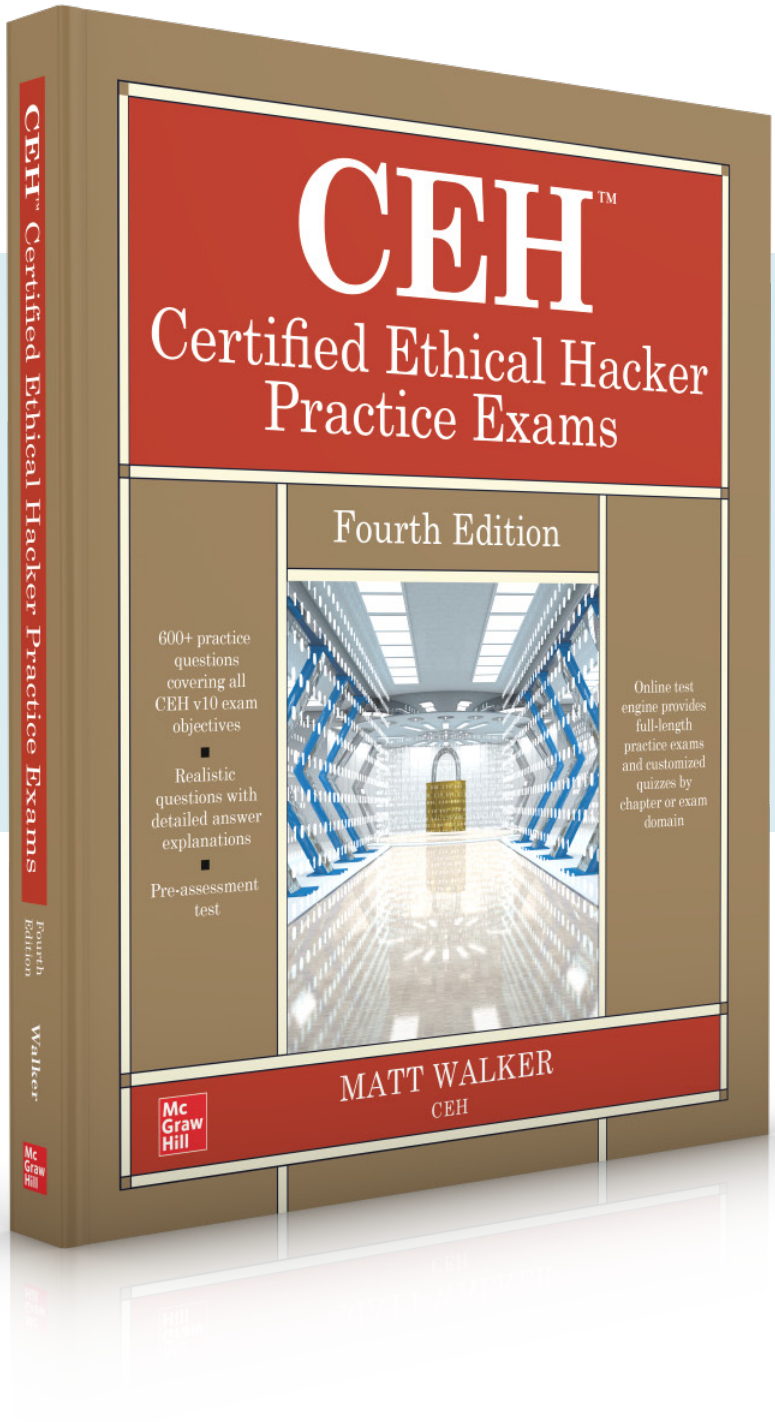
Mc Graw Hill

CEH™ Certified Ethical Hacker Practice Exams

Sample Chapter

CHAPTER 10:
Trojans and
Other Attacks



LEARN MORE

BUY NOW

Because learning changes everything.®

mhprofessional.com

CHAPTER 10

Trojans and Other Attacks

This chapter includes questions from the following topics:

- Describe malware types and their purpose
- Identify malware deployment methods
- Describe the malware analysis process
- Identify malware countermeasures
- Describe DoS attacks and techniques
- Identify DoS detection and countermeasure actions
- Describe session hijacking and sequence prediction

Every new hobby and activity ends up with a huge learning curve, with all sorts of lingo and terminology to figure out. And, usually, it winds up costing a lot of money. For example, suppose you decide to get into photography. All of a sudden you're learning about ISO ratings and saturation—and buying insanely expensive cameras and lenses because you *need* them. What if you decide to take up shooting? Well, now you're learning about calibers, double versus single action, trigger pull, and IWB versus OWB—and you'll wind up purchasing multiple weapons of different action and caliber. And bass fishing? Oh, now we're talking about some serious addictions.

Braid versus monofilament line? Fluorocarbon gets my vote for leader material, but braid's great for the back end. Baitcast versus spinning reel? I'd say that depends on the situation, but unless you can figure out the centrifugal braking systems and tension settings, with plenty of time to practice, spinning may be your best bet. Rod material and makeup? Hook style? Knots to use? And don't get me started on electronics for your boat!

And as we also know with every hobby, there are rules and expectations for the use of everything you buy. The people who have been engaging in it for a long time usually look at newcomers with a bemused derision, mocking the misuse of tools and techniques until they get with the program and do what everyone else is doing. In bass fishing, this idea kept loads of people from catching lots of fish.

For decades, the use of a particular bait known as a jig was relegated by those who knew everything to one method of presentation: flip the jig directly into really heavy cover (bushes, sticks, lily pads, and so on) and gently pop it around the bottom until a fish bites. In 1996, a bass professional named Bill Lowen was fishing a tournament with a jig the same way everyone else had been using it since the dawn of artificial bait fishing. He had tossed it in a tree that had

fallen over into the water, and was slowly working it back. Deciding to move to another place, he started reeling the jig back to him and—whammo—fish on! At the next spot, he started fishing again, but decided to try reeling the jig back to him, instead of using it like everyone else did. Whammo!—another fish on. He wound up winning that tournament, and in doing so created a brand-new technique called "swimming" a jig.

Why all this about bass fishing and techniques? Because it's applicable to our work here as ethical hackers. See, there are two ways to catch fish on any given lure—first, by using the lure the way it was designed, and, second, by using it in whatever way it catches fish. Whether the technique is "dead-sticking" a worm or, believe it or not, using a wrench as a lure (don't laugh—I've seen it with my own eyes), whatever works to catch fish is what should be used, right? In ethical hacking, the same thing applies. Malware certainly won't ever be confused with a "good-guy" tool, but maybe you can use it in a different way than it was intended. Your pen test tool set can be augmented by visiting the dark side yourself, wielding tools and actions that may seem a bit unsavory to you and in ways you just haven't thought about.

STUDY TIPS There hasn't been a whole lot of change in version 10 when it comes to malware and other attacks. Most of the questions from the malware sections—especially those designed to trip you up—still will be of the pure memorization type. Stick with key words for each definition (it'll help you in separating good answers from bad ones), especially for the virus types. Don't miss an easy point on the exam because you forgot the difference between polymorphic and multipartite or why a worm is different from a virus. Tool identification should also be relatively straightforward (assuming you commit all those port numbers to memory, like I told you to do).

Finally, as always, get rid of the answers you know to be wrong in the first place. It's actually easier sometimes to identify the ones you downright know aren't relevant to the question. Then, from the remainder, you can scratch your gray matter for the key word that will shed light on the answer.

QUESTIONS

1. Bart receives an e-mail that appears to be from his lawyer containing a ZIP file named Courtdoc.zip. Bart double-clicks the ZIP file to open it, and a message stating "This word document is corrupt" appears. In the background, a file named Courtdoc.doc.exe runs and copies itself to the local APPDATA directory. It then begins beaconing to an external server. Which of the following best describes the malware Bart installed?
   - **A.** Worm
   - **B.** Virus
   - **C.** Trojan
   - **D.** Macro
2. You have established a Netcat connection to a target machine. Which flag can be used to launch a program?
   - **A.** -p
   - **B.** -a
   - **C.** -l
   - **D.** -e
3. Claire is surfing the Web and, after some time, a message pops up stating her system has been infected by malware and offering a button to click for removal of the virus. After she clicks the button, another message window appears stating the system has been quarantined due to the nature of the infection and provides a link with instructions to pay in order to regain control and to clear the virus. Which of the following best describes this infection?
   - **A.** Spyware
   - **B.** Ransomware
   - **C.** Trojan
   - **D.** Adware
4. Matty is examining malware as part of a security effort. She performs analysis of the malware executable without running or installing it. Instead, she examines source and binary code to find data structures, function calls, and other indicators of malicious behavior. Which of the following best describes the type of malware analysis Matty is performing?
   - **A.** Static
   - **B.** Dynamic
   - **C.** File fingerprinting
   - **D.** Code emulation

5. Pen test team member Amy attempts to guess the ISN for a TCP session. Which attack is she most likely carrying out?
   - **A.** XSS
   - **B.** Session splicing
   - **C.** Session hijacking
   - **D.** Multipartite attack
6. An attacker wants to make his malware as stealthy and undetectable as possible. He employs an effort that uses compression to reduce the file size of the malware. Which of the following best describes this?
   - **A.** Crypter
   - **B.** Wrapper
   - **C.** Packer
   - **D.** Compressor
7. An attacker is attempting a DoS attack against a machine. She first spoofs the target's IP address and then begins sending large amounts of ICMP packets containing the MAC address FF:FF:FF:FF:FF:FF. What attack is underway?
   - **A.** ICMP flood
   - **B.** Ping of death
   - **C.** SYN flood
   - **D.** Smurf
   - **E.** Fraggle
8. An attacker makes use of the Beacon implant on a target system to hijack a browser session. Which of the following best describes this attack?
   - **A.** Man in the browser
   - **B.** Man in the middle
   - **C.** Man in the pivot
   - **D.** IE hijacking
9. Claire's Windows system at work begins displaying strange activity, and she places a call to the IT staff. On investigation, it appears Claire's system is infected with several viruses. The IT staff removes the viruses, deleting several file and folder locations and using an AV tool, and the machine is reconnected to the network. Later in the day, Claire's system again displays strange activity and the IT staff is called once again. Which of the following are likely causes of the re-infection? (Choose all that apply.)
   - **A.** Claire revisits a malicious website.
   - **B.** Claire opens her Microsoft Outlook e-mail client and newly received e-mail is loaded to her local folder (.pst file).

C. Claire uses a system restore point to regain access to deleted files and folders.

D. Claire uses the organization's backup application to restore files and folders.

10. In regard to Trojans, which of the following best describes a wrapper?

A. The legitimate file the Trojan is attached to

B. A program used to bind the Trojan to a legitimate file

C. A method of obfuscation using compression

D. A software tool that uses encryption and code manipulation to hide malware

11. In May of 2017, this ransomware took advantage of a Windows SMB vulnerability known as the Eternal Blue exploit and spread worldwide in a matter of hours. A hidden kill switch inside the coding was quickly discovered, halting its spread. Which of the following best fits this description?

A. Petya

B. WannaCry

C. Zeus

D. Botnet

12. Which of the following is a legitimate communication path for the transfer of data?

A. Overt

B. Covert

C. Authentic

D. Imitation

E. Actual

13. In what layer of the OSI reference model is session hijacking carried out?

A. Data Link layer

B. Transport layer

C. Network layer

D. Physical layer

14. A pen test team member types the following command:

```
nc222.15.66.78 -p 8765
```

Which of the following statements is true regarding this attempt?

A. The attacker is attempting to connect to an established listening port on a remote computer.

B. The attacker is establishing a listening port on his machine for later use.

C. The attacker is attempting a DoS against a remote computer.

D. The attacker is attempting to kill a service on a remote machine.

15. Examine the partial command-line output listed here:

```
Active Connections
Proto  Local Address          Foreign Address      State
  TCP    0.0.0.0:912          COMPUTER11:0          LISTENING
  TCP    0.0.0.0:3460         COMPUTER11:0          LISTENING
  TCP    0.0.0.0:3465         COMPUTER11:0          LISTENING
  TCP    0.0.0.0:8288         COMPUTER11:0          LISTENING
  TCP    0.0.0.0:16386        COMPUTER11:0          LISTENING
  TCP    192.168.1.100:139    COMPUTER11:0          LISTENING
  TCP    192.168.1.100:58191  173.194.44.81:https  ESTABLISHED
  TCP    192.168.1.100:58192  173.194.44.81:https   TIME_WAIT
  TCP    192.168.1.100:58193  173.194.44.81:https   TIME_WAIT
  TCP    192.168.1.100:58194  173.194.44.81:https   ESTABLISHED
  TCP    192.168.1.100:58200  bk-in-f138:http       TIME_WAIT
```

Which of the following is a true statement regarding the output?

A. This is output from a **netstat -an** command.

B. This is output from a **netstat -b** command.

C. This is output from a **netstat -e** command.

D. This is output from a **netstat -r** command.

16. You are discussing malware with a new pen test member who asks about restarting executables. Which registry keys within Windows automatically run executables and instructions? (Choose all that apply.)

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

C. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

17. Which of the following is a true statement?

A. Sequence prediction attacks are specific to TCP.

B. Using a protocol in a way it is not intended to be used is an example of an overt channel.

C. All DoS and DDoS attacks are specific to TCP.

D. Fraggle is a TCP-based attack.

18. Which denial-of-service attack involves using multiple intermediary and secondary machines to contribute to the DoS effort?

A. SYN flood

B. DRDoS

C. Application-level flood

D. LOIC

19. Which of the following takes advantage of weaknesses in the fragment reassembly functionality of TCP/IP?
    - **A.** Teardrop
    - **B.** SYN flood
    - **C.** Smurf attack
    - **D.** Ping of death
20. IPSec is an effective preventative measure against session hijacking. Which IPSec mode encrypts only the data payload?
    - **A.** Transport
    - **B.** Tunnel
    - **C.** Protected
    - **D.** Spoofed
21. What provides for both authentication and confidentiality in IPSec?
    - **A.** AH
    - **B.** IKE
    - **C.** OAKLEY
    - **D.** ESP
22. Which of the following statements best describes the comparison between spoofing and session hijacking?
    - **A.** Spoofing and session hijacking are the same thing.
    - **B.** Spoofing interrupts a client's communication, whereas hijacking does not.
    - **C.** Hijacking interrupts a client's communication, whereas spoofing does not.
    - **D.** Hijacking emulates a foreign IP address, whereas spoofing refers to MAC addresses.
23. Which of the following is an effective deterrent against TCP session hijacking?
    - **A.** Install and use an HIDS on the system.
    - **B.** Install and use Tripwire on the system.
    - **C.** Enforce good password policy.
    - **D.** Use unpredictable sequence numbers.
24. Which of the following is a group of Internet computers set up to forward transmissions to other computers on the Internet without the owner's knowledge or permission?
    - **A.** Botnet
    - **B.** Zombie
    - **C.** Honeypot
    - **D.** DDoS

25. Within a TCP packet dump, a packet is noted with the SYN flag set and a sequence number set at A13F. What should the acknowledgment number in the return SYN/ACK packet be?

A. A131

B. A130

C. A140

D. A14F

26. When is session hijacking performed?

A. Before the three-step handshake

B. During the three-step handshake

C. After the three-step handshake

D. After a FIN packet

QUICK ANSWER KEY

1. C
2. D
3. B
4. A
5. C
6. C
7. D
8. A
9. A, C, D
10. B
11. B
12. A
13. B
14. A
15. A
16. A, B, C, D
17. A
18. B
19. A
20. A
21. D
22. C
23. D
24. A
25. C
26. C

A ANSWERS

1. Bart receives an e-mail that appears to be from his lawyer containing a ZIP file named Courtdoc.zip. Bart double-clicks the ZIP file to open it, and a message stating "This word document is corrupt" appears. In the background, a file named Courtdoc.doc.exe runs and copies itself to the local APPDATA directory. It then begins beaconing to an external server. Which of the following best describes the malware Bart installed?

   A. Worm

   B. Virus

   C. Trojan

   D. Macro

   ☑ **C.** The definition of a Trojan is a non-self-replicating program that appears to have a useful purpose but in reality has a different, malicious purpose. In other words, it looks harmless but, when activated, is not. This is precisely what is going on in this example. E-mail is not the *only* method to spread a Trojan, but phishing certainly does seem to work well.

   ☒ **A** is incorrect because this does not describe a worm. A worm is a self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

   ☒ **B** is incorrect because this does not describe a virus. A virus is a malicious computer program with self-replication capabilities that attaches to another file and moves with the host from one computer to another.

   ☒ **D** is incorrect because this does not describe a macro. A macro is a single instruction that expands automatically into several instructions to perform a specific task (usually associated with Microsoft Office products, as far as your exam is concerned).

2. You have established a Netcat connection to a target machine. Which flag can be used to launch a program?

   A. -p

   B. -a

   C. -l

   D. -e

   ☑ **D.** Netcat is often referred to as the Swiss Army knife of hacking efforts. You can use it to set up a listening port on target machines that you can then revisit to wreak all sorts of havoc. The flag associated with launching a program is -e. For example, issuing the command

   ```
   nc -L -p 12657 -t -e cmd.exe
   ```

   will open a Windows command shell on the target machine; the -t flag sets up a Telnet connection over the port you defined with the -p flag (12657).

☒ **A** is incorrect because the -p flag indicates the protocol port you want to use for your session.

☒ **B** is incorrect because -a is not a recognized Netcat flag.

☒ **C** is incorrect because the -l flag indicates Netcat should open the port for listening. As an aside, the -L flag does the same thing; however, it restarts listening after the inbound session completes.

3. Claire is surfing the Web and, after some time, a message pops up stating her system has been infected by malware and offering a button to click for removal of the virus. After she clicks the button, another message window appears stating the system has been quarantined due to the nature of the infection and provides a link with instructions to pay in order to regain control and to clear the virus. Which of the following best describes this infection?

A. Spyware

B. Ransomware

C. Trojan

D. Adware

☑ **B.** Ransomware isn't anything new, but it sure has attracted new attention from EC-Council. The name itself gives away its purpose: the malware infects your system and then restricts access to your files and folders, demanding a ransom payment to get control back. ECC lists five different ransomware families: Cryptorbit, Cryptolocker, Cryptodefense, Cryptowall, and police-themed. Usually the online payment involves bitcoin, but can take other avenues. In any case, never pay off the attacker—you're only signing yourself up for future terror. Cleaning off ransomware may involve booting into Safe Mode, or even using a system restore on Windows systems. You may even get away with an external AV scan as a fix action, but be sure to scrub the system for hidden files and folders the ransomware may have left behind. Lastly, I can't overstate enough the value of good, solid, dependable backups. Even if you're foolish enough to pay the ransom, there is no guarantee any of your files will remain accessible after the "unlock"—and could you trust them anyway? Invest in good backups and run them religiously.

☒ **A** is incorrect because this does not describe spyware. Spyware is type of malware that covertly collects information about a user.

☒ **C** is incorrect because this does not describe a Trojan. A Trojan is a non-self-replicating program that appears to have a useful purpose but in reality has a different, malicious purpose.

☒ **D** is incorrect because this does not describe adware. Adware is software that has advertisements embedded within it. It generally displays ads in the form of pop-ups.

4. Matty is examining malware as part of a security effort. She performs analysis of the malware executable without running or installing it. Instead, she examines source and binary code to find data structures, function calls, and other indicators of malicious behavior. Which of the following best describes the type of malware analysis Matty is performing?

   A. Static

   B. Dynamic

   C. File fingerprinting

   D. Code emulation

   ☑ **A.** EC-Council defines two main types of malware analysis—static and dynamic. In static analysis, the examiner never actually installs or executes the malware. It's considered a "safe" analysis, as the suspect file isn't installed or allowed to execute; however, as this is obviously a touchy area, it's always a best and recommended practice to perform analysis in a closed environment. This is largely a manual process, but there are static analysis tools that can assist.

   ☒ **B** is incorrect because dynamic analysis is the process of examining malware behavior by actually installing and running it in a monitored environment.

   ☒ **C** is incorrect because file fingerprinting involves computing a hash value for a given binary code.

   ☒ **D** is incorrect because code emulation is a detection method where antivirus executes the malicious codes on a virtual machine to simulate CPU and memory activities.

5. Pen test team member Amy attempts to guess the ISN for a TCP session. Which attack is she most likely carrying out?

   A. XSS

   B. Session splicing

   C. Session hijacking

   D. Multipartite attack

   ☑ **C.** The idea behind session hijacking is fairly simple: the attacker waits for a session to begin and, after all the pesky authentication gets done, jumps in to steal the session for herself. In practice, it's a little harder and more complicated than that, but the key to the whole attack is in determining the initial sequence number (ISN) used for the session. The ISN is sent by the initiator of the session in the first step (SYN). This is acknowledged in the second step of the handshake (SYN/ACK) by incrementing that ISN by 1, and then another ISN is generated by the recipient. This second number is acknowledged by the initiator in the third step (ACK), and from there on out communication can occur. Per EC-Council, the following steps describe the session hijack:

      1. Sniff the traffic between the client and the server.
      2. Monitor the traffic and predict the sequence numbering.

3. Desynchronize the session with the client.
4. Predict the session token and take over the session.
5. Inject packets to the target server.

For what it's worth, pulling this attack off via EC-Council's take on the whole matter requires you to do some fairly significant traffic sniffing. And if you're already positioned to sniff the traffic in the first place, wouldn't the whole scenario possibly be a moot point? You need to know it for the exam, but real-world application may be rare.

☒ **A** is incorrect because cross-site scripting is a web application attack.

☒ **B** is incorrect because session splicing is an IDS evasion method. The attacker delivers a payload that the IDS would have otherwise seen by "slicing" it over multiple packets. The payload can be spread out over a long period of time.

☒ **D** is incorrect because *multipartite* refers to a virus type, not an attack that requires ISN determination.

6. An attacker wants to make his malware as stealthy and undetectable as possible. He employs an effort that uses compression to reduce the file size of the malware. Which of the following best describes this?

A. Crypter
B. Wrapper
C. Packer
D. Compressor

☑ **C.** A packer uses compression to pack the malware executable into a smaller size. Not only does this reduce the file size, but it serves to make the malware harder to detect for some antivirus engines. It works much like a ZIP file, except that the extraction occurs in memory and not on the disk.

☒ **A** is incorrect because a crypter is a software tool that uses a combination of encryption and code manipulation to render malware undetectable to AV and other security monitoring products (in Internet lingo, it's referred to as *fud,* for "fully undetectable").

☒ **B** is incorrect because a wrapper is used to bind a Trojan and a legitimate program together so the Trojan will be installed when the legitimate program is executed.

☒ **D** is included merely as a distractor and is not a legitimate term.

7. An attacker is attempting a DoS attack against a machine. She first spoofs the target's IP address and then begins sending large amounts of ICMP packets containing the MAC address FF:FF:FF:FF:FF:FF. What attack is underway?

A. ICMP flood
B. Ping of death
C. SYN flood
D. Smurf
E. Fraggle

☑ **D.** A smurf attack is a generic denial-of-service (DoS) attack against a target machine. The idea is simple: have so many ICMP requests going to the target that all its resources are taken up. To accomplish this, the attacker spoofs the target's IP address and then sends thousands of ping requests from that spoofed IP to the subnet's broadcast address. This, in effect, pings every machine on the subnet. Assuming it's configured to do so, every machine will respond to the request, effectively crushing the target's network resources.

☒ **A** is incorrect because an ICMP flood does not act this way. In this attack, the hacker sends ICMP Echo packets to the target with a spoofed (fake) source address. The target continues to respond to an address that doesn't exist and eventually reaches a limit of packets per second sent.

☒ **B** is incorrect because a ping of death does not act this way. It's not a valid attack with modern systems because of preventative measures in the OS; in the ping of death, an attacker fragments an ICMP message to send to a target. When the fragments are reassembled, the resulting ICMP packet is larger than the maximum size and crashes the system. As an aside, each OS has its own method of dealing with network protocols, and the implementation of dealing with particular protocols opens up hacking (DDoS and otherwise) options like this.

☒ **C** is incorrect because a SYN flood takes place when an attacker sends multiple SYN packets to a target without providing an acknowledgment to the returned SYN/ACK. This is another attack that does not necessarily work on modern systems.

☒ **E** is incorrect because in a fraggle attack, UDP packets are used. The same principle applies—spoofed IP and Echo requests sent to the broadcast address—but it's just with UDP.

8. An attacker makes use of the Beacon implant on a target system to hijack a browser session. Which of the following best describes this attack?

A. Man in the browser

B. Man in the middle

C. Man in the pivot

D. IE hijacking

☑ **A.** Most have heard of session hijacking and man in the middle, but what about man in the browser? A man-in-the-browser (MITB) attack occurs when the hacker sends a Trojan to intercept browser calls. The Trojan basically sits between the browser and libraries, allowing a hacker to watch, and interact within, a browser session. Cobalt Strike creator Peiter C. Zatko added this feature a couple years back (www.advancedpentest.com/help-browser-pivoting). If you have his Beacon (the name of his implant) on a box, you can "browser pivot" such that all of the target's active sessions become your own. All of them. It effectively sets up a local proxy port so you can point your browser to it, and it directs all your requests through the Beacon on the target machine. Now you're browsing in your own browser as the target, without them even knowing it.

☒ **B** is incorrect because this does not necessarily describe a man-in-the-middle (MITM) attack, which is an attack where the hacker positions himself between the client and the server to intercept (and sometimes alter) data traveling between the two.

☒ **C** and **D** are incorrect because these are not legitimate terms.

9. Claire's Windows system at work begins displaying strange activity, and she places a call to the IT staff. On investigation, it appears Claire's system is infected with several viruses. The IT staff removes the viruses, deleting several file and folder locations and using an AV tool, and the machine is reconnected to the network. Later in the day, Claire's system again displays strange activity and the IT staff is called once again. Which of the following are likely causes of the re-infection? (Choose all that apply.)

A. Claire revisits a malicious website.

B. Claire opens her Microsoft Outlook e-mail client and newly received e-mail is loaded to her local folder (.pst file).

C. Claire uses a system restore point to regain access to deleted files and folders.

D. Claire uses the organization's backup application to restore files and folders.

☑ **A, C, D.** Virus removal can be tricky, especially if nobody knows how and when the virus got on the system in the first place. As a matter of fact, in many places I've worked, discovering the source of the virus is as important as cleaning the system in the first place. Cleaning a virus off the system usually involves scrubbing the Microsoft registry, deleting files and folders (don't forget to check for hidden ones), and a host of other details and actions. Sometimes AV removal applications can help with this process, but sometimes it's an involved, manual process.

Even with tools to help in removal, administrators can't afford to overlook system restore points, backups, and user behavior. If a virus is on a system during a system restore copy action, then any restoration of that point will reinstall the virus. The same thing goes for data backups themselves—it should follow that an infected file while being backed up will remain infected during the restore action. As for user behavior, if the user is re-infected immediately following a specific website visit, or after using a USB (or other removable media), at least you can pinpoint the source and hopefully stop it from happening again.

☒ **B** is incorrect because new e-mail from the server wouldn't necessarily be the cause of the original infection.

10. In regard to Trojans, which of the following best describes a wrapper?

A. The legitimate file the Trojan is attached to

B. A program used to bind the Trojan to a legitimate file

C. A method of obfuscation using compression

D. A software tool that uses encryption and code manipulation to hide malware

☑ **B.** *Wrappers* are programs that allow you to bind an executable of your choice (Trojan) to an innocent file your target won't mind opening. For example, you might use a program such as EliteWrap to embed a backdoor application with a game file (.exe). A user on your target machine then opens the latest game file (maybe to play a hand of cards against the computer or to fling a bird at pyramids built by pigs) while your backdoor is installing and sits there waiting for your use later. As an aside, many wrappers themselves are considered malicious and will show up on any up-to-date virus signature list.

☒ **A** is incorrect because the wrapper is not the legitimate file the malware is bound to.

☒ **C** is incorrect because this describes a packer.

☒ **D** is incorrect because this describes a crypter.

11. In May of 2017, this ransomware took advantage of a Windows SMB vulnerability known as the Eternal Blue exploit and spread worldwide in a matter of hours. A hidden kill switch inside the coding was quickly discovered, halting its spread. Which of the following best fits this description?

A. Petya

B. WannaCry

C. Zeus

D. Botnet

☑ **B.** WannaCry was one of the fastest spreading, most dangerous ransomware variants of all time. Taking advantage of Eternal Blue (interestingly enough, an exploit discovered by and shared from the NSA), WannaCry spread to systems worldwide in a matter of hours, demanding ransom payment in bitcoin. Despite patching being available, due to many and varied reasons, multiple millions of systems were unpatched and unprepared for the attack. A built-in kill switch—sending a reply packet to a nonexistent domain, which was registered by a researcher to stop the spread—was discovered within days.

☒ **A** is incorrect because Petya—while also exploiting Eternal Blue—had a few differences with its WannaCry sibling. Petya, in large measure, appeared to be ransomware you couldn't pay off. Given its release, appearance, and general exclusivity (at least initially) in Ukraine, speculation was that it was more of a politically motivated and destructive type of malware than a legitimate ransomware effort.

☒ **C** is incorrect because Zeus is a banking Trojan.

☒ **D** is incorrect because a botnet refers to a group of zombie systems controlled by an attacker.

12. Which of the following is a legitimate communication path for the transfer of data?

A. Overt

B. Covert

C. Authentic

D. Imitation

E. Actual

☑ **A.** This is another one of those easy, pure-definition questions you simply can't miss on your exam. Whether it's inside a computer, between systems, or across the Internet, any legitimate channel used for communications and data exchange is known as an *overt channel.* And don't let the inherit risk with any channel itself make the decision for you—even if the channel itself is a risky endeavor, if it is being used for its intended purpose, it's still overt. For example, an IRC or a gaming link is still an overt channel, so long as the applications making use of it are legitimate. Overt channels are legitimate communication channels used by programs across a system or a network, whereas covert channels are used to transport data in ways they were not intended for.

☒ **B** is incorrect because a covert channel, per EC-Council's own definition, is "a channel that transfers information within a computer system or network in a way that violates security policy." For example, a Trojan might create a channel for stealing passwords or downloading sensitive data from the machine.

☒ **C, D,** and **E** are incorrect because none of these is a term for the communications channel; they are included here as distractors.

13. In what layer of the OSI reference model is session hijacking carried out?

A. Data Link layer

B. Transport layer

C. Network layer

D. Physical layer

☑ **B.** If you think about a session hijack, this makes sense. Authentication has already occurred, so we know both computers have already found each other. Therefore, the Physical, Data Link, and Network layers have already been eclipsed. And what is being altered and played with in these hijacking attempts? Why, the sequence numbers, of course, and sequencing occurs at the Transport layer. Now, for all you real-world folks out there screaming that communications can be, and truly are, hijacked at every level, let me caution your outrage with something I've said repeatedly throughout this book: sometimes the exam and reality are two different things, and if you want to pass the test, you'll need to memorize this the way EC-Council wants you to. Session hijacking is taught in CEH circles as a measure of guessing sequence numbers, and that's a Transport layer entity. In the real world, your Physical layer interception of a target would result in access to everything above, but on the exam just stick with "session hijacking = Transport layer."

☒ **A, C,** and **D** are incorrect because these layers are not where a session hijack attack is carried out.

14. A pen test team member types the following command:

```
nc222.15.66.78 -p 8765
```

Which of the following statements is true regarding this attempt?

A. The attacker is attempting to connect to an established listening port on a remote computer.

B. The attacker is establishing a listening port on his machine for later use.

C. The attacker is attempting a DoS against a remote computer.

D. The attacker is attempting to kill a service on a remote machine.

☑ **A.** As stated earlier, Netcat is a wonderful tool that allows remote access wizardry on a machine, and you'll need to be able to recognize the basics of the syntax. In the command example, Netcat is being told, "Please attempt a connection to the machine with the IP address of 222.15.66.78 on port 8765; I believe you'll find the port in a listening state, waiting for our arrival." Obviously at some point previous to issuing this command on his local machine, the pen tester planted the Netcat Trojan on the remote system (222.15.66.78) and set it up in a listening state. He may have set it up with command-shell access (allowing a Telnet-like connection to issue commands at will) using the following command:

```
nc -L -p 8765 -t -e cmd.exe
```

☒ **B** is incorrect because this command is issued on the client side of the setup, not the server side. At some point previously, the port was set to a listening state, and this Netcat command will access it.

☒ **C** is incorrect because this command is not attempting a denial of service against the target machine. It's included here as a distractor.

☒ **D** is incorrect because this command is not attempting to kill a process or service on the remote machine. It's included here as a distractor.

15. Examine the partial command-line output listed here:

```
Active Connections
Proto  Local Address          Foreign Address      State
  TCP    0.0.0.0:912            COMPUTER11:0          LISTENING
  TCP    0.0.0.0:3460           COMPUTER11:0          LISTENING
  TCP    0.0.0.0:3465           COMPUTER11:0          LISTENING
  TCP    0.0.0.0:8288           COMPUTER11:0          LISTENING
  TCP    0.0.0.0:16386          COMPUTER11:0          LISTENING
  TCP    192.168.1.100:139      COMPUTER11:0          LISTENING
  TCP    192.168.1.100:58191    173.194.44.81:https   ESTABLISHED
  TCP    192.168.1.100:58192    173.194.44.81:https   TIME_WAIT
  TCP    192.168.1.100:58193    173.194.44.81:https   TIME_WAIT
  TCP    192.168.1.100:58194    173.194.44.81:https   ESTABLISHED
  TCP    192.168.1.100:58200    bk-in-f138:http       TIME_WAIT
```

Which of the following is a true statement regarding the output?

A. This is output from a **netstat -an** command.

B. This is output from a **netstat -b** command.

C. This is output from a **netstat -e** command.

D. This is output from a **netstat -r** command.

☑ **A.** You'll need to get to know Netstat before your exam. It's not a huge thing, and you won't get bogged down in minutiae, but you do need to know the basics. Netstat is a great command-line tool built into every Microsoft operating system. From Microsoft's own description, Netstat "displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols)." It's a great, easy way to see which ports you have open on your system, helping you to identify any Trojans that may be hanging around. A netstat -an command will show all connections and listening ports in numerical form.

☒ **B** is incorrect because the -b option displays the executable involved in creating each connection or listening port. Its output appears something like this:

```
Proto  Local Address    Foreign Address  State
  TCP    127.0.0.1:5354   COMPUTER11:49155 ESTABLISHED
 [mDNSResponder.exe]
  TCP    127.0.0.1:27015  COMPUTER11:49175 ESTABLISHED
 [AppleMobileDeviceService.exe]
  TCP    127.0.0.1:49155  COMPUTER11:5354  ESTABLISHED
 [AppleMobileDeviceService.exe]
  TCP    127.0.0.1:49175   COMPUTER11:27015 ESTABLISHED
 [iTunesHelper.exe]
```

☒ **C** is incorrect because the -e flag displays Ethernet statistics for the system. The output appears something like this:

```
                           Received            Sent
Bytes                     125454856        33551337
Unicast packets              164910          167156
Non-unicast packets             570           15624
Discards                          0               0
Errors                            0             268
Unknown protocols                 0
```

☒ **D** is incorrect because the -r flag displays the route table for the system. Here's a sampling of the output:

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination         Netmask     Gateway     Interface Metric
          0.0.0.0         0.0.0.0 192.168.1.1 192.168.1.100    25
         15.0.0.0       255.0.0.0     On-link 16.213.104.24    26
   15.195.201.216 255.255.255.255 192.168.1.1 192.168.1.100    26
   15.255.255.255 255.255.255.255     On-link 16.213.104.24   281.
```

16. You are discussing malware with a new pen test member who asks about restarting executables. Which registry keys within Windows automatically run executables and instructions? (Choose all that apply.)

    A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

    B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

    C. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

    D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

    ☑ **A, B, C, D.** Creating malware and infecting a machine with it is accomplishing only the basics. Getting it to hang around by having it restart when the user reboots the machine? Now we're talking. The Run, RunOnce, RunServices, and RunServicesOnce registry keys within the HKEY_LOCAL_MACHINE hive are great places to stick executables. Because of this, it's helpful to run registry monitoring on occasion to check for anything suspicious. Sys Analyzer, Regshot, and TinyWatcher are all options for this.

17. Which of the following is a true statement?

    A. Sequence prediction attacks are specific to TCP.

    B. Using a protocol in a way it is not intended to be used is an example of an overt channel.

    C. All DoS and DDoS attacks are specific to TCP.

    D. Fraggle is a TCP-based attack.

    ☑ **A.** Sequence prediction attacks are specific to TCP because TCP uses sequence numbers. Unlike the fire-and-forget method employed by UDP, TCP uses sequence numbers and windowing to keep track of conversations. Sequence prediction is a session hijacking procedure where the attacker guesses the next sequence number and launches himself into the data connection between client and server.

    ☒ **B** is incorrect because this is an example of a covert channel.

    ☒ **C** is incorrect because not all DoS and DDoS attacks are TCP based.

    ☒ **D** is incorrect because fraggle is a UDP-based DoS attack.

18. Which denial-of-service attack involves using multiple intermediary and secondary machines to contribute to the DoS effort?

    A. SYN flood

    B. DRDoS

    C. Application-level flood

    D. LOIC

☑ **B.** A *distributed reflection denial-of-service* (DRDoS) attack is also known as a "spoofed" attack and makes use of multiple intermediary and secondary machines. The bad guy sends attack information to the intermediary machines, which, in turn, send the messages out to the secondary machines. This makes tracking the real source of the attack very difficult to determine (the investigators will see and react to the secondaries, not the originator).

☒ **A** is incorrect because a SYN flood takes advantage of tons of half-open connections and does not use intermediary systems.

☒ **C** is incorrect because an application-level flood is a DoS action that floods applications or disrupts application-database communications.

☒ **D** is incorrect because Low Orbit Ion Cannon (LOIC) is a simple-to-use DDoS tool that floods a target with TCP, UDP, or HTTP requests. It was originally written as open source to attack various Scientology websites but has since had many people voluntarily joining a botnet to support a variety of attacks. LOIC was once used in a coordinated attack against Sony's PlayStation network, and the tool has a track record of other successful hits: the Recording Industry Association of America, PayPal, MasterCard, and several other companies have all fallen victim to LOIC.

19. Which of the following takes advantage of weaknesses in the fragment reassembly functionality of TCP/IP?

A. Teardrop

B. SYN flood

C. Smurf attack

D. Ping of death

☑ **A.** ECC can be rather capricious in their choice of which malware to test and which not to, and sometimes they look far into the past for question material. In a teardrop attack, overlapping, mangled packet fragments are sent in an effort to confuse a target system, causing it to reboot or crash. Teardrop attacks exploit an overlapping IP fragment bug present in Windows 95, Windows NT, and Windows 3.1 machines, as well as some early versions of Linux—all more than ten years old. The attack was really more of an annoyance than anything because a reboot clears it all up; however, anything that was open and altered, sitting unsaved on the device, would be lost. In modern systems, finding this attack in use is virtually impossible.

☒ **B** is incorrect because a SYN flood attack exhausts connections on a device by flooding it with thousands of open SYN packets, never sending any acknowledgments to the return SYN/ACKs.

☒ **C** is incorrect because a smurf attack involves spoofing the target's address and then pinging the broadcast address with it. The resulting responses of thousands of ICMP packets kill the machine.

☒ **D** is incorrect because the ping of death attack involves sending a ping request with an unusually large payload. The ping would be fragmented and, when put together, would kill the target machine.

20. IPSec is an effective preventative measure against session hijacking. Which IPSec mode encrypts only the data payload?

A. Transport

B. Tunnel

C. Protected

D. Spoofed

☑ **A.** IPSec is a wonderful encryption mechanism that can rather easily be set up between two endpoints or even across your entire subnet if you configure the hosts appropriately. You won't need to know all the bells and whistles with IPSec (and thank goodness, because there's a lot to write about), but you do need the basics. Transport mode does not affect the header of the packet at all and encrypts only the payload. It's typically used as a secured connection between two endpoints, whereas Tunnel mode creates a VPN-like connection protecting the entire session. Additionally, Transport mode is compatible with conventional network address translation (NAT).

☒ **B** is incorrect because Tunnel mode encapsulates the entire packet, including the header. This is typically used to form a VPN connection, where the tunnel is used across an untrusted network (such as the Internet). For pretty obvious reasons, it's not compatible with conventional NAT; when the packet goes through the router (or whatever is performing NAT for you), the source address in the packet changes because of Tunnel mode and, therefore, invalidates the packet for the receiving end. There are workarounds for this, generally lumped together as NAT traversal (NAT-t). Many home routers take advantage of something referred to as *IPSec passthrough* to allow just this.

☒ **C** and **D** are incorrect because they are invalid terms involving IPSec.

21. What provides for both authentication and confidentiality in IPSec?

A. AH

B. IKE

C. OAKLEY

D. ESP

☑ **D.** Encapsulation Security Payload (ESP) is a member of the IPSec protocol suite, and it provides data authentication (proving the data is actually from who it's supposed to be from) and confidentiality (by encrypting the data). In Transport mode, ESP doesn't provide integrity and authentication for the entirety of the packet, but it does in Tunnel mode (excluding the outer IP header, of course).

☒ **A** is incorrect because Authentication Header (AH) provides authentication but not encryption.

☒ **B** is incorrect because Internet Key Exchange (IKE) is a protocol that produces the security keys.

☒ **C** is incorrect because OAKLEY is a protocol used to create a master key as well as a key specific to each session in the data transfer. It makes use of the Diffie-Hellman algorithm for this process.

22. Which of the following statements best describes the comparison between spoofing and session hijacking?

A. Spoofing and session hijacking are the same thing.

B. Spoofing interrupts a client's communication, whereas hijacking does not.

C. Hijacking interrupts a client's communication, whereas spoofing does not.

D. Hijacking emulates a foreign IP address, whereas spoofing refers to MAC addresses.

☑ **C.** Hijacking and spoofing can sometimes be confused with each other, although they really shouldn't be. *Spoofing* refers to a process where the attacking machine pretends to be something it is not. Whether by faking a MAC address or an IP address, the idea is that other systems on the network will communicate with your machine (that is, set up and tear down sessions) as if it's the target system. Generally this is used to benefit sniffing efforts. Hijacking is a totally different animal. In hijacking, the attacker jumps into an already existing session, knocking the client out of it and fooling the server into continuing the exchange. In many cases, the client will simply reconnect to the server over a different session, with no one the wiser: the server isn't even aware of what happened, and the client simply connects again in a different session. As an aside, EC-Council describes the session hijack in these steps:

1. Sniff the traffic between the client and the server.
2. Monitor the traffic and predict the sequence numbering.
3. Desynchronize the session with the client.
4. Predict the session token and take over the session.
5. Inject packets to the target server.

☒ **A** is incorrect because spoofing and hijacking are different. An argument can be made that hijacking makes use of some spoofing, but the two attacks are separate entities: spoofing pretends to be another machine, eliciting (or setting up) sessions for sniffing purposes, whereas hijacking takes advantage of existing communications sessions.

☒ **B** is incorrect because spoofing doesn't interrupt a client's existing session at all; it's designed to sniff traffic and/or set up its own sessions.

☒ **D** is incorrect because spoofing isn't relegated to MAC addresses only. You can spoof almost anything, from MAC and IP addresses to system names and services.

23. Which of the following is an effective deterrent against TCP session hijacking?

A. Install and use an HIDS on the system.

B. Install and use Tripwire on the system.

C. Enforce good password policy.

D. Use unpredictable sequence numbers.

☑ **D.** As noted already, session hijacking requires the attacker to guess the proper upcoming sequence number(s) to pull off the attack, pushing the original client out of the session. Using unpredictable session IDs (or, better stated in the real world, using a modern operating system with less predictable sequence numbers) in the first place protects against this. Other countermeasures for session hijacking are fairly common sense: use encryption to protect the channel, limit incoming connections, minimize remote access, and regenerate the session key after authentication is complete. And, lastly, don't forget user education: if the users don't know any better, they might not think twice about clicking past the security certificate warning or reconnecting after being suddenly shut down.

☒ **A** is incorrect because a host-based intrusion detection system may not deter session hijacking at all.

☒ **B** is incorrect because Tripwire is a file integrity application and won't do a thing for session hijacking prevention.

☒ **C** is incorrect because system passwords have nothing to do with session hijacking.

24. Which of the following is a group of Internet computers set up to forward transmissions to other computers on the Internet without the owner's knowledge or permission?

A. Botnet

B. Zombie

C. Honeypot

D. DDoS

☑ **A.** A botnet is a group of systems an attacker has control over, without the owner's knowledge or permission. Each zombie system in the network sends messages and data transmissions for the botnet controller—everything from spam and e-mail to viruses and ads. Although they are probably best known for their roles in distributed denial-of-service attacks, botnets can be used for a variety of activities. As an aside, ECC maintains that botnets are most commonly controlled via IRC (Internet Relay Chat), but in the real world they can be controlled by a host of methods.

☒ **B** is incorrect because while a botnet is made up of zombie computers, a single zombie does not make up a botnet.

☒ **C** is incorrect because a honeypot is a system set up specifically to be hacked, so security staff can watch what an attacker is doing.

☒ **D** is incorrect because a distributed denial-of-service attack may be carried out by a botnet, but it does not define one.

25. Within a TCP packet dump, a packet is noted with the SYN flag set and a sequence number set at A13F. What should the acknowledgment number in the return SYN/ACK packet be?

A. A131

B. A130

C. A140

D. A14F

☑ **C.** We've been over the need for predicting sequence numbers before, so I won't bore you with it again other than to restate the salient point here: the ISN is incremented by 1 in the SYN/ACK return packet. Because these values were given in hex instead of decimal, all you need to know is what the next hex value after A13F is. You could split it out into binary (each hex digit is 4 bits, so this would equate to 1010000100111111) and then pick the next available number (1010000101000000) and split it back into hex (1010 = A, 0001 = 1, 0100 = 4, and 0000 = 0). Alternatively, you could convert directly to decimal (41279), add 1, and then convert back to hex. And, yes, you do need to know number conversion from decimal to binary to hex, so stop complaining.

☒ **A, B,** and **D** are incorrect hex equivalents for decimal 41280 (the next number acknowledgment for the ISN).

26. When is session hijacking performed?

A. Before the three-step handshake

B. During the three-step handshake

C. After the three-step handshake

D. After a FIN packet

☑ **C.** This question should be an easy one for you, but it's included here to reinforce the point that you need to understand session hijacking steps well for the exam. Of course, session hijacking should occur after the three-step handshake. As a matter of fact, you'll probably need to wait quite a bit after the three-step handshake so that everything on the session can be set up—authentication and all that nonsense should be taken care of before you jump in and take over.

☒ **A** and **B** are incorrect because session hijacking occurs after a session is already established, and the three-step handshake must obviously occur first for this to be true.

☒ **D** is incorrect because the FIN packet brings an orderly close to the TCP session. Why on Earth would you wait until the session is over to start trying to hijack it?