

# EXAM✓CRAM

# CEH

## Certified Ethical Hacker



Cram  
Sheet



Flash  
Cards



Practice  
Tests



Dr. CHUCK EASTTOM

# Table of Contents

<b>Introduction</b> . . . . .	<b>xx</b>
-------------------------------	-----------

## **CHAPTER 1:**

<b>Reconnaissance and Scanning</b> . . . . .	<b>1</b>
Reconnaissance Types . . . . .	1
Passive Reconnaissance Techniques . . . . .	3
Active Reconnaissance Techniques . . . . .	22
SSDP Scan . . . . .	25
Nmap . . . . .	26
hping . . . . .	28
Banner Grabbing . . . . .	29
TTL and TCP Scanning . . . . .	29
Evading IDS/Firewall . . . . .	30
What Next? . . . . .	32

## **CHAPTER 2:**

<b>Enumeration and Vulnerability Scanning</b> . . . . .	<b>33</b>
Scanning . . . . .	33
TCP Scanning . . . . .	34
ICMP Scanning . . . . .	37
Scanning Process . . . . .	43
Network Mapping . . . . .	45
Network Packet Capture . . . . .	52
tcpdump . . . . .	52
tcpdump -i eth0 . . . . .	53
tcpdump -c 500 -i eth0 . . . . .	53
tcpdump -D . . . . .	53
Wireshark . . . . .	54
Vulnerability Scanning . . . . .	57
Scoring Vulnerabilities . . . . .	59
Nessus . . . . .	60
Nexpose . . . . .	61
SAINT . . . . .	61
Additional Vulnerability Assessment Tools . . . . .	62
What Next? . . . . .	63

**CHAPTER 3:**

<b>System Hacking</b>	<b>65</b>
CEH Methodology	65
Password Cracking	67
pwdump	70
RainbowCrack	70
Other Password Cracking Tools	71
Pass the Hash	73
LLMNR/NBT-NS Poisoning	74
DLL Hijacking and Injection	74
Alternate Data Streams	75
macOS Attacks	76
Malware	76
Rootkits	77
Spyware	79
Steganography	80
Covering Tracks	83
Metasploit	84
Session Hijacking	89
What Next?	92

**CHAPTER 4:**

<b>Malware</b>	<b>93</b>
Malware Types	94
Trojan Horses	94
Backdoor	99
Spyware	99
Ransomware	100
Rootkits	101
Fileless Malware	102
Botnet	103
Advanced Persistent Threats	103
Exploit Kits	104
How Malware Spreads	104
Malware Components	105
Malware Evasion Techniques	106
Viruses	108
Types of Viruses	109

Creating a Virus . . . . .	111
Logic Bombs . . . . .	114
Protecting Against Malware . . . . .	115
Indicators of Malware . . . . .	116
Sheep Dipping . . . . .	116
Backups . . . . .	117
Malware Analysis . . . . .	117
Antivirus . . . . .	120
What Next? . . . . .	122

## CHAPTER 5:

### **Packet Sniffing and Social Engineering . . . . . 123**

Social Engineering . . . . .	123
Human-Based Social Engineering . . . . .	128
Computer-Based Social Engineering . . . . .	129
Mobile-Based Social Engineering . . . . .	132
Insider Threats . . . . .	132
More on Social Engineering . . . . .	133
Social Engineering Countermeasures . . . . .	134
Packet Sniffing . . . . .	138
Passive Versus Active Sniffing . . . . .	139
Hardware Protocol Analyzers . . . . .	139
Network Information . . . . .	140
Active Attack Techniques . . . . .	142
Protocol Scanning . . . . .	148
What Next? . . . . .	150

## CHAPTER 6:

### **Denial of Service and Session Hijacking . . . . . 151**

Denial of Service . . . . .	151
Protocol Attacks . . . . .	152
Application Layer Attacks . . . . .	154
Volumetric Attacks . . . . .	155
Other DoS Attacks . . . . .	156
Common Tools Used for DoS Attacks . . . . .	159
Countermeasures to DoS and DDoS Attacks . . . . .	162
DoS in the Real World . . . . .	164
Session Hijacking . . . . .	165
The Session Hijacking Process . . . . .	167

Specific Session Hijacking Methods . . . . .	167
Countermeasures for Session Hijacking. . . . .	170
What Next? . . . . .	172

## **CHAPTER 7:**

### **Evading Security Measures . . . . . 173**

Intrusion Detection Systems . . . . .	173
Types of IDSs . . . . .	174
Intrusions . . . . .	180
Firewalls and Honeypots . . . . .	183
Packet Filtering . . . . .	185
Stateful Packet Inspection Firewalls . . . . .	185
Application Gateways . . . . .	185
Next-Generation Firewalls (NGFWs). . . . .	186
Honeypots. . . . .	187
Virtual Private Networks . . . . .	189
IDS Evasion Techniques . . . . .	192
Obfuscation . . . . .	193
Insertion Attacks . . . . .	194
Denial of Service (DoS) Attacks . . . . .	194
Session Splicing . . . . .	194
Fragment Attacks . . . . .	195
Time to Live Attacks . . . . .	195
Invalid RST Packet Attacks . . . . .	196
Urgency Flag. . . . .	196
Polymorphism . . . . .	196
Desynchronization . . . . .	197
Evasion Countermeasures . . . . .	197
Firewall Evasion Techniques . . . . .	198
Firewall Identification. . . . .	200
Obfuscation. . . . .	200
Source Routing . . . . .	201
Tunneling . . . . .	201
WAF Bypass . . . . .	202
Firewall Evasion Tools . . . . .	202
Firewall Evasion Countermeasures . . . . .	203
What Next? . . . . .	204

<b>CHAPTER 8:</b>	
<b>Hacking Web Servers and Web Applications</b>	<b>205</b>
Web Servers	205
Web Server Architecture	207
Web Server Issues	208
Attacks on Web Servers	209
Web Shells	211
Securing the Web Server	211
Web Applications	214
SQL Script Injection	216
XSS	220
Remote File Inclusion	221
CSRF	221
Forceful Browsing	222
Parameter Tampering	222
Cookie Poisoning	223
LDAP Injection	223
Command Injection	224
Web API	224
Webhook	224
OWASP Top 10	225
Web Footprinting	227
Metasploit	229
What Next?	232
<b>CHAPTER 9:</b>	
<b>Hacking Wireless</b>	<b>233</b>
Wireless Technology	233
Wireless Terminology	234
IEEE 802.11 Standard	235
Wi-Fi Security	239
Bluetooth	243
Zigbee	243
Hacking Wireless	245
General Attacks	246
Wi-Fi Discovery and Scanning	246
Rogue Access Attacks	247
MAC Spoofing	248
Key Reinstallation (KRACK) Attacks	248

Jamming Attacks . . . . .	249
Geo Mapping Wi-Fi . . . . .	250
Aircrack-ng . . . . .	250
Wireless ARP Poisoning . . . . .	251
Wireless Security . . . . .	252
Bluetooth Attacks . . . . .	252
Creating a Wireless Hot Spot . . . . .	255
What Next? . . . . .	258
<b>CHAPTER 10:</b>	
<b>Hacking Mobile . . . . .</b>	<b>259</b>
Mobile Technologies . . . . .	259
Cellular Networks . . . . .	260
Cell System Components . . . . .	263
Mobile Operating Systems . . . . .	265
Mobile Threats . . . . .	274
Mobile Attack Vectors . . . . .	275
SSL Stripping . . . . .	276
Mobile Spam . . . . .	276
Open Access Points . . . . .	276
Vulnerable Sandboxing . . . . .	276
Smishing . . . . .	277
Malicious Apps . . . . .	277
Attack Software . . . . .	280
Pen Testing Methodology . . . . .	281
What Next? . . . . .	282
<b>CHAPTER 11:</b>	
<b>IOT and OT Hacking . . . . .</b>	<b>283</b>
IoT Fundamentals . . . . .	283
V2X . . . . .	287
Protocols . . . . .	287
MQTT . . . . .	289
Wired . . . . .	290
NFC . . . . .	290
Operating Systems . . . . .	290
IoT Architectures . . . . .	291
SCADA/ICS . . . . .	293

Operational Technology (OT) . . . . .	294
Healthcare IoT . . . . .	294
IoT Platforms . . . . .	294
IOT Security and Hacking. . . . .	296
IoT Security Layers . . . . .	297
HVAC Exploitation . . . . .	297
BlueBorne Attack . . . . .	298
Mirai . . . . .	298
Sybil Attacks . . . . .	299
Black Hole Attacks . . . . .	299
Rushing Attacks . . . . .	299
Rolling Code Attacks . . . . .	299
Jamming Attacks . . . . .	300
Hello Flood. . . . .	300
Mozi Botnet . . . . .	300
Attify Zigbee . . . . .	300
OWASP TOP 10 . . . . .	300
Ethical Hacking Process . . . . .	302
Scanning . . . . .	304
Attacking. . . . .	307
What Next? . . . . .	308

## CHAPTER 12:

<b>Cloud Computing and Hacking</b> . . . . .	<b>309</b>
Cloud Fundamentals . . . . .	309
Basic Cloud Concepts . . . . .	310
Cloud Security Issues . . . . .	317
Serverless Computing . . . . .	321
Containers. . . . .	321
Cloud Computing Attacks . . . . .	323
General Threats . . . . .	324
Service Hijacking . . . . .	325
Cross-Site Scripting . . . . .	326
SOAP Attacks . . . . .	326
Man-in-the-Cloud Attacks. . . . .	327
DNS Attacks . . . . .	327
Side-Channel Attacks . . . . .	328
Authentication Attacks . . . . .	328



Specific Vulnerabilities . . . . .	329
Cloud Penetration Testing . . . . .	329
What Next? . . . . .	331

## **CHAPTER 13:**

### **Cryptography . . . . . 333**

Cryptography Concepts . . . . .	333
Symmetric Ciphers . . . . .	335
Asymmetric Ciphers . . . . .	337
Hashes . . . . .	342
Cryptographic Tools . . . . .	346
PKI . . . . .	349
Digital Certificates . . . . .	351
Digital Signatures . . . . .	352
SSL/TLS . . . . .	352
Cryptographic Attacks . . . . .	357
Cryptanalysis . . . . .	358
Rainbow Tables . . . . .	360
The Birthday Paradox . . . . .	362
DUHK . . . . .	363
Poodle . . . . .	363
DROWN . . . . .	363
CRIME . . . . .	364
What Next? . . . . .	365

### **Glossary . . . . . 367**

### **Index . . . . . 391**

## CHAPTER 6

# Denial of Service and Session Hijacking

**This chapter covers the following CEH exam objectives:**

- ▶ Understand various DoS attacks
- ▶ Be able to implement DoS countermeasures
- ▶ Use common DoS tools
- ▶ Comprehend session hijacking techniques
- ▶ Implement session hijacking countermeasures

## Denial of Service

Denial of service (DoS) attacks, as the name suggests, are not about breaking into a system but rather about denying legitimate users the opportunity to use the system. In most cases, a DoS attack is easy to execute. This makes DoS attacks a very serious problem. Every technology has limits; if you can exceed those limits, then you can make a system unusable.

## CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Sharia has detected an attack on her company web server. In this attack, the message body is sent quite slowly. What best describes this attack?
  - A. Slowloris
  - B. HTTP post
  - C. Smurf
  - D. PDoS
2. Todd is concerned about DoS attacks against his network. He is particularly worried about attacks that used malformed ICMP packets. What type of attack is Todd concerned about?
  - A. PoD
  - B. Teardrop
  - C. PDoS
  - D. Smurf
3. How does SPI help mitigate DoS?
  - A. By detecting anomalies in the stream such as too many SYN packets from the same IP source
  - B. By blocking fake IP addresses and sending their traffic to a black hole
  - C. By carefully examining each packet and tracing back its origin
  - D. By encrypting traffic, preventing many attacks

## Answers

1. **B.** This is an HTTP post attack. Slowloris involves partial HTTP requests.
2. **A.** This is a PoD (ping of death) attack.
3. **A.** SPI (stateful packet inspection) looks at not just the individual packet but all the packets that came before it in the session. It can detect a range of DoS attacks.

## Protocol Attacks

A protocol attack tries to exploit some vulnerability in the protocol being used. Exploiting such vulnerabilities can cause a system to become unresponsive. The magnitude of a protocol attack is measured in packets per second (pps).

**ExamAlert**

**Objective** For the CEH exam, make certain you know the categories of attacks as well as how the magnitude is measured for each category.

## TCP SYN Flood Attacks

A TCP SYN flood attack is an older type of DoS attack, but it illustrates the concepts of denial of service quite well. This particular type of attack depends on the hacker's knowledge of how connections to a server are made. When a session is initiated between a client and a server in a network using TCP, a packet is sent to the server with a 1-bit flag called a SYN flag set. (SYN is short for synchronize.) This packet is asking the target server to synchronize communications. The server allocates appropriate resources and then sends to the client a packet with both the SYN (synchronize) and ACK (acknowledge) flags set. The client machine is then supposed to respond with an ACK flag set. This process, called a three-way handshake, is summarized as follows:

1. The client sends a packet with the SYN flag set.
2. The server allocates resources for the client and then responds with the SYN and ACK flags set.
3. The client responds with the ACK flag set.

There have been a number of well-known SYN flood attacks on web servers. This attack type is popular because any machine that engages in TCP communication is vulnerable to it—and all machines connected to the Internet engage in TCP communications. Such communication is obviously the entire reason for web servers. The easiest way to block DoS attacks is via firewall rules.

## Teardrop Attacks

Fragmentation attacks in general try to prevent targets from being able to reassemble packet fragments. They usually involve sending a large number of fragmented packets to the target. A teardrop attack is a specific type of fragmentation attack. In a teardrop attack, the attacker sends a fragmented message, where the two fragments overlap in ways that make it impossible to reassemble them properly without destroying the individual packet headers. Therefore, when the victim attempts to reconstruct the message, the message is destroyed. This causes the target system to halt or crash. There are a number of variations on the basic teardrop attack, such as TearDrop2, Boink, targa, Nestea Boink, NewTear, and SYNdrop.

## ACK Flood Attacks

As the name suggests, an ACK flood attack involves sending a flood of TCP ACK packets. Normally an ACK packet is an acknowledgment of something being received, be it data or a synchronization request. Some devices or services are stateful, which means they process each packet. When a target receives a flood of ACK packets, it tries to process it but, because it is not actually an acknowledgment of anything, it can overwhelm the target.

## TCP State Exhaustion Attacks

There are a variety of state exhaustion attacks, and the idea behind them all is essentially the same. They attack weaknesses in Layers 3 and 4 of the protocol stack and overconsume resources. Invalid name queries to a DNS server are a type of state exhaustion attack. TCP state exhaustion attacks operate on some aspect of the TCP handshake. For example, a SYN flood attack is a type of TCP state exhaustion.

## Application Layer Attacks

Application layer DoS attacks work to consume a given application's resources. The magnitude is usually measured in requests per second (rps). Basically, overwhelming a target server with too many requests is the basis for most application layer attacks.

## HTTP Post DoS Attacks

An HTTP post DoS attack involves sending a legitimate HTTP post message. Part of the post message is the content length, which indicates the size of the message to follow. In this type of attack, the attacker sends the actual message body at an extremely slow rate. The web server is then hung as it waits for the message to complete. For more robust servers, the attacker needs to use multiple HTTP post attacks simultaneously.

## Slowloris Attacks

A Slowloris attack is another attack against web servers. The attacker sends partial HTTP requests. When the target receives these requests, it opens a connection and waits for the requests to complete. But rather than complete a request, the attacker continues to send multiple partial requests. Eventually, the

server has opened so many connections that it exhausts its maximum connection pool limit and can no longer respond to legitimate requests.

## Volumetric Attacks

All volumetric attacks seek to overwhelm the target with an overwhelming number of packets. These attacks are not particularly sophisticated or difficult. They simply overwhelm the target. The magnitude of a volumetric attack is usually measured in bits per second (bps).

## Smurf IP Attacks

A UDP attack is a type of volumetric attack, and a Smurf attack is a very popular version of a DoS attack. An ICMP (Internet Control Message Protocol) packet is sent out to the broadcast address of the network. The network responds by echoing the packet out to the network hosts, which then send it to the spoofed source address. Also, the spoofed source address can be anywhere on the Internet, not just on the local subnet. A hacker who can continually send such packets can cause the network itself to perform a DoS attack on one or more of its member servers. This attack is clever and rather simple. The only problem for the hacker is getting the packets started on the target network. This task can be accomplished via some software, such as a virus or Trojan horse, that begins sending the packets.

In a Smurf attack, there are three people/systems involved: the attacker, the intermediary (who can also be a victim), and the victim. The attacker first sends an ICMP echo request packet to the intermediary's IP broadcast addresses. Since this is sent to the IP broadcast address, many of the machines on the intermediary's network receive this request packet and send back an ICMP echo reply packet. If all the machines on a network are responding to this request, the network becomes congested, and there may be outages.

The attacker impacts the third party—the intended victim—by creating forged packets that contain the spoofed source address of the victim. Therefore, when all the machines on the intermediary's network start replying to the echo request, those replies flood the victim's network. Thus, another network becomes congested and could become unusable. This type of attack is illustrated in Figure 4.4 in Chapter 4, “Malware.”

## UDP Flood Attacks

The UDP flood attack is another example of a volumetric attack. Keep in mind that UDP (User Datagram Protocol) is a protocol that does not verify each packet's delivery. In a UDP flood attack, the attacker sends a UDP packet to a random port on a target system. When the target system receives a UDP packet, the attacker determines what application is listening on the destination port. Then, if the attacker wants to attack that application, he or she just starts a flood of UDP packets to the IP address and port. If enough UDP packets are delivered to ports on the target, the system becomes overloaded trying to determine awaiting applications (which do not exist) and then generating and sending packets back.

## ICMP Flood Attacks

The ICMP flood attack is another volumetric attack. ICMP flood attacks are usually accomplished by broadcasting a large number of either pings or UDP packets. Like other flood attacks, the idea is to send so much data to the target system that the system slows down. If it can be forced to slow down enough, the target will time out (i.e., not send replies fast enough) and be disconnected from the Internet. This type of attack is far less effective against modern computers than it was against older ones. Even a low-end desktop PC now has 4 GB (or more) of RAM and a dual-core processor, making it difficult to generate enough pings to knock the machine offline. However, at one time, this was a very common form of DoS attack.

## Ping of Death Attacks

A ping of death attack, often simply called a PoD attack, is accomplished by sending malformed ICMP packets (e.g., sending a packet that is 65,536 bytes in size). RFC 791 specifies a maximum packet size of 65,535 bytes. A PoD attack can cause a vulnerable system to crash.

## Other DoS Attacks

Some DoS attack types don't fit neatly into one of the previously discussed categories. These attacks can nonetheless be quite effective against target systems.

## Multi-Vector Attacks

As the name suggests, a multi-vector attack is a combination of two or more of the other attacks (e.g., launching a SYN flood attack and a teardrop attack at the same time). Another method is to launch one type of attack and then, after a time, to shift to a different attack vector. This method can overcome DoS countermeasures the target may have implemented.

## DHCP Starvation Attacks

DHCP (Dynamic Host Configuration Protocol) is used to dynamically assign IP addresses to systems on a network. If an attacker floods a target network with DHCP requests for dynamic IP addresses, the attacker can completely exhaust the address space allocated by the DHCP server. Then legitimate users cannot get an IP address assigned and thus cannot connect to the network. There are tools such as gobblers that can do this for an attacker.

## PDoS Attacks

Though not terribly common, it is possible to have a DoS attack that leaves the system either inoperable or needing the operating system completely reinstalled. These are referred to as *permanent denial of service (PDoS) attacks*, or phlashing. Such attacks usually involve DoS attacks on a device's firmware.

## Registration DoS Attacks

A registration DoS attack is a very simplistic attack used against websites. The attacker creates a script or program that just keeps registering fake users on a website. This is one reason many registration websites use CAPTCHA.

## Login DoS Attacks

Login DoS attacks are similar to registration DoS attacks and also frequently use scripts or programs. The attacker tries to overload the login process by continually sending login information. This can overwhelm the target system or at least slow it down. Many websites use CAPTCHA to prevent automated login attempts.



## DDoS Attacks

Perhaps the most common form of DoS attack today is the *DDoS attack*. This type of attack is accomplished by getting various machines to attack the target. This is commonly done by sending out a Trojan horse that causes infected computers to attack a specified target at a particular date and time—which is a very effective way to execute a DDoS attack on any target. In this form of DDoS attack, the attacker does not have direct control of the various machines used in the attack. These machines are simply infected by some malware that causes them to participate in the attack on a particular date and at a particular time.

Another method is to use a botnet to orchestrate a DDoS attack. A *botnet* is a network of computers that have been compromised by an attacker so that the attacker has control of the computers. This is often accomplished via delivery of a Trojan horse. However, unlike in the previous DDoS example, the attacker has direct control over the attacking machines in the botnet.

A botnet usually has a command and control (C&C) that controls the various compromised machines. Then the botnet can be used for whatever the attacker wishes. DDoS is only one application of a botnet. Password cracking and sending phishing emails are other uses. The compromised systems can be attacked in any of the ways that malware is usually distributed: via phishing emails, compromised websites, vulnerable target systems, etc.

## Peer-to-Peer Attacks

While peer-to-peer (P2P) apps have become quite popular, so have P2P DoS attacks. One method is to force the client to disconnect from the legitimate P2P hub and get the client to connect to the attacker's fake hub. There have also been massive DDoS attacks on peer-to-peer networks. In addition, attackers attempt to exploit flaws in the protocols used, such as the Direct Connect (DC++) protocol that is used to share files between peer-to-peer clients.

## Distributed Reflection DoS Attacks

As previously stated, DDoS attacks are becoming more common. Most such attacks rely on getting various machines (i.e., servers or workstations) to attack the target. A distributed reflection DoS attack is a special type of DoS attack. As with all such attacks, it is accomplished by the hacker getting a number of machines to attack the selected target. However, this attack works a bit differently than other DoS attacks. Rather than getting computers to attack the target, this method tricks Internet routers into attacking a target.

Many of the routers on the Internet backbone communicate on port 179, particularly using BGP (Border Gateway Protocol) to exchange routing information. A distributed reflection DoS attack exploits that communication line and gets routers to attack a target system. What makes this attack particularly wicked is that it does not require the routers in question to be compromised in any way. The attacker does not need to get any sort of software on a router to get it to participate in the attack. Instead, the hacker sends a stream of packets to the various routers, requesting a connection. The packets have been altered so that they appear to come from the target system's IP address. The routers respond by initiating connections with the target system. What occurs is a flood of connections from multiple routers, all hitting the same target system. This has the effect of rendering the target system unreachable.

#### ExamAlert

**Objective** For the CEH exam, you must be able to fully describe each of the attacks discussed in this section. It is worth your time to memorize these attacks.

## Common Tools Used for DoS Attacks

As with any of the other security issues discussed in this book, you will find that hackers have at their disposal a vast array of tools in the DoS arena. While it is certainly well beyond the scope of this book to begin to categorize or discuss all of these tools, a brief introduction to just a few of them will prove useful.

### LOIC

LOIC (Low Orbit Ion Cannon) is one of the most widely known DoS tools available. It has a very easy-to-use graphical user interface, shown in Figure 6.1.

This tool is very easy to use. As you can see in Figure 6.1, it simply requires the user to enter the target URL or IP address and then begin the attack. Fortunately, this tool also does nothing to hide the attacker's address and thus makes it relatively easy to trace the attack back to its source. It is an older tool but still widely used today. There is a tool similar to this named HOIC, which we discuss later in this section.



FIGURE 6.1 LOIC

## DoSHTTP

DoSHTTP is another tool that is simple to use. You select the target, the agent (i.e., the browser type to simulate), the number of sockets, and the requests and then start the flood. You can see this in Figure 6.2.

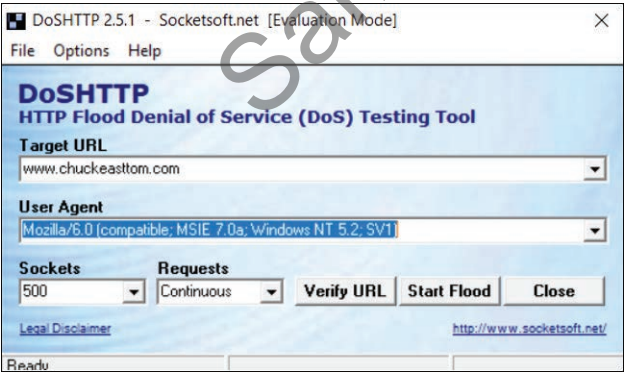


FIGURE 6.2 DoSHTTP

---

## Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. What Cisco command enables TCP intercept?
  - ☐ A. **access-list access-list-number {deny | permit} tcp any destination destination-wildcard**
  - ☐ B. **ip tcp Intercept list access-list-number**
  - ☐ C. **ip tcp Intercept-enable**
  - ☐ D. **access-list access-list-number intercept-enable**
  
2. Which attack is based on an ICMP (Internet Control Message Protocol) packet sent to the broadcast address of the network?
  - ☐ A. Teardrop attack
  - ☐ B. Slowloris attack
  - ☐ C. Smurf attack
  - ☐ D. PDoS attack
  
3. What is the most effective countermeasure for registration DoS attacks?
  - ☐ A. Using an SPI firewall
  - ☐ B. Using CAPTCHA
  - ☐ C. Encrypting traffic
  - ☐ D. Using Cisco configuration

## Answers

1. **C.** If you are not familiar with Cisco router/switch commands, this can be one of the more challenging parts of the CEH exam.
  2. **B.** A Smurf attack works by sending a flood of broadcast messages to the target system router, impersonating the target machine's IP address.
  3. **B.** This is one reason so many sites use CAPTCHA: It prevents scripts from running registration DoS attacks.
- 

## Session Hijacking

Conceptually, session hijacking is quite simple. The goal is to find an authentic TCP session and to take over that session. This is possible because, generally speaking, the session is authenticated at the beginning. Clearly, session hijacking is easier with some systems than with others.