Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**10**

**Risk Management**

* [Module Introduction](javascript://)
* **10-1**[Security Risks](javascript://)
  + **10-1a**[People Risks](javascript://)
  + **10-1b**[Technology Risks](javascript://)
  + **10-1c**[Malware Risks](javascript://)
* **10-2**[Risk Assessment and Management](javascript://)
  + **10-2a**[Attack Simulations](javascript://)
  + **10-2b**[Red Team–Blue Team Exercise](javascript://)
  + **10-2c**[Scanning Tools](javascript://)
  + **10-2d**[Honeypots and Honeynets](javascript://)
* **10-3**[Physical Security](javascript://)
  + **10-3a**[Prevention Methods](javascript://)
  + **10-3b**[Detection Methods](javascript://)
* **10-4**[Device Hardening](javascript://)
  + **10-4a**[Updates and Security Patches](javascript://)
  + **10-4b**[Administrative Credentials](javascript://)
  + **10-4c**[Services and Protocols](javascript://)
  + **10-4d**[Passwords](javascript://)
  + **10-4e**[Anti-Malware Software](javascript://)
  + **10-4f**[Asset Disposal](javascript://)
* **10-5**[Security Policies for Users](javascript://)
  + **10-5a**[Security Policy Goals](javascript://)
  + **10-5b**[BYOD (Bring Your Own Device)](javascript://)
  + **10-5c**[AUP (Acceptable Use Policy)](javascript://)
  + **10-5d**[NDA (Non-Disclosure Agreement)](javascript://)
  + **10-5e**[Password Policy](javascript://)
  + **10-5f**[Privileged User Agreement](javascript://)
  + **10-5g**[Anti-Malware Policy](javascript://)
* **10-6**[Module Review](javascript://)
  + **10-6a**[Module Summary](javascript://)
  + **10-6b**[Key Terms](javascript://)
  + **10-6c**[Review Questions](javascript://)
  + **10-6d**[Hands-On Projects](javascript://)
  + **10-6e**[Capstone Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Introduction

### Objectives

After reading this module and completing the exercises, you should be able to:

* **1**Identify people, technology, and malware security risks to a network
* **2**Increase network security through risk assessment and management
* **3**Use physical security to prevent and detect intrusions
* **4**Implement device hardening techniques
* **5**Explain how security policies guide users’ activities on a network

**On the Job**

Security often involves synthesizing tidbits of information from many disparate sources to form an accurate picture of what has happened. My team once responded to a report that desktop computers at a biomedical corporation were crashing. Their hard drives had been erased, apparently, by a virus that circumvented the company’s antivirus protections.

While examining an affected PC, we noticed that a few processes were still running—thanks to the fact that the operating system generally won’t allow the deletion of files that are in use. Among these processes were several instances of svchost.exe. Closer examination revealed that one of these had the same name as the legitimate Windows executable, but was in fact an impostor: A saboteur was at work.

Using a disassembler, we determined that the Trojan checked a folder on a server every minute for the presence of a command file. It would then execute the contents of the command file. We built a program to monitor that directory and archive copies of any files that appeared; our program also recorded the user account that put the file there and the name of the system from which this was done.

The account had domain administrator privileges, and this led us to examine the domain’s logon scripts, where we found the code that installed the Trojan on users’ workstations. We wrote a second program to record the MAC address of the system when it registered its name with the DHCP server and inspect the ARP tables from the network’s switches to find the physical port to which it was connected. Then, with a building wiring diagram, we were able to track the culprit to a specific cubicle.

Finding the source of this problem involved knowledge about network infrastructure, operating systems, administration techniques, programming, and reverse engineering. This is an extreme example, to be sure, but real-world security problems seldom confine themselves to a single technical area of specialization.

**Peyton Engel**

**Technical Architect, CDW Corporation**

In the early days of computing, when secured mainframes acted as central hosts and data repositories were accessed only by dumb terminals with limited rights, network security was all but unassailable. As networks have become more geographically distributed and heterogeneous, however, the risk of their misuse has increased astronomically. Consider the largest, most heterogeneous network in existence: the Internet. Because it contains billions of points of entry, millions of servers, and billions of miles of transmission paths, it leads to millions of attacks on private networks every day. The threat of an outsider accessing an organization’s network via the Internet, and then stealing or destroying data, is very real.

In this module, you will learn about numerous threats to your network’s data and infrastructure, how to manage those vulnerabilities, and, perhaps most important, how to convey the importance of network security to the rest of your organization through an effective security policy. Later, you’ll continue your study of network security and go behind the scenes with ways to secure network access and activity. If you choose to specialize in network security, consider attaining CompTIA’s Security+ certification, which requires deeper knowledge of the topics covered in this course.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 10-1Security Risks

### Certification

* 3.2

Explain the purpose of organization documents and policies.

* 4.1

Explain common security concepts.

* 4.2

Compare and contrast common types of attacks.

* 4.5

Explain the importance of physical security.

Average reading time: 36 minutes

The exact nature of security risks varies widely for different types of organizations. For example, if you work for a large savings and loan institution that allows its clients to view their current loan status online, you must consider risks associated with data and access. If someone obtains unauthorized access to your network, all your customers’ personal financial data could be vulnerable. On the other hand, if you work for a local car wash that uses its internal LAN only to track assets and sales, you may be less concerned if someone gains access to your network because the implications of unauthorized access or use of sensitive data, called a [**data breach**](javascript://), are less dire. When considering security risks, the fundamental questions are “What is at risk?” and “What do I stand to lose if it is stolen, damaged, or eradicated?”

To understand how to manage network security, you first need to know how to identify threats to your network. And to do that, you must be familiar with the terms coined by network security experts to help in identifying specific risks and protective measures. A [**hacker**](javascript://), in the original sense of the word, is someone who masters the inner workings of computer hardware and software to better understand them. To be called a hacker used to be a compliment, reflecting extraordinary computer skills. Today, hacker is used more generally to describe individuals who gain unauthorized access to systems or networks with or without malicious intent. Hacking might also refer to finding a creative way around a problem, increasing functionality of a device or program, or otherwise manipulating resources beyond their original design, and has even come to be used in reference to noncomputer-related scenarios, such as life hacking or guitar hacks.

Hackers are categorized according to their intent and the prior approval of the organizations whose networks they’re hacking. Consider the following categories:

* **White hat hacker**—These IT security experts are hired by organizations to assess the company’s security and risks. They’re sometimes called ethical hackers because their goal is to identify security vulnerabilities the organization needs to resolve for its own protection. The scope of this hacking is usually clearly defined in a written contract before testing begins, and hacking activities are limited by existing laws and restrictions. At no point is private data compromised outside of that trusted relationship.
* **Black hat hacker**—These groups or individuals use their skills to bypass security systems with the intent to cause damage, steal data, or compromise privacy. They’re not concerned with legal restrictions, and their goal is to achieve personal gain or execute a personal agenda against an individual or organization. Some black hat hackers and groups are also available for hire to serve someone else’s agenda.
* **Gray hat hacker**—These hackers abide by a code of ethics all their own. Although they might engage in illegal activity, their intent is to educate and assist. For example, a computer hobbyist who hacks a local business’s weak Wi-Fi password—and then reports that weakness to the business owners without damaging or stealing the company’s data—has engaged in gray hat hacking. Gray hats are vulnerable to legal prosecution and, therefore, often go to great lengths to remain anonymous.

As you can see, while hackers’ motivations can vary from malicious to beneficial, the goal of hacking is to find weaknesses in the security system. A weakness of a system, process, or architecture that could lead to compromised information or unauthorized access is known as a [**vulnerability**](javascript://). The act of taking advantage of a vulnerability is known as an [**exploit**](javascript://). For example, [Figure 10-1](javascript://) shows an intruder climbing over a low fence. The low fence is a vulnerability. The act of breaching that fence is an exploit and is also a crime. For a more technical example, recall that an unauthorized access point can act as an evil twin. Once unsuspecting clients associate with such access points, the hacker can steal data in transit or access information on the client’s system. The evil twin masquerades as a valid access point, using the same SSID (service set identifier) and potentially other identical settings. In other words, the evil twin is an exploit that takes advantage of a vulnerability inherent in wireless communications in which SSIDs are openly broadcast and Wi-Fi clients scan for connections.

**Figure 10-1**

Vulnerability versus exploit



Enlarge Image

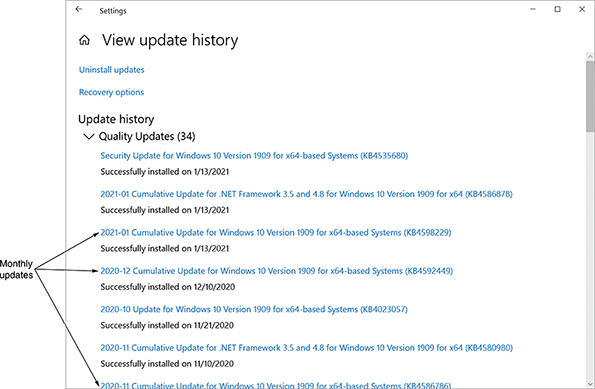
PK Studio/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

Cybersecurity vulnerabilities are often made public, in which case they are tracked by The MITRE Corporation in the [**CVE (Common Vulnerabilities and Exposures)**](javascript://) dictionary. This project is funded by the U.S. Department of Homeland Security. The list is free to access, use, and analyze, but only MITRE can make changes to it. While the CVE doesn’t contain details of the vulnerabilities themselves, it does provide a tracking system that is used by vulnerability databases. Each vulnerability receives a standardized identifying number, which makes it easier to track vulnerabilities across systems. You can learn more about the CVE and download your own copy at [cve.mitre.org](http://cve.mitre.org/" \t "_blank).

A [**zero-day exploit**](javascript://), or zero-day attack, is one that takes advantage of a software vulnerability that hasn’t yet or has only very recently become public. Zero-day exploits are particularly dangerous because the vulnerability is exploited before the software developer can provide a solution for it or before the user applies the published solution. For example, Microsoft schedules regular security updates to Windows on the second (and sometimes fourth) Tuesday of each month, called Patch Tuesday (see [Figure 10-2](javascript://)). Hackers can use this information to identify recently announced vulnerabilities in Windows and then immediately proceed to attack unpatched machines. Due to the quick timing of these attacks, the day after Patch Tuesday is informally dubbed Exploit Wednesday. Most current vulnerabilities, however, are well known. Throughout this module, you will learn about several kinds of exploits and how to prevent or counteract security threats.

**Figure 10-2**

Updates installed the day after each Patch Tuesday



Enlarge Image

As you read about each vulnerability, think about whether it applies to your network (and if so, how damaging it might be), how an exploit of the vulnerability could be prevented, and how it relates to other security threats. Keep in mind that malicious and determined intruders may use one technique, which then allows them to use a second technique, which then supports a third technique, and so on. For example, a hacker might discover someone’s username by watching them log on to the network. The hacker might then use a password-cracking program to access the network and plant a small program file. This code, when activated, generates an extraordinary volume of traffic that overwhelms and disables the network. None of the risks discussed in this module stand alone. Any risk can open the door to further exploitation.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-1aPeople Risks

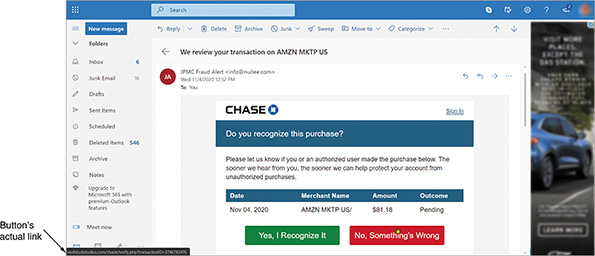
By some estimates, human error, ignorance, and omission cause more than half of all security breaches sustained by networks. Human error alone accounts for so many security breaches because taking advantage of people is often an easy way to circumvent network security. End-user awareness and training can be a monumental task that requires regular attention and due diligence. Ultimately, it is the company’s responsibility to ensure that its employees adhere to applicable standards and policies. An uninformed employee’s inadvertent missteps that cause a data breach can result in extreme litigation expenses for a company.

One of the most common methods by which an intruder gains access to a network is to simply ask users for their passwords. As bold as this might sound, it’s not uncommon for an intruder to pose as a technical support analyst who needs to know a user’s password to troubleshoot a problem. This strategy is called [**social engineering**](javascript://) because it involves manipulating social relationships to gain access. Common types of social engineering include the following:

* [**Phishing**](javascript://)—Communication that appears to come from a legitimate source and requests access or authentication information. For example, a hacker might send an email asking you to submit your username and password to a website whose link is provided in the message, claiming that it’s necessary to verify your account, a purchase, or other account information. Phishing emails are extremely effective, especially the more sophisticated ones. When well-executed, these emails can trick even a savvy IT security professional. For example, the phishing email shown in [Figure 10-3](javascript://) appears to come from Chase, a credit card company. If the victim has a Chase card, they might decide they at least need to read the email to find out if it’s real. The email creates a sense of urgency by saying the receiver’s credit card might have been compromised. The logo and formatting give the email a sense of formality, which implies authority. The seeming detail in the alleged charge gives a sense of credibility to build trust. However, further investigation reveals this email to be a scam. Notice the cursor in the figure is floating over the red button, revealing the button’s target address in the lower left corner of the image. If you clicked the button, this is the address the link would go to. Even though the link lists a transaction ID, which might be convincing, the link itself does not go to the Chase website. Scrolling to the bottom of the email, the fine print shown in [Figure 10-4](javascript://) is even more revealing—the email claims to come from Chase, but the company listed in the fine print is Capital One, a completely different company. Once you know what you’re looking for, it can be fun to pick apart a phishing email to discover its flaws.
* **Baiting**—A malware-infected file, such as a free music download, or a malware-infested device, such as a USB flash drive, is seemingly left unguarded for someone to take and attempt to use on their own computer. The malware then infects the computer and gives the attacker access to the victim’s computer, data, or online accounts. Leaving malware-infested flash drives lying in a parking lot or other obvious location is a favorite tactic among many hackers. This is especially common at hacking conventions, where attendees should know better than to plug an unknown flash drive into their computer, and yet still many take the bait.
* **Quid pro quo**—A free gift or service is offered in exchange for private information or “temporary” access to the user’s computer system. This tactic is surprisingly effective with people who have not been adequately trained to detect social engineering attempts.

**Figure 10-3**

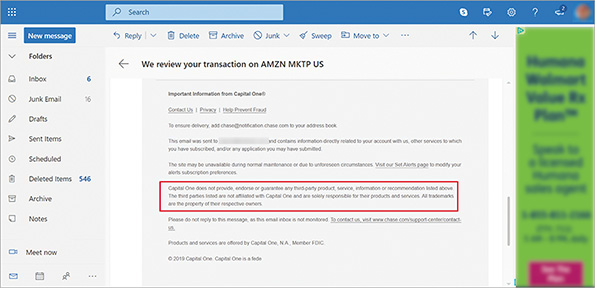
Phishing emails often include legitimate-looking logos, buttons, instructions, and fine print



Enlarge Image

**Figure 10-4**

Careful investigation reveals clues the email is fake



Enlarge Image

Social engineering doesn’t necessarily require lengthy processes of building relationships with victims. More transient in nature, the following attack types are related to the ways foot traffic flows in and out of a building or other space. With a little good acting, an attacker can “hide in plain sight,” appearing to belong while acting with malicious intent. Consider the following examples:

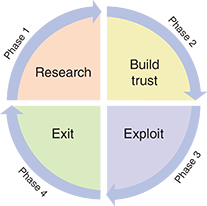
* [**Tailgating**](javascript://)—An unauthorized person follows an authorized person into a secure area without the authorized person’s knowledge or cooperation. For example, you might punch in a code on a keypad to enter a gated neighborhood and drive off, unaware that another car has followed you through the gate before it closed.
* [**Piggybacking**](javascript://)—A person uses deception to follow an authorized employee into a restricted area. For example, someone who appears to be a delivery person and is carrying a large box might ask you to “hold the door,” which gives the attacker access through an otherwise secure door. Similarly, a friendly sounding conversation with an employee as they walk into a building might get an intruder past the front desk security. It might feel rude to deny someone’s request for assistance in holding open a secure door or to chat politely when someone strikes up a conversation, but not everyone who is nice has good intentions.
* [**Shoulder surfing**](javascript://)—A person secretly observes an authorized person entering their credentials to access a secure area and then uses that information later. You should always be aware of who is around you and what they can see. For example, when entering a code into a keypad on a secured door, cover the keypad with your hand so no one can see your code.

Increasing environmental awareness, or situational awareness, is key to protecting secure spaces from unauthorized access. For example, teach employees that they can and should hold firm boundaries with people they don’t know when entering through a secure door or gate. Management should support employees who enforce access policies, even when it results in a legitimate customer becoming angry.

Hackers use psychological insights to develop and refine their techniques. The more you understand their processes—and teach your coworkers about these techniques—the more effectively you can defend against them. [Figure 10-5](javascript://) shows the typical social engineering attack cycle. Phase 1, research, is the most important, and it often requires the most time investment. Attackers build familiarity by initially asking for seemingly benign information. As they gather more data, they use these tidbits to build trust and gain access to more private information. This is Phase 2, building trust.

**Figure 10-5**

This cycle might happen quickly over a few seconds, or take much longer, even several years

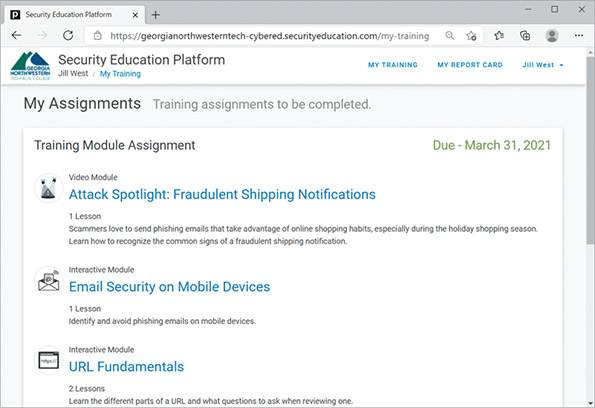


Phase 3, exploit, is the point of action on the part of the victim that gives the attacker the access they desire. This might be as simple as holding the door open, or it might be more involved, such as divulging trade secrets with someone the victim believes to be a colleague. Finally, in Phase 4, exit, the attacker executes an exit strategy in such a way that does not leave evidence or raise suspicion. The attacker might then repeat the cycle, gaining deeper access until the objective is achieved.

The most important defense against social engineering is employee training, along with frequent reminders and tips regarding the latest scams. Employee training programs might be regularly scheduled throughout the year with required compliance and pass rates (see [Figure 10-6](javascript://)). This technique follows the “use it or lose it” principle so employees are regularly exposed to cybersecurity concepts and best practices. It’s easy to forget this information for those who don’t work in IT, and frequent review can help employees more consistently apply these practices.

**Figure 10-6**

Security awareness training



Enlarge Image

Source: Proofpoint, Inc.

Less predictably, IT security staff can provide updates on current threats and the measures the company is taking to protect everyone. This helps build a sense of urgency and vigilance as employees recognize the importance of their role in protecting company data and other IT resources. Updates and training programs should be mindfully designed and written with professionalism to encourage users to engage with the information. Further, organizations can build a sense of accountability by occasionally conducting practice runs. These simulations can identify weaknesses in employee understanding of their cybersecurity responsibilities. You’ll learn more about this technique later in this module.

Employee training helps protect a company from external threats. However, it doesn’t address internal threats from insiders. An insider is someone who is or was trusted by an organization, such as an employee, former employee, contractor, or other associate. When a trusted person has or develops malicious intent, this presents an [**insider threat**](javascript://). These attackers pose a particularly high risk to an organization due to their knowledge of the company’s systems, procedures, and layers of security.

Whether people-related risks come from malicious insiders or naïve, trusted users, companies can take measures to reduce these risks, such as the following:

* Perform background checks for new hires and, where relevant, for contractors.
* Enforce the [**principle of least privilege**](javascript://), meaning employees and contractors are only given enough access and privileges to do their jobs, and these privileges are terminated as soon as the person no longer needs them.
* Design checks and balances on employee behavior, such as scheduled access, mandatory vacations, and job rotations.
* Deploy a [**DLP (data loss prevention)**](javascript://) solution that identifies sensitive data on the network and prevents it from being copied (such as downloading to a flash drive) or transmitted off the network (such as emailing or posting to cloud storage).

**Applying Concepts 10-1**

### Social Engineering in Action

One of the most eye-opening experiences in learning to protect against social engineering is to see an attack in action. Complete the following steps:

1. 1

Take a few moments to search online for a video showing a social engineering attack, such as a demonstration at a conference or for research. What’s the link to the video you found?

1. 2

As you watch the video, notice the psychological techniques the attacker uses, such as mixing truth with lies, creating a sense of urgency or scarcity, implying authority, playing on emotions, intimidation, generalizing to cover for unknown details, feigning familiarity, appealing to empathy, or offering favors to create a sense of owing a favor in return. What tactics did you identify in the video?

1. 3

What technical expertise (if any) was required to complete the attack?

1. 4

What advice could you give coworkers, friends, or family members to protect themselves from this kind of attack?

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-1bTechnology Risks

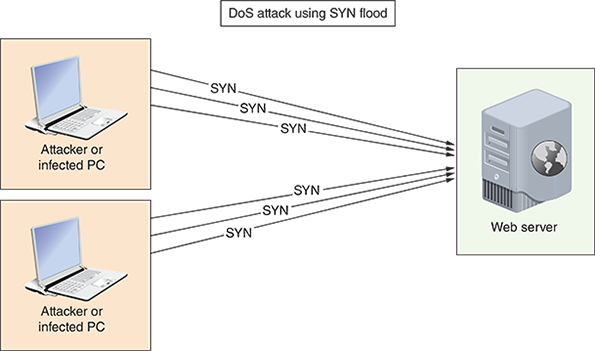


This section describes security risks inherent in all seven layers of the OSI model. Attacks on transmission media, NICs, network access methods (for example, Ethernet), switches, routers, access points, and gateways require more technical sophistication than those that take advantage of human errors. For instance, to eavesdrop on transmissions passing through a switch, an intruder must use a device such as a protocol analyzer (like Wireshark) connected to one of the switch’s ports. Because a router connects one type of network to another, an intruder might take advantage of the router’s security flaws by sending a flood of TCP/IP transmissions to the router, thereby disabling it from carrying legitimate traffic.

A [**DoS (denial-of-service) attack**](javascript://) occurs when legitimate users are unable to access normal network resources, such as a web server, because of an attacker’s intervention. Most often, this type of attack is achieved by flooding a system with so many requests for services that it can’t respond to any of them, as shown in [Figure 10-7](javascript://). As a result, all data transmissions are disrupted.

**Figure 10-7**

A simple DoS attack flooding a web server with SYN requests



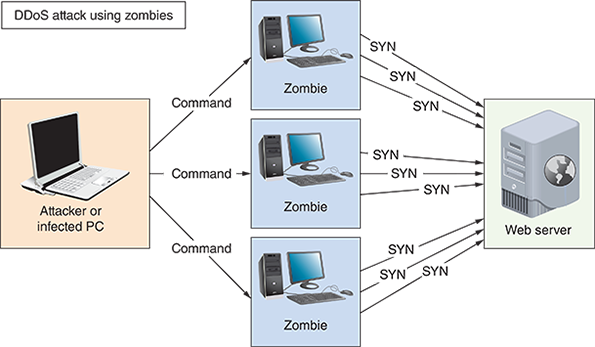
Enlarge Image

This incursion is a relatively simple attack to launch (for example, a hacker could create a looping program that sends thousands of email messages to your system per minute). DoS attacks can also result from malfunctioning software. Because DoS attacks are so common, let’s look at several DoS subtypes:

* [**DDoS (distributed DoS) attack**](javascript://)—Whereas a DoS attack comes from one or a few sources owned by the attacker, DDoS attacks are orchestrated through many sources, as shown in [Figure 10-8](javascript://). Most of these machines are zombies, which means the owners are unaware that their computers are being used in the coordinated attack. A type of malware called a bot is installed on each machine and gives the bot herder, or central controller, remote control of the computer. Many people believe their computers are not at high risk of security compromise if they don’t keep valuable information on the computer. They don’t realize their computing resources are also a target. Computers can be requisitioned as part of a botnet, also called a zombie army, in coordinated DDoS attacks without the owners’ knowledge or consent. These botnets are sometimes made available for hire on the black market. The traffic spike caused by so many attackers is much more difficult to defend against than an attack from a single source. Effective firewalls can greatly reduce the chances of a computer being drafted into illegal botnets.

**Figure 10-8**

A SYN flood coordinated through several malware-infected, zombie computers

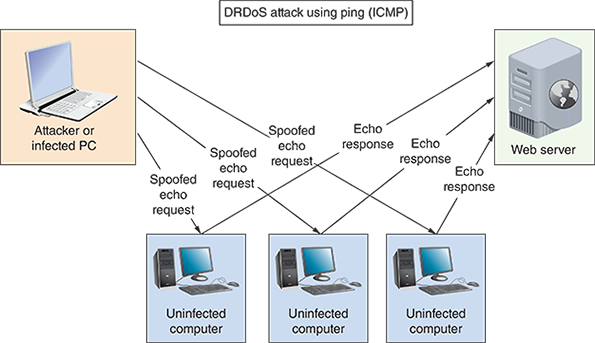


Enlarge Image

* **DRDoS (distributed reflection DoS) attack**—A DRDoS attack is a type of DDoS attack that is bounced off uninfected computers, called reflectors, before being directed at the target. This is achieved by spoofing the source IP address in the attack to make it look like all the requests for response are being sent by the target. As a result, all the reflectors send their responses to the target, thereby flooding the target with traffic, as shown in [Figure 10-9](javascript://).

**Figure 10-9**

Spoofed ICMP echo requests appear to come from the victim computer

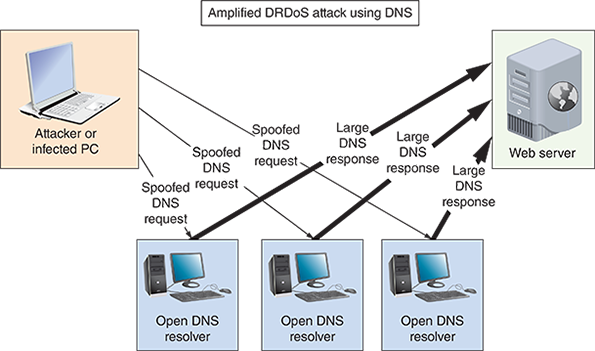


Enlarge Image

* **Amplified DRDoS attack**—A DRDoS attack can be amplified when conducted using small, simple requests that trigger very large responses from the target, as shown in [Figure 10-10](javascript://). Several protocols lend themselves to being used in these kinds of attacks, including DNS, NTP, ICMP, SNMP, and LDAP.

**Figure 10-10**

Spoofed DNS requests prompt large responses sent to the victim



Enlarge Image

* **PDoS (permanent DoS) attack**—A PDoS attack damages a device’s firmware beyond repair. This is called “bricking” the device because it effectively turns the device into a brick. PDoS attacks usually target routers or switches.
* **Friendly DoS attack**—An unintentional DoS attack, or friendly attack, is not done with malicious intent. An example might be when a website is flooded with an unexpectedly high amount of shopping traffic during a flash sale, or when a significant event is reported on the news and people flood to certain, related websites, especially if a specific website was mentioned in news reports.

Other technology risks are related to weaknesses of wireless transmissions, authentication vulnerabilities, lack of encryption, or flaws in software design. Consider the following types of attacks and vulnerabilities:

* [**On-path attack**](javascript://)—An on-path attack, previously called a MitM (man-in-the-middle) attack, relies on intercepted transmissions and can take several forms. In all these forms, the attacker redirects and captures secure transmissions as they occur. For example, in the case of an evil twin attack (a type of on-path attack), a hacker could intercept transmissions between clients and a rogue access point. Through these captured transmissions, the attacker can learn users’ passwords or even supply users with a phony website that looks valid but presents clickable options capable of harming their systems.
* [**Deauth (deauthentication) attack**](javascript://)—When a Wi-Fi client is legitimately connected to a wireless access point, the AP or the client can send a deauthentication frame to tell the other device that the authentication session is being terminated. A valid deauth frame could come from the wireless client or AP for any number of legitimate reasons, including inactivity, the client is leaving the area, the AP is overwhelmed with too many clients, or an unspecified reason. These frames are unencrypted and are easily spoofed. In a deauth (deauthentication) attack, the attacker sends faked deauthentication frames to the AP, the client, or both (or as a broadcast to the whole wireless network) to trigger the deauthentication process and knock one or more clients off the wireless network. This is essentially a Wi-Fi DoS attack in that valid users are prevented from having normal access to the network. At minimum, it can be a frustrating experience for users. In the hands of a skilled attacker, further information can be collected for more destructive attacks, such as an on-path attack.
* **Insecure protocols and services**—Certain TCP/IP protocols are inherently insecure. For example, IP addresses can be falsified, checksums can be thwarted, UDP requires no authentication, and TCP requires only weak authentication. FTP is notorious for its vulnerabilities. In a well-known exploit called [**FTP bounce**](javascript://), hackers take advantage of this insecure protocol. When a client running an FTP utility requests data from an FTP server, the client normally specifies its own IP address and FTP’s default port number. However, it is possible for the client to specify any port on any host’s IP address. By commanding the FTP server to connect to a different computer, a hacker can scan the ports on other hosts and transmit malicious code. To thwart FTP bounce attacks, most modern FTP servers will not issue data to hosts other than the client that originated the request. Other insecure protocols include HTTP (use HTTPS with SSL/TLS instead), Telnet (use along with IPsec), SNMPv1, and SNMPv2 (use SNMPv3 instead). You’ll learn more about SNMP later in this course.
* [**DNS poisoning**](javascript://) **or DNS spoofing**—By altering DNS records on a DNS server, an attacker can redirect Internet traffic from a legitimate web server to a phishing website, which is called DNS poisoning or DNS spoofing. Because of the way DNS servers share their cached entries, poisoned DNS records can spread rapidly to other DNS servers, ISPs, home and business networks, and individual computers. In fact, intentional DNS spoofing is one way China maintains its so-called “Great Firewall,” which blocks its citizens from accessing websites such as YouTube, Pinterest, and Facebook. However, in 2010, China’s DNS records somehow leaked into neighboring countries’ DNS root servers. The altered DNS records started spreading around the world, blocking Internet traffic in other countries from accessing popular websites and redirecting that traffic to Chinese servers.
* **Back doors**—Software might contain back doors, which are security flaws that allow unauthorized users to gain access to the system. Unless the network administrator performs regular updates, a hacker might exploit these flaws. Legacy systems are particularly notorious for leaving these kinds of gaps in a network’s overall security net.

Go to pg.

[**help**](javascript://)

Application Opened

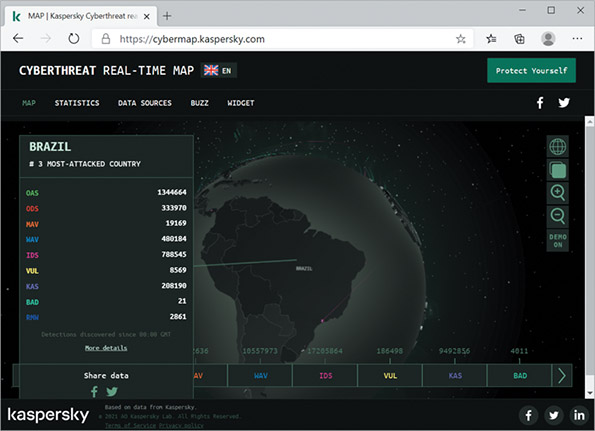
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-1cMalware Risks

[**Malware (malicious software)**](javascript://) refers to any program or piece of code designed to intrude upon or harm a system or its resources. Included in this category are viruses, Trojan horses, worms, bots, and ransomware. You can find lists and maps online of recent outbreaks of malware, intrusions, and attacks. [Figure 10-11](javascript://) shows Kaspersky’s interactive world map ([cybermap.kaspersky.com/](http://cybermap.kaspersky.com/" \t "_blank)) where you can explore attack statistics by country based on data gathered by Kasperky’s security tools. [Figure 10-12](javascript://) shows where further statistics analysis is available to compare countries and detection types.

**Figure 10-11**

Security professionals track the emergence of new threats

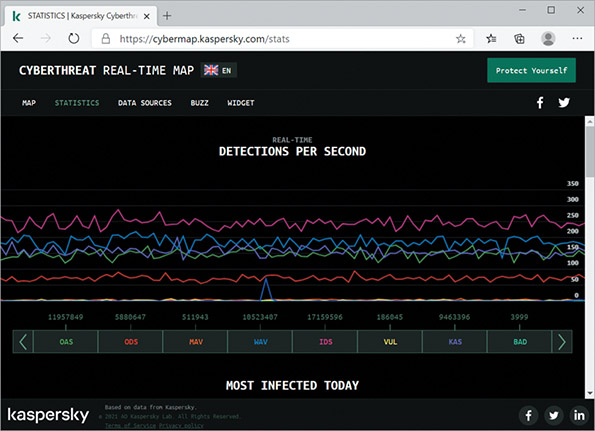


Enlarge Image

Source: AO Kaspersky Lab

**Figure 10-12**

Cyberattack statistics grouped by detection type



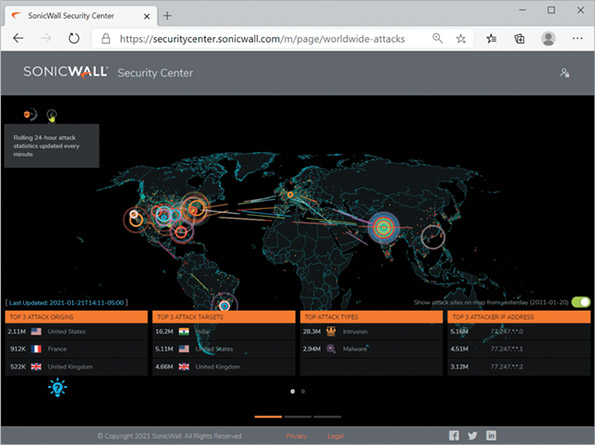
Enlarge Image

Source: AO Kaspersky Lab

Other companies provide similar maps and reporting dashboards. For example, [Figure 10-13](javascript://) shows a map and statistics streamed by SonicWall ([securitycenter.sonicwall.com/m/page/worldwide-attacks](http://securitycenter.sonicwall.com/m/page/worldwide-attacks" \t "_blank)). Digging deeper, you can find additional statistics and threat metrics on the SonicWall site (see [Figure 10-14](javascript://)). Notice the breakdown of attack types, including malware, ransomware, spam volume, cryptojacking, and IoT malware. Statistics on this site report that IoT malware has risen by more than 350 percent over the previous year with a particularly noticeable spike in October of 2019.

**Figure 10-13**

World map showing top three attack origins and top three attack targets according to SonicWall data

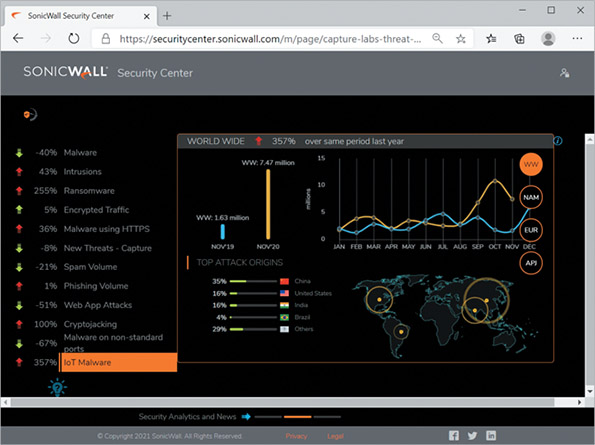


Enlarge Image

Source: SonicWall

**Figure 10-14**

Statistics showing change in attack volumes over time



Enlarge Image

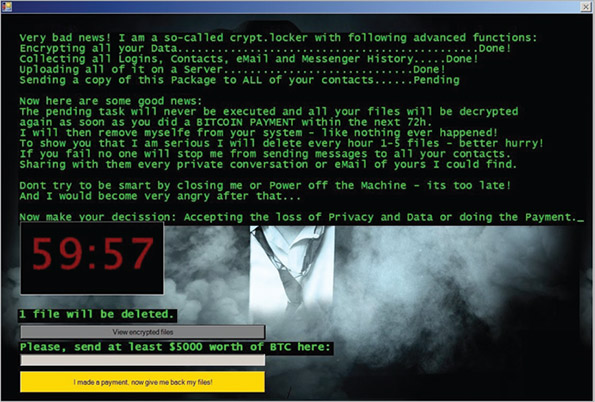
Source: SonicWall

These cyberattack maps break down statistics according to attack types, such as malware, spam, phishing, and more. Malware is a generalized term that refers to many kinds of malicious software, as described in the following list:

* **Virus**—A program that replicates itself with the intent to infect more computers, either through network connections when it piggybacks on other files or through the exchange of external storage devices. A virus might damage files or systems, or it might simply annoy users by, for example, flashing messages or pictures on the screen.
* **Trojan horse (or Trojan)**—A program that disguises itself as something useful but actually harms your system; named after the famous wooden horse in which soldiers were hidden. Because Trojan horses do not replicate themselves, they are not considered viruses. An example of a Trojan horse is an executable file that someone sends you over the Internet, promising that the executable will install a great new game, when in fact it erases data on your hard disk or mails spam to all the users in your email app’s address book.
* **Worm**—A program that runs independently of other software and travels between computers and across networks. They may be transmitted by any type of file transfer, including email attachments. Worms do not alter other programs in the same way that viruses do, but they can carry viruses. Because they can transport and hide viruses, you should be concerned about picking up worms when you exchange files on the Internet, via email, or on flash drives.
* **Bot** (short for robot)—A process that runs automatically, without requiring a person to start or stop it. Bots can be beneficial or malicious. Especially when used for ill intent, it does not require user interaction to run or propagate itself. Instead, it connects to a central server called a [**C&C (command-and-control) server**](javascript://), which then commands an entire [**botnet**](javascript://) of similarly infected devices. Bots can be used to damage or destroy a computer’s data or system files, issue objectionable content, launch DoS attacks, or open back doors for further infestation. Bots are especially difficult to contain because of their fast, surreptitious, and distributed dissemination.
* [**Ransomware**](javascript://)—A program that locks a user’s data or computer system until a ransom is paid. In most cases, the infection encrypts data on the computer and can also encrypt data on backup devices, removable storage devices, and even cloud storage accounts connected to the computer, such as Dropbox or OneDrive. The victim receives a message, such as the one shown in [Figure 10-15](javascript://), with the demand for payment and instructions on how to make the payment, usually through untraceable online payment systems. The amount of ransom varies, and for large organizations, has reached well into the millions of dollars. To add a sense of urgency, some ransomware starts deleting data at certain time increments, showing a countdown clock to the next scheduled deletion. Even if victims pay the ransom, they don’t always get their data back. Currently, the only mostly reliable defense is to make manual backups of data on a regular basis and disconnect the backup media from the computer between backups. However, some ransomware threatens to send the user’s files to email contacts stored on the computer or to post stolen data online. Researchers are finding that ransomware victims are increasingly paying the ransom in exchange for keeping their data private, even if they have sufficient backups in place.

**Figure 10-15**

This version of the Jigsaw ransomware threatens to send all the user’s data to all contacts collected from the computer



Enlarge Image

Source: New Jersey Cybersecurity & Communications Integration Cell

Certain characteristics can make malware harder to detect and eliminate. Some of these characteristics, which can be found in any type of malware, include the following:

* **Encryption**—Some malware is encrypted to prevent detection. Most anti-malware software searches files for a recognizable string of characters that identifies the virus. However, encryption can thwart the anti-malware program’s attempts to detect it.
* **Stealth**—Some malware disguises itself as legitimate programs or replaces part of a legitimate program’s code with destructive code.
* **Polymorphism**—Polymorphic malware changes its characteristics (such as the arrangement of bytes, size, and internal instructions) every time it’s transferred to a new system, making it harder to identify.
* **Time dependence**—Some malware is programmed to activate on a particular date. This type of malware can remain dormant and harmless until its activation date arrives. One example of time-dependent malware is a [**logic bomb**](javascript://), which is code (or a bug in code) that will start when certain conditions are met. (Logic bombs can also activate when other types of conditions, such as a specific change to a file, are met, and they are not always malicious.)

Malware can exhibit more than one of the preceding characteristics. The Natas virus, for example, combines polymorphism and stealth techniques to create a very destructive virus. Hundreds of new viruses, worms, Trojan horses, bots, and ransomware are unleashed on the world’s computers each month. Although it is impossible to keep abreast of every virus in circulation, you should at least know where you can find out more information about malware. An excellent resource for learning about new malware, their characteristics, and ways to get rid of them is the McAfee Threat Center at [mcafee.com/enterprise/en-us/threat-center.html](http://mcafee.com/enterprise/en-us/threat-center.html" \t "_blank).

**Remember This…**

* Compare internal versus external threats.
* Explain the CVE and zero-day attacks.
* Compare technology-based attacks, including DoS, DDoS, botnets, on-path attacks, ransomware, deathentication, and malware.
* Compare human and environmental attacks, including phishing, tailgating, piggybacking, and shoulder surfing.
* Discuss strategies for employee training.

**Self-Check**

1. The ability to insert code into a database field labeled “Name” is an example of a(n) \_\_\_\_\_\_\_\_\_.

Answer

* 1. attack.
  2. vulnerability.
  3. breach.
  4. exploit.

1. Which of the following social engineering attack types most likely requires that the attacker have existing knowledge about the victim?

Answer

* 1. Tailgating
  2. Shoulder surfing
  3. Piggybacking
  4. Phishing

1. You’re playing a game on your Xbox when you suddenly get bumped off your Wi-Fi network. You reconnect and start playing, then get bumped off again. What type of attack is most likely the cause?

Answer

* 1. On-path attack
  2. FTP bounce
  3. Deauth attack
  4. DDoS

**You’re Ready**

You’re now ready to complete [Project 10-1: Play with Windows Sandbox](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 10-2Risk Assessment and Management

### Certification

* 3.2

Explain the purpose of organization documents and policies.

* 4.1

Explain common security concepts.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

Average reading time: 17 minutes

Before spending time and money changing your network security, first identify and examine your network’s current security risks. Consider the effect that a loss or breach of data, applications, or access would have on your network. The more serious the potential consequences, the more attention you need to pay to security. To accurately evaluate your risk and vulnerabilities, you’ll need to conduct several security assessments.

Effective risk management happens at two layers, as follows:

* A [**security risk assessment**](javascript://) evaluates threats to and vulnerabilities of the network.
* A [**business risk assessment**](javascript://) evaluates the impact of potential threats on business processes.

To determine these risks to the business, you must first have a good understanding of the various processes the business relies on. A [**business process**](javascript://) is a series of steps that accomplishes a defined goal. For example, the series of steps involved in receiving an order from a customer, delivering a product or service, and billing the customer is an operations business process. The steps needed to assemble a product is a manufacturing business process. Business professionals use techniques to identify, define, evaluate, and analyze these various business processes. From the IT perspective, then, a [**process assessment**](javascript://) ensures that you and others responsible for network security understand your company’s business processes, which will help you minimize the impact of security threats on those processes.

Similarly, a [**vendor risk assessment**](javascript://) (also called a third-party risk assessment) evaluates security and compliance risks related to suppliers and vendors a company does business with. Not all security threats are directly implemented against your own company—sometimes, the attack is routed through a business partner of some kind. During a vendor risk assessment, you’ll need to get the answers to several important questions: Is the vendor trustworthy? Are they financially stable? Do they maintain compliance standards? Is their IT security reliable? These and many other questions should be explored and answered before beginning a formal relationship with a vendor and periodically (perhaps annually) during the relationship. This assessment might require the cooperation of people from many departments to cover all vendors. For example, a compromised HVAC vendor could result in a network-wide data breach. It’s critical to evaluate all possible avenues of compromise to your network, considering not just technical vulnerabilities but also security gaps caused by business processes and relationships.

Every organization should assess its network’s security risks by conducting a [**posture assessment**](javascript://), which is a thorough examination of each aspect of the network to determine how it might be compromised. One component of a posture assessment might include a [**threat assessment**](javascript://), which identifies specific security threats to the network and related risk factors. A threat’s consequences might be severe, potentially resulting in a network outage or the dispersal of top-secret information, or it might be mild, potentially resulting in a lack of access for one user or the dispersal of a relatively insignificant piece of corporate data. The more devastating a threat’s effects and the more likely it is to happen, the more rigorously your security measures should address it. An assessment process might include the following steps:

1. 1

Identify threats and risk factors.

1. 2

Determine which resources (people, equipment, data, etc.) might be harmed by each threat.

1. 3

Develop plans for responding to threats if they occur and, in the meantime, for reducing identified risks.

1. 4

Document findings and next steps.

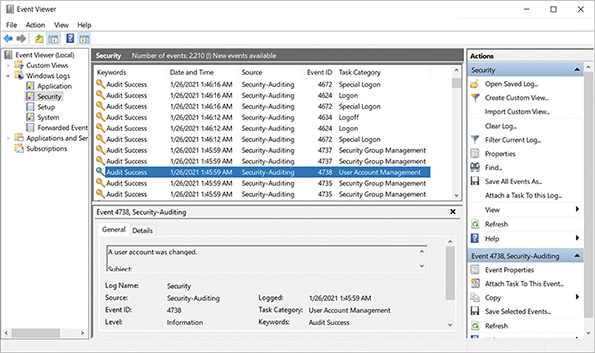
Posture assessments should be performed at least annually and preferably quarterly. They should also be performed after making any significant changes to the network. If your IT Department has sufficient skills and time for routine posture assessments, they can be performed in-house. A qualified consulting company can also assess the security of your network. If the company is accredited by an agency that sets network security standards, the assessment qualifies as a [**security audit**](javascript://), also called an IT audit.

Certain customers—for example, a military agency—might require your company to pass an accredited security audit before they’ll do business with you. Regulators require some types of companies, such as accounting firms, to host periodic security audits. But even if an audit is optional, the advantage of having an objective third party analyze your network is that they might find risks you overlooked because of your familiarity with your environment. Security audits might seem expensive, but if your network hosts confidential and critical data, they are well worth the cost. Beyond meeting requirements imposed by business partners, an audit and assessment report can help you deeply evaluate your organization’s security posture and close vulnerabilities.

In addition, you can set auditing policies on your network’s devices and servers to constantly monitor activities that might need attention. For example, [Figure 10-16](javascript://) shows Event Viewer in Windows Server, which logs security events such as changing user accounts. You’ll learn more about log management later in this course.

**Figure 10-16**

Audit logs in Event Viewer



Enlarge Image

In this section of the module, you’ll first learn about attack simulations and various scanning tools used for posture assessments and security audits. Then you’ll see how you can bait hackers so you can learn more about their activities.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-2aAttack Simulations

To ensure that your security efforts are thorough, it helps to think like a hacker. During a posture assessment, for example, you might use some of the same methods a hacker uses to identify cracks in your security architecture. In fact, security experts often conduct simulated attacks on a network to determine its weaknesses. Let’s look at three types of attack simulations.

### Vulnerability Assessment

A [**vulnerability assessment**](javascript://) is used to identify vulnerabilities in a network. It’s often performed by a company’s own employees and does not attempt to exploit any vulnerabilities. A vulnerability assessment might also be the first step in other attack simulations or in a real attack. During attack simulations, there are two types of vulnerability assessments:

* **Authenticated**—In this case, the attacker is given the same access to the network as a trusted user would have, such as an employee or an intruder who has somehow hacked into a user’s account.
* **Unauthenticated**—In this case, the attacker begins on the perimeter of the network, looking for vulnerabilities that do not require trusted user privileges.

### Penetration Testing

[**Pen (penetration) testing**](javascript://) takes advantage of ethical hacking techniques to identify weaknesses and the extent of those weaknesses. This attack simulation begins with a vulnerability assessment using various tools and then attempts to exploit those vulnerabilities. A penetration test might be something as simple as a network admin clicking around through the network to see what vulnerabilities surface, such as discovering that the default credentials for a networked HVAC system were never changed. Or it might consist of a much more robust process, relying on a professional pen testing organization to conduct a thorough examination of the company’s network and resulting in a lengthy report recommending important, critical, and urgent changes to make to the network.

You’ve already used or read about many pen testing tools, including Wireshark and Nmap. Other pen testing tools might include the following:

* SimplyEmail to gather information posted online related to an email address
* Hashcat or John the Ripper to crack passwords
* Aircrack-ng to monitor and manipulate wireless transmissions
* Metasploit for vulnerability scanning
* PowerShell scripts to perform multiple tasks at a time

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-2bRed Team–Blue Team Exercise

During a [**red team–blue team exercise**](javascript://), the red team conducts the attack, and the blue team attempts to defend the network, as illustrated in [Figure 10-17](javascript://). Usually, the red team is a hired attacker, such as a consultant or security organization, and the blue team is the company’s own IT, security, and other staff. In some cases, the blue team has no warning of the impending attack to better evaluate day-to-day defenses. The red team relies heavily on social engineering to attempt to access the company’s private data, accounts, or systems without getting caught. In this case, the company’s detection and response to the attack is the primary focus, rather than the technical vulnerabilities of the network itself.

**Figure 10-17**

Working against each other, the red team and the blue team collaboratively improve the organization’s security posture

A picture containing text

Description automatically generated

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-2cScanning Tools

Scanning tools provide hackers—and you—with a simple and reliable way to discover crucial information about your network, including but not limited to the following:

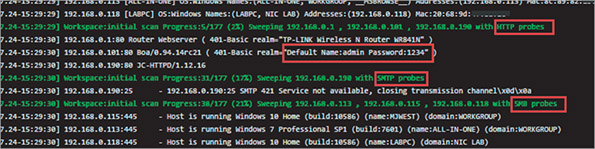
* Every available host
* Each host’s running services and software, including operating systems, applications, and their versions
* Software configurations
* Open, closed, and filtered ports on every host
* Existence, type, placement, and configuration of firewalls
* Unencrypted or poorly encrypted sensitive data

Used intentionally on your own network, scanning tools improve security by pointing out insecure ports, software and firmware that must be patched, permissions that should be restricted, and so on. They can also contribute valuable data to asset management and audit reports. Let’s look at three popular scanning tools you can use:

* **Nmap**—The scanning tool Nmap and its GUI version, Zenmap, are designed to scan large networks quickly and provide information about a network and its hosts. (You used both of these in an earlier module.) Nmap began as a simple [**port scanner**](javascript://), which is an application that searches a device for open ports indicating which insecure service might be used to craft an attack. For example, if a server’s port 23 is open, Telnet can be used to remote into the target device and take control of it. Developers later expanded Nmap’s capabilities to include gathering information about hosts and their software. When running Nmap, you can choose what type of information to discover, thereby customizing your scan results. In a project at the end of this module, you’ll use another app, Advanced Port Scanner, to find open protocol ports on your network.
* **Nessus**—Developed by Tenable Security ([tenable.com](http://tenable.com/" \t "_blank)), Nessus performs even more sophisticated vulnerability scans than Nmap. Among other things, Nessus can identify unencrypted, sensitive data (such as credit card numbers) saved on your network’s hosts. The program can run on your network or from off-site servers continuously maintained and updated by the developer.
* **Metasploit**—This popular penetration testing tool combines known scanning and exploit techniques to explore potentially new attack routes. For example, [Figure 10-18](javascript://) shows a Metasploit scan using HTTP, SMTP, and SMB probes; the application also employs Nmap, Telnet, FTP, and UDP probes. Notice that the scan successfully identified the administrative username and password transmitted in plaintext for this home network’s SOHO router. You can download an open source version of the Metasploit framework from their website at [metasploit.com](http://metasploit.com/" \t "_blank).

**Figure 10-18**

Metasploit detected a SOHO router’s administrative username and password



Enlarge Image

Source: Rapid7 LLC

As you can see, these tools can provide useful insights into your network’s weaknesses that need attention. Used by hackers—or more likely, by bots—these tools can instead lead to compromised security. In other words, each of these tools can be used for legitimate purposes as well as illegal ones. However, even if the scanning tools are used against you, you can learn from them. For example, a properly configured firewall will collect information about scanning attempts in its log. By reviewing the log, you will discover what kinds of exploits could be—or have been—attempted against your network. Therefore, another way to learn about hackers is to lure them to your network on purpose, as described next.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-2dHoneypots and Honeynets

Staying a step ahead of hackers and constantly evolving exploits requires vigilance. Those who want to learn more about hacking techniques or nab a hacker in the act might create a [**honeypot**](javascript://), which is a decoy system that is purposely vulnerable and filled with what appears to be sensitive (though false) content, such as financial data. To lure hackers, the system might be given an enticing name, for example, one that indicates a DNS name server or a storage location for confidential data. Once hackers access the honeypot, a network administrator can use monitoring software and logs to track the intruder’s moves. In this way, the network administrator might learn about new vulnerabilities that must be addressed on real networked hosts.

To fool hackers and gain useful information, honeypots should not appear too blatantly insecure, and tracking mechanisms must be well hidden. Hackers know honeypots exist and are often skilled at detecting them. In addition, a honeypot must be isolated from secure systems to prevent a savvy hacker from using it as an intermediate host for other attacks. In more elaborate setups, several honeypots might be connected to form a [**honeynet**](javascript://). Honeypot software options include KFSensor ([keyfocus.net](http://keyfocus.net/" \t "_blank)), Thinkst Canary ([canary.tools](http://canary.tools/" \t "_blank)), and Honeyd ([honeyd.org](http://honeyd.org/" \t "_blank)).

Honeypots and honeynets can provide unique information about hacking behavior and, if configured well, are low maintenance sources of information with few false positives. But in practice, security researchers or those merely curious about hacking trends are more likely than overworked network administrators to establish and monitor these decoy systems.

Now that you understand the variety of risks facing networks and several ways of identifying these risks on a specific network, you’re ready to learn about techniques for securing the network’s physical devices, beginning with physical security.

**Remember This…**

* Explain common assessment types, including business risk assessments (process assessment and vendor risk assessment), and security risk assessments (posture assessment and threat assessment).
* Compare common attack simulations, including vulnerability assessment, penetration testing, and red team–blue team exercises.
* Use a port scanner.

**Self-Check**

1. What is the first step in improving network security?

Answer

* 1. Document next steps.
  2. Identify risks.
  3. Determine which resources might be harmed.
  4. Develop plans for responding to threats.

1. Which assessment type would most likely discover a security risk related to employee on-boarding?

Answer

* 1. Vendor risk assessment
  2. Process assessment
  3. Threat assessment
  4. Posture assessment

1. Which team might ask a user for a password?

Answer

* 1. Red team
  2. Blue team

**You’re Ready**

You’re now ready to complete [Project 10-2: Scan a Network with Advanced Port Scanner](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 10-3Physical Security

### Certification

* 2.1

Compare and contrast various devices, their features, and their appropriate placement on the network.

* 4.5

Explain the importance of physical security.

Average reading time: 13 minutes

Physical access to a network’s critical components must be restricted and controlled. Consider the damage that could be done if an intruder were able to steal devices, directly connect their own computer to unprotected console ports, damage or destroy expensive equipment, or simply reset these devices by pressing the physical reset button. Only trusted networking staff should have access to secure computer rooms, data rooms, network closets, storage rooms, entrance facilities, and locked equipment cabinets. Furthermore, only authorized staff should have access to the premises, such as offices and data centers, where these rooms are located.

Preventative measures such as locked doors can make it more difficult for unauthorized people to get into these areas. However, it’s also important to have good detection measures in place for those times when someone is able to breach a secured perimeter. Let’s look at physical security methods you can use for both prevention and detection.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-3aPrevention Methods

If computer rooms are not locked, intruders may steal equipment or sabotage software or hardware. For example, a malicious visitor could slip into an unsecured computer room and take control of a server where an administrator is logged on, then steal data or reformat the server’s hard drive. Although a security policy defines who has access to the computer room, locking the locations that house networking equipment is necessary to keep unauthorized individuals out. Physical access control devices can minimize unauthorized access to secured areas and devices. Access control hardware ranges from a simple deadbolt to more sophisticated options and can manage access to buildings, rooms, or storage spaces. Consider the following access control technologies:

* **Keypad, or cipher lock**—Requires the entry of a code to open the door, which can reduce the inherent risk of lost keys. Changing the cipher lock’s code regularly can also help increase security. Cipher locks are not designed solely for physical security, such as on an outside door, so much as for the purpose of controlling access to an area, such as an indoor data room. The cipher lock can be used to log who comes and goes, enable or disable unescorted entry, schedule open access times, and even respond to access made under duress (with a special hostage code that trips an alarm when entered). [Figure 10-19](javascript://) shows one example of a cipher lock.

**Figure 10-19**

A cipher lock can document who enters an area and when



[iStock.com/richterfoto](http://istock.com/richterfoto" \t "_blank)

* [**Access badge**](javascript://)—Identifies the person by name and perhaps includes a photo, title, and other information. Additionally, many organizations provide electronic access badges, or [**smart cards**](javascript://). When the smart card is swiped through a [**badge reader**](javascript://), the door unlocks and the person’s access to the secured area is time stamped and logged in a database. These badges can be programmed to allow their owner access to some, but not all, rooms in a building. Some badges, such as the one in [Figure 10-20](javascript://), are proximity cards (also called prox cards), which do not require direct contact with a proximity reader to be detected. In fact, the reader can be concealed inside a wall or other enclosure and requires very little maintenance. With a typical range of about 5–10 cm, the card can be detected even while it’s inside a wallet or purse. [Figure 10-21](javascript://) depicts a typical badge access security system.

**Figure 10-20**

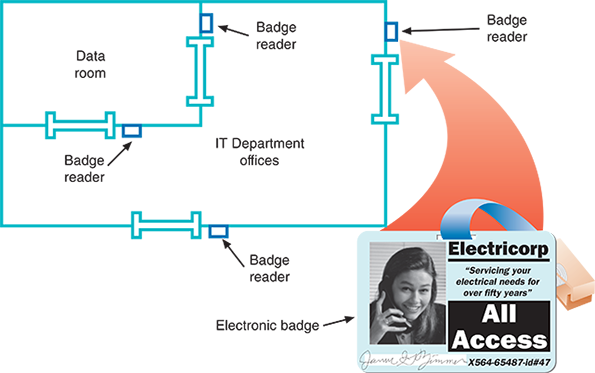
A proximity card does not require physical contact with a proximity reader



gifted/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

**Figure 10-21**

Badge access security system



Enlarge Image

* [**Biometrics**](javascript://)—Involves biorecognition access in which a device scans an individual’s unique physical characteristics (called biometrics) such as iris color patterns or hand geometry to verify the person’s identity. Organizations might use biometric devices to regulate entrance through gates or other physical barriers to their campuses. See [Figure 10-22](javascript://).

**Figure 10-22**

Fingerprint scanner



[iStock.com/tongo51](http://istock.com/tongo51" \t "_blank)

* [**Access control vestibule**](javascript://)—Previously known as a mantrap, creates a confined space between two locking doors where one door must lock closed before the other can open.
* [**Locking rack**](javascript://) and [**locking cabinet**](javascript://)—Provides a final layer of physical defense should an attacker gain access to a data room or some other controlled space. Locking racks restrict physical access to servers, routers, switches, and firewalls installed on the rack to prevent an intruder from making configuration changes to these devices. Locking cabinets might be used to store hardware not in use, such as spare devices, radio equipment, or tools.
* [**Smart locker**](javascript://)—Allows controlled access to equipment, computers, packages, hardware in need of repair, or even to written account credentials stored for emergency access. To open a locker, the user must provide more sophisticated authentication, such as a barcode on their phone, so specific users are logged as having accessed the locker and when. This way, equipment can be checked out for temporary use and only by specific people. The smart locker can also generate an alert if equipment is not returned by a specific time. Temporary credentials can be issued as needed, such as for packages arriving at a public smart locker. In [Figure 10-23](javascript://), this Amazon Hub Locker on a college campus allows students to receive Amazon packages without needing to visit the mail center, thus saving time for students and employees. When a package arrives, the student receives an email on their smartphone with a bar code. As shown in [Figure 10-24](javascript://), the bar code is scanned at the locker’s authentication panel to open the appropriate slot containing the student’s package.

**Figure 10-23**

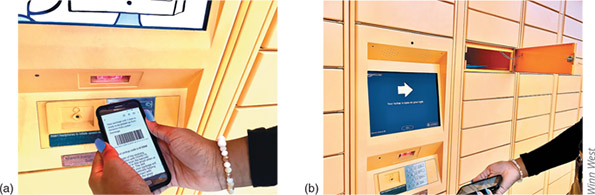
Amazon Locker on a college campus



Winn West

**Figure 10-24**

Scan the barcode from an email to access the package



Enlarge Image

Winn West

### Caution

A door might not be the only way to enter a room containing sensitive equipment. Drop ceilings, also called suspended ceilings, can provide easy access to someone determined to get around a locked door. Secured rooms should be completely surrounded by impenetrable walls, ceilings, and floors. If a data room does have a drop ceiling, make sure the walls extend all the way up to the true ceiling beyond the drop ceiling grid.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-3bDetection Methods

Despite all precautions, sometimes breaches do occur. The key to protecting sensitive data and systems is to detect intrusions as quickly as possible and be prepared to respond appropriately. Beyond detecting the presence of an intruder, however, security detection technologies can detect other types of events as well. For example, the temperature of vaccines in transit, the movement of delivery and transportation vehicles, and the expiration of food items can all be monitored for the safety and security of the people who use these items. The following list explores some methods of detecting physical intrusions and other kinds of events:

* [**Motion detection**](javascript://)—Triggers an alarm when it detects movement within its field of view. Sensors like the one in [Figure 10-25](javascript://) are often found in home security systems. To reduce false alarms, AI-powered motion detectors can discern between different types of movement, such as small animals passing by, plants or trees blowing in the wind, or humans approaching a door. Motion sensors might be configured to simply record the date and time of motion detection or to trigger lights, alarms, or video cameras.

**Figure 10-25**

Motion detectors trigger an alarm when movement is detected



[iStock.com/MileA](http://istock.com/MileA" \t "_blank)

* **Cameras**—Placed in data centers, computer rooms, data rooms, and data storage areas, as well as facility entrances. The camera feeds are centrally managed through a video surveillance system, called [**CCTV (closed-circuit TV)**](javascript://), to monitor activity in these secure areas (see [Figure 10-26](javascript://)). Security cameras might run continuously, or they might be equipped with motion detectors to start recording when movement occurs within their viewing area.

**Figure 10-26**

Security professionals monitor CCTV cameras



Africa Studio/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

IT technicians might be called upon to install and service a video surveillance system for the entire company (see [Figure 10-27](javascript://)). The video footage generated from these cameras is contained within a secure segment of the network, and it’s usually saved for a period of time in case it’s needed later in a security breach investigation or prosecution procedures.

**Figure 10-27**

IT personnel might be responsible for the installation and maintenance of a CCTV network



APChanel/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

* [**Tamper detection**](javascript://)—Identifies physical penetration, temperature extremes, input voltage variations, input frequency variations, or certain kinds of radiation. Many devices that need protection can’t be kept within a secure area. For example, utility meters, parking meters, entry doors, ATMs, network cables, and even security cameras are potential targets. Tamper detection sensors might trigger defensive measures such as an alarm or shutdown, or it might activate a video camera or other security system. Another tamper detection option is a sticker or latch, as shown in [Figure 10-28](javascript://). Any damage to the sticker or latch tells you the device was tampered with.

**Figure 10-28**

A single-use, plastic security seal



[iStock.com/Maudib](http://istock.com/Maudib" \t "_blank)

* [**Asset tags**](javascript://)—Monitor the movement and condition of equipment, inventory, and people. Whether a simple barcode or a wireless-enabled transmitter, such as the RFID label on the box in [Figure 10-29](javascript://), asset tracking enables constant or periodic collection of information. This data is then reported to a central management application for monitoring, logging, and reporting. As wireless technologies have improved, these asset tracking systems have grown beyond Wi-Fi-dependent systems, which tend to be expensive and require frequent battery replacement for each asset being tracked. Today, these systems often use Bluetooth, RFID (such as NFC), cellular, and GPS wireless technologies. These technologies are sometimes combined with cloud technology to provide deeper insights through data analytics and with IoT technology to increase the security of IoT networks.

**Figure 10-29**

The RFID label on this box allows the delivery service to track its progress



[iStock.com/nullplus](http://istock.com/nullplus" \t "_blank)

As with other security measures, the most important way to ensure physical security is to plan for it. You can begin your planning by asking questions related to physical security checks in your security audit. Consider the following questions:

* Which rooms contain critical systems or data and must be secured?
* Through what means might intruders gain access to the facility, computer room, data room, network closet, or data storage areas (including doors, windows, adjacent rooms, ceilings, large vents, temporary walls, hallways, and so on)?
* How and to what extent are authorized personnel granted entry? Do they undergo background or reference checks? Is their need for access clearly justified? Can their hours of access be restricted? Who ensures that lost keys or ID badges are reported?
* Are employees instructed on how to ensure security as they enter or leave secured areas (for example, by not propping open doors)?
* Are authentication methods (such as ID badges) difficult to forge or circumvent?
* Do supervisors or security personnel make periodic physical security checks?
* Are all combinations, codes, or other access means to computer facilities protected at all times, and are these combinations changed frequently?
* What is the plan for documenting and responding to physical security breaches?

**Remember This…**

* Explain common detection methods, including cameras, motion detection, asset tags, and tamper detection.
* Explain common prevention methods, including badge readers, biometrics, locking racks, locking cabinets, access control vestibule, and smart lockers.

**Self-Check**

1. Which physical security device works through wireless transmission?

Answer

* 1. Badge reader
  2. Access control vestibule
  3. Cipher lock
  4. Biometrics

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 10-4Device Hardening

### Certification

* 3.2

Explain the purpose of organization documents and policies.

* 4.1

Explain common security concepts.

* 4.3

Given a scenario, apply network hardening techniques.

* 4.5

Explain the importance of physical security.

* 5.5

Given a scenario, troubleshoot general networking issues.

Average reading time: 31 minutes

Besides securing network devices from external tampering, you can take many steps to secure the device from network- or software-supported attacks as well. These practices are called [**device hardening**](javascript://). There are many layers of defense you can implement, although the options vary from one device to another. In this section, you’ll learn about device hardening practices that apply generically to many types of devices. Later you’ll explore device hardening techniques that are more specific to networking devices and require a deeper understanding of a network’s design.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-4aUpdates and Security Patches

Updates to applications, operating systems, and device firmware address several issues, including fixing bugs, adding new features, and closing security gaps. The content in this module is primarily concerned with security issues. Because of the urgency of protecting networks and data from being compromised, security gaps are often addressed in smaller, more frequent updates called patches. Consider a situation where a single, failed patch compromised the personal identification information of more than 100 million people.

In September 2017, Equifax (one of the three major consumer credit reporting agencies) announced a major data breach where hackers accessed confidential information repeatedly from mid-May through July of that year. Names, Social Security numbers, birthdates, addresses, and, in some cases, driver’s license numbers for approximately 143 million people, mostly U.S. residents, were compromised. That’s nearly half the U.S. population. For about 209,000 of those people, credit card numbers were also stolen. How did this happen?

According to reports, a web server bug had been discovered months earlier in an open source software package used by Equifax. The bug allowed extensive back-door access to web servers run by major banking, government, retail, and other organizations. While a patch was issued by the software developer one day after the bug was discovered, security professionals suspect that Equifax either failed to apply the patch or inadequately implemented the patch in their systems before the breach occurred. Further, it appears Equifax had failed to renew a public key certificate that should have allowed Equifax’s internal security systems to fully monitor data traversing their network. This means attackers were able to remove high volumes of data without Equifax’s knowledge. To learn more about this story, do a search online for “Equifax breach technical details” or something similar. Look for authoritative news sources that specialize in the IT industry, such as [krebsonsecurity.com](http://krebsonsecurity.com/" \t "_blank), [techradar.com](http://techradar.com/" \t "_blank), or [computerworld.com](http://computerworld.com/" \t "_blank), and also look for government websites with official, public notices.

### Caution

To help protect your personal and financial information, experts recommend that you check your credit report at least once a year. U.S. residents can do this for free at [annualcreditreport.com](http://annualcreditreport.com/" \t "_blank), a federal government approved site sponsored by all three major credit reporting agencies (Equifax, Experian, and TransUnion). Type that address directly into your browser’s address bar to make sure you don’t end up on a spoofed website. You can order a free, annual report from each of the three agencies through this site, either all at once or spaced throughout the year.

If you’re concerned about any indications of fraud on your account, you can contact one of these agencies to report the fraud and try to resolve the problem. You can also place a temporary fraud alert on your account for 90 days or more at no charge. A fraud alert notifies potential creditors to take extra security precautions before approving a new line of credit on your account.

The process of properly managing and applying security patches includes the following:

* **Discovery**—In this first phase, you investigate what’s on your network so that you can protect it. Good documentation will help indicate whether a newly discovered vulnerability and its patch applies to your network, how extensively the issue affects your systems, how urgent the change is, and what you’ll need to do to implement the patch correctly.
* **Standardization**—Updating OS and application versions consistently across the network will simplify the change process for future updates.
* **Defense in depth**—Recall that the term “defense in depth” refers to applying multiple layers of defense. For layered security to be effective, you need to understand how these various solutions interact and look for any gaps in coverage.
* **Vulnerability reporting**—Identifying and prioritizing relevant security issues and patch releases is essential. In some organizations, one or more staff members take primary responsibility for this task. Network administrators can also subscribe to reporting services from vendors, third parties, and government organizations.
* **Implementation**—Implementing patches includes validating, prioritizing, testing, and applying them. Careful implementation is especially important with security patches, which, as you have seen, can serve a critical role in protecting a business’s interests. Performing patch rollouts in phases, or tiers, requires formal change management processes.
* **Assessment**—In this phase, you evaluate the success of patch implementation and the overall effectiveness of the patch. Was the patch applied everywhere it was needed? Is it working as expected? Can you detect any further gaps in security?
* **Risk mitigation**—In some cases, it may not be possible to apply a patch where needed. For example, a new patch might not be compatible with legacy software on a server. In this case, the server can’t support the patch without compromising the older software. To lessen the resulting risk, you should apply other layers of protection to the affected devices and applications.

**Note 10-1**

Opinions about how to handle firmware updates vary widely. Some network admins take the approach, “If it ain’t broke, don’t fix it.” That is, they don’t upgrade firmware unless they see a pressing reason to do so. Others prefer to address firmware upgrades routinely, alongside other regular updates. Customer support technicians often tell clients to update the firmware on their device and then call back if there’s still a problem. On the job, be sure to research firmware upgrades thoroughly before deciding whether to implement them. If possible, perform the firmware upgrade locally rather than remotely. And be prepared to troubleshoot unexpected problems after the upgrade.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-4bAdministrative Credentials

Most devices that can be configured through a management interface come with a default access account. Often, the username (if there is one) is something like “admin”. The password might be “password”, “admin”, or “1234”. Because these default credentials are so commonly used, they’re also extremely insecure. Surprisingly, many network administrators—even in large organizations—never take the time to change these credentials to something more difficult to crack. When configuring a device, make it a habit to change the default administrative credentials before you do anything else and record this information in a safe place. When you do so, avoid common usernames and passwords. You’ll learn more about how to create secure passwords later in this module.

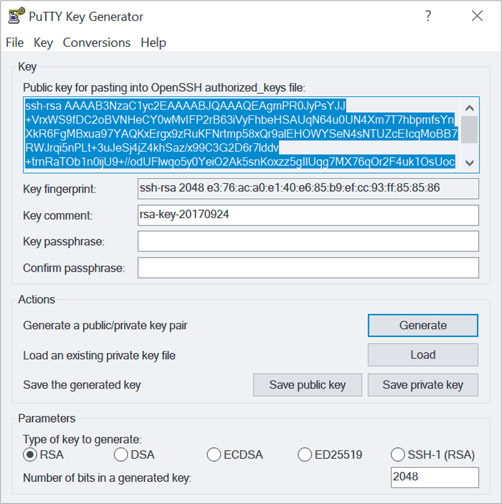
### Caution

Be careful to configure secure usernames and passwords on all devices connected to any part of your network, even if the device itself seems to be an insignificant security threat, such as the chiller for an HVAC system or security cameras in a CCTV network. Any access point into the network can be used to compromise the network’s data or other resources.

Recall that many devices are managed through remote access connections, the most common of which is SSH. Also recall that SSH keys can be used to authenticate devices making the remote connection. This is especially helpful for power users such as system administrators or when using SSH connections for automated processes such as file transfers, financial transactions, or configuration updates. Over long-distance connections, using SSH keys is more secure than using passwords because a securely encrypted key is more difficult to crack than a password. However, just like usernames and passwords, these authentication credentials should be changed from the provider’s default settings. To do this, first remove the existing keys with the rm command. Then generate a new key pair with the ssh-keygen command. [Figure 10-30](javascript://) shows the PuTTY Key Generator, which can also be used to create SSH key pairs.

**Figure 10-30**

Use the PuTTY Key Generator to create a public/private key pair



Source: Simon Tatham

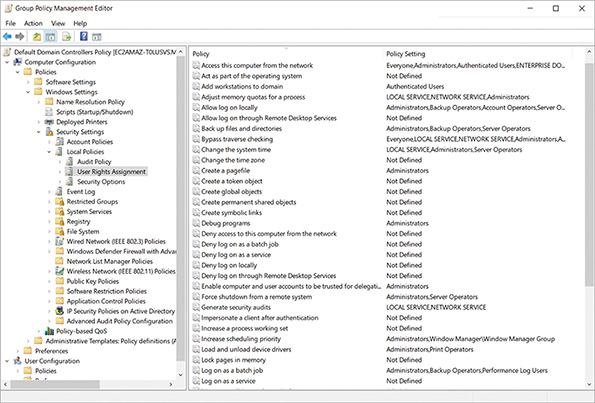
Many devices offer the option to configure several administrative accounts with varying levels of access. Additionally, user accounts on an enterprise’s domain might be capable of accessing different features within a device’s management interface. For example, a support technician in a company might be given an admin account with the ability to configure certain features on a single device or on all similar devices within a domain, such as workstations or certain servers. A high-level network administrator might, instead, have a domain admin account, which allows the person to make changes to Active Directory on a server, access private customer information in a database, or recover from a backup after a system failure.

Some user accounts are given [**privileged access**](javascript://), which allows these users to perform more sensitive tasks, such as viewing or changing financial information, making configuration changes, or adjusting access privileges for other users. [Figure 10-31](javascript://) shows some of the rights that can be assigned to users in a Windows Server domain. Security precautions that might be taken for these accounts include the following:

* **Limited use**—These accounts should only be used when those higher privileges are necessary to accomplish a task. Even those employees who have a privileged user account should also have a lower-level account for normal activities. In fact, anyone who has a user account of any kind should be given only the least privilege, or least amount of access, needed to do a specific job.
* **Limited location**—Many companies require the privileged account be accessed only on location so that no one, not even a legitimate network administrator, can access the device remotely and make high-level changes from outside the protected network. One advantage to this restriction is that access credentials for this account will never be cached on a workstation or other end user device.
* **Limited duration**—Privileged accounts should be carefully accounted for and disabled as soon as they’re not needed, such as when an employee is terminated.
* **Limited access**—The passwords for these accounts should be especially secure and difficult to crack. Passwords should also be stored securely, and when possible, multi-factor authentication should be required, which you’ll learn more about in a later module.
* **Limited privacy**—A privileged account can be used for destructive activity, whether malicious or not. For that reason, every user action in these accounts should be logged and monitored by someone other than the owner of that account. In fact, this logging activity provided key information in troubleshooting the network infiltration described in this module’s [On the Job](javascript://) story. Privileged user monitoring software is available from companies such as Imperva ([imperva.com](http://imperva.com/" \t "_blank)), ManageEngine ([manageengine.com](http://manageengine.com/" \t "_blank)), and Splunk ([splunk.com](http://splunk.com/" \t "_blank)).

**Figure 10-31**

In Active Directory, users are organized by groups, which assign rights and privileges



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-4cServices and Protocols

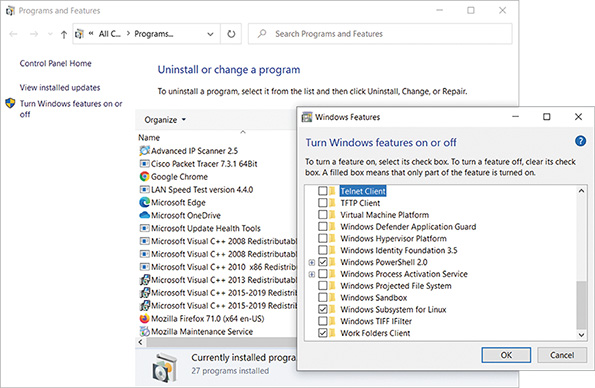
Imagine that a hacker wants to bring a library’s database and mail servers to a halt. Suppose also that the library’s database is public and can be searched by anyone on the web. The hacker might begin by scanning for ports on the database server to determine which ports are open to certain processes or services. If they found an open port on the server, the hacker might connect to the system and deposit code that would, a few days later, damage operating system files. Or they could launch a heavy stream of traffic that overwhelms the database server and prevents it from functioning. They might also use the newly discovered access to determine the root password on the system, gain access to other systems, and launch a similar attack on the library’s mail server, which is attached to the database server. In this way, even a single vulnerability on one server (an unprotected open port) can daisy-chain into destructive access to multiple systems.

Insecure services and protocols, such as Telnet and FTP, should be disabled in a system whenever possible (see [Figure 10-32](javascript://)). Leaving these software ports open and services running practically invites an intrusion because it’s so easy to crack into a system through these open doors. To protect devices from these threats, follow these guidelines:

* **Reduce access paths**—Disable unneeded connection technologies, such as Bluetooth, Wi-Fi, NFC, and IR.
* **Choose secure protocols**—Use secure protocols, such as SSH and SFTP, instead of insecure protocols, such as Telnet and FTP.
* **Reduce start-up processes**—Minimize the number of start-up programs to include only those apps that you really need.
* **Disable unneeded services**—Stop any running services on a computer or network that are not needed. You can Google your OS and “unneeded services” to determine which services are most likely good candidates for disabling.
* **Declutter software**—Disable or uninstall applications that are no longer needed.
* **Streamline the network**—Remove network segments that are no longer needed.
* **Close unused ports**—Close TCP/IP ports on the local firewall and the network firewall that are not used for ongoing activities. For example, port 22 for SSH should not be open unless you need to remotely access that device. Ports 137-139 for NetBIOS should be closed to prevent legacy access methods that can be exploited by common malware such as WannaCry ransomware. [Figure 10-33](javascript://) shows the results of a port scan that revealed insecure ports open on a lab computer.

**Figure 10-32**

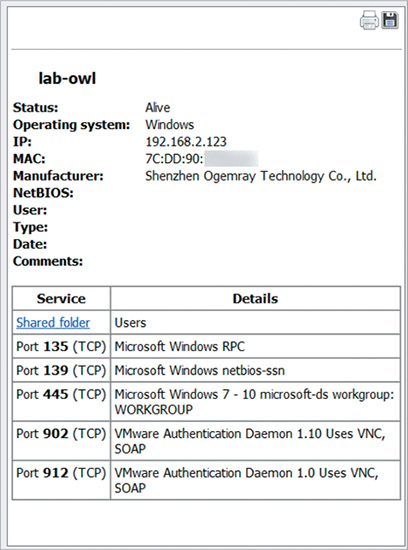
Disable Telnet in Windows



Enlarge Image

**Figure 10-33**

Insecure open ports on a lab computer



Enlarge Image

Source: Famatech Corp.

Go to pg.

[**help**](javascript://)

Application Opened

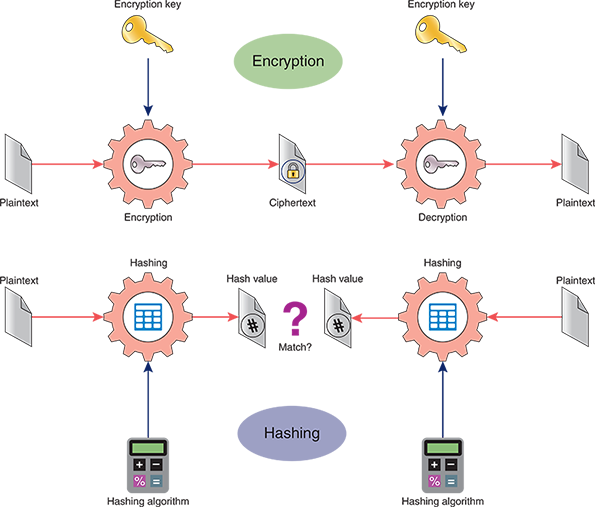
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-4dPasswords

To understand how best to secure passwords, you first need to understand how hashing works. [**Hashing**](javascript://) means to transform data through an algorithm that is mathematically irreversible. Hashing is not the same as encryption, though it’s often listed as a type of encryption and does, in a similar manner, transform data from one format to another. Encrypted data can be decrypted, but hashed data cannot (see [Figure 10-34](javascript://)). Hashing is mostly used to ensure data integrity—that is, to verify the data has not been altered, which is similar to the purpose of a checksum. However, hashes can play a critical role in a good encryption protocol.

**Figure 10-34**

Encryption can be undone; hashing cannot



Enlarge Image

If a secure algorithm is used, hashing is realistically impossible to reverse. Instead, you can take known data, hash it using the same hashing function, and compare the new hash with the stored, hashed data. If the hashes match, this indicates the known data is exactly the same as the original data. If the output does not match, this indicates the data has likely been altered. In fact, this is often the most secure way to store and use passwords.

A well-designed password database does not store passwords in plaintext, but rather, it stores the hash of each password. When the user enters their password, the system hashes that password and then compares the hashed password with the stored hash for that password. If the hashes match, the system knows the user entered the correct password. This way, only the hash is transported and examined. Even if hackers access the stored hashes, they can’t reverse the hashes to determine the original passwords. And the system won’t accept the hash for authentication, only the original password that successfully generates the expected hash.

The most commonly used hashing algorithm today is some form of [**SHA (Secure Hash Algorithm)**](javascript://). You might hear this pronounced “shaw” or “shay.” The primary advantage of SHA over older hashing algorithms is its resistance to collisions. A collision is when two different data sources result in the same hash. A prevalence of collisions from a hashing algorithm essentially defeats the purpose of hashing. However, the added security to avoid collisions means the hashing process takes longer than with less secure options. On this note, there are several versions of SHA:

* **SHA-0**—The original version of SHA was developed by the NSA and was later dubbed SHA-0. It used a 160-bit hash function.
* **SHA-1**—The original version was quickly replaced by the next, slightly modified version, SHA-1, due to an undisclosed flaw in SHA-0. SHA-1 has also since been retired in favor of the next two iterations of SHA, although many systems still rely on the easily cracked SHA-1.
* **SHA-2**—Also designed by the NSA, SHA-2 supports a variety of hash sizes, the most popular of which are SHA-256 (with a 256-bit hash) and SHA-512 (with a 512-bit hash). Note that the 2 in SHA-2 refers to the version number, whereas the larger numbers in SHA-256 and SHA-512 refer to the length of the hash functions.
* **SHA-3**—The most recent iteration of SHA, SHA-3, was developed by private designers for a public competition in 2012. SHA-3 is very different in design from SHA-2, even though it uses the same 256- and 512-bit hash lengths.

SHA-2 and SHA-3 are often implemented together for increased security. It’s also common for data to be hashed in multiple passes along with encryption passes layered into the process.

What does hashing have to do with device hardening? Consider the following options:

* Passwords are often stored in hashed form to prevent them from being read even if they were to be accessed. Using a highly secure hash algorithm nearly guarantees that stolen passwords will be useless to the thief.
* Entire files can also be hashed. File hashing is accomplished by applying a hash algorithm to all the data in a file. Some sites provide hashes of files you might download from their site. If you hash your downloaded file and the hash matches the provider’s hash, then you can be fairly confident your copy of the file has not been infected or corrupted.

**Applying Concepts 10-2**

### Hash a Text String

Several hashing tools are available free online. One website, [onlinemd5.com](http://onlinemd5.com/" \t "_blank), lets you choose between three hashing algorithms: MD5 (an older, outdated hashing algorithm), SHA-1, and SHA-256. Complete the following steps:

1. 1

In your browser, go to **onlinemd5.com**. The first tool shown on this page can hash an entire file, but you’ll practice with smaller portions of text. Scroll down to the MD5 & SHA1 Hash Generator For Text box (see [Figure 10-35](javascript://)).

1. 2

**MD5** should be selected by default. Type a string of text into the box and watch the hash output calculate automatically as you type. What do you notice about the length of the string hash as you enter each additional letter?

1. 3

Copy the final string hash into a text document for later comparison. Windows Notepad works well for this purpose.

1. 4

Select **SHA1** and copy the new string hash into your text document for comparison.

1. 5

Select **SHA-256** and copy the new string hash into your text document for comparison. Which string hash is longer? Why do you think that is?

1. 6

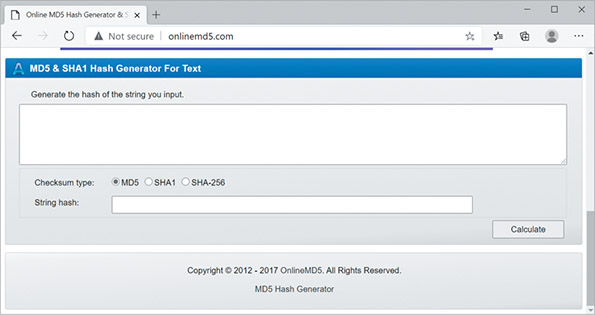
Change exactly one character in your original text. What happens to the string hash?

1. 7

Just a single character change results in a completely different hash. What if your original text is much longer than what you have now? Type a lot more text into the hash generator. What happens to the string hash?

**Figure 10-35**

Input text to hash



Enlarge Image

Source: OnlineMD5

You can also use the command line in Windows PowerShell, macOS Terminal, and Linux Terminal to hash an entire file. Search online for the commands used for each CLI listed in [Table 10-1](javascript://) and write the correct commands in the Command column.

**Table 10-1**

### Hashing Commands in Windows, macOS, and Linux

| **OS** | **Task** | **Command** |
| --- | --- | --- |
| Windows | Hash a file using MD5 |  |
| Windows | Hash a file using SHA-1 |  |
| Windows | Hash a file using SHA-256 (default) |  |
| macOS | Hash a file using MD5 |  |
| macOS | Hash a file using SHA-1 (default) |  |
| macOS | Hash a file using SHA-256 |  |
| Linux | Hash a file using MD5 |  |
| Linux | Hash a file using SHA-1 |  |
| Linux | Hash a file using SHA-256 |  |

Go to pg.

[**help**](javascript://)

Application Opened

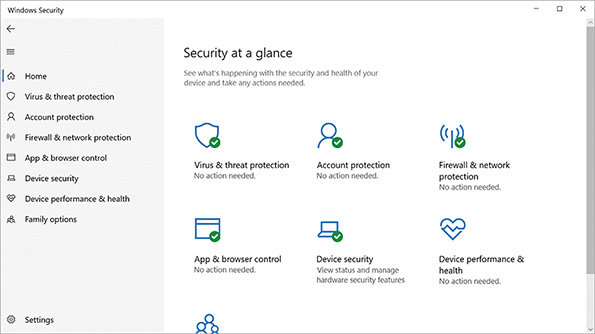
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-4eAnti-Malware Software

You might think that you can simply install a virus-scanning program on your network and move to the next issue. In fact, protection against harmful code involves more than just installing anti-malware software. It requires choosing the most appropriate anti-malware program for your environment, monitoring the network, continually updating the anti-malware program, and educating users. Anti-malware on devices might consist of software embedded in the OS, such as Microsoft Defender Antivirus (see [Figure 10-36](javascript://)), or you might install third-party anti-malware solutions, such as Bitdefender ([bitdefender.com](http://bitdefender.com/" \t "_blank)), Kaspersky ([kaspersky.com](http://kaspersky.com/" \t "_blank)), and Malwarebytes ([malwarebytes.com](http://malwarebytes.com/" \t "_blank)), the last of which is especially good for removing malware if it does infect your computer.

**Figure 10-36**

Built-in Windows anti-malware



Enlarge Image

Even if a user doesn’t immediately notice malware on their system, the harmful software generally leaves evidence of itself, whether by changing the operation of the machine or by announcing its signature characteristics in the malware code. Although the latter can be detected only via anti-malware software, users can typically detect the operational changes without any special software. For example, you might suspect a virus on your system if any of the following symptoms arise:

* Unexplained increases in file sizes
* Significant, unexplained decline in system or network performance (for example, a program takes much longer than usual to start or to save a file)
* Unusual error messages with no apparent cause
* Significant, unexpected loss of system memory
* Periodic, unexpected rebooting
* Fluctuations in display quality

When implementing anti-malware software on devices and the network, one of your most important decisions is where to install the software. Some scenarios include the following:

* **Host-based**—If you install anti-malware software on every desktop, you have addressed the most likely point of entry but ignored the most important files that might be infected—those on the servers. Host-based anti-malware also provides insufficient coverage when a significant portion of the network is virtualized.
* **Server-based**—If the anti-malware software resides on the servers and checks every file and transaction, you will protect important files but slow your network performance considerably.
* **Network-based**—Securing the network’s gateways, where the Internet connects with the interior network, can provide a formidable layer of defense against the primary source of intrusion—the Internet. However, this does nothing to prevent users from putting the network at risk with infected files on flash drives, laptops, or smartphones, and it cannot respond to problems that manage to wriggle through the edge defenses. Network-based firewalls and defenses must be implemented throughout the network, not just on the perimeter. In a later module, you’ll learn more about security in network design.
* **Cloud-based**—Many anti-malware solutions already employ cloud-based resources within their programming. And cloud-based anti-malware provides the same kinds of benefits as other cloud-based solutions, such as scalability, cost efficiency, and shared resources. These cloud vendors are still working out bugs, and it can be a challenge to ensure that coverage soaks the entire network with no blind spots. Cloud solutions also increase the amount of Internet traffic to perform their duties, which can increase costs.

To find a balance between sufficient protection and minimal impact on performance, you must examine your network’s vulnerabilities and critical performance needs. However, be aware that anti-malware is not a completely reliable form of protection. Other methods of device hardening are more effective, especially when multiple layers of security are put in place.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-4fAsset Disposal

Securing your network devices doesn’t stop when you’re finished with those devices. You might think it doesn’t matter what happens to a device after you throw it in the garbage or drop it off at the recycling center. However, mining data from discarded devices is a lucrative business that can yield significant insights into a company’s operations, proprietary systems, and sensitive data. IT assets of all kinds must be carefully tracked both during and after their service time, as your company is legally responsible for the data contained on those devices even after you stop using them. IT devices that must be tracked include workstations, laptops, tablets, smartphones, printers, copiers, fax machines, scanners, servers, firewalls, routers, switches, and any other device or media that stores data (such as flash drives, tape drives, and hard drives).

In many cases, companies will hire professional disposal services that adequately sanitize or destroy devices so no data can be recovered. Reputable vendors provide end-to-end insurance coverage for hardware and data from the moment they take possession of each device. Typically, hard drives are destroyed before devices leave the customer’s premises. Devices slated for disposal are then inventoried, tracked (possibly with GPS tracking), transported securely, and treated according to relevant data protection and environmental regulations and laws. The vendor returns certification of the following information:

* Chain of custody, that is, who had possession of each device and when, at what time the device arrived at the disposal facility, and the device’s final destination (for example, if it’s resold)
* Date and time of sanitization and methods used
* Valuation of any resaleable devices
* Whether each device was resold if reasonable, recycled if possible, or destroyed if necessary

The certificate the disposal service provides, which is called a [**CEED (Certificate of Electronic Equipment Destruction)**](javascript://), serves as legal protection should data later be recovered from your devices. This kind of documentation must be presented during some types of audits.

When not using a disposal service, you take full responsibility to ensure any sensitive data on disposed devices is completely unusable. Recall that many devices, especially mobile devices like smartphones and tablets, are configured to allow a remote wipe of all data should the device be lost or stolen. While a remote wipe or factory reset can clear much of a device’s data, often this process only makes the data inaccessible by conventional means. A skilled forensics investigator or hacker could still recover this data. Therefore, when the device is still in your possession, it must be thoroughly sanitized before disposal. To conform to this requirement, make sure all employees know to return aged devices to IT staff for proper disposal.

**Remember This…**

* Describe common hardening and security policies.
* Explain the principle of least privilege and the concept of defense in depth.
* Apply device hardening best practices, including port security, disabling unneeded services, changing default passwords, and patching firmware.
* Properly dispose of IT assets.
* Compare host-based and network-based firewalls.

**Self-Check**

1. The following ports were listed as open during a recent port scan. Which one is no longer used except by legacy software and should be closed?

Answer

* 1. 22
  2. 53
  3. 139
  4. 443

1. You sent a coworker a .exe file to install an app on their computer. What information should you send your coworker so they can ensure the file has not been tampered with in transit?

Answer

* 1. Public encryption key
  2. Hash of the encryption key
  3. Private encryption key
  4. Hash of the file

**You’re Ready**

You’re now ready to complete [Project 10-3: Secure a Workstation](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 10-5Security Policies for Users

### Certification

* 3.2

Explain the purpose of organization documents and policies.

* 4.2

Compare and contrast common types of attacks.

* 4.3

Given a scenario, apply network hardening techniques.

* 5.5

Given a scenario, troubleshoot general networking issues.

Average reading time: 29 minutes

Most network security breaches begin or continue due to human error. This section describes hardening techniques designed to minimize break-ins by communicating with and effectively managing the users in your organization with well-planned security policies.

A [**security policy**](javascript://) for network users identifies your security goals, risks, levels of authority, designated security coordinator and team members, responsibilities for each team member, and responsibilities for each employee. In addition, it specifies how to address security breaches. It should not state exactly which hardware, software, architecture, or protocols will be used to ensure security, nor how hardware or software will be installed and configured. These details change from time to time and should be shared only with authorized network administrators or managers.

This section discusses written security policies that guide a user’s activity on a network. You might also think of the term “security policy” in regard to rules programmed into a computer or other device. A software security policy programmed into an operating system or a firewall defines the conditions that must be met for a device or transmission to be given access to a network or computing resource. For example, you can set a network-wide security policy that prompts users to change their passwords every three months, and it requires a minimum number of characters for those passwords.

This provides two levels of protection. On one hand, there’s the written rule, included in an Employee Handbook, specifying that users must comply with password restrictions. On the other hand, there’s the security policy configured in Active Directory or a similar directory service. This policy is programmed into the device or network by a network administrator to enforce the rules written in the Employee Handbook. Later in this module, you’ll get a chance to practice setting local security policies in Windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5aSecurity Policy Goals

Before drafting a security policy, you should understand why the security policy is necessary and how it will serve your organization. Typical goals for security policies include the following:

* Ensure that authorized users have appropriate access to the resources they need.
* Prevent unauthorized users from gaining access to the network, systems, applications, or data.
* Protect sensitive data from unauthorized access, both from within and from outside the organization.
* Prevent accidental or intentional damage to hardware or software.
* Create an environment in which the network and systems can withstand and, if necessary, quickly respond to and recover from any type of threat.
* Communicate each employee’s responsibilities with respect to maintaining data integrity and system security.
* For each employee, obtain a signed consent to monitoring form, which is a document that ensures employees are made aware that their use of company equipment and accounts can be monitored and reviewed as needed for security purposes.

**Note 10-2**

A company’s security policy need not pertain exclusively to computers or networks. For example, it might state that each employee must shred paper files that contain sensitive data or that each employee is responsible for signing in their visitors at the front desk and obtaining a temporary badge for those visitors.

After defining the goals of your security policy, you can devise a strategy to attain them. First, you might form a committee composed of managers and interested parties from a variety of departments in addition to your network administrators. The more decision makers you include, the more effective the policy created by the committee will ultimately be. This committee can assign a security coordinator, who will then drive the creation of the security policy.

To increase the acceptance of your security policy in your organization, tie security measures to business needs and clearly communicate the potential effects of security breaches. For example, if your company sells clothing over the Internet, make sure users and managers understand that a two-hour outage (as could be caused by a hacker who uses IP spoofing to gain control of your systems) could cost the company $100,000 in lost sales. With this understanding, employees are more likely to embrace the security policy.

A security policy must address an organization’s specific risks. To understand your risks, you should conduct a posture assessment that identifies vulnerabilities and that rates both the severity of each threat and its likelihood of occurring, as described earlier in this module. After you have identified risks and assigned responsibilities for managing them, you’re ready to outline the policy’s content, as described in this section. Although compiling all this information might seem daunting, the process ensures that everyone understands the organization’s stance on security and the reasons it is so important.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5bBYOD (Bring Your Own Device)

Recall that BYOD (bring your own device) refers to the practice of allowing people to bring their smartphones, laptops, or other technology into a facility for the purpose of performing work or school responsibilities. Variations on this theme include the following:

* **BYOA (bring your own application)**—Employees or students supply their choice of software on a computer or mobile device.
* **BYOC (bring your own cloud)**—Employees or students supply their choice of cloud application or storage.
* **BYOT (bring your own technology)**—A generic reference that includes the other BYO options.
* **CYOD (choose your own device)**—Employees or students are allowed to choose a device from a limited number of options, usually supplied by the company or school.

These days, BYOD doesn’t necessarily refer to “bringing” a device anywhere. As more employees and students work from home, organizations are needing to adopt BYOD-friendly policies more than ever (see [Figure 10-37](javascript://)). Employees and students need to keep in touch and complete work on a wide variety of devices, and this can create a security nightmare as companies work through these BYOD challenges.

**Figure 10-37**

Employees and students are relying more heavily on their own devices for connecting to organizational resources



Bojan Milinkov/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

Organizations offering BYOD options need detailed policies concerning what is allowed and what isn’t, what reimbursements or allowances the company might offer, what restrictions will keep the organization’s data and networks safe, and what configurations to the device are required to comply with the policies. BYOD practices can be cheaper for organizations to implement and tend to improve efficiency and morale for employees and students. However, security and legal compliance concerns must be sufficiently addressed in clearly defined BYOD policies and protocols.

Part of a BYOD policy might include on-boarding and off-boarding procedures. Recall that the process of configuring wireless clients for network access is called on-boarding. These configurations can be handled automatically by [**MDM (mobile device management)**](javascript://) software. MDM works with all common mobile platforms and their service providers, and it can add or remove devices remotely. Examples of MDM software include VMware’s Workspace ONE ([vmware.com/products/workspace-one.html](http://vmware.com/products/workspace-one.html" \t "_blank)) and Cisco’s Meraki Systems Manager ([meraki.cisco.com/products/systems-manager/](http://meraki.cisco.com/products/systems-manager/" \t "_blank)).

MDM software can automate enrollment, enforce password policies and other security restrictions, encrypt data on the device, sync data across corporate devices, wipe the device, and monitor the device’s location and communications. The best MDM packages include granular control over these options. For example, an administrator might configure the software to remove corporate data from all devices while leaving personal data untouched. A less intrusive option is MAM (mobile application management), which targets specific apps on a device rather than controlling the entire device.

Go to pg.

[**help**](javascript://)

Application Opened

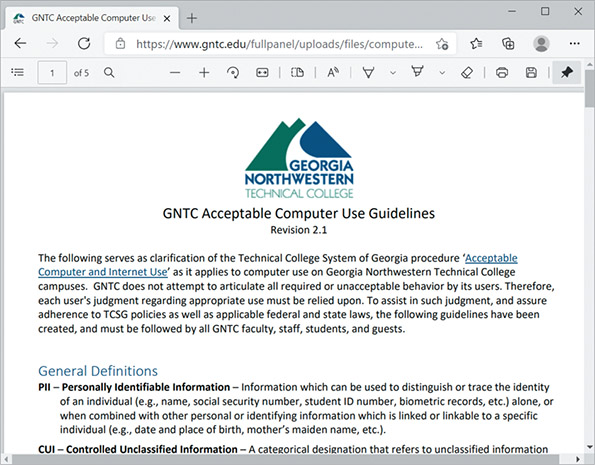
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5cAUP (Acceptable Use Policy)

An [**AUP (acceptable use policy)**](javascript://) explains to users what they can and cannot do while accessing a network’s resources. It also explains penalties for violations and might describe how these measures protect the network’s security. For example, [Figure 10-38](javascript://) shows one school’s AUP for all faculty, staff, students, and guests who use the campus computer labs and other technology resources. This AUP details what kind of information is protected, how to protect it, whose responsibility it is to keep each user account secure, what the computers can be used for, what kinds of activities are prohibited, and much more. The AUP also includes details explaining why these measures are helpful for everyone who needs these resources for school and work.

**Figure 10-38**

A good AUP gives some explanation on the importance of included rules and restrictions



Enlarge Image

Source: Georgia Northwestern Technical College

Employers should never assume that employees inherently know what is acceptable use of company IT resources and what is not. Detailing this information clarifies expectations for everyone. Some of the restrictions might include the following:

* Use company resources to fulfill job obligations and not for personal tasks that should be performed outside of business hours using the employee’s own resources.
* Be aware that activities on the network can be and are monitored and may be formally audited.
* Immediately report any suspected compromise of confidential data or customer privacy.
* Always sign off or lock a device when not in use.
* Don’t do anything illegal using company devices or other resources.
* Don’t try to circumvent network security restrictions.
* Don’t market products or services to other network users.
* Don’t forward spam email.
* Don’t violate the rights of any person or organization.
* Don’t violate copyright, trade secret, patent, intellectual property, or other regulations. This includes but is not limited to the following:
  + Don’t install, use, or distribute pirated materials.
  + Don’t copy, digitize, or distribute copyrighted materials.
* Don’t export software, technical information, or encryption technology.

**Note 10-3**

International and regional export controls limit what software, data, technology, and devices can cross certain political boundaries. For example, you might need an export license to travel internationally with encrypted data, and some countries might require that you decrypt data before entering the country. In some countries, authorities might confiscate devices temporarily or permanently. For this reason, you should never carry confidential data about patients, clients, or customers internationally.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5dNDA (Non-Disclosure Agreement)

A security policy should also define what confidential and private mean to the organization. This is often done in an [**NDA (non-disclosure agreement)**](javascript://). In general, information is confidential if it could be used by other parties to impair an organization’s functioning, decrease customers’ confidence, cause a financial loss, damage an organization’s status, or give a significant advantage to a competitor. However, if you work in an environment such as a hospital, where most data is sensitive or confidential, your security policy should classify information in degrees of sensitivity that correspond to how strictly its access is regulated. For example, top-secret data may be accessible only by the organization’s CEO and vice presidents, whereas confidential data may be accessible only to those who must modify or create it to do their jobs (for example, doctors or hospital accountants).

**Note 10-4**

Any information covered by an NDA might also be protected from international export.

Go to pg.

[**help**](javascript://)

Application Opened

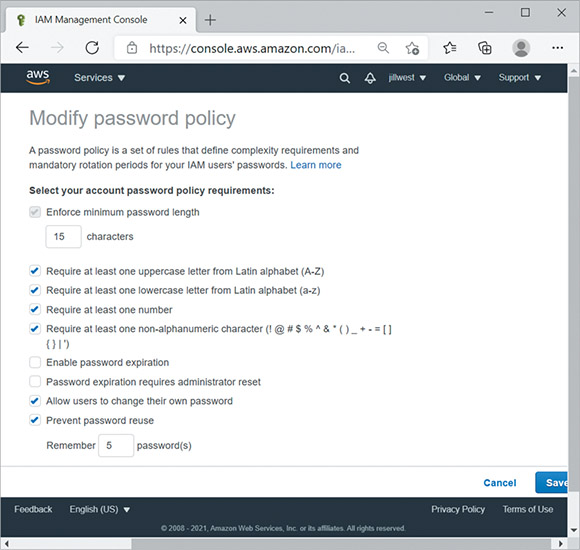
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5ePassword Policy

Choosing a secure password is one of the easiest and least expensive ways to help guard against unauthorized access. Unfortunately, too many people prefer to use an easy-to-remember password. If your password is obvious to you, however, it might also be easy for a hacker to figure out. An organization can enforce password policies to require that all users create passwords conforming to certain restrictions. [Figure 10-39](javascript://) shows password policies that can be configured for all of an organization’s IAM (Identity and Access Management) users to require that they create secure passwords on AWS’s cloud platform.

**Figure 10-39**

Set minimum password configuration policies



Enlarge Image

Source: Amazon Web Services, Inc.

The following guidelines for creating passwords should be part of your organization’s security policy. It is especially important for network administrators to choose well designed passwords, and also to keep passwords confidential and change them frequently. Tips for making and keeping passwords secure include the following:

* **Change default passwords**—Always change system default passwords after installing new software or equipment. For example, after installing a router, the default administrator’s password on the router might be set by the manufacturer to password, with this information printed on a sticker on the bottom of the device. Change administrative credentials before making any other configuration changes.
* **Avoid personal information**—Do not use familiar information, such as your name, nickname, birth date, anniversary, pet’s name, child’s name, spouse’s name, user ID, phone number, address, favorite color, favorite hobby, or any other words or numbers that others might associate with you.
* **Avoid real words**—Do not rely solely on words that might appear in a dictionary, even an “urban” or “slang” dictionary. Hackers can use programs that try a combination of your user ID and every word in a dictionary to gain access to the network. This is known as a [**dictionary attack**](javascript://), and it is typically the first technique a hacker uses when trying to guess a password (besides asking the user for their password). A dictionary attack will take into account typical user behavior regarding passwords, such as starting with short possibilities, checking words commonly used for passwords, and making common symbol substitutions for letters (such as using @ for the letter a). Other kinds of password attacks include the following:
  + **Rainbow table attack**—This more technically challenging attack involves matching known passwords with hashes in a database of hashed passwords to identify as many passwords as possible. For example, you can determine that the word “password”—when hashed with MD5—is 5f4dcc3b5aa765d61d8327deb882cf99. Then you check through the hacked password database and find all the hashes that list this particular hash. You then know which of the passwords, in their original plaintext, are “password”. To defend against this type of attack, organizations will salt passwords, which means to add some extraneous characters that only the organization knows about.
  + **Brute-force attack**—Recall that, in a brute-force attack, a hacker attempts numerous possible character combinations until the correct combination is found. Many hackers using this approach will start with common passwords (such as “password”, “123456”, or “qwerty”) and then alter one character at a time until finding a successful combination (such as “p@ssword”). The primary defenses against a brute-force attack are using a long password and using two-factor authentication, which you’ll learn more about later.
* **Long is strong**—Make the password longer than eight characters—the longer, the better. Statistically speaking, a shorter password is more vulnerable to a brute-force attack than a longer one is. Current recommendations suggest that passwords should consist of at least 15 characters if the application or website allows that length. Remember this mantra: “Long is strong.”
* **Increase complexity**—A well-designed password benefits from both length and complexity characteristics. Consider the following tips:
  + Choose a combination of letters, numbers, and symbols. However, don’t use common replacements of certain numbers or symbols for certain letters as hackers already know to look for these, and they’re harder for you to remember.
  + Use a combination of uppercase and lowercase letters, preferably in a random pattern instead of starting with a capital letter at the beginning of the password.
  + Add special characters, such as exclamation marks or hyphens, if allowed.
  + Do not repeat words or number sequences.
  + Do not use a single letter, number, or symbol more than twice in succession (such as “passworddddddddddd”).
  + Do not use easily recognized phrases such as a line from a famous song, poem, or movie.

**Note 10-5**

Current research indicates that a long, random string of words, such as correcthorsebatterystaple, is easier to remember, more secure, and takes longer to crack than a seemingly randomized series of letters, numbers, and symbols that is short enough for a human to remember. The idea is to combine length with randomness in a way that works well for human memory and is statistically challenging for computers to crack. You can then add some complexity by inserting numbers and symbols and by intentionally misspelling one or more words in the series, such as correct12HORSbatery!@STAPL.

* **Don’t use sticky notes**—Do not write down your password or share it with others, including coworkers or family members. Never store passwords in an unencrypted spreadsheet or document or in a web browser. Many browsers store these passwords in plaintext and can be easily hacked.
* **Update passwords**—Change your password at least every 60 days or more frequently. If you are a network administrator, establish controls through directory services that force users to change their passwords every 60 days.
* **Don’t reuse passwords**—Do not allow passwords to be reused for the same account after they have expired. And use different passwords for different applications, accounts, and websites. For example, choose separate passwords for your email account, online banking, VPN connection, and so on. That way, if someone learns one of your passwords, they won’t be able to use the same information to access all your secured accounts.
* **Use a password manager**—Make it easier to keep a secure record of long, random passwords by installing and using password management software such as LastPass ([lastpass.com](http://lastpass.com/" \t "_blank)), KeePass ([keepass.info](http://keepass.info/" \t "_blank)), or 1Password ([1password.com](http://1password.com/" \t "_blank)). These applications can generate unique strings of random letters, numbers, and symbols for each password, and store them securely in an encrypted database which is accessible from multiple devices through a single, master password. This way, users only need to remember one, well-formed password that is sufficiently long and random to help maximize security of their password database.

Password guidelines should be clearly communicated to everyone in your organization through your security policy. Although users might grumble about designing memorable but secure, long, random passwords and changing their passwords frequently, you can assure them that the company’s financial, proprietary, and personnel data is safer as a result.

**Note 10-6**

Even if data is encrypted, at some point data is accessed, stored, or otherwise manipulated in its unencrypted form, and this is when vulnerability is greatest. This threat is called endpoint vulnerability because data is exposed in its unencrypted form at an endpoint of use, such as when a password is entered on a user’s smartphone. For example, suppose a user has taken all precautions to create a long, complex password for their online bank account. The bank’s website stores the account access information in a securely encrypted database. However, if the user then writes the password on a sticky note and hides it under the keyboard on their desk, this highly secured bank account is still extremely vulnerable to thieves.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5fPrivileged User Agreement

A [**PUA (privileged user agreement)**](javascript://), or privileged access agreement, addresses the specific concerns related to privileged access given to administrators and certain support staff. For example, doctors who have access to HIPAA-protected patient information must sign a privileged user agreement that defines what they can and can’t do with that patient data and what special precautions they must take to protect the patient’s privacy. Certain checks and balances must also be maintained and defined in the PUA. For example, the person who can authorize vendor payments should not be the same person who creates vendor accounts.

The privileged user agreement outlines guidelines, rules, restrictions, and consequences of violations, all of which help minimize the risk involved in allowing privileged access to some users. When accessing a privileged account, the user is advised to stay signed into the account only as long as necessary to perform the needed tasks, and then sign off, not relying on the time-out feature to sign them out. Privileged users need more frequent training and reminders to avoid falling for social engineering attacks of various types. And in many cases, activity in privileged accounts will be specially monitored through a PAM (privileged account management) tool, such as BeyondTrust’s ([beyondtrust.com](http://beyondtrust.com/" \t "_blank)) PAM products or CyberArk’s ([cyberark.com](http://cyberark.com/" \t "_blank)) solutions on-premises or in the cloud.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 10-5gAnti-Malware Policy

Anti-malware software alone will not keep your network safe from malicious code. Because most malware infections can be prevented by applying a little technology and forethought, it’s important that all network users understand how to prevent the spread of malware. An anti-malware policy provides rules for using anti-malware software and policies for installing programs, sharing files, and using external storage such as flash drives. To be most effective, an anti-malware policy should be authorized and supported by the organization’s management staff. Suggestions for anti-malware policy guidelines include the following:

* Every computer in an organization should be equipped with malware detection and cleaning software that regularly scans for malware. This software should be centrally distributed and updated to stay current with newly released malware.
* Users should not be allowed to alter or disable the anti-malware software.
* Users should know what to do in case their anti-malware program detects malware. For example, you might recommend that the user stop working on their computer and instead call the help desk to receive assistance in disinfecting the system.
* An anti-malware team should be appointed to focus on maintaining the anti-malware measures. This team would be responsible for choosing anti-malware software, keeping the software updated, educating users, and responding in case of a significant malware outbreak.
* Users should be prohibited from installing any unauthorized software on their systems. This edict might seem extreme, but in fact, users downloading programs (especially games) from the Internet is a common source of malware. If your organization permits game playing, you might institute a policy in which every game must first be checked for malware and then installed on a user’s system by a technician.
* System-wide alerts should be issued to network users notifying them of a serious malware threat and advising them how to prevent infection, even if the malware hasn’t been detected on your network yet.

When drafting an anti-malware policy, bear in mind that these measures are not meant to restrict users’ freedom, but rather to protect the network from damage and downtime. Explain to users that the anti-malware policy protects their own data as well as critical system files. If possible, automate the anti-malware software installation and operation so users barely notice its presence. Do not rely on users to run their anti-malware software each time they insert a USB drive or open an email attachment because they will quickly forget to do so.

**Applying Concepts 10-3**

### Has Your Email Been Hacked?

How can you know if one of your accounts has been hacked if you can still get to the account and you don’t yet notice any changes? Perhaps your username and password have been posted for sale as part of a hacked password database, waiting for the highest bidder to exploit your compromised credentials. Perhaps your email is posted publicly on the dark web for hackers to peruse at their pleasure. How can you know?

Troy Hunt ([troyhunt.com](http://troyhunt.com/" \t "_blank)) has developed a website called Have I Been Pwned, pronounced “powned” as a play on the words “owned” and “pawned” (as in chess). Troy analyzes user credentials after a breach to determine patterns in passwords that are easily hacked. While no one has a list of all successful hacks, the HIBP (Have I Been Pwned) website provides an in-depth resource to identify emails posted publicly in hacking databases.

To determine whether your email address is included in a published hack, complete the following steps:

1. 1

In your browser, go to [haveibeenpwned.com](http://haveibeenpwned.com/" \t "_blank). Go to the FAQs page and answer the following questions:

* 1. How does the website owner choose which data breaches to include in his site?
  2. How does the website protect the privacy of those whose data is included in the reported data breaches?
  3. What does the website do with information you submit in checking if your accounts have been included in a data breach?
  4. What can you conclude if your email address is not found in the site’s database?

1. 2

Return to the home page. Enter your email address (you can choose any of your email addresses) to see if that address has been pwned. What results did you get?

1. 3

Based on these results, what steps do you need to take to further secure your accounts?

**Remember This…**

* Explain the roles of password policies, AUPs, BYOD policies, and NDAs in network security.
* Compare various password attack types, including brute-force and dictionary attacks.
* Use good password management techniques.

**Self-Check**

1. What kind of software can be used to secure employee-owned devices?

Answer

* 1. PUA
  2. NDA
  3. MDM
  4. BYOD

1. Which of the following is the most secure password?

Answer

* 1. p@$$w0rd
  2. yellowMonthMagneficant
  3. $t@rw@r$
  4. 09181973

1. An attacker guesses an executive’s password (“M@nd@lori@n”) to a sensitive database after chatting for a while at a club. What kind of password attack did the hacker use?

Answer

* 1. Dictionary attack
  2. Brute-force attack
  3. Zero-day attack
  4. Rainbow table attack

**You’re Ready**

You’re now ready to complete [Project 10-4: Create a Secure Master Password in LastPass](javascript://), or you can wait until you’ve finished the Review Questions for this module.

**You’re Ready**

After you finish the Hands-On Projects, you’re ready to complete the [Module 10 Capstone Projects](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 10-6a**Module Summary**

### Security Risks

* A weakness of a system, process, or architecture that could lead to compromised information or unauthorized access is known as a vulnerability. The act of taking advantage of a vulnerability is known as an exploit.
* Social engineering involves manipulating social relationships to gain access. Common types of social engineering include phishing, baiting, quid pro quo, tailgating, piggybacking, and shoulder surfing.
* A DoS (denial-of-service) attack occurs when legitimate users are unable to access normal network resources, such as a web server, because of an attacker’s intervention. Several DoS subtypes include DDoS (distributed DoS) attack, DRDoS (distributed reflection DoS) attack, amplified DRDoS attack, PDoS (permanent DoS) attack, and friendly DoS attack.
* Common technology-based attacks and vulnerabilities include on-path attacks, deauth (deauthentication) attacks, insecure ports and protocols, FTP bounce, and back doors.
* Malware is a generalized term that refers to many kinds of malicious software, including virus, Trojan, worm, bot, and ransomware.

### Risk Assessment and Management

* Effective risk management happens at two layers: the network layer and the business layer. A security risk assessment evaluates threats to and vulnerabilities of the network. A business risk assessment evaluates the impact of potential threats on business processes.
* Every organization should assess its security risks by conducting a posture assessment, which is a thorough examination of each aspect of the network to determine how it might be compromised. One component of a posture assessment might include a threat assessment, which identifies specific security threats to the network and related risk factors. If the company performing the posture assessment is accredited by an agency that sets network security standards, the assessment qualifies as a security audit, also called an IT audit.
* A vulnerability assessment is used to identify vulnerabilities in a network. Pen (penetration) testing takes advantage of ethical hacking to identify weaknesses and the extent of those weaknesses. This attack simulation begins with a vulnerability assessment using various tools and then attempts to exploit those vulnerabilities. During a red team–blue team exercise, the red team conducts the attack, and the blue team attempts to defend the network.
* Scanning tools—such as Nmap, Nessus, and Metasploit—can provide useful insights into your network’s weaknesses that need attention. Used by hackers (or more likely, by bots) these tools can instead lead to compromised security.
* A honeypot is a decoy system that is purposely vulnerable and filled with what appears to be sensitive (though false) content. In more elaborate setups, several honeypots might be connected to form a honeynet.

### Physical Security

* Access control hardware ranges from a simple deadbolt to more sophisticated options and can manage access to buildings, rooms, or storage spaces. Physical access control technologies include a keypad or cipher lock, an access badge system, biometrics, an access control vestibule, locking racks and locking cabinets, and smart lockers.
* Despite all precautions, sometimes breaches do occur. The key to protecting sensitive data and systems is to detect intrusions as quickly as possible and be prepared to respond appropriately. Methods of detecting physical intrusions and other kinds of events include motion detection, security cameras, tamper detection, and asset tags.

### Device Hardening

* Besides securing network devices from external tampering, you can take many steps to secure the device from network- or software-supported attacks as well. These practices are called device hardening. There are many layers of defense you can implement, although the options vary from one device to another.
* Updates to applications, operating systems, and device firmware address several issues, including fixing bugs, adding new features, and closing security gaps. Because of the urgency of protecting networks and data from being compromised, security gaps are often addressed in smaller, more frequent updates called patches.
* Because default credentials are so commonly used, they’re also extremely insecure. When configuring a device, make it a habit to change the default administrative credentials before you do anything else and record this information in a safe place. When you do so, avoid common usernames and passwords.
* Insecure services and protocols, such as Telnet and FTP, should be disabled in a system whenever possible. Leaving these software ports open and services running practically invites an intrusion because it’s so easy to crack into a system through these open doors.
* Passwords are often stored in hashed form to prevent them from being read even if they were to be accessed. Using a highly secure hash algorithm nearly guarantees that stolen passwords will be useless to the thief.
* When implementing anti-malware software on devices and the network, one of your most important decisions is where to install the software. Some scenarios include host-based, server-based, network-based, or cloud-based.
* IT assets of all kinds must be carefully tracked both during and after their service time, as your company is legally responsible for the data contained on those devices even after you stop using them. IT devices that must be tracked include workstations, laptops, tablets, smartphones, printers, copiers, fax machines, scanners, servers, firewalls, routers, switches, and any other device or media that stores data (such as flash drives, tape drives, and hard drives). Disposal services provide a CEED (Certificate of Electronic Equipment Destruction), which serves as legal protection should data later be recovered from your devices. This kind of documentation must be presented during some types of audits.

### Security Policies for Users

* A security policy for network users identifies your security goals, risks, levels of authority, designated security coordinator and team members, responsibilities for each team member, and responsibilities for each employee. In addition, it specifies how to address security breaches. It should not state exactly which hardware, software, architecture, or protocols will be used to ensure security, nor how hardware or software will be installed and configured. These details change from time to time and should be shared only with authorized network administrators or managers.
* To increase the acceptance of your security policy in your organization, tie security measures to business needs and clearly communicate the potential effects of security breaches.
* Organizations offering BYOD options need detailed policies concerning what is allowed and what isn’t, what reimbursements or allowances the company might offer, what restrictions will keep the organization’s data and networks safe, and what configurations to the device are required to comply with the policies. BYOD practices can be cheaper for organizations to implement and tend to improve efficiency and morale for employees and students. However, security and legal compliance concerns must be sufficiently addressed in clearly defined BYOD policies and protocols.
* An AUP (acceptable use policy) explains to users what they can and cannot do while accessing a network’s resources. It also explains penalties for violations and might describe how these measures protect the network’s security.
* A security policy should also define what confidential and private mean to the organization. This is often done in an NDA (non-disclosure agreement).
* An organization’s security policy should include guidelines for creating secure passwords. It is especially important for network administrators to choose well designed passwords, and also to keep passwords confidential and change them frequently. Tips for making and keeping passwords secure include the following: Change default passwords, avoid personal information, avoid real words, use long passwords, increase complexity, don’t use sticky notes, update passwords, don’t reuse passwords, and use a password manager.
* A PUA (privileged user agreement), or privileged access agreement, addresses the specific concerns related to privileged access given to administrators and certain support staff.
* An anti-malware policy provides rules for using anti-malware software and policies for installing programs, sharing files, and using external storage such as flash drives. To be most effective, an anti-malware policy should be authorized and supported by the organization’s management staff.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 10-6b**Key Terms**

* [**access badge**](javascript://)
* [**access control vestibule**](javascript://)
* [**asset tag**](javascript://)
* [**AUP (acceptable use policy)**](javascript://)
* [**badge reader**](javascript://)
* [**biometrics**](javascript://)
* [**botnet**](javascript://)
* [**business process**](javascript://)
* [**business risk assessment**](javascript://)
* [**C&C (command-and-control) server**](javascript://)
* [**CCTV (closed-circuit TV)**](javascript://)
* [**CEED (Certificate of Electronic Equipment Destruction)**](javascript://)
* [**CVE (Common Vulnerabilities and Exposures)**](javascript://)
* [**data breach**](javascript://)
* [**DDoS (distributed DoS) attack**](javascript://)
* [**deauth (deauthentication) attack**](javascript://)
* [**device hardening**](javascript://)
* [**dictionary attack**](javascript://)
* [**DLP (data loss prevention)**](javascript://)
* [**DNS poisoning**](javascript://)
* [**DoS (denial-of-service) attack**](javascript://)
* [**exploit**](javascript://)
* [**FTP bounce**](javascript://)
* [**hacker**](javascript://)
* [**hashing**](javascript://)
* [**honeynet**](javascript://)
* [**honeypot**](javascript://)
* [**insider threat**](javascript://)
* [**locking cabinet**](javascript://)
* [**locking rack**](javascript://)
* [**logic bomb**](javascript://)
* [**malware (malicious software)**](javascript://)
* [**MDM (mobile device management)**](javascript://)
* [**motion detection**](javascript://)
* [**NDA (non-disclosure agreement)**](javascript://)
* [**on-path attack**](javascript://)
* [**pen (penetration) testing**](javascript://)
* [**phishing**](javascript://)
* [**piggybacking**](javascript://)
* [**port scanner**](javascript://)
* [**posture assessment**](javascript://)
* [**principle of least privilege**](javascript://)
* [**privileged access**](javascript://)
* [**process assessment**](javascript://)
* [**PUA (privileged user agreement)**](javascript://)
* [**ransomware**](javascript://)
* [**red team–blue team exercise**](javascript://)
* [**security audit**](javascript://)
* [**security policy**](javascript://)
* [**security risk assessment**](javascript://)
* [**SHA (Secure Hash Algorithm)**](javascript://)
* [**shoulder surfing**](javascript://)
* [**smart card**](javascript://)
* [**smart locker**](javascript://)
* [**social engineering**](javascript://)
* [**tailgating**](javascript://)
* [**tamper detection**](javascript://)
* [**threat assessment**](javascript://)
* [**vendor risk assessment**](javascript://)
* [**vulnerability**](javascript://)
* [**vulnerability assessment**](javascript://)
* [**zero-day exploit**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 10-6c**Review Questions**

1. Your organization has just approved a special budget for a network security upgrade. What procedure should you conduct to develop your recommendations for the upgrade priorities?
   1. Data breach
   2. Security audit
   3. Exploit
   4. Posture assessment
2. Which type of DoS attack orchestrates an attack bounced off uninfected computers?
   1. FTP bounce
   2. Ransomware
   3. DRDoS attack
   4. PDoS attack
3. A company accidentally sends a newsletter with a mistyped website address. The address points to a website that has been spoofed by hackers to collect information from people who make the same typo. What kind of attack is this?
   1. Phishing
   2. Tailgating
   3. Quid pro quo
   4. Baiting
4. A former employee discovers six months after he starts work at a new company that his account credentials still give him access to his old company’s servers. He demonstrates his access to several friends to brag about his cleverness and talk badly about the company. What kind of attack is this?
   1. Principle of least privilege
   2. Insider threat
   3. Vulnerability
   4. Denial of service
5. What type of attack relies on spoofing?
   1. Deauth attack
   2. Friendly DoS attack
   3. Tailgating
   4. Pen testing
6. You need to securely store handheld radios for your network technicians to take with them when they’re troubleshooting problems around your campus network. What’s the best way to store these radios so all your techs can get to them and so you can track who has the radios?
   1. Locking rack
   2. Smart locker
   3. Locking cabinet
   4. Access control vestibule
7. Leading up to the year 2000, many people expected computer systems the world over to fail when clocks turned the date to January 1, 2000. What type of threat was this?
   1. Ransomware
   2. Logic bomb
   3. Virus
   4. Worm
8. Which of the following attack simulations detect vulnerabilities and attempt to exploit them? Choose two.
   1. Red team–blue team exercise
   2. Vulnerability assessment
   3. Security audit
   4. Pen testing
9. Which of the following is considered a secure protocol?
   1. FTP
   2. SSH
   3. Telnet
   4. HTTP
10. A company wants to have its employees sign a document that details some project-related information that should not be discussed outside the project’s team members. What type of document should they use?
    1. AUP
    2. NDA
    3. MDM
    4. BYOD
11. What is the difference between a vulnerability and an exploit?
12. What are the four phases in the social engineering attack cycle?
13. List five subtypes of DoS attacks.
14. What type of scan process might identify that Telnet is running on a server?
15. Give an example of biometric detection.
16. What unique characteristic of zero-day exploits makes them so dangerous?
17. What steps should your company take to protect data on discarded devices?
18. A neighbor hacks into your secured wireless network on a regular basis, but you didn’t give her the password. What loophole was most likely left open?
19. Which form of SHA was developed by private designers?
20. Why might organizations be willing to take on the risk of BYOD?

Go to pg.

[**help**](javascript://)