UNIT 3

Intrusion Detection Systems

Intrusion Detection Systems (IDSes) and their Placement An intrusion detection system is used to monitor and protect networks or systems for malicious activities. To alert security personnel about intrusions, intrusion detection systems are highly useful. IDSes are used to monitor network traffic. An IDS checks for suspicious activities. It notifies the administrator about intrusions immediately. Q An intrusion detection system (IDS) gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy, including unauthorized access, as well as misuse 0 An IDS is also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols, usually TCP/IP © The packets are analyzed after they are captured Q An IDS evaluates a suspected intrusion once it has taken place and signals an alarm

How an IDS Works

The main purposes of IDSes are that they not only prevent intrusions but also alert the administrator immediately when the attack is still going on. The administrator could identify methods and techniques being used by the intruder and also the source of attack. An IDS works in the following way: © IDSes have sensors to detect signatures and some advanced IDSes have behavioral activity detection to determine malicious behavior. Even if signatures don't match this activity detection system can alert administrators about possible attacks. © If the signature matches, then it moves to the next step or the connections are cut down from that IP source, the packet is dropped, and the alarm notifies the admin and the packet can be dropped. © Once the signature is matched, then sensors pass on anomaly detection, whether the received packet or request matches or not. Q If the packet passes the anomaly stage, then stateful protocol analysis is done. After that through switch the packets are passed on to the network. If anything mismatches again, the connections are cut down from that IP source, the packet is dropped, and the alarm notifies the admin and packet can be dropped.

Firewalls

A firewall is a set of related programs located at the network gateway server that protects the resources of a private network from users on other networks. Firewalls are a set of tools that monitor the flow of traffic between networks. A firewall, placed at the network level and working closely with a router, filters all network packets to determine whether or not to forward them toward their destinations. A firewall is often installed away from the rest of the network so that no incoming request can get directly to a private network resource. If configured properly, systems on one side of the firewall are protected from systems on the other side of the firewall. © A firewall is an intrusion detection mechanism. Firewalls are specific to an organization's security policy. The settings of the firewalls can be changed to make appropriate changes to the firewall functionality. 0 Firewalls can be configured to restrict incoming traffic to POP and SNMP and to enable email access. Certain firewalls block the email services to secure against spam. Q Firewalls can be configured to check inbound traffic at a point called the "choke point/′ where security audit is performed. The firewall can also act as an active "phone tap" tool in

identifying the intruder's attempt to dial into the modems within the network that is secured by firewall. The firewall logs consist of logging information that reports to the administrator on all the attempts of various incoming services. Q The firewall verifies the incoming and outgoing traffic against firewall rules. It acts as a router to move data between networks. Firewalls manage access of private networks to host applications. 0 All the attempts to log in to the network are identified for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to login. Firewalls can filter packets based on address and types of traffic. They identify the source, destination addresses, and port numbers while address filtering, and they identify types of network traffic when protocol filtering. Firewalls can identify the state and attributes of the data packets.

EVADING IDS

Insertion Attack

The process where the attacker confuses the IDS by forcing it to read the invalid packets is known as insertion, that is, the packet would not be accepted by the system to which it is addressed. If a packet is malformed or if it does not reach its actual destination, the packet is invalid. Ifthe IDS read an invalid packet, the IDS will become confused. To understand how insertion becomes a problem for a network IDS, it is important to understand how IDSes detect attacks. The IDS employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. For example, IDSes might look for the string "phf" in an HTTP request to discover a PHF Common Gateway Interface (CGI) attack. An attacker who can insert packets into the IDS can prevent pattern matching from working. For instance, an attacker can send the string "phf" to a web server, attempting to exploit the CGI vulnerability, but force the IDS to read "phoneyf" (by "inserting" the string "oney") instead. One simple insertion attack involves intentionally corrupting the IP checksum. Every packet transmitted on an IP network has a checksum that is used to verify whether the packet was corrupted in transit. IP checksums are 16-bit numbers that are computed by examining information in the packet. If the checksum on an IP packet does not match the actual packet, the host to which it is addressed will not accept it, while the IDS might consider it as part of the effective stream.

For example, the attacker can send packets whose Time to live fields have been crafted to reach the IDS but not the target computers. An attacker confronts the IDS with a stream of onecharacter packets (the attacker-originated data stream), in which one of the characters (the letter 'X') will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings.

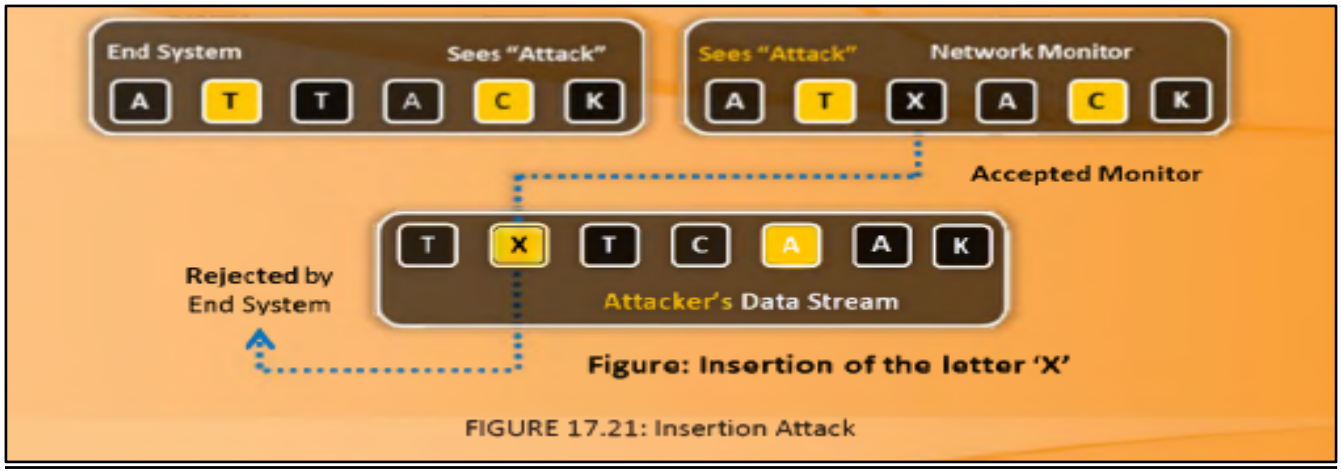
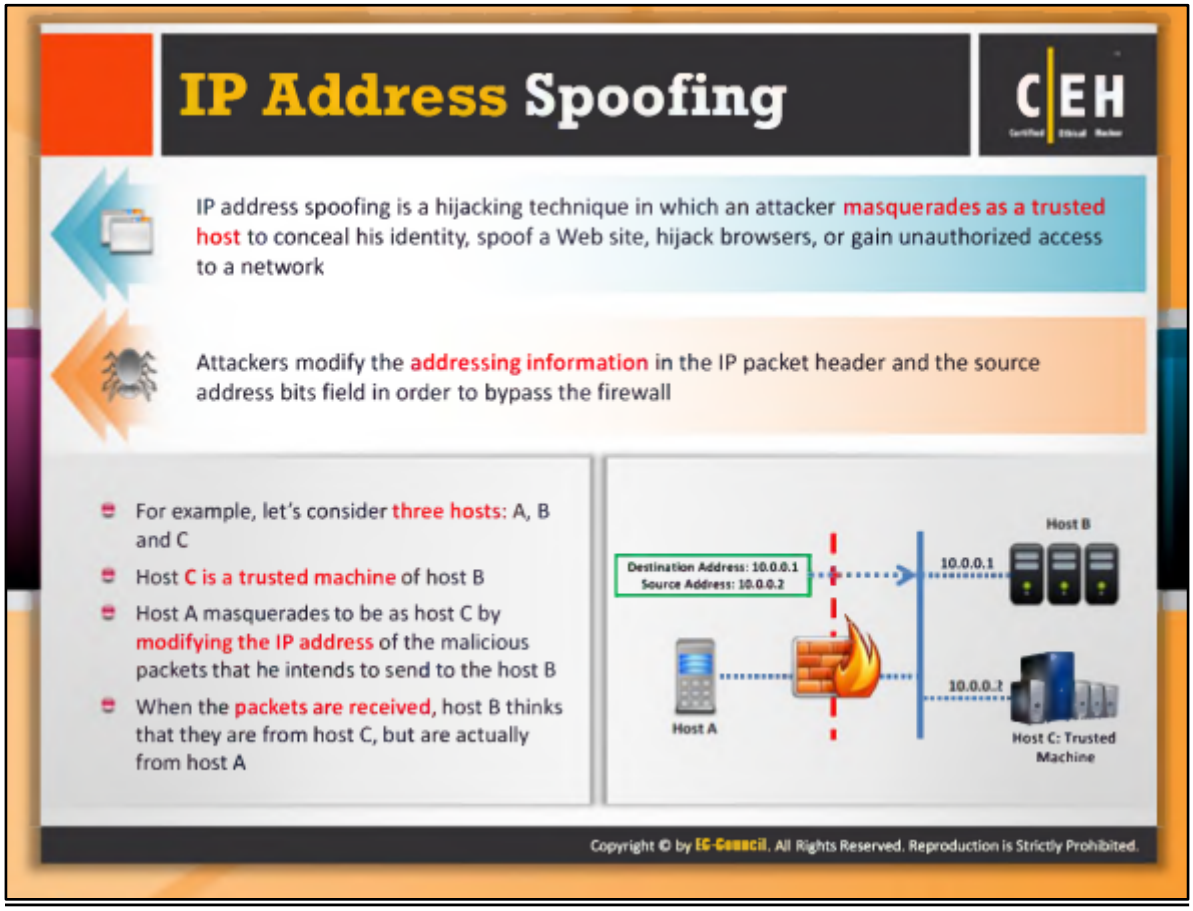


FIGURE 17.21: Insertion Attack

EVADING FIREWALL

IP address spoofing



IP address spoofing or IP spoofing is one of the ways that an attacker tries to evade firewall restrictions. IP spoofing is a technique where the attacker creates Internet protocol packets by using a forged IP address and gains access over the system or network without any authorization. The attacker spoofs the messages and they appear to be sent from a reliable source. Thus, the attacker succeeds in impersonating others' identities with help of IP spoofing. Hackers generally use this technique for not getting caught while spamming and various other activities.

The following scenario shows how an attacker bypasses a firewall by impersonating a different identity with the help of th IP spoofing technique:

- Let's consider three hosts: A, B, and C
- Host C is a trusted machine of host B
- Host A wants to send some packets to host B and A impersonates itself to be C by changing the IP address of these packets
- When these packets are received, B thinks that these packets are from C, but actually they are from A

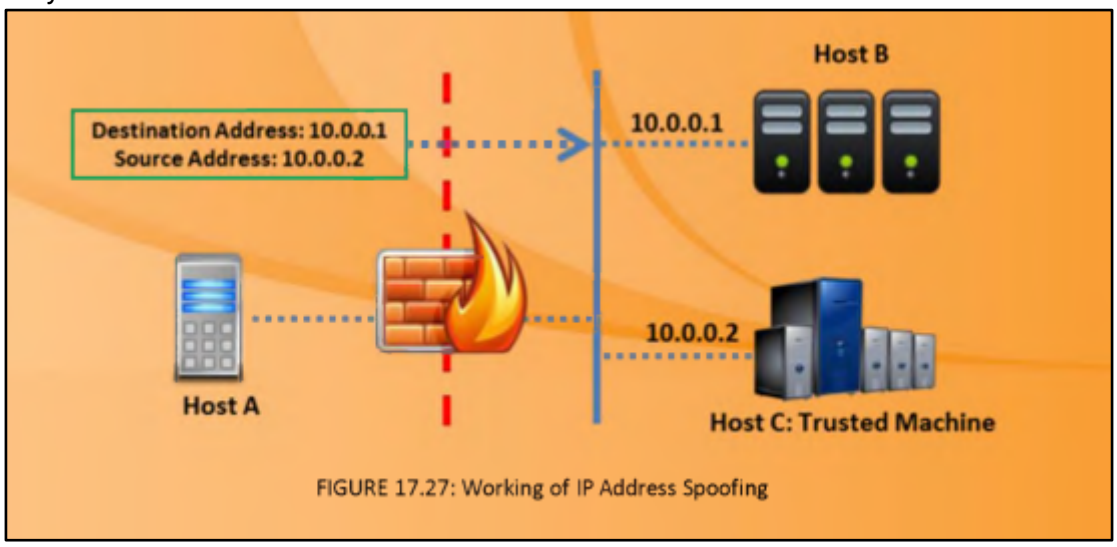


FIGURE 17.27: Working of IP Address Spoofing