effectively protect them. It is also critical that you acquire a basic understanding of the terminology used by both security professionals and those who would seek to compromise your security.

Test Your Skills

Multiple Choice Questions Chapter 1

1. You are trying to explain security to a nontechnical manager. She has taken a rather extreme view of computer security. Which of the following is one of the extreme viewpoints about computer security discussed in this chapter?

   A. The federal government will handle security.

   B. Microsoft will handle security.

   C. There are no imminent dangers to your system.

   D. There is no danger if you use Linux.

2. You have just taken over as network security administrator for a small community college. You want to take steps to secure your network. Before you can formulate a defense for a network, what do you need?

   A. Appropriate security certifications

   B. A clear picture of the dangers to be defended against

   C. To finish this textbook

   D. The help of an outside consultant

3. Mary is teaching an introductory cybersecurity course to freshmen. She is explaining to them the major threats. Which of the following is not one of the three major classes of threats?

   A. Attempts to intrude on the system

   B. Online auction fraud

   C. Denial of service attacks

   D. A computer virus

4. Being able to define attack terms is an important skill for a cybersecurity professional. What is a computer virus?

   A. Any program that is downloaded to your system without your permission

   B. Any program that self-replicates

   C. Any program that causes harm to your system

   D. Any program that can change your Windows Registry

5. Being able to define attack terms is an important skill for a cybersecurity professional. What is spyware?

   A. Any software that monitors your system

   B. Only software that logs keystrokes

   C. Any software used to gather intelligence

   D. Only software that monitors what websites you visit

6. What is a penetration tester?

   A. A person who hacks a system without being caught

   B. A person who hacks a system by faking a legitimate password

   C. A person who hacks a system to test its vulnerabilities

   D. A person who is an amateur hacker

7. Elizabeth is explaining various hacking terms to a class. She is in the process of discussing the history of phone system hacking. What is the term for hacking a phone system?

A. Telco-hacking

B. Hacking

C. Cracking

D. Phreaking

8. What is malware?

A. Software that has some malicious purpose

B. Software that is not functioning properly

C. Software that damages your system

D. Software that is not properly configured for your system

9. What is war-driving?

A. Driving and seeking a computer job

B. Driving while using a wireless connection for hacking

C. Driving looking for wireless networks to hack

D. Driving and seeking rival hackers

10. What is the name for the hacking technique that involves using persuasion and deception to get a person to provide information to help compromise security?

A. Social engineering

B. Conning

C. Human intel

D. Soft hacking

11. There are many threats on the Internet. Which one is currently the most common may change over time, but certain threats have always been more common than others. Which of the following is the most common threat on the Internet?

A. Auction fraud

B. Phreaking

C. Computer viruses

D. Illegal software

12. What are the three approaches to security?

A. Perimeter, layered, hybrid

B. High security, medium security, low security

C. Internal, external, and hybrid

D. Perimeter, complete, none

13. Defining your security strategy is an important step in securing a network. You are trying to classify devices based on the approach they take to security. An intrusion detection system is an example of which of the following?

A. Proactive security

B. Perimeter security

C. Hybrid security

D. Good security practices

14. Which of the following is the most basic security activity?

A. Authentication

B. Firewalls

C. Password protection

D. Auditing

15. The most desirable approach to security is one that is which of the following?

A. Perimeter and dynamic

B. Layered and dynamic

C. Perimeter and static

D. Layered and static

16. According to a survey of 223 computer professionals prepared by the Computer Security Institute, which of the following was most often cited as an issue by respondents?

A. Internal systems

B. Employee abuse

C. Routers

D. Internet connection

17. Which of the following types of privacy law affects computer security?

A. Any state privacy law

B. Any privacy law applicable to your organization

C. Any privacy law

D. Any federal privacy law

18. The first computer incident-response team is affiliated with what university?

A. Massachusetts Institute of Technology

B. Carnegie-Mellon University

C. Harvard University

D. California Technical University

19. Which of the following is the best definition of the term *sensitive information*?

A. Any information that has an impact on national security

B. Any information that is worth more than $1,000

C. Any information that if accessed by unauthorized personnel could damage your organization in any way

D. Any information that is protected by privacy laws

20. Which of the following is a major resource for detailed information on a computer virus?

A. The MIT Virus Library

B. The Microsoft Virus Library

C. The F-Secure Virus Library

D. The National Virus Repository

Exercises

Exercise 1.1: How Many Virus Attacks Have Occurred This Month?

1. Using some website resource, such as www.f-secure.com, look up recent computer virus outbreaks.

2. How many virus outbreaks have occurred in the past 7 days?

3. Write down how many outbreaks have occurred in the past 30 days, 90 days, and 1 year.

4. Are virus attacks increasing in frequency?

How is DNS is accomplished; that is, how does a URL get translated into an IP address? How does a computer know what IP goes with what URL? There are servers known as DNS servers that are set up just to do this task. If you are on a corporate network, you probably have a DNS server on your network. If you are not, then your ISP has one. These servers maintain a table of IP-to-URL entries. From time to time there are transfers of DNS data, called *zone transfers*, that allow one DNS server to send its changes to another. Across the Internet, there are root DNS servers that are maintained with centralized data for all registered URLs/IP addresses.

Summary

This chapter cannot make you a networking expert. However, you should now have a basic understanding of how networks and the Internet work. Before you move on to subsequent chapters, you should make certain you completely understand basic hardware such as switches, NICs, routers, and hubs. You should also be familiar with the basic protocols presented in this chapter. It is important that you be comfortable with the utilities presented. It is strongly suggested that you experiment with these utilities extensively. It is also important that you be comfortable with the basics of the OSI model. Many students struggle with it at first, but at least make sure you have a general understanding of it before you move on to Chapter 3, "Cyber Stalking, Fraud, and Abuse."

The material in this chapter will be critical in later chapters. If you are new to this material, you should thoroughly study this chapter before continuing. In the exercises at the end of this chapter, you will be able to practice using `IPConfig`, `tracert`, and `ping`.

Test Your Skills

Multiple Choice Questions Chapter 2

1. Malek is purchasing cable to use in setting up small office networks. He wants to stock up on commonly used cable. What type of cable do most networks use?

   A. Net cable

   B. STP

C. Phone cable

D. UTP

2. You are assigned with attaching connectors to segments of cable. What type of connector is used with network cables?

A. RJ-11

B. RJ-85

C. RJ-12

D. RJ-45

3. What type of cable is used in most networks?

A. Unshielded twisted-pair

B. Shielded twisted-pair

C. Unshielded untwisted-pair

D. Shielded untwisted-pair

4. John is trying to simply connect three computers in a small network. He does not need any sort of routing capability and is not concerned about network traffic. What is the simplest device for connecting computers?

A. NIC

B. Interface

C. Hub

D. Router

5. Sharice is trying to teach a new technician basic networking terms. What should she tell this new technician NIC stands for?

A. Network interface card

B. Network interaction card

C. Network interface connector

D. Network interaction connector

6. Which of the following is a device used to connect two or more networks?

A. Switch

B. Router

C. Hub

D. NIC

7. Juan has just installed a new T1 line in a medical office. The front desk receptionist has asked what speed they can expect. A T1 line sends data at what speed?

A. 100Mbps

B. 1.54Mbps

C. 155Mbps

D. 56.6Kbps

8. How big is a TCP packet header?

A. The size depends on the data being sent.

B. The size is always 20 bytes.

C. The size depends on the protocol being used.

D. The size is always 40 bytes.

9. What protocol translates web addresses into IP addresses?

A. DNS

B. TFTP

C. DHCP

D. SMTP

10. What protocol is used to send email, and on what port does it work?

A. SMTP, port 110

B. POP3, port 25

C. SMTP, port 25

D. POP3, port 110

11. Gunther is setting up encrypted remote communications so that the server administrators can remotely access servers. What protocol is used for remotely logging on to a computer in a secure manner?

A. SSH

B. HTTP

C. Telnet

D. SMTP

12. Mohammed needs to open a firewall port so that web traffic can be passed through the firewall. What protocol is used for web pages, and on which port does it work?

A. HTTP, port 21

B. HTTP, port 80

C. DHCP, port 80

D. DHCP, port 21

13. What is the name for the point where the backbones of the Internet connect?

A. Connectors

B. Routers

C. Network access points

D. Switches

14. You are examining a list of IP addresses. Some are internal, some are external, and some are not valid. Which of the following is not a valid IP address?

A. 127.0.0.1

B. 295.253.254.01

C. 131.156.5.2

D. 245.200.11.1

15. What class of address is the IP address 193.44.34.12?

A. A

B. B

C. C

D. D

16. The IP address 127.0.0.1 always refers to your what?

A. Nearest router

B. ISP

C. Self

D. Nearest NAP

17. Internet addresses of the form www.chuckeasttom.com are called what?

A. User-friendly web addresses

B. Uniform resource locators

C. User-accessible web addresses

D. Uniform address identifiers

18. Which U.S. government agency created the distributed network that formed the basis for the Internet?

A. Advanced Research Projects Agency

B. Central Intelligence Agency

C. NASA

D. Department of Energy

19. Which of the following was one of the three universities involved in the original distributed network set up by a government agency?

A. UC Berkeley

B. Harvard

C. MIT

D. Princeton

20. You are explaining the history of networking to a group of first-year students. What did Vince Cerf invent?

A. The World Wide Web

B. Email

C. TCP

D. The first computer virus

21. You are explaining the history of networking to a group of first-year students. What did Tim Berners-Lee invent?

A. The World Wide Web

B. Email

C. TCP

D. The first computer virus

22. John is working with command-line utilities to gather diagnostic information about a computer that cannot connect to the network. Which utility provides information about a machine's network configuration?

    A. `Ping`

    B. `IPConfig`

    C. `Tracert`

    D. `MyConfig`

23. Sheryl is explaining the OSI model to new technicians at her company. She is trying to explain what protocols operate at the various layers of the OSI model. At what layer of the OSI model does TCP operate?

    A. Transport

    B. Application

    C. Network

    D. Data link

24. Which layer of the OSI model is divided into two sublayers?

    A. Data link

    B. Network

    C. Presentation

    D. Session

25. Which of the following is a unique hexadecimal number that identifies your network card?

    A. NIC address

    B. MAC address

    C. NIC ID

    D. MAC ID

Exercises

Exercise 2.1: Using `IPConfig`

1. Open your command prompt or (Just type cmd at the search bar In Windows 10)

Summary

Clearly, fraud and identity theft are very real and growing problems. In this modern age of instant access to information and online purchasing, it is critical that you take steps to protect yourself against this issue. You must work to protect your privacy using steps outlined in this chapter. It is also imperative for law enforcement officers to obtain the skills needed to investigate and solve these sorts of cybercrimes.

Cyber stalking is one area that is often new to both civilians and law enforcement. It is very important that both groups have a clear understanding of what is, and is not, cyber stalking because, unfortunately, cyber stalking cases can escalate into real-world violence.

Test Your Skills

Multiple Choice Questions Chapter 3

1. Candice is discussing Internet fraud with a colleague. She is trying to explain the most common types of fraud. What is the term for the most common type of Internet investment fraud?

   A. The Nigerian fraud

   B. The Manhattan fraud

   C. The pump and dump

   D. The bait and switch

2. You have become quite active in online investing. You want to get some advice but are concerned about the veracity of the advice you receive. What is the most likely problem with unsolicited investment advice?

   A. You might not earn as much as claimed.

   B. The advice might not be truly unbiased.

   C. The advice might not be from a legitimate firm.

   D. You might lose money.

3. Juan is a security officer for an investment firm. He is explaining various scams to the brokers. What is the term for artificially inflating a stock in order to sell it at a higher value?

   A. Bait and switch

   B. The Nigerian fraud

   C. Pump and dump

   D. The Wall Street fraud

4. What is the top rule for avoiding Internet fraud?

   A. If it seems too good to be true, it probably is.

   B. Never use your bank account numbers.

   C. Only work with people who have verifiable email addresses.

   D. Don't invest in foreign deals.

5. Which of the following is not one of the Security and Exchange Commission's tips for avoiding investment fraud?

   A. Don't invest online.

   B. Consider the source of the offer.

   C. Always be skeptical.

   D. Always research the investment.

6. Aliya is active on online auctions but wants to avoid auction fraud. What are the four categories of auction fraud?

   A. Failure to send, failure to disclose, sending to wrong address, failure to deliver

   B. Failure to send, failure to disclose, sending something of lesser value, failure to deliver

   C. Failure to disclose, sending something to wrong address, failure to send, failure to deliver

   D. Failure to disclose, sending something of lesser value, failure to send, sending something of greater value

7. What is the term for a seller bidding on her own item to drive up the price?

   A. Bid siphoning

B. Bid shielding

C. Shill bidding

D. Ghost bidding

8. What is the term for submitting a fake but very high bid to deter other bidders?

A. Bid siphoning

B. Bid shielding

C. Shill bidding

D. Ghost bidding

9. What is typically the goal of identity theft?

A. To make illicit purchases

B. To discredit the victim

C. To avoid criminal prosecution

D. To invade privacy

10. According to the U.S. Department of Justice, identity theft is generally motivated by what?

A. Malicious intent

B. Personal hostility toward the victim

C. Economic gain

D. Thrill seeking

11. Clarence is a police detective with a small-town police department. He is trying to consider how seriously to take reports of cyber stalking. Why is cyber stalking a serious crime?

A. It is frightening to the victim.

B. It can be a prelude to violent crime.

C. It is using interstate communication.

D. It can be a prelude to identity theft.

12. What is cyber stalking?

A. Any use of the Internet to send or post threats

B. Any use of electronic communications to stalk a person

C. The use of email to send threats

D. The use of email to stalk a person

13. What do law enforcement officials usually require of a victim in order to pursue harassment allegations?

A. A verifiable threat of death or serious injury

B. A credible threat of death or serious injury

C. A verifiable threat of harm

D. A credible threat of harm

14. If you are posting anonymously in a chat room and another anonymous poster threatens you with assault or even death, is this person's post harassment?

A. Yes; any threat of violence is harassment.

B. Probably not because both parties are anonymous, so the threat is not credible.

C. Yes; chat room threats are no different from threats in person.

D. Probably not because making a chat room threat is not the same as making a threat in person.

15. What must exist for cyber stalking to be illegal in a state or territory?

A. Specific laws against cyber stalking in that state or territory

B. Specific laws against cyber stalking in that nation

C. Nothing; existing stalking laws can apply

D. Nothing; existing international cyber stalking laws apply

16. What is the first step in protecting yourself from identity theft?

A. Never provide personal data about yourself unless absolutely necessary.

B. Routinely check your records for signs of identity theft.

C. Never use your real name on the Internet.

D. Routinely check for spyware on your computer.

17. What can you do on your local computer to protect your privacy?

A. Install a virus scanner.

B. Install a firewall.

C. Set your browser's security settings.

D. Set your computer's filter settings.

18. What is a cookie?

A. A piece of data that web servers gather about you

B. A small file that contains data and is stored on your computer

C. A piece of data that your web browser gathers about you

D. A small file made that contains data and then is stored on the web server

19. Which of the following is not an efficient method of protecting yourself from auction fraud?

A. Only use auctions for inexpensive items.

B. Only use reputable auction sites.

C. Only work with well-rated sellers.

D. Only bid on items that seem realistic.

20. What is the top rule for chat room safety?

A. Make certain you have antivirus software installed.

B. Never use your real name or any real personally identifying characteristics.

C. Only use chat rooms that encrypt transmissions.

D. Use chat rooms that are sponsored by well-known websites or companies.

21. Why is it useful to have a separate credit card dedicated to online purchases?

A. If the credit card number is used illegally, you will limit your financial liability.

B. You can keep better track of your auction activities.

C. If you are defrauded, you can possibly get the credit card company to handle the problem.

D. You can easily cancel that single card if you need to do so.

22. What percentage of cyber stalking cases escalate to real-world violence?

    A. Fewer than 1%

    B. About 25%

    C. 90% or more

    D. About 19%

23. If you are a victim of cyber stalking, what should you do to assist the police?

    A. Nothing; it is their job, and you should stay out of it.

    B. Attempt to lure the stalker into a public place.

    C. Keep electronic and hard copies of all harassing communications.

    D. Try to provoke the stalker into revealing personal information about himself.

24. What is the top way to protect yourself from cyber stalking?

    A. Do not use your real identity online.

    B. Always use a firewall.

    C. Always use a virus scanner.

    D. Do not give out email addresses.

Exercises

Exercise 3.1: Setting Web Browser Privacy in Microsoft Edge

1. This process is described in detail with images in the chapter, but here you should actually walk through the process on your own:

    - Select Settings from the ellipsis (…) drop-down menu in the right-hand corner of the Microsoft Edge window and then choose Settings.
    - Scroll down and select View Advanced Settings.
    - Scroll down to the Privacy and Services section.

DoS attack, that traffic is sent to a *black hole*—that is, a nonexistent server/interface. This is often done by Internet service providers. *Sinkholes* are IP addresses that are used to analyze traffic and reject bad packets. Traffic is sent to a sinkhole so that it can be analyzed.

In addition, intrusion prevention systems (IPSs) are commonly used to examine traffic and block denial of service attacks.

As previously stated, none of these steps will make your network totally secure from either being the victim of a DoS attack or being the launch point for one, but they will help reduce the chances of either occurring. A combination of blackholing and sinkholing at the ISP with IPS on the network can provide reasonable protection. A good resource for this topic is the SANS Institute website, at www.sans.org/dosstep/. This site has some good tips on how to prevent DoS attacks.

Summary

DoS attacks are among the most common attacks on the Internet. They are easy to perform, do not require a great deal of sophistication on the part of the perpetrator, and can have devastating effects on the target system. Only virus attacks are more common. (And, in some cases, a virus can be the source of a DoS attack.) In the exercises, you will practice stopping a DoS attack.

Test Your Skills

Multiple Choice Questions Chapter 4

1. When considering the various attacks that can be executed on your system, it is important to understand which attacks are most common. Of the following, which is one of the most common and simplest attacks on a system?

   A. Denial of service attack

   B. Buffer overflow

C. Session hacking

D. Password cracking

2. All DoS attacks are predicated on overwhelming a system's workload capacity. Therefore, measuring the workload of a system is critical. Which of the following is not a valid way to define a computer's workload?

A. Number of simultaneous users

B. Storage capacity

C. Maximum voltage

D. Speed of network connection

3. What do you call a DoS attack launched from several machines simultaneously?

A. Wide-area attack

B. Smurf attack

C. SYN flood

D. DDoS attack

4. It is important to understand the different types of DoS attacks and the symptoms of those attacks. Leaving a connection half open is a symptom of which type of attack?

A. Smurf attack

B. Partial attack

C. SYN flood attack

D. DDoS attack

5. While there are a wide range of different ways to execute a DoS attack, they all are predicated on the same idea. What is the basic concept behind a DoS attack?

A. Computers don't handle TCP packets well.

B. Computers can handle only a finite load.

C. Computers cannot handle large volumes of TCP traffic.

D. Computers cannot handle large loads.

6. What is the most significant weakness in a DoS attack from the attacker's viewpoint?

   A. The attack is often unsuccessful.

   B. The attack is difficult to execute.

   C. The attack is easy to stop.

   D. The attack must be sustained.

7. What is the most common class of DoS attacks?

   A. Distributed denial of service

   B. Smurf attacks

   C. SYN floods

   D. Ping of death

8. A range of countermeasures can help defend against DoS attacks. What are three methods for protecting against SYN flood attacks?

   A. SYN cookies, RST cookies, and stack tweaking

   B. SYN cookies, DoS cookies, and stack tweaking

   C. DoS cookies, RST cookies, and stack deletion

   D. DoS cookies, SYN cookies, and stack deletion

9. Juan is explaining various DoS attacks to security operators at his company. Which attack mentioned in this chapter causes a network to perform a DoS attack on one of its own servers?

   A. SYN flood

   B. Ping of death

   C. Smurf attack

   D. DDoS

10. What is the name for a defense that depends on a hash being sent back to the requesting client?

    A. Stack tweaking

    B. RST cookies

C. SYN cookies

D. Hash tweaking

11. What type of defense depends on sending the client an incorrect SYN/ACK?

A. Stack tweaking

B. RST cookies

C. SYN cookies

D. Hash tweaking

12. You are attempting to explain various DoS attacks to a new security technician. You want to make sure she can differentiate between these different attacks and notice the signs of a specific attack. What type of defense depends on changing the server so that unfinished handshaking times out sooner?

A. Stack tweaking

B. RST cookies

C. SYN cookies

D. Hash tweaking

13. What type of attack is dependent on sending packets that are too large for the server to handle?

A. Ping of death

B. Smurf attack

C. Slammer attack

D. DDoS

14. You want to make sure your team can identify the various DoS attack vectors. What type of attack uses the victim's own network routers to perform a DoS attack on the target?

A. Ping of death

B. Smurf attack

C. Slammer attack

D. DDoS

15. There have been many different types of attacks over the years. Which of the following is an example of a DDoS attack?

A. MyDoom virus

B. Bagle virus

C. DoS virus

D. Smurf virus

16. How can securing internal routers help protect against DoS attacks?

A. Attacks cannot occur if the internal router is secured.

B. Because attacks originate outside the network, securing internal routers cannot help protect against DoS.

C. Securing the router will only stop router-based DoS attacks.

D. It will prevent an attack from propagating across network segments.

17. What can you do to your internal network routers to help defend against DoS attacks?

A. Disallow all traffic that is not encrypted

B. Disallow all traffic that comes from outside the network

C. Disallow all traffic that comes from inside the network

D. Disallow all traffic that comes from untrusted sources

18. There are classic attacks that, while several years old, are worthy of study due to their significance in the history of cybersecurity. Which of the following was rated by many experts (at the time) to be the fastest growing virus on the Internet?

A. MyDoom virus

B. Bagle virus

C. Slammer virus

D. Smurf virus

19. No attack mitigation strategy is perfect, and you need to allow at least some traffic into and out of your network, or else your network is of no use. What can you do with your firewall to defend against at least some DoS attacks?

    A. Block all incoming traffic

    B. Block all incoming TCP packets

    C. Block all incoming traffic on port 80

    D. Block all incoming ICMP packets

20. You are trying to identify all potential DoS attack vectors. In doing so, you hope to provide mitigation for each of these attack vectors. Why will protecting against Trojan horse attacks reduce DoS attacks?

    A. Many denial of service attacks are conducted by using a Trojan horse to get an unsuspecting machine to execute the DoS attack.

    B. If you can stop a Trojan horse attack, you will also stop DoS attacks.

    C. A Trojan horse will often open ports and thus allow DoS attacks.

    D. A Trojan horse has much the same effect as a DoS attack.

Exercises

Exercise 4.1: Executing a DoS Attack

Note that this exercise is best done in a laboratory setting where there are several machines available for use.

1. Set up one machine (preferably a machine with very limited capacity) to run a small web server. (You can download Apache for free for either Windows or Linux from www.apache.org.)

2. Use the `ping` utility with various other computers to attempt to perform a simple DoS attack on that web server. This attempt is accomplished by getting other machines to begin a

should be obvious by this point that securing your system is absolutely critical. In the upcoming exercises, you will try out antivirus programs by Norton and McAfee.

Another theme that is driven home throughout this chapter is that many, if not most, attacks are preventable. The exercises ahead will give you practice in figuring out how to prevent the Sasser and Sobig viruses. In most cases, prompt and regular patching of the system, use of antivirus tools, and blocking of unneeded ports would prevent such attacks. The fact that so many systems do get infected is an indication of the very real problem of network professionals not being skilled in computer security.

Test Your Skills

Multiple Choice Questions

Chapter 5

1. John is a network security administrator for a midsized college. He is trying to explain to a new hire what a virus is. Which of the following is the best definition of virus?

   A. A program that causes harm on your computer

   B. A program used in a DoS attack

   C. A program that slows down networks

   D. A program that self-replicates

2. Isabelle is responsible for cybersecurity at her company. She is concerned that a virus would cause damage to the IT systems. What is the most common damage caused by virus attacks?

   A. Slowing down networks by the virus traffic

   B. Deleting files

   C. Changing the Windows Registry

   D. Corrupting the operating system

3. You are trying to form policies for your organization to mitigate the threat of viruses. You want to ensure that you address the most common way for a virus to spread. What is the most common way for a virus to spread?

   A. By copying to shared folders

B. By email attachment

C. By FTP

D. By download from a website

4. Which of the following is the primary reason that Microsoft Outlook is so often a target for virus attacks?

A. Many hackers dislike Microsoft.

B. Outlook copies virus files faster.

C. It is easy to write programs that access Outlook's inner mechanisms.

D. Outlook is more commonly used than other email systems.

5. Which of the following virus attacks used a multimodal approach?

A. Slammer virus

B. Mimail virus

C. Sobig virus

D. Bagle virus

6. What factor about the WannaCry virus is especially interesting to security practitioners?

A. It could have been prevented with good patch management.

B. It deleted critical system files.

C. It was difficult to protect against.

D. It was very sophisticated and likely an example of nation-state weaponized malware.

7. What is the name of the very first virus ever detected?

A. Creeper

B. Wabbit

C. Mimail

D. Unnamed

8. Which of the following reasons most likely enabled the Bagle virus to spread so rapidly?

A. The email containing it claimed to be from the system administrator.

B. It copied itself across the network.

C. It was a sophisticated virus.

D. It was particularly virulent.

9. What made the Bagle virus so dangerous?

A. It changed Windows Registry settings.

B. It disabled antivirus software.

C. It deleted key system files.

D. It corrupted the operating system.

10. Which of the following is a method that any person can use to protect against virus attacks?

A. Set up a firewall.

B. Use encrypted transmissions.

C. Use secure email software.

D. Never open unknown email attachments.

11. You are trying to develop methods to mitigate the threat of viruses in your company. Which of the following is the safest way to send and receive attachments?

A. Use a code word indicating that an attachment is legitimate.

B. Send only spreadsheet attachments.

C. Use encryption.

D. Use virus scanners before opening attachments.

12. Shelly is trying to teach new employees how to handle emailed security alerts. Which of the following is true regarding emailed security alerts?

A. You must follow them.

B. Most companies do not send alerts via email.

C. You can trust attachments on security alerts.

D. Most companies send alerts via email.

13. Which of the following is something a Trojan horse might do?

A. Open a backdoor for malicious software.

B. Change your memory configuration.

C. Change ports on your computer.

D. Alter your IP address.

14. Jared is explaining various attacks to students in an introduction to cybersecurity class. He wants to make certain they fully understand the different attacks. What does a buffer-overflow attack do?

A. It overflows a port with too many packets.

B. It puts more email in an email system than it can hold.

C. It overflows the system.

D. It puts more data in a buffer than it can hold.

15. What virus exploited buffer overflows?

A. Sobig virus

B. Mimail virus

C. Sasser virus

D. Bagle virus

16. What can you do with a firewall to help protect against virus attacks?

A. There is nothing you can do on a firewall to stop virus attacks.

B. Shut down all unneeded ports.

C. Close all incoming ports.

D. None of the above are correct.

17. Malek is explaining various malware types to new technical support personnel. He is explaining to them the various types of malware so that they can recognized them. What type of malware is a key logger?

A. Virus

B. Buffer overflow

C. Trojan horse

D. Spyware

18. Which of the following is a step that all computer users should take to protect against virus attacks?

A. Purchase and configure a firewall.

B. Shut down all incoming ports.

C. Use nonstandard email clients.

D. Install and use antivirus software.

19. What is the primary way a virus scanner works?

A. By comparing files against a list of known virus profiles

B. By blocking files that copy themselves

C. By blocking all unknown files

D. By looking at files for virus-like behavior

20. What other way can a virus scanner work?

A. By comparing files against a list of known virus profiles

B. By blocking files that copy themselves

C. By blocking all unknown files

D. By looking at files for virus-like behavior

Exercises

Exercise 5.1: Using Norton Antivirus

1. Go to the Norton AntiVirus website (www.symantec.com/downloads) and download the trial version of its software.

2. Install and run the software.

3. Carefully study the application, noting features that you like and dislike.

Exercise 5.2: Using McAfee Antivirus

1. Go to the McAfee antivirus website (http://www.mcafeee.com) and download the trial version of its software.

2. Install and run the software.

3. Carefully study the application, noting features you like and dislike.

Multiple Choice Questions

1. Elizabeth is describing web-based attacks to a group of students in a computer security course. What does an SQL injection attack require?

   A. Having database admin privileges

   B. Creating an SQL statement that is always true

   C. Creating an SQL statement that will force access

   D. Understanding web programming

2. Juan is looking for a vulnerability scanner that is specifically tailored to Windows systems. Which of the following is a vulnerability scanner specifically for Windows systems?

   A. Nmap

   B. ophcrack

   C. Nessus

   D. MBSA

3. You are responsible for security on an e-commerce system. You want to mitigate as many attacks as you can. How can you prevent cross-site scripting?

   A. Filter user input.

   B. Use an IDS.

   C. Use a firewall.

   D. It cannot be prevented.

4. What is an advantage of using Nessus? (Use your favorite search engine to research Nessus to answer this question.)

   A. It is free for businesses.

   B. It can check for a wide range of vulnerabilities.

   C. It is designed for Windows systems.

   D. It includes an IDS.

5. Perez is exploring different password cracking tools. A friend has told him about ophcrack. ophcrack depends on the attacker doing what?

   A. Getting physical access to the machine

   B. Getting domain admin privileges

   C. Using social engineering

   D. Using a scanning tool

6. If you wish to view items that have been removed from a website, what is the best way to do so?

   A. Use Nessus.

   B. Use Nmap.

   C. Use www.netcraft.com.

   D. Use www.archive.org.

7. Malek needs a port scanner so he can scan open ports on his own network. Which of the following is a popular port scanner?

   A. Nessus

   B. ophcrack

   C. MBSA

   D. Nmap

8. Jane wants to mitigate as many attacks as she can. A colleague suggested that she block ICMP packets. Blocking incoming ICMP packets will prevent what type of scan?

   A. SYN

   B. Ping

   C. FIN

   D. Stealth

9. It is important that you understand cybersecurity terminology, including terms for different actors in cybersecurity. What is the correct term for a person who uses hacking techniques for illegal activities?

   A. A hacker

   B. A gray hat hacker

   C. A phreaker

   D. A cracker

10. What is the term for a person who hacks into phone systems?

    A. A hacker

    B. A gray hat hacker

    C. A phreaker

    D. A cracker

11. Penelope is teaching an introductory cybersecurity course and is trying to explain the terminology to students. What is the term for a person who uses tools to hack without understanding the underlying technology?

    A. A script kiddy

    B. A gray hat hacker

    C. A novice

    D. A white hat hacker

12. What is the name for the process of trying to list all the servers on a network?

    A. Port scanning

    B. Enumeration

    C. Vulnerability scanning

    D. Scouting

13. Terrance is trying to enumerate his network resources. Which of the following is a popular enumeration tool?

    A. Nessus

    B. Nmap

    C. MBSA

    D. Cheops

14. Jaron is trying to do a port scan of his own company. He wants to test to see if the company's security systems will be able to detect his scan. Which of the following is considered the most stealthy port scan?

    A. SYN

    B. Connect

    C. Ping

    D. Nmap

15. What is the most stealthy way to find out what type of server a website is running?

    A. Use Nmap.

B. Use Cain and Abel.

C. Use www.netcraft.com.

D. Use www.archive.org.

Exercises

Exercise 6.1: Using www.archive.org

This exercise gives you practice using www.archive.org. Go to www.archive.org and pull up at least two previous versions of your college's/university's website. What information can you find that is no longer on the website?

Exercise 6.2: Using Nmap

This exercise introduces you to the Nmap tool. You should download and install Nmap. Then run at least three different scans on either your own computer or a designated lab computer. (While it is not illegal to scan a computer, it may violate some security policies for some colleges and universities. Make certain you scan only a designated lab computer.)

Exercise 6.3: Using ophcrack

Download ophcrack to a CD. Then reboot your own machine to the ophcrack CD and attempt to crack your own local passwords. (It is critical that you do this only on your own machine or a designated lab machine. Doing this on other machines would probably violate security policies at your college/university/company.)

Exercise 6.4: Using Netcraft.com

Visit www.netcraft.com and do a search on at least three different websites of your choosing. Note what information you are able to gather about each website.

Projects

Project 6.1: Passive Reconnaissance

Select a local organization and conduct passive reconnaissance on it. This should include searching job boards, the organization's own website, user groups/bulletin boards, social networking sites, www.archive.org, and more. Gather as much information about the target network as you can.

Project 6.2: Port Scanners

Use your favorite search engine to locate at least two other port scanners besides Nmap. Download and install them and then try them on your own machine or a designated lab computer. Compare and contrast these tools to Nmap. Are they easier to use? More informative?

Project 6.3: MBSA

Download and install MBSA and run a vulnerability scan on your own computer or on a designated lab computer. What problems did you find? Was the tool easy to use?

Case Study

Jane is a hacker intent on breaking into the XYZ Corporation. She uses a variety of passive reconnaissance techniques and gathers extensive information about the company. Jane finds out from network administrator questions/comments in user groups the model of routers being used in the company. She finds a complete list of the IT staff and their phone numbers from a personnel directory on the company website. She also finds out what services are running by using a port scan.

Based on this scenario, consider the following questions:

1. What reasonable steps could the company have taken to prevent Jane from finding out router models and other company hardware?
2. What steps should the company take to prevent or at least reduce the efficacy of port scans?

might be made to appeal to that specific subgroup of people. Or the attacker might even take the time to learn personal details of a few of these individuals and target them specifically. This technique has been used against executives at various companies. In 2010 and 2011, this problem began to grow significantly.

Whaling is a form of phishing in which an attacker attempts to compromise information regarding a specific highly valuable employee. It involves the same techniques as phishing but is highly customized to increase the chances that the single individual target will be fooled and actually respond to the phishing attempt.

Summary

A number of conclusions can be drawn from this chapter's examination of industrial espionage. The first conclusion: It does indeed occur. The case studies clearly demonstrate that industrial espionage is not some exotic fantasy dreamed up by paranoid security experts. It is an unfortunate, but quite real, aspect of modern business. If your firm's management chooses to ignore these dangers, then they do so at their own peril.

The second thing that can be concluded from this brief study of industrial espionage is that there are a variety of methods by which espionage can take place. An employee revealing confidential information is perhaps the most common. However, compromising information systems is another increasingly popular means of obtaining confidential and potentially valuable data. You will want to know the best way to protect your company and yourself. In the upcoming exercises, you will run screen-capture software, key loggers, and antispyware so you can learn more about espionage tactics and how to deal with them.

Test Your Skills

Multiple Choice Questions Chapter 7

1. Terrance is trying to explain industrial espionage to a group of new security techs. What is the ultimate goal of espionage?

   A. To subvert a rival government

   B. To obtain information that has value

   C. To subvert a rival business

   D. To obtain information not otherwise available

2. In order to truly understand industrial espionage, you need to understand the mindset of the spy. What is the best outcome for a spy attempting an espionage activity?

   A. To obtain information without the target even realizing he did so

   B. To obtain information with or without the target realizing he did so

   C. To obtain information and discredit the target

   D. To obtain information and cause harm to the target

3. What is the usual motivating factor for corporate/industrial espionage?

   A. Ideological

   B. Political

   C. Economic

   D. Revenge

4. Which of the following types of information would be a likely target for industrial espionage?

   A. A new algorithm that the company's IT department has generated

   B. A new marketing plan that the company has formulated

   C. A list of all the company's customers

   D. All of the above

5. Accurate statistics on corporate espionage are difficult to obtain. One reason is that the victims don't always report the crime, as they often don't want the incidents to become public. Which of the following is a likely reason that an organization might be reluctant to admit it has been a victim of corporate espionage?

   A. It would embarrass the IT department.

   B. It would embarrass the CEO.

   C. It might cause stock value to decline.

   D. It might lead to involvement in a criminal prosecution.

6. What is the difference between *corporate* and *industrial* espionage?

   A. None; they are interchangeable terms.

   B. Industrial espionage only refers to heavy industry, such as factories.

   C. Corporate espionage only refers to executive activities.

   D. Corporate espionage only refers to publicly traded companies.

7. Information is a valuable asset. It can be useful to calculate that value in order to determine how much effort should be put into protecting it. What formula can you use to calculate the value of information?

   A. Resources needed to produce the information plus resources gained from the information

   B. Resources needed to produce the information multiplied by resources gained from the information

   C. Time taken to derive the information plus money needed to derive the information

   D. Time taken to derive the information multiplied by money needed to derive the information

8. If a company purchases a high-end UNIX server to use for its research and development department, what is probably the most valuable part of the system?

   A. The high-end UNIX server

   B. The information on the server

   C. The devices used to protect the server

   D. The room to store the server

9. Information is an asset to your company if it

   A. Cost any sum of money to produce

   B. Cost a significant sum of money to produce

   C. Might have economic value

   D. Might cost significant money to reproduce

10. What is the greatest security risk to any company?

    A. Disgruntled employees

    B. Hackers

    C. Industrial spies

    D. Faulty network security

11. Which of the following is the best definition for *spyware*?

    A. Software that assists in corporate espionage

    B. Software that monitors activity on a computer

    C. Software that logs computer keystrokes

    D. Software that steals data

12. What is the highest level of security you can expect to obtain?

A. A level of security that makes the effort required to get information more costly than the value of the information

B. A level of security comparable with government security agencies, such as the Central Intelligence Agency

C. A level of security that has a 92.5% success rate in stopping intrusion

D. A level of security that has a 98.5% success rate in stopping intrusion

13. In the context of preventing industrial espionage, why might you wish to limit the number of company CD burners and control access to them in your organization?

A. An employee could use such media to take sensitive data.

B. An employee could use such media to copy software from the company.

C. CDs could be a vehicle for spyware to get on your system.

D. CDs could be a vehicle for a virus to get on your system.

14. Why would you want to scan an employee's computer when he leaves the organization?

A. To check the workflow prior to his leaving

B. To check for signs of corporate espionage

C. To check for illegal software

D. To check for pornography

15. What is the reason for encrypting hard drives on laptop computers?

A. To prevent a hacker from reading the data while you are online

B. To ensure that data transmissions are secure

C. To ensure that another user on that machine will not see sensitive data

D. To prevent a thief from getting data off of a stolen laptop

Exercises

Exercise 7.1: Learning About Industrial Espionage

1. Using the Web, library, journals, or other resources, look up a case of industrial or corporate espionage that was not already mentioned in this chapter.

2. Write a brief essay describing the facts in the case. The parties in the case and the criminal proceeding are of interest, but most of your

MULTIPLE CHOICE QUESTIONS

1. It is important to understand the concepts and application of cryptography. Which of the following most accurately defines encryption?

   A. Changing a message so it can only be easily read by the intended recipient
   B. Using complex mathematics to conceal a message
   C. Changing a message using complex mathematics
   D. Applying keys to a message to conceal it

2. Which of the following is the oldest encryption method discussed in this text?

   A. PGP
   B. Multi-alphabet encryption
   C. Caesar cipher
   D. Cryptic cipher

3. Many classic ciphers are easy to understand but not secure. What is the main problem with simple substitution?

   A. It does not use complex mathematics.
   B. It is easily broken with modern computers.
   C. It is too simple.
   D. It maintains letter and word frequency.

4. Classic ciphers were improved with the addition of multiple shifts (multiple substitution alphabets). Which of the following is an encryption method that uses two or more different shifts?

   A. Caesar cipher
   B. Multi-alphabet encryption
   C. DES
   D. PGP

5. Which binary mathematical operation can be used for a simple (but unsecured) encryption method and is in fact a part of modern symmetric ciphers?

   A. Bit shift
   B. OR
   C. XOR
   D. Bit swap

6. Why is binary mathematical encryption not secure?

   A. It does not change letter or word frequency.
   B. It leaves the message intact.
   C. It is too simple.
   D. The mathematics of it is flawed.

7. Which of the following is most true regarding binary operations and encryption?

   A. They are completely useless.
   B. They can form a part of viable encryption methods.
   C. They are only useful as a teaching method.
   D. They can provide secure encryption.

8. What is PGP?

   A. Pretty Good Privacy, a public key encryption method

B. Pretty Good Protection, a public key encryption method

C. Pretty Good Privacy, a symmetric key encryption method

D. Pretty Good Protection, a symmetric key encryption method

9. Which of the following methods is available as an add-in for most email clients?

A. DES

B. RSA

C. Caesar cipher

D. PGP

10. Which of the following is a symmetric key system that uses 64-bit blocks?

A. RSA

B. DES

C. PGP

D. Blowfish

11. What is the advantage of a symmetric key system using 64-bit blocks?

A. It is fast.

B. It is unbreakable.

C. It uses asymmetric keys.

D. It is complex.

12. What size key does a DES system use?

A. 64 bit

B. 128 bit

C. 56 bit

D. 256 bit

13. What type of encryption uses different keys to encrypt and decrypt the message?

A. Private key

B. Public key

C. Symmetric

D. Secure

14. Which of the following methods uses a variable-length symmetric key?

A. Blowfish

B. Caesar

C. DES

D. RSA

15. What should you be most careful of when looking for an encryption method to use?

A. Complexity of the algorithm

B. Veracity of the vendor's claims

C. Speed of the algorithm

D. How long the algorithm has been around

16. Which of the following is most likely to be true of an encryption method that is advertised as unbreakable?

A. It is probably suitable for military use.

B. It may be too expensive for your organization.

C. It is likely to be exaggerated.

D. It is probably one you want to use.

17. Which of the following is most true regarding certified encryption methods?

    A. These are the only methods you should use.

    B. It depends on the level of certification.

    C. It depends on the source of the certification.

    D. There is no such thing as certified encryption.

18. Which of the following is most true regarding new encryption methods?

    A. Never use them until they have been proven.

    B. You can use them, but you must be cautious.

    C. Use them only if they are certified.

    D. Use them only if they are rated unbreakable.

Exercises

Exercise 8.1: Using the Caesar Cipher

This exercise is well suited for group or classroom exercises.

1. Write a sentence in normal text.
2. Use a Caesar cipher of your own design to encrypt it.
3. Pass it to another person in your group or class.
4. Time how long it takes that person to break the encryption.
5. (Optional) Compute the mean time for the class to break Caesar ciphers.

Exercise 8.2: Using Multi-Alphabet Ciphers

This exercise also works well for group settings and is best used in conjunction with Exercise 8.1.

1. Write a sentence in normal text.
2. Use a multi-alphabet cipher of your own design to encrypt it.
3. Pass it to another person in your group or class.
4. Time how long it takes that person to break the encryption.
5. (Optional) Compute the mean time for the class to break these and compare that to the mean time required to break the Caesar ciphers.

Exercise 8.3: Using PGP

1. Download a PGP attachment for your favorite email client. A web search for PGP and your email client (that is, PGP and Outlook or PGP and Eudora) should locate both modules and instructions.
2. Install and configure the PGP module.
3. Working with a classmate, send encrypted messages back and forth.

Exercise 8.4: Finding Good Encryption Solutions

1. Scan the Web for various commercial encryption algorithms.
2. Find one that you feel may be “snake oil.”
3. Write a brief paper explaining your opinion.

the IEEE 802.11i standard, provides Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP), which provides data confidentiality, data origin authentication, and data integrity for wireless frames. (Some of these terms you should recall from Chapter 8.) CBC prevents known plain text attacks.

The MAC preserves message integrity and ensures that packets are not altered in transit, either accidentally or intentionally. This means that WPA2 uses very strong encryption along with message integrity.

WPA3

WPA3, which was released on 2018, has many interesting features. Among its more interesting new properties is that all traffic to and from the wireless access point (WAP) is encrypted. WPA3 also requires attackers to interact with your Wi-Fi for every password guess they attempt, which makes brute-force attacks less likely to be successful.

Summary

It is absolutely critical that every network have a firewall and proxy server between the network and the outside world. It is critical that all machines in a network (servers and workstations alike) have updated virus protection. It is also a good idea to consider implementing an IDS and antispyware. In the upcoming exercises, you will have an opportunity to practice setting up various types of firewalls and IDSs.

Test Your Skills

Multiple Choice Questions

Chapter 9

1. Which of the following is the most common way for a virus scanner to recognize a virus?

   A. To compare a file to known virus attributes

   B. To use complex rules to look for virus-like behavior

   C. To look for only TSR programs

D. To look for TSR programs or programs that alter the Registry

2. What is one way of checking emails for virus infections?

A. Block all emails with attachments.

B. Block all active attachments (for example, ActiveX, scripting).

C. Look for subject lines that are from known virus attacks.

D. Look for emails from known virus sources.

3. What are TSR programs?

A. Terminal signal registry programs, which alter the system Registry

B. Terminate and system remove programs, which erase themselves when complete

C. Terminate and scan remote programs, which scan remote systems prior to terminating

D. Terminate and stay resident programs, which stay in memory after you shut them down

4. What is the name for scanning that depends on complex rules to define what is and is not a virus?

A. Rules-based scanning (RBS)

B. Heuristic scanning

C. TSR scanning

D. Logic-based scanning (LBS)

5. Which of the following is not one of the basic types of firewalls?

A. Screening firewall

B. Application gateway

C. Heuristic firewall

D. Circuit-level gateway

6. Which of the following is the most basic type of firewall?

A. Screening firewall

B. Application gateway

C. Heuristic firewall

D. Circuit-level gateway

7. Which of the following is a disadvantage to using an application gateway firewall?

A. It is not very secure.

B. It uses a great deal of resources.

C. It can be difficult to configure.

D. It can only work on router-based firewalls.

8. What does SPI stand for?

A. Stateful packet inspection

B. System packet inspection

C. Stateful packet interception

D. System packet interception

9. What is the term for a firewall that is software installed on an existing server?

A. Network host-based firewall

B. Dual-homed firewall

C. Router-based firewall

D. Screened host

10. What is a major weakness with a network host-based firewall?

A. Its security depends on the underlying operating system.

B. It is difficult to configure.

C. It can be easily hacked.

D. It is very expensive.

11. What is the term for blocking an IP address that has been the source of suspicious activity?

A. Preemptive blocking

B. Intrusion deflection

C. Proactive deflection

D. Intrusion blocking

12. What is the term for a fake system designed to lure intruders?

    A. Honey pot

    B. Faux system

    C. Deflection system

    D. Entrapment

13. Which of the following is the correct term for making a system less attractive to intruders?

    A. Intrusion deterrence

    B. Intrusion deflection

    C. Intrusion camouflage

    D. Intrusion avoidance

14. What method do most IDS software implementations use?

    A. Anomaly detection

    B. Preemptive blocking

    C. Intrusion deterrence

    D. Infiltration

15. How do most antispyware packages work?

    A. By using heuristic methods

    B. By looking for known spyware

    C. The same way antivirus scanners work

    D. By seeking out TSR cookies

Exercises

Exercise 9.1: Setting Up a Firewall

Microsoft Windows (in every version since XP, including Windows 10) and Linux both offer built-in packet-filtering firewalls of some sort. Ideally, if you have access to both operating systems, the best exercise is to experiment with setting up firewalls for both.

1. Using the documentation for whichever operating system you have, decide what packets you wish to block.

2. Set your firewall to filter those packets.

In this chapter, you learned that technology is not enough to ensure a secure network. You must have clear and specific policies detailing procedures on your network. Those policies must cover employee computer resource use, new employees, outgoing employees, access rights, how to respond to an emergency, and even the security of code in applications and websites.

User policies must cover all aspects of how the user is expected to use company technology. In some cases, such as with instant messaging and Web use, policies may be difficult to enforce, but they must still be in place. If your user policies fail to cover a particular area of technology use, then you will have difficulty taking any action against an employee who performs that particular misuse.

We also learned that it is not just the end user who will need policies. The IT staff needs clearly delineated policies covering how to handle various situations. Of particular concern are policies dictating how to handle new users or exiting users. You also need a carefully considered change management policy.

Test Your Skills

Multiple Choice Questions

Chapter 10

1. Which of the following does not demonstrate the need for policies?

   A. Antivirus software cannot prevent a user from downloading infected files.

   B. The most secure password is not at all secure if it's posted on a note by the computer.

   C. End users are generally not particularly bright and must be told everything.

   D. Technological security measures are dependent upon the employees' implementation.

2. Which of the following is not an area that user policies need to cover?

   A. Minimum length of passwords

   B. What websites a user can or cannot visit

   C. If and when to share passwords

   D. What a user should do if she believes her password has been compromised

3. Which of the following is not an example of a user password policy?

   A. Users may not keep copies of passwords in their office.

   B. Passwords must be eight characters long.

   C. A user may only share passwords with his or her assistant.

   D. Passwords may not be shared with any employee.

4. What should an employee do if she believes her password has been revealed to another party?

   A. If it is a trusted employee or friend, just ignore it.

   B. Change the password immediately.

   C. Notify the IT department.

   D. Ignore it.

5. Which of the following should not be recommended as acceptable email attachments?

   A. Flash animations

   B. Excel spreadsheets from a colleague

   C. Attachments you were expecting

   D. Plain text attachments from known sources

6. Which of the following is the best reason users should be prohibited from installing software?

   A. They may not install it correctly, which could cause security problems for the workstation.

B. They may install software that circumvents security.

C. Software installation is often complex and should be done by professionals.

D. If a user's account does not have installation privileges, then it is likely that a Trojan horse will not be inadvertently installed under their account.

7. Which of the following is not a significant security risk posed by instant messaging?

A. Employees may send harassing messages.

B. Employees might send out confidential information.

C. A virus or worm might infect the workstation via instant messaging.

D. An instant messaging program could actually be a Trojan horse.

8. What must all user policies have in order to be effective?

A. They must be reviewed by an attorney.

B. They must state consequences.

C. They must be notarized.

D. They must be properly filed and maintained.

9. Which of the following is the appropriate sequence of events for a new employee?

A. IT is notified of the new employee and the requested resources > employee is granted access to those resources > employee is briefed on security/acceptable use > employee signs acknowledging receipt of a copy of security rules.

B. IT is notified of the new employee and the requested rights > employee is given access to those resources > employee signs acknowledging a receipt of a copy of security rules.

C. IT is notified of the new employee and assigns default rights > employee is briefed on security/acceptable use >

employee signs acknowledging receipt of a copy of security rules.

D. IT is notified of the new employee and assigns default rights > employee signs acknowledging receipt of company security rules.

10. Which of the following is the appropriate sequence of events for a departing employee?

A. IT is notified of the departure > all logon accounts are shut down > all access (physical and electronic) is disabled.

B. IT is notified of the departure > all logon accounts are shut down > all access (physical and electronic) is disabled > the employee's workstation is searched/scanned.

C. IT is notified of the departure > all physical access is shut down > all electronic access is shut down.

D. IT is notified of the departure > all electronic access is shut down > all physical access is shut down.

11. Which of the following is the appropriate sequence for a change request?

A. Business unit manager requests change > IT unit verifies request > request is implemented.

B. Business unit manager requests change > IT unit verifies request > security unit verifies request > request is scheduled with rollback plan > request is implemented.

C. Business unit manager requests change > IT unit verifies request > request is scheduled with rollback plan > request is implemented.

D. Business unit manager requests change > IT unit verifies request > security unit verifies request > request is implemented.

12. What is the first step when discovering a machine(s) has been infected with a virus?

A. Log the incident.

B. Scan and clean the infected machine(s).

C. Notify appropriate management.

D. Quarantine the infected machine(s).

13. What is the rule in access control?

A. Grant the most access you can securely give

B. Grant the least access job requirements allow

C. Grant standard access for all users

D. Strictly limited access for most users

14. After dealing, on a technical level, with any security breach, what is the last thing to be done for a security breach?

A. Quarantine infected machines.

B. Study the breach to learn how to prevent recurrence.

C. Notify management.

D. Log the incident.

15. Which of the following is a list of items that should be implemented in all secure code?

A. All code checked for backdoors or Trojans, all buffers have error handling to prevent buffer overruns, all communication activity thoroughly documented

B. All code checked for backdoors or Trojans, all buffers have error handling to prevent buffer overruns, all communication adheres to organizational guidelines, all communication activity thoroughly documented

C. All code checked for backdoors or Trojans, all buffers have error handling to prevent buffer overruns, all communication adheres to organizational guidelines

D. All code checked for backdoors or Trojans, all communication adheres to organizational guidelines, all communication activity thoroughly documented

Exercises

Each of these exercises is intended to give the student experience writing limited portions of a policy. Together, the exercises create a complete policy for a college campus computer network.

Anyone who seems reluctant to provide any of these items should be avoided. Therefore, an ideal security consultant might be a person with 5 or more years of experience, a degree in a computer-related discipline, a certification in your organization's operating systems as well as one of the major security certifications, and a completely clean background, with references. As a rule, you simply cannot be too careful in hiring a security consultant.

Unless you have a highly trained security expert on staff, you should consider bringing in a security consultant to assess your system at least once. In our current legal environment, liability for security breaches is still being hotly debated. Companies are being sued for failing to practice due diligence in computer security. It is simply a wise move, both from a computer industry perspective as well as from a legal perspective, to do everything reasonable to ensure the security of your systems.

Summary

This chapter has outlined some basic items to look for in any security assessment. You should periodically assess your network/system for security vulnerabilities. A general recommendation would be a quarterly assessment for noncritical/low-security sites and perhaps as frequently as a weekly assessment for high-security sites. In any case, what are outlined in this chapter are the basics of assessing the security of a network, and they should give you a start toward securing your own network.

Safe computing is a matter of securing your computer, your network, and your servers and using common sense on the Web. It is important to rigorously apply security practices and standards to all computers, whether they are home computers or part of an organizational network.

Test Your Skills

Multiple Choice Questions

Chapter 11

1. What are the six *P*s of security?

A. Patch, ports, personnel, privacy, protect, policies

B. Ports, patch, protect, probe, policies, physical

C. Physical, privacy, patch, ports, probe, protect

D. Ports, patch, probe, physical, privacy, policies

2. John is now responsible for system security at a small bookkeeping firm. He wants to ensure that he implements good fundamental security. What is the most basic rule of computer security?

A. Keep systems patched.

B. Always use an IDS.

C. Install a firewall.

D. Always use antispyware.

3. You work in the network security department of a large bank. One of your jobs is to keep all systems patched. How might you ensure that system patches are kept up to date?

A. Use an automated patching system.

B. Patch any time you receive a vendor notification of a new patch.

C. Patch whenever a new threat is announced.

D. Use periodic scheduled patching.

4. Teresa is explaining basic security to a new technician. She is teaching him how to secure ports on any server or workstation. What is the rule about ports?

A. Block all incoming ports.

B. Block ICMP packets.

C. Block all unused ports.

D. Block all nonstandard ports.

5. Miguel is trying to secure a web server. He has decided to shut down any services that are not needed. His supervisor has told him to check dependencies first. Which of the following is a good reason to check dependencies before shutting down a service?

A. To determine whether you will need to shut down other services as well

B. To determine whether shutting down this service will affect other services

C. To find out what this service does

D. To find out whether this service is critical to system operations

6. If your machine is not used as a server and is not on a local network, what packet-filtering strategy should you use?

A. Block all ports except 80.

B. Do not block any ports.

C. Block all ports that you don't need.

D. Do not block well-known ports.

7. You are trying to implement good fundamental security for a small company. Which of the following is the least essential device for protecting your network?

A. Firewall

B. Virus scanners on all machines

C. IDS system

D. Proxy server

8. Mohammed is responsible for security policies at a university. He is trying to ensure proper access policies. What is the rule of thumb on data access?

A. Data must be available to the widest range of people possible.

B. Only administrators and supervisors should access sensitive data.

C. Only those with a need for the specific data should have access.

D. All employees should have access to any data used in their department.

9. What is password age?

A. How long a user has had a password

B. The length of the password history

C. A reference to the sophistication (maturity) of the password

D. A reference to a password's length

10. What is the minimum frequency for system probing and audits?

A. Once per month

B. Once per year

C. Every other year

D. Every other month

11. An audit should check what areas?

A. Perform system patching, review policies, check personnel records of all managers, and probe for flaws

B. Only probe for flaws

C. Perform system patches, probe for flaws, check logs, and review policies

D. Check all machines for illicit software, perform complete system virus scan, and review firewall policies

12. Jerod is setting up security for a server room for a university. Which of the following is true of the room in which the server is located?

A. It should be in the most fire-resistant room in the building.

B. It should have a strong lock with a strong door.

C. It should be accessible only to those who have a need for access.

D. All of the above.

13. Elizabeth is responsible for security policies at her policies. She is trying to implement sound end user security policies. What would be most important to block end users from doing on their own machine?

A. Running programs other than those installed by the IT staff

B. Surfing the Web and using chat rooms

C. Changing their screensaver and using chat rooms

D. Installing software or changing system settings

14. What is the preferred method for storing backups?

A. Near the server for quick restore if needed

B. Offsite in a secure location

C. In the IT manager's office for security

D. At the home of one of the IT staff

15. Which of the following is a step you would definitely take with any server but might not be required for a workstation?

A. Uninstall all unneeded programs/software.

B. Shut down unneeded services.

C. Turn off the screensaver.

D. Block all Internet access.

16. Which of the following is a step you might take for large networks but not for smaller networks?

A. Use an IDS.

B. Segment the network with firewalls between the segments.

C. Use antivirus software on all machines on the network.

D. Do criminal background checks for network administrators.

17. Which of the following is a common way to establish security between a web server and a network?

A. Block all traffic between the web server and the network.

B. Place virus scanning between the network and the web server.

C. Put a firewall between the web server and the network.

D. Do not connect your network to the web server.

18. What is the rule on downloading from the Internet?

A. Never download anything.

B. Only download if the download is free of charge.

C. Only download from well-known, reputable sites.

D. Never download executables. Only download graphics.

19. Which of the following certifications is the most prestigious?

A. CISSP

B. PE

C. MCSA

D. Security+

20. Which of the following set of credentials would be best for a security consultant?

A. Ten years of IT experience, 1 year in security, CIW Security analyst, M.B.A.

B. Eight years of IT experience, 3 years in security, CISSP, B.S. in computer science

C. Eleven years of IT experience, 3 years in security, MCSE and CISSP, M.S. in information systems

D. Ten years of experience as a hacker and cracker, MCSE/CIW and Security +, Ph.D. in computer science

Exercises

Exercise 11.1: Patching Systems

1. Using a lab system, find and apply all operating system patches.

2. Check with all vendors of software installed on that machine and apply patches for those applications as well (if available).

3. Note the time taken to fully patch a machine. Consider how long it would take to patch a 100-machine network.

4. Write an essay that answers the following questions: Are there ways you could speed the process of patching a 100-machine network? How might you approach such a task?

Exercise 11.2: Learning About Policies

1. Using the resources given or other resources, find at least one sample security policy document.

2. Analyze that document.

3. Write a brief essay giving your opinion of that policy. Did it miss items? Did it include items you had not thought of?

Exercise 11.3: Learning About Disaster Recovery

1. Using the resources given or other resources, find at least one sample disaster recovery plan.

economic hardship could use seemingly unimportant information. In the exercises at the end of this chapter, you will have a chance to explore various cyber terrorism and information warfare threats.

Test Your Skills

Multiple Choice Questions

1. What is the most likely damage from an act of cyber terrorism?

   A. Loss of life

   B. Military strategy compromised

   C. Economic loss

   D. Disrupted communications

2. Which of the following is not an example of financial loss due to cyber terrorism?

   A. Lost data

   B. Transferring money from accounts

   C. Damage to facilities including computers

   D. Computer fraud

3. Which of the following military/government systems would most likely be the target of a successful computer hack?

   A. The most sensitive systems of the CIA

   B. Nuclear systems at NORAD

   C. Low-security logistical system

   D. Military satellite control systems

4. Which of the following might be an example of domestic cyber terrorism?

   A. Sasser virus

   B. Mimail virus

   C. Sobig virus

   D. MyDoom virus

5. What differentiates cyber terrorism from other computer crimes?

   A. It is organized.

   B. It is politically or ideologically motivated.

   C. It is conducted by experts.

   D. It is often more successful.

6. Which of the following is a political group that has already used the Internet for political intimidation?

   A. Internet Black Tigers

   B. Al Qaeda

   C. Mafia

   D. IRA

7. What is information warfare?

   A. Spreading disinformation

   B. Spreading disinformation or gathering information

   C. Gathering information

   D. Spreading disinformation or secure communications

8. Which of the following would most likely be considered an example of information warfare?

   A. Radio Free Europe during the Cold War

   B. Radio political talk show

   C. Normal news reports

   D. Military press releases

9. Which of the following is a likely use of Internet newsgroups in information warfare?

   A. To spread propaganda

   B. To monitor dissident groups

   C. To send encoded messages

   D. To recruit supporters

10. Sending a false message with weak encryption, intending it to be intercepted and deciphered, is an example of what?

A. Poor communications

B. Need for better encryption

C. Disinformation

D. Propaganda

11. Which of the following best describes the communication goal of any intelligence agency?

A. To send clear communications to allies and noise to all other parties

B. To send clear communications to allies and noise only to the enemy

C. To send disinformation to the enemy

D. To send clear communications to allied forces

12. Which of the following conflicts had a cyber warfare component?

A. 1989 invasion of Panama

B. 1990 Kosovo crisis

C. 1990 Somalia crisis

D. Vietnam War

13. Which of the following agencies has allegedly had one of its cyber spies actually caught?

A. NSA

B. KGB

C. FBI

D. CIA

14. Which of the following is a cyber attack that would likely cause imminent loss of life?

A. Disruption of banking system

B. Disruption of water

C. Disruption of security systems

D. Disruption of chemical plant control systems

Exercises

Summary

We have seen in this chapter that the Internet can be a valuable resource for any sort of investigation. It is often one of the tools that hackers and identity thieves use to gain information about their target. However, it can also be a valuable tool for you in researching a prospective employee or business partner. In addition, it can be invaluable for you to routinely find out what information is on the Internet about you. Seeing strange data that is not accurate can be an indication that you have already been the victim of identity theft.

Test Your Skills

Multiple Choice Questions

Chapter 13

1. How might an identity thief use the Internet to exploit his victim?

   A. He might find even more information about the target and use this information to conduct his crime.

   B. He could find out how much the target has in her savings account.

   C. An identity thief usually does not use the Internet to accomplish his task.

   D. He could use the Internet to intercept the target's email and thus get access to the target's personal life.

2. Which of the following is not an ideal place to seek out phone numbers and addresses?

   A. Yahoo! People Find

   B. People Search

   C. The international phone registry

   D. Infobel

3. Why do you not want too much personal data about you on the Internet?

   A. It might reveal embarrassing facts about you.

   B. It might be used by an identity thief to impersonate you.

C. It might be used by a potential employer to find out more about you.

D. There is no reason to worry about personal information on the Internet.

4. How could a hacker use information about you found through Internet searches?

A. It could be used to guess passwords if your passwords are linked to personal information such as your birth date, address, or phone number.

B. It could be used to guess passwords if your passwords are linked to your interests or hobbies.

C. It could be used in social engineering to ascertain more information about you or your computer system.

D. All of the above.

5. If you are hiring a new employee, which of the following should you do?

A. Verify degrees and certifications.

B. Call references.

C. Perform an Internet search to verify contact information and to check for a criminal record.

D. All of the above.

6. Which of the following would be *least* important to know about a potential business partner?

A. Past bankruptcies

B. A 15-year-old marijuana possession arrest

C. A lawsuit from a former business partner

D. A recent DUI

7. What information would provide the most accurate results for locating a person?

A. First name and state

B. First name, last name, and state

C. Last name and state

D. First name and last name

8. Of the websites listed in this chapter, which would be the most useful in obtaining the address and phone number of someone who does not live in the United States?

A. The FBI website

B. Yahoo!

C. Infobel

D. Google

9. Where would you go to find various state sex offender registries?

A. The FBI website

B. The national sex offender online database

C. The interstate online sex offender database

D. The special victims unit website

10. What is most important to learn about a person listed in a sex offender registry?

A. The extent of his punishment

B. How old she was when she committed her crime

C. How long he has been out of prison

D. The nature of her specific crime

11. Which web search approach is best when checking criminal backgrounds?

A. Check primarily the person's state of residence.

B. Check primarily federal records.

C. Check the current and previous state of residence.

D. Check as many places as might have information.

12. What advantages are there to commercial web search services?

A. They can get information you cannot.

B. They can get the information faster than you can.

C. They can do a more thorough job than you can.

D. They are legally entitled to do searches; you are not.

13. Which would you use to begin a search for information on a United States court case?

    A. The National Center for State Courts Website

    B. Infobel

    C. Yahoo! People Search

    D. Google Groups

14. Which of the following is the most accurate description of Usenet?

    A. A nationwide bulletin board

    B. A repository of computer security information

    C. A large-scale chat room

    D. A global collection of bulletin boards

15. Which of the following is the most helpful data you might get from Usenet on a person you are investigating?

    A. Postings by the individual you are investigating

    B. Security tips to help you investigate

    C. Criminal records posted

    D. Negative comments made by others about your target

Exercises

For all exercises and projects in this chapter, you will concentrate your investigation on some person. It is best if you investigate yourself (which makes it easier to evaluate the accuracy of what you find) or someone in the class or the instructor who volunteers to be the target of the investigation. There are ethical issues with simply investigating random people without their knowledge or permission. It is also important to avoid embarrassing someone in the classroom. So the volunteer targets of the investigation should be certain they will not be embarrassed by whatever is found. Substitute the name of the person you are investigating for John Doe or Jane Doe in the projects and exercises.

Exercise 13.1: Finding Phone Numbers

Individual cloud implementations might have additional utilities, such as administration consoles that allow a network administrator to monitor, configure, and administer the cloud.

There are two issues with cloud forensics. The first is jurisdictional. Often cloud data is replicated across servers in different countries, each with its own laws. Then there is the technical issue of getting the data. It is very unlikely that you would be able to image the entire cloud in question. So you will probably have to perform a logical copy of the data in question or even a live analysis.

Summary

In this chapter, you have seen the basics of computer forensics. The most important things you have learned are to make a forensics copy to work with and to document everything. You simply cannot over document. You have also learned how to retrieve browser information and recover deleted files, and you have learned some commands that may be useful forensically. You have explored the forensic value of the Windows Registry and even cloud forensics.

Test Your Skills

Multiple Choice Questions Chapter 14

1. In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

   A. Rules of evidence

   B. Law of probability

   C. Chain of custody

   D. Policy of separation

2. Ian is performing a forensic examination on a Linux server. He is trying to recover emails. Where does Linux store email server logs?

   A. /var/log/mail.*

   B. /etc/log/mail.*

   C. /mail/log/mail.*

   D. /server/log/mail.*

3. Why should you note all cable connections for a computer you want to seize as evidence?

   A. To know what outside connections existed

   B. In case other devices were connected

   C. To know what peripheral devices exist

   D. To know what hardware existed

4. Pedro is examining a Windows 7 computer. He has extracted the index.dat file and is examining that file. What is in the Index.dat file?

   A. Internet Explorer information

   B. General Internet history, file browsing history, and so on for a Windows machine

   C. All web history for Firefox

   D. General Internet history, file browsing history, and so on for a Linux machine

5. What is the name of the standard Linux command that is also available as a Windows application that can be used to create bitstream images and make a forensic copy?

   A. `mcopy`

   B. `image`

   C. `MD5`

D. `dd`

6. When cataloging digital evidence, the primary goal is to do what?

   A. Make bitstream images of all hard drives.

   B. Preserve evidence integrity.

   C. Avoid removing the evidence from the scene.

   D. Prohibit the computer from being turned off.

7. Mahmoud is using a range of Windows utilities to extract information from a computer he is triaging. He has just used the `Openfiles` command. The command `Openfiles` shows what?

   A. Any files that are opened

   B. Any shared files that are opened

   C. Any system files that are opened

   D. Any files open with ADS

8. "Interesting data" is what?

   A. Data relevant to your investigation

   B. Pornography

   C. Documents, spreadsheets, and databases

   D. Schematics or other economic-based information

9. Which of the following are important to the investigator regarding logging?

   A. The logging methods

   B. Log retention

   C. Location of stored logs

   D. All of the above

Exercises

Exercise 14.1: DiskDigger

Download DiskDigger and search your computer for deleted files. Attempt to recover one file of your choice.

Exercise 14.2: Making a Forensic Copy

This exercise requires two computers. You must also download either Kali Linux or Knoppix. (Both are free.) Then attempt to make a forensic copy of computer A by sending its data to computer B.

Exercise 14.3: OSForensics

Download a trial copy of OSForensics from https://www.osforensics.com/osforensics.html.

Using tutorials at https://www.osforensics.com/faqs-and-tutorials/video_demonstrations.html, perform basic forensics on your own computer with OSForensics.

This diagram is intentionally simple. The goal is to make the process one that cybersecurity engineers can efficiently use with minimal training required. The concept it to ensure that all data flow points have been identified, and that mitigation measures have been identified. This diagram is used to examine the system of interest and to determine what, if any mitigation strategies have been put into place for each data interface. This is essentially a limited interface diagram.

Security Block Diagram

Unified Modeling Language (UML), which was the basis for SysML, has a component diagram. In UML, component diagrams are used to identify components in software and to model how they connect. For example, UML contains assembly connectors that model a connection when one component requires another component. The delegation connector links an external component.

This section described the foundations of SecML, which is based on the preexisting SysML. It may be that further research leads to enhancements to these models, and the addition of new models to SecML. As with all modeling language, it is expected that SecML will be revised and expanded.

Summary

In this chapter, you have seen the application of systems engineering to cybersecurity. The goal is that you would begin to apply a methodical, systematic approach to cybersecurity. Penetration testing, as one example, should not be just a set of random hacking attempts. Rather, it should be a carefully engineered process that is mapped to specific testing requirements. It is also beneficial to model cybersecurity scenarios in order to better understand system security requirements. The SecML modeling language that was briefly introduced in this chapter provides such a methodology.

Test Your Skills

Multiple Choice Questions

Chapter 15

1. What type of diagram is used to show how any entity might interact with a system?

   A. Use-case diagram

   B. Sequence diagram

   C. Data interface diagram

   D. Requirements diagram

2. What is the most appropriate tool for capturing the requirements of any security process or system?

   A. Use-case diagram

   B. Sequence diagram

   C. SysML

   D. Traceability matrix

3. Which of the following cybersecurity activities would be most accurately described as engineering?

   A. Implementing complex IPS rules

   B. Implementing asymmetric cryptography

   C. Creating a requirements traceability matrix

   D. Conducting a forensic investigation

4. Which modeling language is used by systems engineers?

   A. SecML

   B. SysML

   C. UML

   D. DML

5. What does this symbol represent in SecML?

   A. A forbidden action

   B. A blocked system

C. A countermeasure

D. An attack

6. What does this symbol represent in SecML?

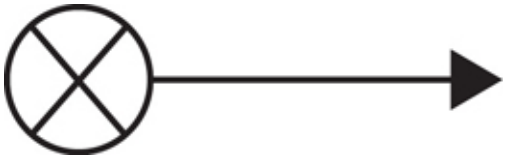
A. Attack victim

B. System abuser

C. System user

D. Isolated user

7. What does this system represent in SecML?



A. Blocked activity

B. External attack

C. Unauthorized activity

D. Internal attack

Exercises

Exercise 15.1: Misuse-Case Diagram

Create a misuse-case diagram for a specific type of attack. You can choose any attack described in this book.

Exercise 15.2: Requirements Gathering

Consider the cybersecurity requirements of a college campus. Create a requirements traceability matrix for penetration testing a campus computer network.