port is closed.

If there is no response, then the port is open or filtered.

```
NOTE: Use the TCP.flags==0x000 filter in the Wireshark tool to view the packets
moving without a flag set.
```

Detecting Xmas Scan Attempts -

The Xmas scan is a port scan technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device.

If the target has opened the port, then you will receive no response from the remote system.

If the target has closed the port, then you will receive a remote system reply with a RST.

```
NOTE: This scan ONLY WORKS when systems are compliant with the RFC 793-based
TCP/IP implementation; It will not work against any current version of
Microsoft Windows.

NOTE: Use the tcp.flags==0X029 filter in the Wireshark tool to view the
packets with FIN, PSH, and URG TCP flags set.
```

Detecting Sniffing and Spoofing Attacks: Mac Flooding Attempts -

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network by using a software application or a hardware device.

The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port.

A MAC address is a hardware address that uniquely identifies each node of a network. Passive sniffing is used to sniff a hub-based network while active sniffing is used to sniff a switch-based network.

Switches keep a translation table that maps various MAC addresses to the physical ports on the switch. As a result, they can intelligently route packets from one host to another. However, switches have limited memory.

MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches can no longer keep up. Once this happens to a switch, it will enter into the fail-open mode, acting like a hub by broadcasting packets to all the ports on the switch.

Once that happens, it becomes easy to perform sniffing.

Wireshark detects MAC flooded packets using the Expert Information window. Wireshark considers these as malformed packets. To view these malformed packets:

```
▪ Go to the Analyze menu and select Expert Information.
▪ The signs of a MAC flooding are detected by analyzing the source IP,
destination IP, and the TTL values.
▪ Check if the traffic is originating from various IP addresses going to the
same destination IP addresses with the same TTL values. This is an indication
of a MAC flooding attempt on the network.
```

Detecting Sniffing and Spoofing Attacks: ARP Poisoning Attempts -

ARP Spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch. Once a switch is overloaded, it fails open, allowing attackers to sniff all the network packets.

Attackers can also flood a target computer's ARP cache with forged entries, which is known as poisoning. In an ARP poisoning attack, the attacker's MAC address is associated with the IP address of the target host or a number of hosts in the target network.

The incident handler can use the Wireshark tool in order to detect ARP poisoning attempts:

```
▪ Check for "duplicate IP address configured" messages in the Warnings tab
in Wireshark.

▪ To locate duplicate IP address traffic, use the following filter:

    arp.duplicate-address-detected
```

What is the XArp tool? -

It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. The detection mechanism relies on two techniques: inspection modules and discoverers.

```
▪ Inspection modules look at ARP packets and check their correctness and
validity with respect to the databases they have built up.

▪ Discoverers actively validate IP-MAC mappings and actively detect attackers.
```

Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques -

```
▪ Promiscuous Mode - allows a network device to intercept and read each
network packet that arrives in its entirety.
```

NOTE: The sniffer leaves no trace since it does not transmit data.

There are many tools, such as the Nmap, that are available to use for the detection of promiscuous mode.

```
o Use an IDS

o Use Ping to find systems running in promiscuous mode - send a ping request
to the suspected machine with its IP address and incorrect MAC address. The
adapter will reject it since the MAC address does not match, whereas the
suspect machine running the sniffer responds to it, as it does not reject
packets with a different MAC address.

o Looking for evidence of use of Reverse DNS Lookups - Sniffers using reverse
DNS lookup increase network traffic. This increase in network traffic can be
an indication of the presence of a sniffer on the network.

o ARP Method - sends a non-broadcast ARP to all the nodes in the network. The
node that runs in promiscuous mode on the network will cache the local ARP
address. Then it will broadcast a ping message on the network with the local
IP address but a different MAC Address.
```

In this case, only the node that has the MAC address (cached earlier) will be able to respond to your broadcast ping request.

A machine in promiscuous mode replies to the ping message as it has correct information about the host that is sending the ping request in its cache; the rest of the machines will send ARP probes to identify the source of the ping request. This will detect the node on which the sniffer is running.

```
o Nmap - Nmap's NSE script allows you to check if a target on a local Ethernet
has its network card in promiscuous mode. Command to detect NIC in promiscuous
 mode:

nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
```

Detecting Firewall and IDS Evasion Attempts: Techniques Used to Evade Firewall -

Following are some firewall evasion/bypass techniques:

```
▪ Port Scanning
▪ Firewalking
▪ Banner Grabbing
▪ IP Address Spoofing
▪ Source Routing
▪ Tiny Fragments
▪ Using IP Address in Place of URL
▪ Using Anonymous Website Surfing Sites
▪ Using Proxy Server
▪ ICMP Tunneling
▪ ACK Tunneling
▪ HTTP Tunneling
▪ SSH Tunneling
▪ Through External Systems
▪ Through MITM Attack
▪ Through Content
▪ Through XSS Attack
```

Detecting Firewall and IDS Evasion Attempts: Techniques Used to Evade IDS -

IDS evasion is all about modifying an attack to fool the IDS/IPS systems into interpreting that the attack traffic is legitimate in order to prevent the IDS triggering an alert.

Following are some IDS evasion/bypass techniques:

```
▪ Insertion Attack
▪ Evasion
▪ Denial-of-Service Attack
▪ Obfuscating
▪ False Positive Generation
▪ Session Splicing
▪ Unicode Evasion
▪ Fragmentation Attack
▪ Overlapping Fragments
▪ Time-To-Live Attacks
▪ Invalid RST Packets
▪ Urgency Flag
▪ Polymorphic Shellcode
▪ ASCII Shellcode
▪ Application-Layer Attacks
▪ Desynchronization
▪ Encryption
▪ Flooding
```

Detecting Firewall and IDS Evasion Attempts: General Indications of Intrusions -

```
▪ File System Intrusions -

    o The presence of new, unfamiliar files, or programs
    o Changes in file permissions o Unexplained changes in a file’s size
    o Rogue files on the system that do not correspond to your master list of
    signed files
    o Missing files


▪ Network Intrusions -

    o Repeated probes of the available services on your machines
    o Connections from unusual locations
    o Repeated login attempts from remote hosts
    o Sudden influx of log data


▪ System Intrusions -

    o Short or incomplete logs
    o Unusually slow system performance
    o Missing logs or logs with incorrect permissions or ownership
    o Modifications to system software and configuration files
    o Unusual graphic displays or text messages
    o Gaps in system accounting
    o System crashes or reboots
    o Unfamiliar processes
```

What are the steps that IH&R team members should take to contain Unauthorized Access Incidents? -

- Isolate the affected systems - By performing port scans for any backdoors, isolation of the affected system prevents the further compromise of the system

- Disable the affected service - The services like FTP should be disabled temporarily or permanently to prevent further damage

- Eliminate the attacker’s route into the network - Examine the attacker’s route into the network and block the connections which prevent incoming connections or disconnect the remote access server

- Disable user accounts used in the attack - The affected user accounts should be disabled or the passwords should be changed

- Enhance physical security measures - Increase the security of the server rooms and other places which are vulnerable to security breach