CENGAGE
Learning®

EC-Council | Press

ETHICAL HACKING
AND COUNTERMEASURES

WEB APPLICATIONS AND DATA SERVERS

Second Edition

Book 3 of 4

C|EH™
Certified Ethical Hacker

Web Applications and Data Servers

EC-Council | Press

Book 3 of 4

C|EH™

Certified Ethical Hacker

Certification

CENGAGE Learning®

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CENGAGE
Learning®

Ethical Hacking and Countermeasures: Web Applications and Data Servers (CEH)

EC-Council Press

SVP, GM Skills & Global Product Management: Dawn Gerrain

Product Director: Kathleen McMahon

Product Team Manager: Kristin McNary

Associate Product Manager: Amy Savino

Senior Director, Development: Marah Bellegarde

Product Development Manager: Leigh Hefferon

Managing Content Developer: Emma Newsom

Senior Content Developer: Natalie Pashoukos

Product Assistant: Abigail Pufpaff

Vice President, Marketing Services: Jennifer Ann Baker

Marketing Coordinator: Cassie Cloutier

Senior Production Director: Wendy Troeger

Production Director: Patty Stephan

Senior Content Project Manager: Brooke Greenhouse

Managing Art Director: Jack Pendleton

Software Development Manager: Pavan Ethakota

Cover Image(s): Istockphoto.com/gong hangxu and Istockphoto.com/Turnervisual

EC-Council:

President | EC-Council: Jay Bavisi
Vice President, North America | EC-Council: Steven Graham

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product,
submit all requests online at **www.cengage.com/permissions**.
Further permissions questions can be e-mailed to
permissionrequest@cengage.com.

Library of Congress Control Number: 2016930622

ISBN: 978-1-305-88345-1

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Notice to the Reader

Cengage Learning and EC-Council do not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Cengage Learning and EC-Council do not assume, and expressly disclaim, any obligation to obtain and include information other than that provided to them by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. Cengage Learning and EC-Council make no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and Cengage Learning and EC-Council take no responsibility with respect to such material. Cengage Learning and EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2016

Brief Table of Contents

Table of Contents

CHAPTER 3

CHAPTER 4

CHAPTER 5

Preface

Hacking and electronic crimes sophistication is consistently growing at an exponential rate. Recent reports have indicated that cybercrime already surpasses the illegal drug trade! Unethical hackers, better known as *black hat hackers*, are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting them and profiting from the exercise. High-profile crimes have proven that the traditional approach to computer security is simply not sufficient, even with the strongest perimeter; properly configured defense mechanisms such as firewalls, intrusion detection, and prevention systems; strong end-to-end encryption standards; and antivirus software. Hackers have proven their dedication and ability to systematically penetrate networks all over the world. In some cases, black hat hackers may be able to execute attacks so flawlessly that they can compromise a system, steal everything of value, and completely erase their tracks in less than 20 minutes!

The EC-Council | Press is dedicated to stopping hackers in their tracks.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization comprised of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker* (C|EH) program. The goal of this program is to teach the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the C|EH program has rapidly gained popularity around the globe and is now delivered in more than 70 countries by more than 600 authorized training centers. More than 100,000 information security practitioners have been trained.

C|EH is the benchmark for many government entities and major corporations around the world. Shortly after C|EH was launched, EC-Council developed the *Certified Security Analyst* (E|CSA). The goal of the E|CSA program is to teach groundbreaking analysis methods that must be applied while conducting advanced penetration testing. The E|CSA program leads to the *Licensed Penetration Tester* (L|PT) status. The *Computer Hacking Forensic Investigator* (C|HFI) was formed with the same design methodologies and has become a global standard in certification for computer forensics. EC-Council, through its impervious network of professionals and huge industry following, has developed various other programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Being provided with a true hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

About the EC-Council | Press

The EC-Council | Press was formed in late 2008 as a result of a cutting-edge partnership between global information security certification leader EC-Council and leading educational content, technology, and services company Cengage Learning. This partnership marks a revolution in academic textbooks and courses of study in information security, computer forensics, disaster recovery, and end-user security. By identifying the essential topics and content of EC-Council professional certification programs, and repurposing this world-class content to fit academic programs, the EC-Council | Press was formed. The academic community is now able to incorporate this powerful cutting-edge content into new and existing information security programs. By closing the gap between academic study and professional certification, students and instructors are able to leverage the power of rigorous academic focus and high-demand industry certification. The EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating the growing epidemic of cybercrime and the rising threat of cyber-war.

Ethical Hacking and Countermeasures Series

The EC-Council | Press *Ethical Hacking and Countermeasures* series is intended for those studying to become security officers, auditors, security professionals, site administrators, and anyone who is concerned about or responsible for the integrity of the network infrastructure. The series includes a broad base of topics in offensive network security, ethical hacking, as well as network defense and countermeasures. The content of this series is designed to immerse learners into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, ethical hackers are able to set up strong countermeasures and defensive systems to protect their organization's critical infrastructure and information. The series, when used in its entirety, helps prepare readers to take and pass the C|EH certification exam from EC-Council.

Books in Series

- *Ethical Hacking and Countermeasures: Attack Phases*/9781305883437
- *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*/9781305883444
- *Ethical Hacking and Countermeasures: Web Applications and Data Servers*/9781305883451
- *Ethical Hacking and Countermeasures: Secure Network Operating Systems and Infrastructures*/ 9781305883468

Web Applications and Data Servers

Web Applications and Data Servers provides an overview of session hijacking, how to hack Web servers and database servers, as well as password-cracking techniques and Web application vulnerabilities.

Chapter Contents

Chapter 1, *Session Hijacking*, covers various hacking technologies used in session hijacking, including spoofing methods, the three-way TCP handshake, and how attackers use these methods for man-in-the-middle attacks. Chapter 2, *Hacking Web Servers*, highlights the various security concerns having to do with Web servers including server bugs, malicious code, and network security. Chapter 3, *Web Application Vulnerabilities*, shows the various kinds of vulnerabilities that can be discovered in Web applications, as well as attacks exploiting these vulnerabilities. Chapter 4, *Web-Based Password Cracking Techniques*, explains the relationship between passwords and authentication and discusses passwords within the broader context of authentication. Chapter 5, *Hacking Web Browsers*, provides an understanding of Web browsers, security of, and how to hack various browsers. The browsers discussed include Firefox, Internet Explorer, Opera, and Safari. Chapter 6, *Hacking Database Servers-SQL Injection*, provides an understanding on how database servers are hacked and concentrates on SQL injection, how it works, and what administrators can do to prevent it.

Chapter Features

Many features are included in each chapter, and all are designed to enhance the reader's learning experience. Features include:

- *Objectives* begin each chapter and focus the learner on the most important concepts in the chapter.
- *Key Terms* are designed to familiarize the learner with terms that will be used within the chapter.
- *What If?*, found in each chapter, presents short scenarios followed by questions that challenge the learner to arrive at an answer or solution to the problem presented.
- *Chapter Summary*, at the end of each chapter, serves as a review of the key concepts covered in the chapter.
- *Review Questions* allow learners to test their comprehension of the chapter content.

- *Hands-On Projects* encourage learners to apply the knowledge they have gained after finishing the chapter. Files for the Hands-On Projects can be found in the MindTap or on the Student Resource Center. Visit *www.cengagebrain.com* for a link to the Student Resource Center.

MindTap

MindTap for Ethical Hacking and Countermeasures Series is an online learning solution designed to help students master the skills they need in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps users achieve this with assignments and activities that provide hands-on practice, real-life relevance, and mastery of difficult concepts. Students are guided through assignments that progress from basic knowledge and understanding to more challenging problems.

All MindTap activities and assignments are tied to learning objectives. The hands-on exercises provide real-life application and practice. Readings and "Whiteboard Shorts" support the lecture, while "In the News" assignments encourage students to stay current. Pre- and post-course assessments allow you to measure how much students have learned using analytics and reporting that makes it easy to see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as-is, or pick and choose how the material will wrap around your own. You control what the students see and when they see it. Learn more at *www.cengage.com/mindtap/*.

Student Resource Center

The Student Resource Center contains all the files you need to complete the Hands-On Projects found at the end of the chapters. Visit *www.cengagebrain.com* to access the Student Resource Center.

Additional Instructor Resources

Free to all instructors who adopt *Web Applications and Data Servers* for their courses is a complete package of instructor resources. These resources are available from the Cengage Learning Web site, *www.cengagebrain.com*, by going to the product page for this book in the online catalog and choosing "Instructor Downloads."

Resources include:

- *Instructor's Manual*: This manual includes course objectives and additional information to help your instruction.
- *Cengage Learning Testing Powered by Cognero:* A flexible, online system that allows you to import, edit, and manipulate content from the text's test bank or elsewhere, including your own favorite test questions; create multiple test versions in an instant; and deliver tests from your LMS, your classroom, or wherever you want.
- *PowerPoint Presentations*: A set of Microsoft PowerPoint slides is included for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.

- *Labs*: These are additional hands-on activities to provide more practice for your students.
- *Assessment Activities*: These are additional assessment opportunities including discussion questions, writing assignments, Internet research activities, and homework assignments along with a final cumulative project.
- *Final Exam*: This exam provides a comprehensive assessment of *Web Applications and Data Servers* content.

Cengage Learning Tech Connection: Information Security Community

This site was created for learners and instructors to find out about the latest in information security news and technology.

Visit *http://community.cengage.com/InfoSec2/* to:

- Learn what's new in information security through live news feeds, videos, and podcasts;
- Connect with your peers and security experts through blogs and forums;
- Browse our online catalog.

How to Become C|EH Certified

The C|EH certification focuses on hacking techniques and technology from an offensive perspective. The certification is primarily targeted at security professionals who want to acquire a well-rounded body of knowledge to have better opportunities in this field. Acquiring a C|EH certification means the candidate has a minimum baseline knowledge of security threats, risks, and countermeasures. An organization can rest assured that they have a candidate who is more than a systems administrator, a security auditor, a hacking tool analyst, or a vulnerability tester. The candidate is assured of having both business and technical knowledge.

C|EH certification exams are available through Pearson Vue testing centers. To finalize your certification after your training by taking the certification exam through a Pearson Vue testing center, you must:

1. Apply for and purchase an exam voucher by visiting the EC-Council Academic Center of Excellence at *http://ace.eccouncil.org*, if one was not purchased with your book.
2. If you have a Pearson Vue voucher, please contact a local Pearson Vue testing center accordingly to schedule your exam, or visit *www.pearsonvue.com/eccouncil/*.
3. Take and pass the C|EH certification examination with a score of 70 percent or better.

Additional EC-Council | Press Products

Computer Forensics Series

The EC-Council | Press *Computer Forensics* series, preparing learners for C|HFI certification, is intended for those studying to become police investigators and other law enforcement personnel; defense and military personnel; e-business security professionals; systems administrators; legal professionals; banking, insurance and other professionals; government agencies; and IT managers. The content of this program is designed to expose the learner to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Advanced techniques in computer investigation and analysis with interest in generating potential legal evidence are included. In full, this series prepares the learner to identify evidence in computer-related crime and abuse cases as well as track the intrusive hacker's path through client system. The series when used in its entirety helps prepare readers to take and pass the C|HFI Certified Forensic Investigator certification exam from EC-Council.

Books in Series

- *Computer Forensics: Investigation Procedures and Response*/9781305883475
- *Computer Forensics: Investigating File and Operating Systems, Wireless Networks and Storages*/9781305883482
- *Computer Forensics: Investigating Data and Image Files*/9781305883499
- *Computer Forensics: Investigating Network Intrusions and Cybercrime*/9781305883505

EC-Council's Supporting Events

TakeDownCon

TakeDownCon is a highly technical forum that focuses on the latest vulnerabilities, the most potent exploits, and current security threats. The best and the brightest come to share their knowledge, giving delegates the opportunity to learn about the industry's most important issue. With two days and two dynamic tracks, delegates will spend Day 1 on the Attack, learning how even the most protected systems can be breached. Day 2 is dedicated to Defense, and delegates will learn if their defense mechanisms are on par to thwart nefarious and persistent attacks.

For more information, visit the Web site: *www.takedowncon.com*.

Hacker Halted

Hacker Halted builds on the educational foundation of EC-Council's courses in ethical hacking, computer forensics, penetration testing, and many others. Hacker Halted brings the industry's leading researchers, practitioners, ethical hackers, and other top IT security professionals together to discuss current issues facing our industry. Hacker Halted has been delivered globally in countries such as Egypt, Mexico, Malaysia, Hong Kong, Iceland, and in the United States, in cities such as Myrtle Beach, Miami, and most recently in Atlanta.

For more information, visit the Web site: *www.hackerhalted.com*.

Global CyberLympics

Global CyberLympics is an online ethical hacking computer network defense competition. The goal is to raise awareness of increased education and ethics in information security through a series of cyber competitions that encompass forensics, ethical hacking, and defense. Teams are made up of four to six players, and each round serves as an elimination round until the top teams remain. The top teams from each region get invited to play live in-person at the world finals.

For more information, visit the Web site: *www.cyberlympics.org*.

Acknowledgments

Michael H. Goldner is the Dean of EC-Council University. He has been involved in the information security arena for over 20 years and has dedicated the last 15 years to developing hands-on academic curricula to help train the world's future cyber leaders. He received his Juris Doctorate from Stetson University College of Law and his undergraduate degree from Miami University. He is an active member of the American Bar Association and a member of the Cyber Law subcommittee. He is a member of IEEE, ISSA ISC2, ISACA and PMI, and holds a number of industrially recognized certifications, including C|CISO, CISSP, CISM, CEI, CEH, CHFI, MCT, MCSE/Security, MCSA, Security +, Network +, and A+.

He has worked closely with EC-Council and Cengage Learning in the creation of this EC-Council Press series on information security and computer forensics, and is passionate about creating a viable international leadership corps to guide our electronically connected society into a safe and prosperous future.

chapter 1

Session Hijacking

After completing this chapter, you should be able to:

- 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

What If?

Daniel is a Web designer for Xeemahoo, Inc., a news agency. Inaccurate or fallacious news on the Web site poses a threat to the company: the agency can be sued for publishing false information. Part of Daniel's responsibilities is to upload HTML files to the Web site each day. He confirms with the editors that the content is accurate. Then he marks up the news with HTML tags and uploads it to the server of AgentonWeb, the hosting site.

One day, Daniel checks the daily upload to ensure that accurate news was posted, but discovers that incorrect, damaging information has been uploaded in place of the marked-up files.

Jason Springfield, an ethical hacker, was called in to investigate the situation at Xeemahoo. Investigations revealed that Daniel's session was hijacked by an Agenton employee during the upload. A disgruntled employee of AgentonWeb had files that contained the fallacious information on his desktop.

- How did this happen?
- Is there a problem with the Web server configuration?
- How can this be prevented in the future?
- Is there a risk in outsourcing Web hosting to third-party service providers?

Introduction to Session Hijacking

This chapter covers various hacking technologies used in session hijacking. It deals with spoofing methods, the three-way TCP handshake, and how attackers use these methods for man-in-the-middle attacks. Various tools that can be used for this purpose have been highlighted to provide insight into session hijacking. Finally, countermeasures to prevent session hijacking are discussed.

Devices that implement IP address–based session management use a specific algorithm. This algorithm is described by the pseudocode shown below:

```
if (submitted username and submitted password) == (credentials on
device config)
    then
    do white-list user's source IP address
```

Devices in environments in which multiple users share a single proxy are vulnerable to administrative session-hijacking attacks. An attacker does not need to intercept or sniff the traffic between the victim's admin user and the target device to attack these devices. In addition, administrative session hijacking performs session hijacking at the HTTP application layer by giving administrative information used by the target devices. Some of this information includes the names of users who have accessed the unauthorized resources on the Web console.

For example, consider a corporate environment in which many employees share the same Internet proxy. Now, assume that the administrator of this vulnerable device does not verify the bypass proxy server for local addresses option is turned on. This means that the administrator configures the vulnerable devices through a proxy now available to every user on the network, including hackers.

A malicious user using the same proxy can mimic administrative privileges and get the full range of administrative access through the Web console by adding the IP address of a device on the address bar of a browser. An administrative session-hijacking attack allows attackers to easily gain access over admin sessions on the Web browser to perform malicious operations, that is, backdoor the device by creating a new administrative account.

Session Hijacking

Session hijacking refers to the exploitation of a valid computer session during which an attacker takes over a session between two computers. The attacker steals a valid session ID and uses it to get into the system and extract the data. During **TCP session hijacking**, an attacker takes control over a TCP session between two machines. An attacker who is logged on to a system can participate in the conversation of other users on other systems by diverting packets to his or her system. This hijacking is carried out through source-routed IP packets. Blind hijacking is another method through which responses on a system can be assumed. The man-in-the-middle (MITM) attack is a method in which a sniffer is used to track down a conversation between two users. A denial-of-service (DoS) attack is executed so that a system crashes, which leads to a greater loss of packets.

The following are the steps in session hijacking:

1. Tracking the connection
2. Desynchronizing the connection
3. Injecting the attacker's packet

Understanding Session Hijacking

At the simplest level, TCP hijacking relies on the violation of the trust relationship between two interacting hosts.

Dissecting the TCP Stack Before going into the details of session hijacking and understanding why this attack is possible, look at the TCP stack shown in Figure 1-1. Consider an

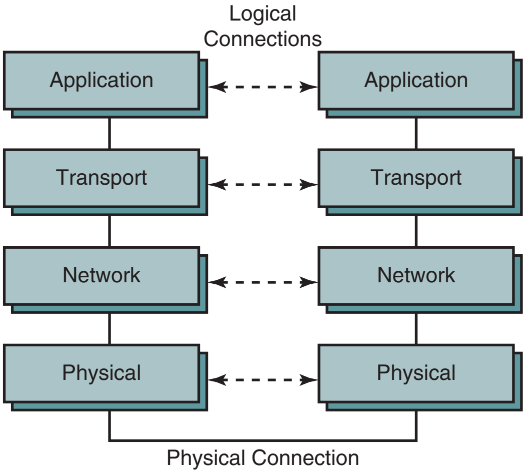

Figure 1-1 The layers of the TCP stack.

everyday scenario in which computers access the Internet using a Web browser such as Internet Explorer (IE):

1. 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.
2. 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, as shown in Figure 1-4) used to establish a reliable connection-oriented session with the Web server.
3. 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.
4. 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.

When the datagram finally reaches its destination, the headers peel off.

Security Issues and Basic Attacks in IPv4 **IPv4 standard** is the fourth revision of the Internet Protocol. The original IPv4 standard should have addressed three basic security issues: authentication, integrity, and privacy. An attacker can easily spoof an IP address and exploit a session, so authentication is critical. 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.

Session hijacking is the process of taking over an existing active session, whereas in a spoofing attack, an attacker does not actively take another user offline to perform the attack. **Spoofing** merely involves pretending to be another user or machine to gain access to a target machine or server.

Spoofing Versus Hijacking

In 1988, the Morris worm, a quickly replicating worm that could hijack sessions, affected nearly 6,000 computers on the ARPANET, the predecessor of the global Internet. Robert T. Morris exploited the predictable nature of the sequence number that formed the security of a TCP/IP connection. His program spread through the computers and performed an action in an infinite loop, copying itself onto every computer within its reach. His program involved both blind spoofing and blind hijacking. 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.

In order to understand blind hijacking, it is important to understand sequence number prediction. 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.

Remember that blind session hijacking relies on the attacker's ability to predict or guess sequence numbers. An attacker cannot spoof a trusted host on a different network and see the reply packets because the packets are not routed back to his or her IP address. Neither can the attacker resort to ARP cache poisoning because routers do not route ARP broadcasts across the Internet. As the attacker is unable to see the replies, he or she is forced to anticipate the responses from the victim and prevent the host from sending a TCP/RST packet to the victim. The attacker predicts sequence numbers the remote host is expecting from the victim and then hops into the communication. This method is used extensively to exploit the trust relationships between users and remote machines.

Simple IP spoofing is fairly easy to do and is used in various attack methods. To create new raw packets, the attacker must have root access on the machine. But, 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.

In the case of IP spoofing not involving a session hijack, guessing the sequence number is not required since there is no session currently open with that IP address. In a session hijack, the traffic would get back to the attacker only if using source routing. **Source routing** is a process that 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. Captured authentication credentials are used to establish a session in session spoofing. Here, active hijacking eclipses a preexisting session. Due to this attack, the legitimate user may lose access or may be deprived of the normal functionality of his or her established telnet session that has been hijacked by the attacker, who now acts with the user's privileges. Since most authentications only happen at the initiation of a session, this allows the attacker to gain access to a target machine. Another method is to use source-routed IP packets. This man-in-the-middle attack allows an attacker to become a part of the target-host conversation by deceptively guiding the IP packets to pass through his or her system.

Session hijacking is more difficult than IP address spoofing. In session hijacking, John (an intruder) would seek to insert himself into a session that Jane (a legitimate user) already had set up with \\Mail. John would wait until she establishes a session, then knock her off the air by some means, such as a denial of service, and then pick up the session as though he were she. Then John would send a scripted set of packets to \\Mail and would be able to see the responses. 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. Knowledge of the ISN would be the least of John's challenges. For instance, he would need a way to knock Jane off the air when he wanted to, and also need a way to know the exact status of Jane's session at the moment he mounted his attack. Both of these require that John have far more knowledge and control over the session than would normally be possible.

However, 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. In the same way, IP address spoofing and session hijacking are not possible if the session uses encryptions such as SSL or PPTP. Consequently, the attacker cannot participate in the key exchange.

In summary, the hijacking of nonencrypted TCP communications requires the presence of nonencrypted session-oriented traffic, the ability to recognize TCP sequence numbers that predict the next sequence number (NSN), and the ability to spoof a host's MAC or IP address in order to receive communications that are not destined for the attacker's host. If the attacker is on the local segment, he or she can sniff and predict the ISN+1 number and route the traffic back to him or her by poisoning the ARP caches on the two legitimate hosts participating in a session.

Steps in Session Hijacking

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.

How does an attacker go about hijacking a session? The hijack can be broken down into three broad phases:

1. Tracking the connection
2. Desynchronizing the connection
3. Injecting the attacker's packet

Tracking the Connection The attacker uses a network sniffer to track a victim and host or uses a tool like Nmap to scan the network for a target with a TCP sequence that is easy to predict. Once the victim is identified, the attacker captures sequence and acknowledgment numbers from the victim. Because packets are checked by TCP through sequence and/or acknowledgment numbers, the attacker uses these numbers to construct packets.

Desynchronizing the Connection A **desynchronized state** occurs when a connection between the 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.

To desynchronize the connection between the target and host, the attacker must change the sequence number or the acknowledgment number (SEQ/ACK) of the server. To do this, the attacker sends null data to the server so that the server's SEQ/ACK numbers will advance, while the target machine will not register such an increment. For example, before desynchronization, the attacker monitors the session without any kind of interference. The attacker then sends a large amount of null data to the server. These data change the ACK number on the server but do not affect anything else. Now the server and target are desynchronized.

Another approach is to send a reset flag to the server to bring down the connection on the server side. Ideally, this occurs in the early setup stage of the connection. The attacker's goal is to break the connection on the server side and create a new connection with a different sequence number.

The attacker listens for a SYN/ACK packet from the server to the host. On detecting the packet, the attacker immediately sends an RST packet to the server and a SYN packet with exactly the same parameters, such as a port number, but with a different sequence number. The server, on receiving the RST packet, closes the connection with the target and initiates another one based on the SYN packet, but with a different sequence number on the same port. After opening a new connection, the server sends a SYN/ACK packet to the target for acknowledgement. The attacker detects (but does not intercept) this and sends back an ACK packet to the server. Now the server is in the established state. The main aim is to keep the target conversant, and switch to the established state when it receives the first SYN/ACK packet from the server. Now both server and target are in a desynchronized, but established, state.

This can also be done using a FIN flag, but this will cause the server to respond with an ACK and give away the attack through an ACK storm. This occurs because of a flaw in this method of hijacking a TCP connection. While receiving an unacceptable packet, the host acknowledges it by sending the expected sequence number. This unacceptable packet generates an acknowledgment packet, thereby creating an endless loop for every data packet. The mismatch in SEQ/ACK numbers results in excess network traffic with both the server and target trying to verify the right sequence. Since these packets do not carry data, they are not retransmitted if the packet is lost. However, since TCP uses IP, the loss of a single packet puts an end to the unwanted conversation between the server and the target.

The desynchronizing stage is added in the hijack sequence so that the target host is ignorant about the attack. Without desynchronizing, the attacker is able to inject data to the server and even keep his or her identity by spoofing an IP address. However, the attacker will have to put up with the server's response being relayed to the target host as well.

Injecting the Attacker's Packet Once the attacker has interrupted the connection between the server and target, he or she can choose either to inject data into the network or actively participate as the man-in-the-middle, passing data from the target to the server, and vice versa, reading and injecting data at will. This process is shown in Figure 1-2.

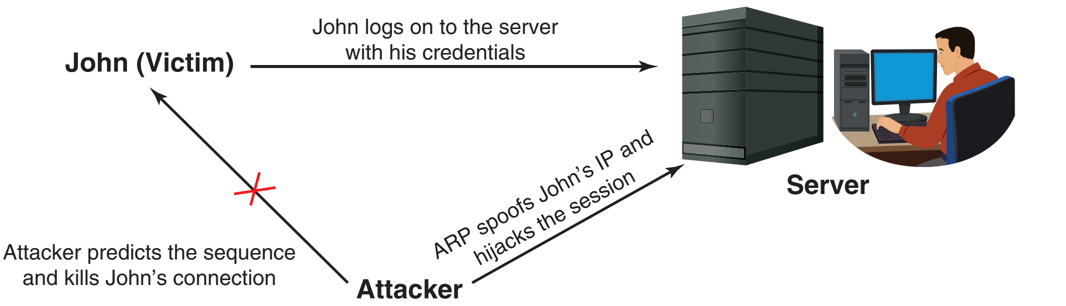
John (Victim)
John logs on to the server with his credentials
Server
Attacker predicts the sequence and kills John's connection
ARP spoofs John's IP and hijacks the session
Attacker

Figure 1-2 In this scenario, John is a valid user. His connection is hijacked once the sequence numbers are predicted and injected.

Types of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker. 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.

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. Countering this attack are methods that range from identification schemes (such as a one-time password like S/KEY) to ticketing identification (such as Kerberos). These techniques protect the data from being sniffed, but they cannot protect it from active attacks unless it is encrypted or carries a digital signature.

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. An example of an active attack is the man-in-the-middle (MITM) attack. For this attack to succeed, the attacker must guess the sequence number before the target responds to the server. 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.

Network-Level Hijacking Network-level hijacking is the interception of packets during the transmission between client and server in a TCP/UDP session. Attacks on network level sessions provide the attacker with critical information to attack application level sessions.

Network-level hijacking includes the following:

- TCP/IP hijacking
- IP spoofing: source-routed packets
- RST hijacking
- Blind hijacking
- Man-in-the-middle: packet sniffer
- UDP hijacking

The Three-Way Handshake When two parties establish a connection using TCP, they perform a three-way handshake. 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. The illustration in Figure 1-3 shows how this exchange works.

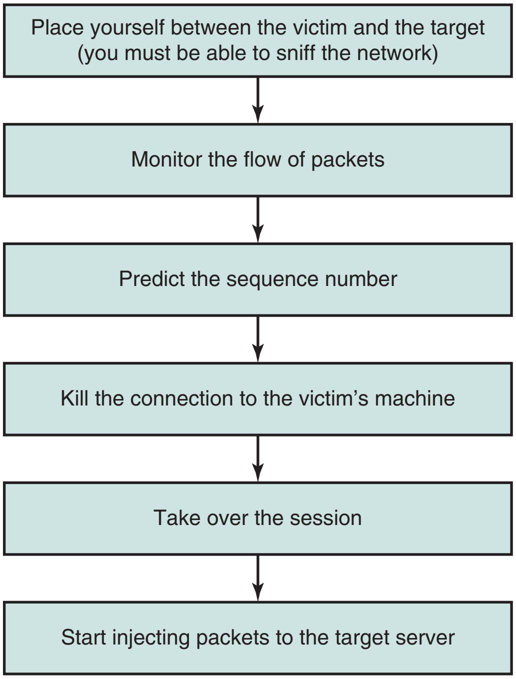
Place yourself between the victim and the target
(you must be able to sniff the network)
Monitor the flow of packets
Predict the sequence number
Kill the connection to the victim's machine
Take over the session
Start injecting packets to the target server

Figure 1-3 If the attacker can anticipate the next sequence and ACK number Bob will send, the attacker can spoof Bob's address and begin communicating with the server.

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.

TCP Concepts On receiving the client's acknowledgement, the server enters the established state and sends back the acknowledgment, incrementing the client's sequence number. The connection can be closed by either using the FIN or RST flag or by timing out.

If the RST flag of a packet is set, the receiving host enters the CLOSED state and frees all resources associated with this instance of the connection. Any additional incoming packets for that connection will be dropped.

If the packet is sent with the FIN flag turned on, the receiving host closes the connection as it enters the CLOSE-WAIT mode. The packets sent by the client are accepted in an established connection if the sequence number is within the range and follows its predecessor.

If the sequence number is beyond the range of the acceptable sequence numbers, the packet is dropped and an ACK packet will be sent using the expected sequence number.