Ethical Hacking and Countermeasures Web Applications and Data Servers 2nd edition EC-Council Solutions Manual

SKU: 9781305883451-SOLUTIONS

CEH-Bk3_Ch01-Review Question Answers

1. What is the main difference between active hijacking and passive hijacking?

   The essential difference between an active and passive hijack is that while an ***active attack*** takes over an existing session, a ***passive hijack*** monitors an ongoing session

2. In what situations might a hacker decide to use passive hijacking?

   A passive attack uses sniffers on the network, allowing attackers to obtain information such as user IDs and passwords. The attacker can later use this information to log on as a valid user and take over privileges. Password sniffing is the simplest attack when raw access to a network is obtained.

   In an active attack, the attacker takes over an existing session by either tearing down the connection on one side of the conversation or by actively participating. . On most current networks, sequence number prediction does not work because operating system vendors use random values for the initial sequence number, which makes sequential numbers harder to predict.

3. What are the four layers of a TCP stack? What is each one's role in hijacking?

   A. IE works at the ***application layer***. When it begins a connection between two hosts, it creates a request datagram to be sent across the Internet to the Web server to establish a connection.

   B. The transport protocol comes into play at the ***transport layer***, the layer of the TCP stack that allows connections between software services on connected systems. At the transport layer, the appropriate protocol header is added to the datagram. This header ensures the reliability of the data transported, and controls many aspects of the communication between the two hosts. The initial segment is a SYN request and the first phase of what is known as the TCP ***three-way handshake*** (SYN, SYN/ACK, and ACK used to establish a reliable connection-oriented session with the Web server.

   C. In the ***network layer***, routers allow the datagram to hop from the source to the destination, one hop at a time. The IP header is added to the packet in the network layer.

   D. The final layer is the ***data link layer***. This layer communicates with the physical hardware and is responsible for the delivery of signals from the source to the destination over a physical communication platform, in this case, the Ethernet. At this layer, the frame header is added to the datagram.

4. Why is it so difficult to predict TCP sequence numbers?

   TCP sequence numbers, unique per byte in a TCP session, provide flow control and data integrity. TCP segments give the initial sequence number (ISN) as a part

of each segment header. ISNs do not start at zero for each session; part of the handshake process is for each participant to state the ISN, and the bytes are numbered sequentially from that point.

In order to establish a spoofed connection using this session hijacking technique, an attacker must know the sequence numbers being used. IP spoofing forces the attacker to forecast the next sequence number. To send a command, an attacker uses blind hijacking, but the response cannot be viewed.

To do this, he would need to know the sequence number in use when he hijacked the session, which could be calculated as a result of knowing the ISN and the number of packets that have been exchanged. Successful session hijacking is difficult without the use of known tools and only possible when a number of factors are under the attacker's control.

5. Name two countermeasures to session hijacks. How does each stop the hijack?

   A. Limit incoming connections:

      a. Establish sessions with limited IP addresses. An example would be the IP address in an intranet where the specifics of the range of IPs are already known.

      b. If possible, try to limit unique session tokens to each browser's instance. For example, generate the token with a hash of the MAC address of the computer and process ID of the browser.

      c. Follow the same general set of countermeasures to prevent replay and brute force attacks.

   B. Use encryption:

      a. Use X.509 certificates (to encrypt via SSL, IPSec, SSH, S/MIME, or PGP) to prevent more traditional types of TCP traffic predictable sequence number hijacking.

      b. Force all incoming connections from the outside world to be fully encrypted. Attackers outside the network will have a difficult time if passwords are not sniffable, and so sessions cannot be hijacked.

      c. Connections to all mission-critical systems must be encrypted. The telnet package allows such administrative policies to be enforced. Kerberos allows encrypted communication.

      d. Communications on the network must be encrypted. Newer systems such as SKIP help a great deal, but they are in their infancy. (Sun Microsystems developed an automated key-management system called "Simple Key Management for Internet Protocols" that was later proposed to the IETF as a standard IPSec key-management scheme.)

e. Encrypted protocols should be used, e.g., those in Open SSH suite.

f. The OpenSSH suite includes the ssh program, which replaces login and telnet. SCP replaces RCP, and SFTP replaces FTP. It also includes sshd, which is the server side of the package, and other basic utilities such as ssh-add, ssh-agent, ssh-keygen, and sftp-server.

C. Minimize remote access:

a. Use strong authentication and peer-to-peer VPNs.

D. Use a secure protocol:

a. Configure the appropriate spoof rules on gateways (internal and external).

b. Monitor for ARP cache poisoning, by using IDS products or Arpwatch.

E. Educate users:

a. A user's identity must be verified at a higher level before conducting a potentially dangerous transaction such as transferring money online or using a credit card for online shopping.

b. Train users about suspicious activity and how to detect a breach in network security.

6. What are the differences between man-in-the-middle hijacking and blind hijacking?

In blind hijacking, a hacker can inject malicious data or commands into intercepted communications in a TCP session, even if source routing is disabled. The hacker can send data or comments, but cannot access the response. In order to get to the response, a man-in-the-middle attack works much better.

A man-in-the-middle attack uses a packet sniffer to intercept the communication between the client and the server. The attacker changes the default gateway of the client's machine and attempts to reroute packets. The technique used is to forge ICMP (Internet Control Message Protocol) packets to redirect traffic between the client and the host through the hijacker's host. The hacker's packets send error messages that indicate problems in processing packets through the original connection. This fools the server and the client to route through its path instead.

7. What is spoofing? What role does it play in hijacking?

Spoofing merely involves pretending to be another user or machine to gain access to a target machine or server.

In ARP spoofing, the IP address is vulnerable, and an attacker can also spoof the MAC address. An attacker sniffing on a network can sniff packets and carry out

simple attacks such as changing, deleting, rerouting, adding, forging, or diverting data

Perhaps the most popular among these attacks is the MITM attack. An attacker can grab unencrypted traffic from a victim's network-based TCP application, further tampering with the authenticity and integrity of the data before forwarding it on to the unsuspecting target.

8. What are the steps in hijacking?

   The hijack can be broken down into three broad phases:

   A. Tracking the connection

   B. Desynchronizing the connection

   C. Injecting the attacker's packet

9. What does a three-way handshake involve?

   A three-way handshake starts the connection and exchanges all the parameters needed for the two parties to communicate. TCP uses a three-way handshake to establish a new connection.

   Initially, the connection on the client side is in the closed state and the one on the server side is in the listening state. The client initiates the connection by sending the initial sequence number (ISN) and setting the SYN flag. Now the client is in the SYN-SENT state.

   When the server receives this packet, it acknowledges the client sequence number and sends its own ISN with the SYN flag set. The server's state is now SYN-RECEIVED. On receipt of this packet, the client acknowledges the server sequence number by incrementing it and setting the ACK flag. The client is now in the established state. At this point, the two machines have established a session and can begin communication.

10. Why is it easier to impersonate an actual user rather than break into a system as an unknown entity?

    It is easier to sneak in to a system as a genuine user than to attempt to enter a system directly. An attacker can hijack a genuine user's session by finding an established session and taking it over after the user has been authenticated. Once the session has been hijacked, the attacker can stay connected for hours without arousing suspicion. All routed traffic destined for the user's IP address comes to the attacker's system. During this time, the attacker can plant backdoors or even gain additional access to a system.

Chapter 1

Session Hijacking

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Additional Resources
- Key Terms

Lecture Notes

Overview

Chapter 1 introduces session hijacking and spoofing. Methods and details of hijacking are presented, along with countermeasures to preventing them. Tools used by both hijackers and network administrators are listed.

Chapter Objectives

- Explain what happens when a session is hijacked
- Describe the difference between spoofing and hijacking
- Name and describe the steps in conducting a session hijacking attack
- Describe different types of session hijacking
- Perform sequence number prediction
- Identify TCP/IP hijacking
- Identify session hijacking tools
- Describe countermeasures to session hijacking

Teaching Tips

Introduction to Session Hijacking

1. Identify methods used to hijack sessions: spoofing methods, the three-way TCP handshake, and man-in-the-middle attacks.

Session Hijacking

1. Define session hijacking: the exploitation of a valid computer session during which an attacker takes over a session between two computers.
2. Also define TCP session hijacking: an attacker takes control over a TCP session between two machines.
3. Point out that an attacker can interfere with or interrupt communication between users by diverting packets to his or her system.
4. Outline these steps in session hijacking:
    a. Tracking the connection.
    b. Desynchronizing the connection.
    c. Injecting the attacker's packet.

Understanding Session Hijacking

1. Insure that students know the terms and purposes of the TCP stack components.
    a. Application layer.

   b. Transport layer.
      i. Three-way handshake.
   c. Network layer.
   d. Data link layer.
2. Explain IPv4 as the fourth revision of the Internet Protocol. Note reasons it was important that IPv4 improved three basic security issues: authentication, integrity, and privacy.
3. Clarify the definition of spoofing: an attacker pretends to be another user or machine to gain access to a target machine or server.

Spoofing Versus Hijacking

1. Present a brief history of the 1988 Morris worm. Note that it combined blind spoofing and blind hijacking.
2. Explain that in blind hijacking an attacker predicts the sequence numbers that a victimized host sends in order to create a connection that appears to originate from the host, or a blind spoof. Further explain the sequence number assignment and prediction.
3. Add the use of source routing to discussion of hijacking. Source routing allows the sender to specify a specific route for an IP packet to take to the destination. The attacker performs source routing and then sniffs the traffic as it passes by the attacker.
4. Alternatively, a man-in-the-middle attack can be launched by an attacker source-routing IP packets through his or her system.
5. Note that IP address spoofing attacks can only be successful if IP addresses are used for authentication. An attacker cannot perform IP address spoofing or session hijacking if per-packet integrity checking is executed. Nor can a session be hijacked if it uses encryptions such as SSL or PPTP, because the attacker cannot participate in the key exchange.

Teaching Tip	Multiple authors have written about the Morris Worm in governmental, legal, technical, and news publications. An intriguing perspective was published by the Washington Post in 2013: https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/

Steps in Session Hijacking

1. Detail the three phases of a hijacking effort:
   a. Tracking the connection.
   b. Desynchronizing the connection.
   c. Injecting the attacker's packet.
2. Tracking the Connection

   a. A network sniffer tool is used to track a victim and host with a TCP sequence that is easy to predict.
   b. Once the victim is identified, the attacker captures sequence and acknowledgment numbers from the victim.
   c. The attacker uses sequence and/or acknowledgment numbers to construct packets.
3. Desynchronizing the Connection
   a. Explain the various conditions that can lead to a desynchronized state.
   b. Further explain the method(s) that attacker may use to desynchronize the target and server.
4. Injecting the Attacker's Packet
   a. Note that the connection between server and target, once interrupted, can be used by the attacker to inject data into the network or actively participate as the man-in-the-middle.

Types of Session Hijacking

1. Differentiate active and passive hijacking: an active attack takes over an existing session; a passive hijack monitors an ongoing session.
   a. Passive attacks use sniffers on the network, allowing attackers to obtain information such as user IDs and passwords. The attacker can later use the information to log on as a valid user and take over privileges.
   b. Active attack: an existing session is taken over by either tearing down the connection on one side of the conversation or by actively participating, such as a MITM.
2. Explain network-level hijacking: the interception of packets during transmission between client and server in a TCP/UDP session. Network-level hijacking includes:
   a. TCP/IP hijacking
   b. IP spoofing: source-routed packets.
   c. RST hijacking.
   d. Blind hijacking.
   e. Man-in-the-middle: packet sniffer.
   f. UDP hijacking.
3. Review the steps and components of the Three-Way Handshake.
4. Continue to review concepts of TCP functionality, noting the client and server states when each type of flag is received. Emphasize that the IP addresses and port numbers remain unchanged during a session, but sequence numbers change; a blind hijack can occur when an attacker guesses the correct sequence number and diverts the communication.
5. As noted, a successful three-way handshake in TCP creates a connection. A connection is uniquely defined by four elements: IP address of the sender, TCP port number of the sender, IP address of the receiver, and TCP port number of the receiver.
6. Show that the incrementing of sequence numbers can be seen in the three-way handshake. Each byte sent from a sender carries a sequence number that is acknowledged by the receiver; the receiver responds to the sender with the same sequence number. For security purposes, the sequence number for each connection is

different, and each session of a TCP connection has a different sequence number. Sequence numbers are 32 bits, so there are more than four billion possible combinations, which makes it very difficult to guess them. They are also critical for an attacker to hijack a session.

7. Randomness in the TCP connection ISN is created using PRNGs. However, over time, even computers choosing random numbers will repeat themselves because the randomness is based on an internal algorithm that a particular operating system uses. Once a sequence number has been agreed to, all the packets that follow will be the ISN+1. This makes injecting data into the communication stream possible.
8. Review some of the terms used in referring to ISN numbers:
    a. *SVR_SEQ*: Sequence number of the next byte to be sent by the server
    b. *SVR_ACK*: Next byte to be received by the server (the sequence number of the last byte received plus one).
    c. *SVR_WIND*: Server's receive window.
    d. *CLT_SEQ*: Sequence number of the next byte to be sent by the client.
    e. *CLT_ACK*: Next byte to be received by the client.
    f. *CLT_WIND*: Client's receive window.
9. Also review the TCP packet header fields:
    a. Source port: number.
    b. Destination port: number.
    c. Sequence number: Sequence number of the first byte in this packet.
    d. Acknowledgment number: Expected sequence number of the next byte to be received.
10. Review the control bits:
    a. *URG*: Urgent pointer
    b. *ACK*: Acknowledgment
    c. PSH: Push function
    d. RST: Reset the connection
    e. SYN: Synchronize sequence numbers
    f. FIN: No more data from sender
    g. Window: Window size of the sender
    h. Checksum: TCP checksum of the header and data
    i. Urgent pointer: TCP urgent pointer
    j. Options: TCP options
    k. SEG_*SEQ*: Refers to the packet sequence number (as seen in the header)
    l. SEG_*ACK*: Refers to the packet acknowledgment number
    m. SEG_*FLAG*: Refers to the control bits
11. Note possible steps an attacker might take:
    a. If a sequence number within the receive window is known, an attacker can inject data into the session stream or terminate the connection if he or she knows the number of bytes so far transmitted in the session (only applicable to a blind hijack).
    b. The attacker can guess a suitable range of sequence numbers and send out a number of packets into the network with different sequence numbers that fall within the appropriate range. Recall that the FIN packet is used to close a connection. Since the range is known, it is likely that the server accepts at least one packet. This way, the attacker does not send a packet for every sequence

number, but can resort to sending an appropriate number of packets with sequence numbers a window size apart.

c. An attacker can determine the number of packets to send by dividing the range of sequence numbers to be covered by the fraction of the window size used as an increment. PRNG takes care of the randomization. The difficulty of carrying out such attacks is directly proportional to the randomness of the ISNs. The more random the ISN, the more difficult it is to attack.

Sequence Number Prediction

1. Demonstrate how an attacker can predict sequence numbers.
   a. Once a client sends a connection request (SYN) packet to the server, the server responds (SYN/ACK) with a sequence number, which the client must then acknowledge (ACK).
   b. The sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from the forged IP address. The attacker does not see the SYN/ACK (or any other packet) from the server, but can guess the correct response. If the source IP address is used for authentication, the attacker can use one-sided communication to break into the server.

TCP/IP Hijacking

1. Explain TCP/IP hijacking: a technique that uses spoofed packets to take over a connection between a victim and a target machine. The attacker's machine must be on the same network as the victim. Steps in TCP/IP hijacking:
   a. The hacker sniffs the communication between the victim and the host in order to obtain the victim's ISN.
   b. Using the ISN, the attacker sends a spoofed packet from the victim's IP address to the host system.
   c. The host machine responds to the victim, assuming that the packet has arrived from it. This increments the sequence number.
2. Step through the process of IP spoofing using source-routed packets. First, the attacker spoofs the trusted host's IP address. The packets are source-routed, where the sender specifies the path for packets from the source to the destination IP. The server is fooled into thinking that it is communicating with the user. The hijacker then alters the sequence number and the acknowledgment number the server expects. Once this number is changed, the attacker must inject forged packets into the TCP session before the client can respond. This leads to the desynchronized state because the sequence and ACK numbers are not synchronized. The original packets are lost, and the server receives a packet with the new ISN. These packets are source-routed to a patched destination IP specified by the attacker.
3. Also explain RST hijacking: a form of TCP/IP hijacking in which an authentic-looking RST packet is added. If the hacker uses an accurate acknowledgement number, the victim's computer will believe that the original source sent the reset packet and will

reset the connection. RST hijacking is a type of DoS attack where access is denied to a service or resource. An RST hijack may utilize these tools:

a. Tcpdump: detects established connections by filtering packets that have the ACK flag turned on.
b. Awk: parses the output obtained from Tcpdump to derive the source and destination addresses, ports, MAC addresses, and sequence and acknowledgment numbers.
c. Nemesis: assembles TCP packets on a command line and injects them into network traffic.

4. Review how a TCP session can be an attractive target to a man-in-the-middle attack that uses a packet sniffer. The sniffer intercepts communication between the client and the server. The attacker changes the default gateway of the client's machine and attempts to reroute packets. The technique used is to forge packets to redirect traffic between the client and the host through the hijacker's host. The hacker's packets send error messages that indicate problems in processing packets through the original connection. This fools the server and the client to route through its path instead.
5. Mention ARP spoofing. Hosts use ARP tables to map local IP addresses to hardware addresses or MAC addresses. The attacker sends forged ARP replies that update the ARP tables at the host that is broadcasting ARP requests. Traffic sent to that IP will instead be delivered to the host.
6. Note that UDP hijacking is easier than TCP hijacking, because UDP does not use packet sequencing and synchronizing. The hijacker forges a server reply to the client UDP request before the server can respond. The server's reply can be easily restricted if sniffing is used. A man-in-the-middle attack in UDP hijacking can minimize the task of the attacker, as it can stop the server's reply from reaching the client in the first place.
7. Point out that session hijacking can take place on the network level and the application level. Network-level hijacking is an interception of packets during a transmission between client and server in TCP and UDP sessions. In application-level hijacking, the attacker gains control of an HTTP user session by obtaining session IDs.
8. In application-level hijacking, the attacker obtains the session IDs to get control of an existing session or to create a new unauthorized session. Following are ways of obtaining session IDs:
    a. Session IDs can be found:
        i. Embedded in the URL, which is received by the GET request in the application when the links embedded within a page are clicked by clients.
        ii. Embedded in the form as a hidden field and submitted to the HTTP's POST command.
        iii. In cookies on the client's local machine.
    b. Sniffing:
        i. Attackers can use packet sniffers. They can redirect traffic through their hosts when the HTTP traffic is unencrypted.
        ii. Unencrypted data carries session IDs, usernames, and passwords in plain text, which makes it easy for the session hijacker to obtain the information.
    c. Brute force:

i. Session IDs can be guessed by using the brute force technique: an attacker tries multiple possibilities of patterns until a session ID works.
ii. An attacker using a DSL line can make up to 1,000 session IDs per second.
iii. Typically used when the algorithm that produces session IDs is not random.

d. Misdirected trust:
i. Misdirected trust uses HTML injection and cross-site scripting to steal session information.
ii. In HTML injection, a malicious HTML code is injected by the attacker and executed by the client. Session data is returned to the hijacker.
iii. Cross-site scripting exploits the Web application's failure and authenticates user inputs before returning to the client system.

Session Hijacking Tools

1. Discuss an assortment of tools available to both hijackers and network administrators.
   a. TTY-Watcher: based on the IP Watcher utility, it is used to monitor and control users on a single system. Allows the user to monitor every TTY session on the system, as well as interact with them, by doing the following:
      i. Sharing a TTY.
      ii. Termination.
      iii. Stealing.
      iv. Returning the TTY.
   b. IP Watcher: a commercial session-hijacking tool that allows an administrator to monitor connections and helps in taking over sessions. Has ability to monitor an entire network.
   c. Remote TCP Session Reset Utility: will display a list of active TCP connections of a target computer. Any or all TCP connections can be reset. Other features:
      i. Reverse DNS lookup of the IP addresses for each session.
      ii. Display "well-known" port names.
      iii. Autorefresh the list of TCP sessions.
      iv. Automatically reset sessions based on the client's IP address.
   d. Paros HTTP Session Hijacking Tool: man-in-the-middle proxy and application vulnerability scanner. Allows users to intercept and modify HTTP and HTTPS data traversing between Web servers and client browsers. Also supports spidering, client certificates, proxy chaining, filtering, and various means of vulnerability scanning. Additional features:
      i. Add URL encoder/decoder in "Tools|Hash/Encoding . . . ."
      ii. Adds a comment panel in the log analyzer to show comments and a script panel in the log analyzer to show scripts.
      iii. Adds two filters, ReplaceRequestHeader and ReplaceRequestBody, to replace text in HTTP requests.
      iv. Can rename cookie tampering to CRLF Injection to better describe the scanner test case.
   e. Dnshijacker: a libnet/libpcap-based packet sniffer and spoofer that supports Tcpdump-type filters that explicitly target victims. DNS answers are forged

based on entries in a "fabrication table" or by forging a single answer to all requests. Also useful for network-level ad blocking and ad removal.

f. Hjksuite: a collection of hijacking programs:
   i. Hjklib: A library that implements a TCP/IP stack over hijacking.
   ii. Hjknetcat: A simple hijacker for textual connections. It allows the hacker to automatically hijack a connection to a port.
   iii. Hjkbnc: A hijacker for IRC connections. It requires the target connection and a port where it can bind.

Dangers Posed by Hijacking

1. Remind students of the potential results of hijacking: risk of identity theft, fraud, and loss of sensitive information.
2. Note that all networks that use TCP/IP are vulnerable to the types of hijacking discussed in this chapter.
3. Explain that even proactive security steps cannot guarantee protection:
   a. One-time passwords (smartcards, S/KEY, challenge-response): All one-time password schemes are vulnerable to connection hijacking. Once the user/service has authenticated, the connection can be taken over.
   b. Kerberos: Encryption is not enabled by default; because of this, security is of major concern because, just like the one-time password scheme, it is easily susceptible to hijacking.
   c. Source address filtering router: A network is susceptible to network address spoof attacks if its security depends on filtering the packets from unknown sources. An unknown host can insert itself midstream into a preexisting connection.
   d. Source address controlled proxies: Many proxies control access to certain commands based on the source address of the requestor. The source address is easily vulnerable to passive or active sniffers.

Teaching Tip	A plethora of resources are available at http://www.openssh.com/ and its umbrella organization, http://www.openbsd.org/

Countermeasures

1. Network administrators can utilize two methods to help prevent session hijacks:
   a. Implement available protections.
   b. Employ IPSec.
2. Protections:
   a. Limit incoming connections:
      i. Establish sessions with limited IP addresses.
      ii. Where possible, try to limit unique session tokens to each browser's instance.

iii. Follow the same general set of countermeasures to prevent replay and brute force attacks.

b. Use encryption:
   i. Use X.509 certificates (to encrypt via SSL, IPSec, SSH, S/MIME, or PGP) to prevent more traditional types of TCP traffic predictable sequence number hijacking.
   ii. Force all incoming connections from the outside world to be fully encrypted.
   iii. Connections to all mission-critical systems must be encrypted.
   iv. Communications on the network must be encrypted.
   v. Encrypted protocols should be used, such as the OpenSSH suite. The OpenSSH suite includes the ssh program, which replaces login and telnet. SCP replaces RCP, and SFTP replaces FTP. It also includes sshd, which is the server side of the package, and other basic utilities such as ssh-add, ssh-agent, ssh-keygen, and sftp-server.
c. Minimize remote access:
   i. Use strong authentication and peer-to-peer VPNs.
d. Use a secure protocol:
   i. Configure the appropriate spoof rules on gateways (internal and external).
   ii. Monitor for ARP cache poisoning, by using IDS products or Arpwatch.
e. Educate users:
   i. A user's identity must be verified at a higher level before conducting a potentially dangerous transaction such as transferring money online or using a credit card for online shopping.
   ii. Train users about suspicious activity and how to detect a breach in network security.

3. Explain IPSec protocols. Note particularly that they support the secure exchange of packets at the IP layer. Policies are assigned through Group Policy configuration of Active Directory domains and organizational units. IPSec deployment can be assigned at the domain, site, or organizational unit level.

Additional Resources

1. Additional insight about TCP hijacking is available in the following Technet article: https://technet.microsoft.com/en-us/magazine/2005.01.sessionhijacking.aspx

2. The Internet Protocol Journal featured a Lander University article on IP Spoofing: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html

3. Information security consultant Scott Helme provides a visual tutorial for session hijacking at his site: https://scotthelme.co.uk/advanced-session-hijacking/

Key Terms

- **Active attack** a hijacking attack in which an attacker finds an active session and hijacks it
- **Application layer** the layer of the TCP stack that provides services for user
- **Blind hijacking** in blind hijacking, an attacker correctly guesses the next ISN of a computer that is attempting to establish a connection; the attacker can send a command, such as setting a password to allow access from another location on the network, but the attacker can never see the response
- **Data link layer** the layer of the TCP stack that communicates with the physical hardware and is responsible for the delivery of signals from the source to the destination over a physical communication platform
- **Desynchronized state** a point when a connection between a target and host is in the established state, or in a stable state with no data transmission, or the server's sequence number is not equal to the client's acknowledgment number, or the client's sequence number is not equal to the server's acknowledgment number
- **IPv4 standard** the fourth revision of the Internet Protocol
- **ISN** *see* sequence numbers
- **Network layer** the layer in the TCP stack that actually moves packets from computer to computer in a network
- **Passive hijack** an attack in which an attacker hijacks a session, but simply watches or records the data flow between the session participants
- **Sequence numbers** a code used during the three-way handshake in TCP that establishes a connection between two computers
- **Session hijacking** the exploitation of a valid computer session where an attacker takes over a session between two computers to gain access to restricted information or services on a network
- **Source routing** a process that allows the sender to specify a specific route for an IP packet to take to the destination
- **Spoofing** a process in which an attacker pretends to be another user or machine to gain access to a target machine or server
- **TCP session hijacking** a process in which an attacker takes over a TCP session between two machines
- **Three-way handshake** the method used to establish a connection between computers in TCP; shorthand for this handshake is SYN, SYN/ACK, ACK
- **Transport layer** the layer of the TCP stack that allows connections between software services on connected systems