Session Hijacking
Objectives

• Define session hijacking
• Understand what session hijacking entails
• Identify the styles of session hijacking
Objectives (continued)

• List some session-hijacking tools
• Explain the differences between TCP and UDP hijacking
• Note measures that defend against session hijacking
TCP Session Hijacking

• Hacker takes control of a TCP session between two hosts
• TCP session can be hijacked only after the hosts have authenticated successfully
  – Session cannot be initiated until the authentication process is finished
TCP Session Hijacking (continued)

Figure 8-1  Hacker intervention in an authenticated TCP connection
Session Hijacking – Hacker’s Point of View

• TCP works with IP to manage data packets
• TCP tracks the packages sent to the receiver
• One popular method of session hijacking is using source-routed IP packets
• If source routing is turned off
  – The hacker can use blind hijacking
  – Guessing the responses of the two machines
• Hacker can also be inline between B and C, using a sniffing program to follow the conversation
Session Hijacking – Hacker’s Point of View (continued)

Figure 8-2  Denial of service
Session Hijacking – Hacker’s Point of View (continued)

• Hacker could find problems for two reasons:
  – Host computer that has been hijacked will continue to send the packets to the recipient
  – Recipient gives an ACK to the host computer after receiving packets from the hacker’s computer
Session Hijacking – Hacker’s Point of View (continued)

**Figure 8-3** ACK attack
Session Hijacking – Hacker’s Point of View (continued)

![Diagram of Session Hijacking](image)

**Figure 8-4** ACK attack without DoS
Session Hijacking – Hacker’s Point of View (continued)

![ACK Loop Diagram]

Figure 8-5  ACK loop
Session Hijacking – Hacker’s Point of View (continued)

- Continuous ACK Transfer
  - Three ways to stop a continuous ACK transfer
    - Losing the ACK packet
    - Ending the connection
    - Resynchronizing the client and server
TCP Session Hijacking with Packet Blocking

• Packet blocking solves the ACK storm issue
  – And facilitates TCP session hijacking
• ACK storm happens because the attacker was not in a place to stop or delete packets sent by trusted computer
• Attacker must be in control of the connection itself
  – So that the session authentication takes place through the attacker’s chosen channel
Figure 8-6 Packet blocking
TCP Session Hijacking with Packet Blocking (continued)

• Hacker can wait for the ACK packet to drop
  – Or manually synchronize the server and client records by spoofing

• If a hacker can block the packets
  – Can drop exact number of packets desired for transfer
Methods

• **Route Table Modification**
  – All computers that use TCP/IP keep a route table
  – A route table shows the way to the address sought
    • Or way to nearest source that might know the address
  – Route table has two sections
    • Active routes and active connections
  – If the route table can’t locate a perfect match of the IP address
    • It searches for the closest possible match in the list of network addresses
Figure 8-7  Linux route table
Methods (continued)

• Route Table Modification (continued)
  – After the match is found, the IP address of Computer A sends the packets to the IP address
  – If the route table cannot find a match, it refers the request to the network gateway
  – Active connections section shows the network addresses of the computers
    • That are connected with the host computer
A page is requested. In the route table, the route to 115.178.25.48 is not listed so the request is sent to the listed recipient for all unlisted addresses, which is 192.168.0.1.

---

Gateway
router
LAN side
192.168.0.1
WAN side
207.45.115.26

115.178.25.48

B. Web server

Via a series of hops from router to router, the request arrives and the connection is initiated.

---

**Figure 8-8** Route table in action
192.168.0.102 sends request to 192.168.100.45. Its route table does not have this address so it sends to the gateway listed in the table, 192.168.0.2. **Switch** 192.168.0.2 receives the request and checks its route table. It discovers that all 192.168.100 addresses can be reached from its LAN-side NIC with an IP of 192.168.100.1. The message is forwarded. 192.168.100.45, a networked HP LJ4200, receives the message and sends an ACK. Eventually, a print job will be accomplished.

**Figure 8-9** Route discovery
Methods (continued)

• **Route Table Modification (continued)**
  – Hacker changes the route table
  – Host computer assumes that the best possible path for the transfer of data packets is through the hacker’s computer
Methods (continued)

• Route Table Modification (continued)
  – Hackers can modify a route table using two methods
    • Erase all necessary records from the route table
      – And then provide the hacker’s own IP address as the default gateway address
    • Change the corresponding route in the route table of the gateway router
192.168.0.103
Route table has been hacked to make the direct route to 15.11.115 through gateway 192.1680.105.

Router gateway 192.168.0.1 receives the request, and checks its route table. It discovers that its default path 0.0.0.0 can reach the requested IP. The message is forwarded.

192.168.0.5 acts as a bridge for packets from 192.168.0.103 to anything in the 15.11.115.* in range. Two-way traffic can be observed, since the router will see the outgoing traffic from 192.168.0.5 to 15.11.115.*.

Figure 8-10  Route table hack
Session Hijacking Tools - Hunt

- Developed by Pavel Krauz
  - Inspired by Juggernaut
- Performs sniffing and session hijacking
- Menu options: listing, watching, and resetting connections
- Hunt tool can hijack a session through ARP attacks
Hunt (continued)

- Hunt allows hacker to synchronize the connection among the host and the server
  - During session hijacking
UDP Hijacking

- **User Datagram Protocol (UDP)**
  - Connectionless protocol that runs on top of IP networks

- **UDP/IP provides very few error recovery services**
  - Offers direct way to send and receive datagrams over an IP network
  - Used primarily for broadcasting messages
UDP Hijacking (continued)

• More vulnerable to hijacking
  – Hacker needs only to sniff the network for a UDP request for a Web site and drop a spoofed UDP packet in before the Web server responds
Prevention and Mitigation

- To defend against session hacking, use encrypted protocols and practice storm watching
Encryption

- Hacker needs to be authenticated on the network to be able to successfully hijack a session
- If the data transfer is encrypted
  - It is far too complicated and time consuming to get authenticated
- Standard protocols like POP3, Telnet, IMAP, and SMTP are excellent targets
  - Because they transfer data as plaintext
Encryption (continued)

Table 8-1  Replace or enhance insecure protocols with secure protocols

<table>
<thead>
<tr>
<th>Insecure protocols</th>
<th>Encrypted Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post Office Protocol (POP3)</td>
<td>POP3 over TLS</td>
</tr>
<tr>
<td>Simple Mail Transfer Protocol (SMTP)</td>
<td>SMTP over TLS</td>
</tr>
<tr>
<td>Internet Message Access Protocol (IMAP)</td>
<td>HTMILS, SSL</td>
</tr>
<tr>
<td>Telnet</td>
<td>Secure Sockets Layer (SSL), SSH</td>
</tr>
<tr>
<td>File Transfer Protocol (FTP)</td>
<td>SSL, SSH</td>
</tr>
<tr>
<td>Hypertext Transport Protocol (HTTP)</td>
<td>Secure Hypertext Transport Protocol (HTTPS), SSL</td>
</tr>
</tbody>
</table>
Encryption (continued)

Alice and Bob both have PKI lockboxes for sending secrets to each other.

Each box has 2 keys. One to encrypt (which means to put into the box, a crypt)... and one to decrypt the message (take it out of the box).

Alice sent Bob her public key and Bob sent his to Alice. They keep their private keys in secure locations.

Unlike a regular message, there is no easy way for anybody else to get a message out of the crypt and read it. Even though the box is very light, it is very strong.

If Alice ever lost her private key, she would have to get a new set of keys, as they always and only work in pairs.

Alice can give copies of her public key away to anybody who wants one. She knows that they cannot be used to decrypt a message or to encrypt a message to anybody but her.

Figure 8-14  PKI with Alice and Bob
Storm Watching

- Refers to setting an IDS rule to watch for abnormal increases in network traffic
  - And to alert the security officer when they occur
- An unexpected increase in traffic could be evidence of an ACK storm
- Packet size can be cached for a short period
  - Two packets with the same header information but different sizes could be evidence of a hijacking in progress