

Covers all Exam Objectives for CEHv6



Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

STUDY GUIDE


Exam 312-50
Exam EC0-350

Kimberly Graves



SERIOUS SKILLS.

Chapter 7. Denial of Service and Session Hijacking.....	1
Section 7.1. Denial of Service.....	2
Section 7.2. Session Hijacking.....	11
Section 7.3. Summary.....	15
Section 7.4. Exam Essentials.....	16
Section 7.5. Review Questions.....	17
Section 7.6. Answers to Review Questions.....	21



Chapter 7

Denial of Service and Session Hijacking

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Understand the types of DoS attacks
- ✓ Understand how a DDoS attack works
- ✓ Understand how BOTs/BOTNETs work
- ✓ What is a “smurf” attack?
- ✓ What is “SYN” flooding?
- ✓ Describe the DoS/DDoS countermeasures
- ✓ Understand spoofing vs. hijacking
- ✓ List the types of session hijacking
- ✓ Understand sequence prediction
- ✓ What are the steps in performing session hijacking?
- ✓ Describe how you would prevent session hijacking



During a denial-of-service (DoS) attack, a hacker renders a system unusable or significantly slows the system by overloading resources or preventing legitimate users from accessing the system. These attacks can be perpetrated against an individual system or an entire network and are usually successful in their attempts. The hacking attack is one of availability, meaning legitimate users no longer have access to the network.

Session hijacking is a hacking method that creates a temporary DoS for an end user when an attacker takes over the session. Session hijacking is used by hackers to take over a current session after the user has established an authenticated session. Session hijacking can also be used to perpetrate a man-in-the-middle attack when the hacker steps between the server and legitimate client and intercepts all traffic.

This chapter explains DoS attacks, distributed denial-of-service (DDoS) attacks, and the elements of session hijacking, such as spoofing methods, the TCP three-way handshake, sequence-number prediction, and how hackers use tools for session hijacking. In addition, the countermeasures for DoS and session hijacking are discussed at the end of this chapter.

Denial of Service

A DoS attack is an attempt by a hacker to flood a user's or an organization's system. As a CEH, you need to be familiar with the types of DoS attacks and should understand how DoS and DDoS attacks work. You should also be familiar with robots (BOTs) and robot networks (BOTNETs), as well as smurf attacks and SYN flooding. Finally, as a CEH, you need to be familiar with various DoS and DDoS countermeasures.

There are two main categories of DoS attacks:

- Attacks sent by a single system to a single target (simple DoS)
- Attacks sent by many systems to a single target (distributed denial of service, or DDoS)

The goal of DoS isn't to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A DoS attack may do the following:

- Flood a network with traffic, thereby preventing legitimate network traffic.
- Disrupt connections between two machines, thereby preventing access to a service.
- Prevent a particular individual from accessing a service.
- Disrupt service to a specific system or person.

Different tools use different types of traffic to flood a victim, but the result is the same: a service on the system or the entire system is unavailable to a user because it's kept busy trying to respond to an exorbitant number of requests.



Real World Scenario

A Denial of Service Attack

On the evening of May 28, 2008, the company I was working for (alfasystems.com) suddenly dropped off the Internet. Their web servers were no longer accessible from the Internet.

Within a minute of the start of the attack, it was clear to the Alpha Systems engineers that they were experiencing a “packet flooding” attack of some sort. After looking at the log files of their Cisco router, it showed that both of their two T1 trunk interfaces to the Internet were receiving some sort of traffic at their maximum 1.54 megabit rate, while their outbound traffic had fallen to nearly zero. They were drowning in a flood of malicious traffic and valid traffic was unable to get out. Alpha Systems was the victim of a denial-of-service attack, more commonly referred to as a DoS. The engineers knew they had to do something quickly to stop the attack and get the web servers back up and accessible for their customers. But no one really knew what to do as this had never happened to the systems before. Then someone thought of the packet filtering capabilities of the router.

Luckily, because this DoS attack was prone to filtering, Alpha Systems was able to weed out the bad packets and return their service to almost normal operation. In two minutes Alpha Systems engineers applied “brute force” filters to their routers, shutting down all UDP and ICMP traffic, and alfasystems.com instantly popped back onto the Internet.

It was finally determined that their server had been attacked by 474 security-compromised Windows PCs containing remote-control attack “zombies,” in a classic DoS attack generated by the coordinated efforts of these hundreds of individual PCs.

A DoS attack is usually an attack of last resort. It's considered an unsophisticated attack because it doesn't gain the hacker access to any information but rather annoys the target and interrupts their service. DoS attacks can be destructive and have a substantial impact when sent from multiple systems at the same time (DDoS attacks).

Hacking Tools

Ping of Death is an attack that can cause a system to lock up by sending multiple IP packets, which will be too large for the receiving system when reassembled. Ping of Death can cause a DoS to clients trying to access the server that has been a victim of the attack.

SSPing is a program that sends several large fragmented, Internet Control Message Protocol (ICMP) data packets to a target system. This will cause the computer receiving the data packets to freeze when it tries to reassemble the fragments.

A LAND attack sends a packet to a system where the source IP is set to match the target system's IP address. As a result, the system attempts to reply to itself, causing the system to create a loop—which will tie up system resources and eventually may crash the OS.

CPUHog is a DoS attack tool that uses up the CPU resources on a target system, making it unavailable to the user.

WinNuke is a program that looks for a target system with port 139 open, and sends junk IP traffic to the system on that port. This attack is also known as an out-of-bounds (OOB) attack and causes the IP stack to become overloaded—eventually the system crashes.

Jolt2 is a DoS tool that sends a large number of fragmented IP packets to a Windows target. This ties up system resources and eventually locks up the system. Jolt2 isn't Windows specific; many Cisco routers and other gateways may be vulnerable to the Jolt2 attack.

Bubonic is a DoS tool that works by sending TCP packets with random settings, in order to increase the load of the target machine so that it eventually crashes.

Targa is a program that can be used to run eight different DoS attacks. The attacker has the option to either launch individual attacks or try all of the attacks until one is successful.

RPC Locator is a service that, if unpatched, has a vulnerability to overflows. Details on patching a system to prevent RPC vulnerabilities will be covered later in the chapter. The RPC Locator service in Windows allows distributed applications to run on the network. It is susceptible to DoS attacks, and many of the tools that perform DoS attacks exploit this vulnerability.



Because DoS attacks are so powerful and can cripple a production system or network, this chapter does not include any DoS tool exercises. If you want to test the tools listed here, ensure that you are not using them on a production network or system. The DoS tools could render the target systems unusable.

DDoS attacks can be perpetrated by BOTs and BOTNETs, which are compromised systems that an attacker uses to launch the attack against the end victim. The system or network that has been compromised is a secondary victim, whereas the DoS and DDoS attacks flood the primary victim or target.

How DDoS Attacks Work

DDoS is an advanced version of the DoS attack. Like DoS, DDoS tries to deny access to services running on a system by sending packets to the destination system in a way that the destination system can't handle. The key of a DDoS attack is that it relays attacks from many different hosts (which must first be compromised), rather than from a single host like DoS. DDoS is a large-scale, coordinated attack on a victim system.

Hacking Tools

Trinoo is a tool that sends User Datagram Protocol (UDP) traffic to create a DDoS attack. The Trinoo master is a system used to launch a DoS attack against one or more target systems. The master instructs agent processes (called daemons) on previously compromised systems (secondary victims) to attack one or more IP addresses. This attack occurs for a specified period of time. The Trinoo agent or daemon is installed on a system that suffers from a buffer overflow vulnerability. WinTrinoo is a Windows version of Trinoo and has the same functionality as Trinoo.

Shaft is a derivative of the Trinoo tool that uses UDP communication between masters and agents. Shaft provides statistics on the flood attack that attackers can use to know when the victim system is shut down; Shaft provides UDP, ICMP, and TCP flooding attack options.

Tribal Flood Network (TFN) allows an attacker to use both bandwidth-depletion and resource-depletion attacks. TFN does UDP and ICMP flooding as well as TCP SYN and smurf attacks. TFN2K is based on TFN, with features designed specifically to make TFN2K traffic difficult to recognize and filter. It remotely executes commands, hides the source of the attack using IP address spoofing, and uses multiple transport protocols (including UDP, TCP, and ICMP).

Stacheldraht is similar to TFN and includes ICMP flood, UDP flood, and TCP SYN attack options. It also provides a secure telnet connection (using symmetric key encryption) between the attacker and the agent systems (secondary victims). This prevents system administrators from intercepting and identifying this traffic.

Mstream uses spoofed TCP packets with the ACK flag set to attack a target. It consists of a handler and an agent portion, but access to the handler is password protected.

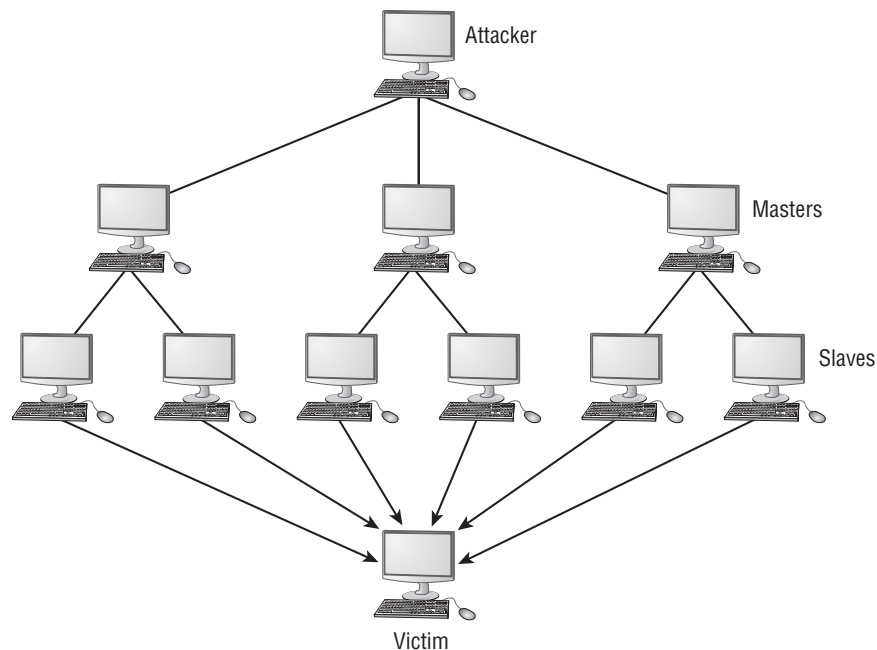
The services under attack are those of the primary victim; the compromised systems used to launch the attack are secondary victims. These compromised systems, which send the DDoS to the primary victim, are sometimes called *zombies* or *BOTs*. They're usually compromised through another attack and then used to launch an attack on the primary victim at a certain time or under certain conditions. It can be difficult to track the source of the attacks because they originate from several IP addresses.

Normally, DDoS consists of three parts:

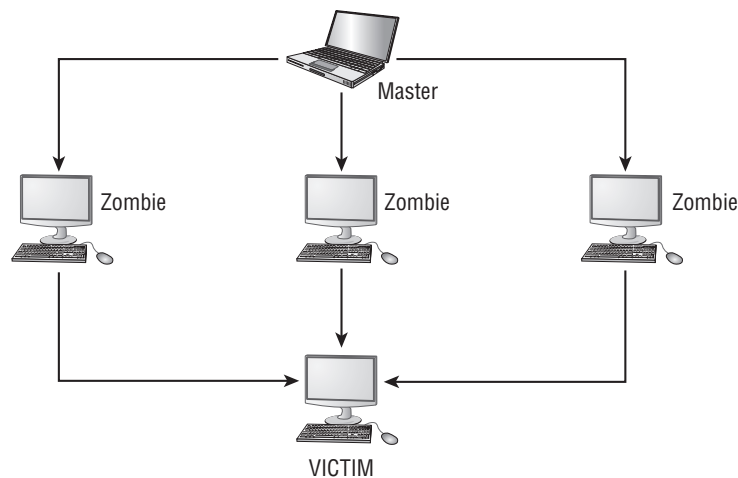
- Master/handler
- Slave/secondary victim/zombie/agent/BOT/BOTNET
- Victim/primary victim

The *master* is the attack launcher. A *slave* is a host that is compromised by and controlled by the master. The *victim* is the target system. The master directs the slaves to launch the attack on the victim system. See Figure 7.1.

FIGURE 7.1 Master and Slaves in a DDoS Attack



DDoS is done in two phases. In the intrusion phase, the hacker compromises weak systems in different networks around the world and installs DDoS tools on those compromised slave systems. In the DDoS attack phase, the slave systems are triggered to cause them to attack the primary victim. See Figure 7.2.

FIGURE 7.2 Bots or Zombie systems

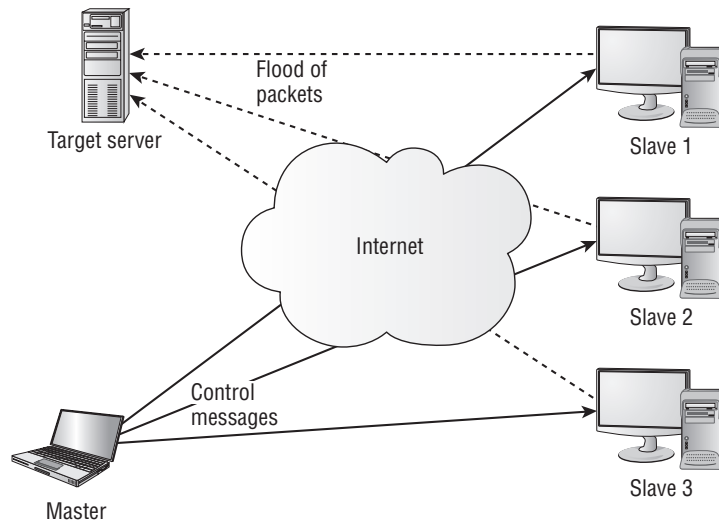
How BOTs/BOTNETs Work

A BOT is short for *web robot* and is an automated software program that behaves intelligently. Spammers often use BOTs to automate the posting of spam messages on newsgroups or the sending of emails. BOTs can also be used as remote attack tools. Most often, BOTs are web software agents that interface with web pages. For example, web crawlers (spiders) are web robots that gather web page information.

The most dangerous BOTs are those that covertly install themselves on users' computers for malicious purposes.

Some BOTs communicate with other users of Internet-based services via instant messaging, Internet Relay Chat (IRC), or another web interface. These BOTs allow IRC users to ask questions in plain English and then formulate a proper response. Such BOTs can often handle many tasks, including reporting weather; providing zip code information; listing sports scores; converting units of measure, such as currency; and so on.

A BOTNET is a group of BOT systems. BOTNETs serve various purposes, including DDoS attacks; creation or misuse of Simple Mail Transfer Protocol (SMTP) mail relays for spam; Internet marketing fraud; and the theft of application serial numbers, login IDs, and financial information such as credit card numbers. Generally a BOTNET refers to a group of compromised systems running a BOT for the purpose of launching a coordinated DDoS attack. See Figure 7.3.

FIGURE 7.3 Anatomy of a Distributed DoS Attack

Smurf and SYN Flood Attacks

A *smurf* attack sends a large amount of ICMP Echo (ping) traffic to a broadcast IP address with the spoofed source address of a victim. Each secondary victim's host on that IP network replies to the ICMP Echo request with an Echo reply, multiplying the traffic by the number of hosts responding. On a multiaccess broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim. IRC servers are the primary victim of smurf attacks on the Internet.

A *SYN flood* attack sends TCP connection requests faster than a machine can process them. The attacker creates a random source address for each packet and sets the SYN flag to request a new connection to the server from the spoofed IP address. The victim responds to the spoofed IP address and then waits for the TCP confirmation that never arrives. Consequently, the victim's connection table fills up waiting for replies; after the table is full, all new connections are ignored. Legitimate users are ignored as well and can't access the server.

A SYN flood attack can be detected through the use of the `netstat` command. An example of the `netstat` output from a system under a SYN flood is shown in Figure 7.4.

Here are some of the methods used to prevent SYN flood attacks:

SYN Cookies SYN cookies ensure the server does not allocate system resources until a successful three-way handshake has been completed.

RST Cookies Essentially the server responds to the client SYN frame with an incorrect SYN ACK. The client should then generate an RST packet telling the server that something

is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.

Micro Blocks Micro blocks prevent SYN floods by allocating only a small space in memory for the connection record. In some cases, this memory allocation is as small as 16 bytes.

Stack Tweaking This method involves changing the TCP/IP stack to prevent SYN floods. Techniques of stack tweaking include selectively dropping incoming connections or reducing the timeout when the stack will free up the memory allocated for a connection.

FIGURE 7.4 netstat output under a SYN flood attack

```
# netstat -n -p TCP
```

tcp	0	0	10.100.0.200:21	237.177.154.8:25082	SYN_RECV
tcp	0	0	10.100.0.200:21	236.15.133.204:2577	SYN_RECV
tcp	0	0	10.100.0.200:21	127.160.6.129:51740	SYN_RECV
tcp	0	0	10.100.0.200:21	230.220.13.25:47393	SYN_RECV
tcp	0	0	10.100.0.200:21	227.200.204.182:60427	SYN_RECV
tcp	0	0	10.100.0.200:21	232.115.18.38:278	SYN_RECV
tcp	0	0	10.100.0.200:21	229.116.93.96:5122	SYN_RECV
tcp	0	0	10.100.0.200:21	236.219.139.207:49162	SYN_RECV
tcp	0	0	10.100.0.200:21	238.100.72.228:37899	SYN_RECV

In Exercise 7.1, you will learn how to prevent SYN flood attacks on Windows 2000 servers.

EXERCISE 7.1

Preventing SYN Flood Attacks on Windows 2000 Servers

1. Run the Windows Registry editor by clicking Start > Run and typing **Regedit**.
2. Navigate to the HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters Registry key.
3. Add the SynAttackProtect=2 DWORD value to the Registry key.
4. Close the regedit program.

This change will allow the operating system to handle more SYN requests. When the value of SynAttackProtect is 2, Windows delays the creation of a socket until the three-way handshake is completed. This change will effectively prevent SYN flood attacks from tying up resources on a Windows server.

DoS/DDoS Countermeasures

There are several ways to detect, halt, or prevent DoS attacks. The following are common security features:

Network-Ingress Filtering All network access providers should implement network-ingress filtering to stop any downstream networks from injecting packets with faked or spoofed addresses into the Internet. Although this doesn't stop an attack from occurring, it does make it much easier to track down the source of the attack and terminate the attack quickly. Most IDS, firewalls, and routers provide network-ingress filtering capabilities.

Rate-Limiting Network Traffic A number of routers on the market today have features that let you limit the amount of bandwidth some types of traffic can consume. This is sometimes referred to as *traffic shaping*.

Intrusion Detection Systems Use an intrusion detection system (IDS) to detect attackers who are communicating with slave, master, or agent machines. Doing so lets you know whether a machine in your network is being used to launch a known attack but probably won't detect new variations of these attacks or the tools that implement them. Most IDS vendors have signatures to detect Trinoo, TFN, or Stacheldraht network traffic.

Automated Network-Tracing Tools Tracing streams of packets with spoofed addresses through the network is a time-consuming task that requires the cooperation of all networks carrying the traffic and that must be completed while the attack is in progress.

Host-Auditing and Network-Auditing Tools File-scanning tools are available that attempt to detect the existence of known DDoS tool client and server binaries in a system. Network-scanning tools attempt to detect the presence of DDoS agents running on hosts on your network.

DoS Scanning Tools

Find_ddos is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.

SARA gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws, such as incorrectly set up or configured network services, well-known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database, and weak policy decisions.

RID is a free scanning tool that detects the presence of Trinoo, TFN, or Stacheldraht clients.

Zombie Zapper instructs zombie routines to go to sleep, thus stopping their attack. You can use the same commands an attacker would use to stop the attack.

Session Hijacking

Session hijacking is when a hacker takes control of a user session after the user has successfully authenticated with a server. Session hijacking involves an attack identifying the current session IDs of a client/server communication and taking over the client's session. Session hijacking is made possible by tools that perform sequence-number prediction. The details of sequence-number prediction will be discussed later in this chapter in the sequence prediction section.

Spoofing attacks are different from hijacking attacks. In a spoofing attack, the hacker performs sniffing and listens to traffic as it's passed along the network from sender to receiver. The hacker then uses the information gathered to spoof or uses an address of a legitimate system. Hijacking involves actively taking another user offline to perform the attack. The attacker relies on the legitimate user to make a connection and authenticate. After that, the attacker takes over the session, and the valid user's session is disconnected.

Session hijacking involves the following three steps to perpetuate an attack:

Tracking the Session The hacker identifies an open session and predicts the sequence number of the next packet.

Desynchronizing the Connection The hacker sends the valid user's system a TCP reset (RST) or finish (FIN) packet to cause them to close their session.

Injecting the Attacker's Packet The hacker sends the server a TCP packet with the predicted sequence number, and the server accepts it as the valid user's next packet.

Hackers can use two types of session hijacking: active and passive. The primary difference between active and passive hijacking is the hacker's level of involvement in the session. In an active attack, an attacker finds an active session and takes over the session by using tools that predict the next sequence number used in the TCP session.

In a passive attack, an attacker hijacks a session and then watches and records all the traffic that is being sent by the legitimate user. Passive session hijacking is really no more than sniffing. It gathers information such as passwords and then uses that information to authenticate as a separate session.

TCP Concepts: Three-Way Handshake

Two of the key features of TCP are reliability and ordered delivery of packets. To accomplish these goals, TCP uses acknowledgment (ACK) packets and sequence numbers. Manipulating these numbers is the basis for TCP session hijacking. To understand session hijacking, let's review the TCP three-way handshake described in earlier chapters:

1. The valid user initiates a connection with the server. This is accomplished by the valid user sending a packet to the server with the SYN bit set and the user's initial sequence number (ISN).

2. The server receives this packet and sends back a packet with the SYN bit set and an ISN for the server, plus the ACK bit set identifying the user's ISN incremented by a value of 1.
3. The valid user acknowledges the server by returning a packet with the ACK bit set and incrementing the server's ISN by 1.

This connection can be closed from either side due to a timeout or upon receipt of a package with the FIN or RST flag set.

Upon receipt of a packet with the RST flag set, the receiving system closes the connection, and any incoming packets for the session are discarded. If the FIN flag is set in a packet, the receiving system goes through the process of closing the connection, and any packets received while closing the connection are still processed. Sending a packet with the FIN or RST flag set is the most common method hijackers use to close the client's session with the server and take over the session by acting as the client.

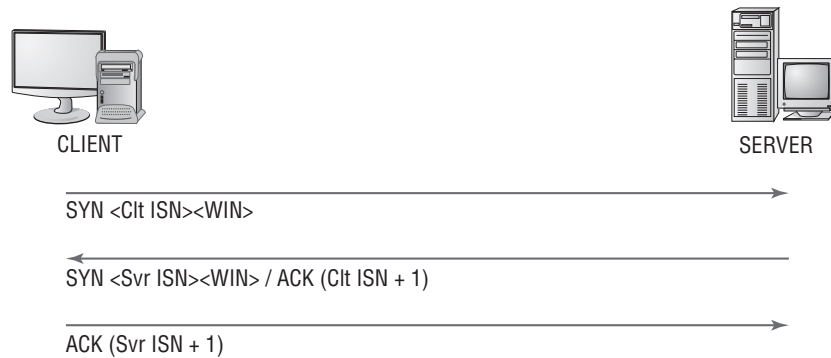
Sequence Prediction

TCP is a connection-oriented protocol, responsible for reassembling streams of packets into their original intended order. Every packet has to be assigned a unique session number that enables the receiving machine to reassemble the stream of packets into their original and intended order; this unique number is known as a *sequence number*. If the packets arrive out of order, as happens regularly over the Internet, then the SN is used to stream the packets correctly. As just illustrated, the system initiating a TCP session transmits a packet with the SYN bit set. This is called a *synchronize packet* and includes the client's ISN. The ISN is a pseudo-randomly generated number with over 4 billion possible combinations, yet it is statistically possible for it to repeat.

When the ACK packet is sent, each machine uses the SN from the packet being acknowledged, plus an increment. This not only properly confirms receipt of a specific packet, but also tells the sender the next expected TCP packet SN. Within the three-way handshake, the increment value is 1. In normal data communications, the increment value equals the size of the data in bytes (for example, if you transmit 45 bytes of data, the ACK responds using the incoming packet's SN plus 45).

Figure 7.5 illustrates the sequence numbers and acknowledgments used during the TCP three-way handshake.

FIGURE 7.5 Sequence numbers and acknowledgment during the TCP three-way handshake



Hacking tools used to perform session hijacking do sequence number prediction. To successfully perform a TCP sequence prediction attack, the hacker must sniff the traffic between two systems. Next, the hacker or the hacking tool must successfully guess the SN or locate an ISN to calculate the next sequence number. This process can be more difficult than it sounds, because packets travel very fast.

When the hacker is unable to sniff the connection, it becomes much more difficult to guess the next SN. For this reason, most session-hijacking tools include features to permit sniffing the packets to determine the SNs.

Hackers generate packets using a spoofed IP address of the system that had a session with the target system. The hacking tools issue packets with the SNs that the target system is expecting. But the hacker's packets must arrive before the packets from the trusted system whose connection is being hijacked. This is accomplished by flooding the trusted system with packets or sending an RST packet to the trusted system so that it is unavailable to send packets to the target system.

Hacking Tools

Juggernaut is a network sniffer that can be used to hijack TCP sessions. It runs on Linux operating systems and can be used to watch for all network traffic, or it can be given a keyword such as a password to look for. The program shows all active network connections, and the attacker can then choose a session to hijack.

Hunt is a program that can be used to sniff and hijack active sessions on a network. Hunt performs connection management, Address Resolution Protocol (ARP) spoofing, resetting of connections, monitoring of connections, Media Access Control (MAC) address discovery, and sniffing of TCP traffic.

TTYWatcher is a session-hijacking utility that allows the hijacker to return the stolen session to the valid user as though it was never hijacked. TTYWatcher is only for Sun Solaris systems.

IP Watcher is a session-hijacking tool that lets an attacker monitor connections and take over a session. This program can monitor all connections on a network, allowing the attacker to watch an exact copy of a session in real time.

T-Sight is a session-monitoring and -hijacking tool for Windows that can assist when an attempt at a network break-in or compromise occurs. With T-Sight, a system administrator can monitor all network connections in real time and observe any suspicious activity that takes place. T-Sight can also hijack any TCP session on the network. For security reasons, En Garde Systems licenses this software only to predetermined IP addresses.

The Remote TCP Session Reset Utility displays current TCP session and connection information such as IP addresses and port numbers. The utility is primarily used to reset TCP sessions.

Dangers Posed by Session Hijacking

TCP session hijacking is a dangerous attack: most systems are vulnerable to it, because they use TCP/IP as their primary communication protocol. Newer operating systems have attempted to secure themselves from session hijacking by using pseudo-random number generators to calculate the ISN, making the sequence number harder to guess. However, this security measure is ineffective if the attacker is able to sniff packets, which gives all the information required to perform this attack.

The following are reasons why it's important for a CEH to be aware of session hijacking:

- Most computers are vulnerable.
- Few countermeasures are available to adequately protect against it.
- Session hijacking attacks are simple to launch.
- Hijacking is dangerous because of the information that can be gathered during the attack.

Preventing Session Hijacking

To defend against session hijack attacks, a network should employ several defenses. The most effective protection is encryption, such as Internet Protocol Security (IPSec). This also defends against any other attack vectors that depend on sniffing. Attackers may be able to

passively monitor your connection, but they won't be able to interpret the encrypted data. Other countermeasures include using encrypted applications such as Secure Shell (SSH, an encrypted telnet) and Secure Sockets Layer (SSL, for HTTPS traffic).

You can help prevent session hijacking by reducing the potential methods of gaining access to your network—for example, by eliminating remote access to internal systems. If the network has remote users who need to connect to carry out their duties, then use virtual private networks (VPNs) that have been secured with tunneling protocols and encryption (Layer 3 Tunneling Protocol [L3TP]/Point-to-Point Tunneling Protocol [PPTP] and IPSec).

The use of multiple safety nets is always the best countermeasure to any potential threat. Employing any one countermeasure may not be enough, but using them together to secure your enterprise will make the attack success rate minimal for anyone but the most professional and dedicated attacker. The following is a checklist of countermeasures that should be employed to prevent session hijacking:

- Use encryption.
- Use a secure protocol.
- Limit incoming connections.
- Minimize remote access.
- Have strong authentication.
- Educate your employees.
- Maintain different username and passwords for different accounts.
- Use Ethernet switches rather than hubs to prevent session hijacking attacks.

Summary

Denial-of-service attacks are used to render a system or network unusable and are considered attacks against the availability of the user data. When other hacking attempts fail, a hacker may resort to DoS attacks as a way of attacking the system. Even though data may not be acquired by a hacker using DoS, the hacker can prevent legitimate users from accessing the data. DoS attacks and especially DDoS attacks are difficult to countermeasure. The best option is to attempt to prevent the attacks by using traffic filtering at the firewall or an IDS.

Session hijacking is used by a hacker to intercept a user's connection and place themselves between the legitimate user and the server. Session hijacking involves predicting sequence numbers and intercepting the legitimate TCP/IP data and replacing it with the hacker's attack exploit. Session hijacking is a dangerous attack used to gather valuable user data, and most systems that run a TCP/IP stack are susceptible to session hijacking.

Exam Essentials

Know the purpose of DoS and DDoS attacks. The purpose of a DoS attack is to send so much traffic to a target system that users are prevented from accessing the system. A distributed denial-of-service (DDoS) attack is a coordinated attack by many systems sent to one target, whereas DoS involves a single system attacking the target.

Know how to prevent DoS attacks. Network traffic filtering, IDS, and auditing tools are all ways to detect and prevent DoS attacks.

Know the two phases of DDoS. During the first phase, systems are compromised and DDoS tools are installed, making the systems zombies or slaves; this is called the intrusion phase. The second phase involves launching an attack against the victim system.

Know what a zombie, slave, and master are in a DDoS attack. A zombie or slave is a system that has been compromised by a hacker and can be commanded to participate in the sending of a DDoS attack to a target system. The master is the controlling system in a DDoS attack scenario. It tells the zombies when to launch the attack.

Understand session hijacking and spoofing. Session hijacking involves taking over another user's session after they have authenticated in order to gain access to a system. Spoofing involves artificial identification of a packet's source address, where that address is often deduced from sniffed network traffic, whereas hijacking refers to a compromised session—normally one in which the attacker takes the user offline and uses their session.

Understand the difference between active and passive session hijacking and some of the tools used. Active session hijacking is the more common of the two types and involves taking over another user's session and desynchronizing the valid user's connection. Passive hijacking monitors the session and allows a hacker to gather confidential information via sniffing packets. Juggernaut, Hunt, TTYWatcher, IP Watcher, T-Sight, and the TCP Reset utility are all session-hijacking tools.

Understand the importance of sequence numbers in a session-hijacking attack. It's necessary to either guess or locate sequence numbers in order to initiate a session-hijacking attack. Sequence numbers are used to order packets and permit a receiving station to reassemble data correctly.

Understand the dangers and countermeasures of session hijacking. Most computers are vulnerable to session-hijacking attacks, and available countermeasures aren't always successful. Confidential and important information, such as passwords, account information, and credit card numbers, can be obtained through session-hijacking attacks. Use encryption, strong authentication, and secure protocols; limit incoming connections; minimize remote access connections; educate employees; and maintain unique usernames and passwords for different accounts.

Review Questions

1. Which is a method to prevent denial-of-service attacks?
 - A. Static routing
 - B. Traffic filtering
 - C. Firewall rules
 - D. Personal firewall
2. What is a zombie?
 - A. A compromised system used to launch a DDoS attack
 - B. The hacker's computer
 - C. The victim of a DDoS attack
 - D. A compromised system that is the target of a DDoS attack
3. The Trinoo tool uses what protocol to perform a DoS attack?
 - A. TCP
 - B. IP
 - C. UDP
 - D. HTTP
4. What is the first phase of a DDoS attack?
 - A. Intrusion
 - B. Attack
 - C. DoS
 - D. Finding a target system
5. Which tool can run eight different types of DoS attacks?
 - A. Ping of Death
 - B. Trinoo
 - C. Targa
 - D. TFN2K
6. What is a smurf attack?
 - A. Sending a large amount of ICMP traffic with a spoofed source address
 - B. Sending a large amount of TCP traffic with a spoofed source address
 - C. Sending a large number of TCP connection requests with a spoofed source address
 - D. Sending a large number of TCP connection requests

7. What is a LAND attack? (Choose all that apply.)
 - A. Sending oversized ICMP packets
 - B. Sending packets to a victim with a source address set to the victim's IP address
 - C. Sending packets to a victim with a destination address set to the victim's IP address
 - D. Sending a packet with the same source and destination address
8. What is the Ping of Death?
 - A. Sending packets that, when reassembled, are too large for the system to understand
 - B. Sending very large packets that cause a buffer overflow
 - C. Sending packets very quickly to fill up the receiving buffer
 - D. Sending a TCP packet with the fragment offset out of bounds
9. How does a denial-of-service attack work? (Choose all that apply.)
 - A. Cracks passwords, causing the system to crash
 - B. Imitates a valid user
 - C. Prevents a legitimate user from using a system or service
 - D. Attempts to break the authentication method
10. What is the goal of a DoS attack?
 - A. To capture files from a remote system
 - B. To incapacitate a system or network
 - C. To exploit a weakness in the TCP/IP stack
 - D. To execute a Trojan using the hidden shares
11. Which of the following tools is only for Sun Solaris systems?
 - A. Juggernaut
 - B. T-Sight
 - C. IP Watcher
 - D. TTYWatcher
12. What is a sequence number?
 - A. A number that indicates where a packet falls in the data stream
 - B. A way of sending information from the sending to the receiving station
 - C. A number that the hacker randomly chooses in order to hijack a session
 - D. A number used in reconstructing a UDP session

13. What type of information can be obtained during a session-hijacking attack? (Choose all that apply.)
- A. Passwords
 - B. Credit card numbers
 - C. Confidential data
 - D. Authentication information
14. Which of the following is essential information to a hacker performing a session-hijacking attack?
- A. Session ID
 - B. Session number
 - C. Sequence number
 - D. Source IP address
15. Which of the following is a session-hijacking tool that runs on Linux operating systems?
- A. Juggernaut
 - B. Hunt
 - C. TTYWatcher
 - D. TCP Reset Utility
16. Which of the following is the best countermeasure to session hijacking?
- A. Port filtering firewall
 - B. Encryption
 - C. Session monitoring
 - D. Strong passwords
17. Which of the following best describes sniffing?
- A. Gathering packets to locate IP addresses in order to initiate a session-hijacking attack
 - B. Analyzing packets in order to locate the sequence number to start a session hijack
 - C. Monitoring TCP sessions in order to initiate a session-hijacking attack
 - D. Locating a host susceptible to a session-hijack attack
18. What is session hijacking?
- A. Monitoring UDP sessions
 - B. Monitoring TCP sessions
 - C. Taking over UDP sessions
 - D. Taking over TCP sessions

19. What types of packets are sent to the victim of a session-hijacking attack to cause them to close their end of the connection?
- A. FIN and ACK
 - B. SYN or ACK
 - C. SYN and ACK
 - D. FIN or RST
20. What is an ISN?
- A. Initiation session number
 - B. Initial sequence number
 - C. Initial session number
 - D. Indication sequence number

Answers to Review Questions

1. B. Traffic filtering is a method to prevent DoS attacks. Static routing will not prevent DoS attacks as it does not perform any traffic filtering or blocking. Firewall rules and personal firewalls will not stop traffic associated with a DoS attack but will help detect an attack.
2. A. A zombie is a compromised system used to launch a DDoS attack.
3. C. Trinoo uses UDP to flood the target system with data.
4. A. The intrusion phase compromises and recruits zombie systems to use in the coordinated attack phase.
5. C. Targa is able to send eight different types of DoS attacks.
6. A. A smurf attack sends a large number of ICMP request frames with a spoofed address of the victim system.
7. A, B. A LAND attack sends packets to a system with that system as the source address, causing the system to try to reply to itself.
8. A. The Ping of Death attack sends packets that, when reassembled, are too large and cause the system to crash or lock up.
9. C. A DoS attack works by preventing legitimate users from accessing the system.
10. B. The goal of a DoS attack is to overload a system and cause it to stop responding.
11. D. TTYWatcher is used to perform session hijacking on Sun Solaris systems.
12. A. A sequence number indicates where the packet is located in the data stream so the receiving station can reassemble the data.
13. A, B, C. Passwords, credit card numbers, and other confidential data can be gathered in a session-hijacking attack. Authentication information isn't accessible because session hijacking occurs after the user has authenticated.
14. C. In order to perform a session-hijacking attack, the hacker must know the sequence number to use in the next packet so the server will accept the packet.
15. A. Juggernaut runs on Linux operating systems.
16. B. Encryption makes any information the hacker gathers during a session-hijacking attempt unreadable.
17. B. Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

- 18. D. The most common form of session hijacking is the process of taking over a TCP session.
- 19. D. FIN (finish) and RST (reset) packets are sent to the victim to desynchronize their connection and cause them to close the existing connection.
- 20. B. ISN is the initial sequence number that is sent by the host and is the starting point for the sequence numbers used in later packets.