Oppos Bootcamp Course Content

07/2025

Contents

Cybersecurity

Protecting digital data is the realm of cybersecurity. You're familiar with the term, but what exactly does it mean? When most people think of cybersecurity, they focus on technology. So, you might think of cybersecurity as the *security of digital systems* or *security of communications*. These definitions are correct, but they don't address all components of cybersecurity. Consider these examples:

- A fraudster emails a person claiming to be from the person's bank. The fraudster asks for their personal identification number (PIN). Is that a cybersecurity concern?
- A private investigator calls an employee of a company. The investigator asks him to print some confidential files and leave the papers in the mail room for the investigator to collect. Is that a cybersecurity concern?

As these examples show, cybersecurity professionals must consider non-technological or non-digital components of attacks. Cybersecurity can have one or more of the following three components: digital, human, or physical. Let's explore how cybersecurity addresses each one.

Digital security involves safeguarding your data and systems from digital threats. These threats range from malware attacks, such as viruses or ransomware, to hacking attempts designed to infiltrate systems and steal sensitive information. Some examples of digital security measures include firewalls and encryption software.

Human security involves protecting data against potential threats caused by human behavior or actions. These threats can be unintentional, such as an employee unknowingly downloading a malicious email attachment. Others are intentional, such as an employee intentionally leaking confidential data. Some examples of human security measures include employee security training and strong password policies.

Physical security involves protecting tangible assets against threats. These physical assets support digital infrastructure, such as workstations, server rooms, and data centers. And the threats to these assets can be intentional or unintentional, such as theft, tampering, or natural disasters. Some examples of physical security measures include surveillance systems, access control measures, and disaster recovery plans.

Good cybersecurity addresses all three components. So again, what is Cybersecurity? Cybersecurity is the practice of protecting and recovering data, networks, devices, and programs from threats. Those threats can have *digital*, *human*, or *physical* components.

Now you know what cybersecurity is. But what is it trying to accomplish? Effective cybersecurity delivers on three objectives:

- Confidentiality
- Integrity
- Availability

These objectives make up the **CIA triad** (**C**onfidentiality, **I**ntegrity, and **A**vailability), a well-known model and a cornerstone of cybersecurity.

Confidentiality means keeping data secret; that is, only authorized people can access or disclose the data. For example, software companies typically keep their applications' source code secret for competitive advantage. To reduce the chances of a source code leak, they restrict access to only the employees who need it. Confidentiality also covers people's private data. One example is that your healthcare provider must ensure that data collected while treating you, such as diagnoses or prescriptions, stays private. With few exceptions, only you, your doctor, and authorized medical staff should have access to that data.

In practice, confidentiality involves implementing safeguards that give the right level of access to the right set of users at the right times, using the right methods.

The CIA triad helps guide cybersecurity-related policies in an organization. Depending on their operations and the scenarios that they encounter, different organizations might prioritize one objective over the others.

Example

Consider some examples to put the objectives of the CIA triad into context.

- **Confidentiality** might be the most crucial objective for government intelligence agencies. These agencies handle sensitive data relevant to national security, ongoing investigations, intelligence reports, and other classified information. An unauthorized leak of this information might help criminals plan more successful illegal activities. It might even put lives in danger.
- **Integrity** might be the most crucial objective for banks. Financial transactions, central to banks' business, rely heavily on data's accuracy and consistency. Unauthorized modifications, deliberate or not, can lead to significant financial losses or legal repercussions.
- **Availability** might be the most crucial objective for an online retailer. As a customer, you probably expect to be able to shop for anything you want online, any time of day. Any downtime, lag, or disruption in services might lead you to take your business elsewhere. It might also reduce your trust

in the company and damage the company's reputation. Companies want to ensure that their website maintains constant uptime, loads quickly, and processes transactions without errors.

Integrity means ensuring that data is trustworthy and accurate by protecting it from unauthorized modification and destruction. Say you spend $10 on a pizza. You might not care whether that purchase is confidential. But what if something alters the transaction amount and you end up spending $10,000 instead? Note that the integrity of this transaction might have been compromised intentionally or unintentionally. Also, consider that although the cause of the error might be technical, it might be human, too. Maybe someone entered the wrong payment amount.

To preserve integrity, you must also prevent unauthorized people from editing the data. In this sense, integrity and confidentiality overlap.

The CIA triad helps guide cybersecurity-related policies in an organization. Depending on their operations and the scenarios that they encounter, different organizations might prioritize one objective over the others.

Example

Consider some examples to put the objectives of the CIA triad into context.

- **Confidentiality** might be the most crucial objective for government intelligence agencies. These agencies handle sensitive data relevant to national security, ongoing investigations, intelligence reports, and other classified information. An unauthorized leak of this information might help criminals plan more successful illegal activities. It might even put lives in danger.
- **Integrity** might be the most crucial objective for banks. Financial transactions, central to banks' business, rely heavily on data's accuracy and consistency. Unauthorized modifications, deliberate or not, can lead to significant financial losses or legal repercussions.
- **Availability** might be the most crucial objective for an online retailer. As a customer, you probably expect to be able to shop for anything you want online, any time of day. Any downtime, lag, or disruption in services might lead you to take your business elsewhere. It might also reduce your trust in the company and damage the company's reputation. Companies want to ensure that their website maintains constant uptime, loads quickly, and processes transactions without errors.

Availability means ensuring timely and reliable access to and use of the data. For example, you expect 24x7 online access to your bank account. To meet that

expectation, your bank must implement and maintain sufficient resources to keep online banking available and functioning properly.

But timely access does not always mean immediate or even continuous access. For example, when you request school transcripts, you might need to wait several days for school employees to locate, process, and send out the documents. And if the school provides transcripts electronically, it might limit the time frame in which recipients can access them. Regardless, the data is available within and for a reasonable amount of time.

The CIA triad helps guide cybersecurity-related policies in an organization. Depending on their operations and the scenarios that they encounter, different organizations might prioritize one objective over the others.

Example

Consider some examples to put the objectives of the CIA triad into context.

- **Confidentiality** might be the most crucial objective for government intelligence agencies. These agencies handle sensitive data relevant to national security, ongoing investigations, intelligence reports, and other classified information. An unauthorized leak of this information might help criminals plan more successful illegal activities. It might even put lives in danger.
- **Integrity** might be the most crucial objective for banks. Financial transactions, central to banks' business, rely heavily on data's accuracy and consistency. Unauthorized modifications, deliberate or not, can lead to significant financial losses or legal repercussions.
- **Availability** might be the most crucial objective for an online retailer. As a customer, you probably expect to be able to shop for anything you want online, any time of day. Any downtime, lag, or disruption in services might lead you to take your business elsewhere. It might also reduce your trust in the company and damage the company's reputation. Companies want to ensure that their website maintains constant uptime, loads quickly, and processes transactions without errors.

Key elements of cybersecurity

There are three key elements of cybersecurity to consider:

People

As counter intuitive as it might be for a highly digital industry, people are the most important part of cybersecurity. First, people are the end users of digital systems and second, people are often those responsible for the design and maintenance of digital systems. Human action is by far the leading cause of cybersecurity incidents. When organizations design a secure system, they must design with people in mind.

A common example of this going wrong is the case of alert fatigue. If people receive too many notifications or alarms, then they eventually become desensitized to it. Good systems will be designed to anticipate and make allowances for human behavior.

Process

In business, most activities follow a clearly defined set of steps. These processes can aid cybersecurity by considering security at each step or hinder cybersecurity by being frustrating for the end user.

Imagine a process which makes a user complete a 20-question survey whenever they wish to report suspicious activity. Many users, who could contribute useful information, might be deterred and give up the process.

Good processes have the following attributes:

- They are clear and as easy as possible. During the process, it should be obvious what to do at every stage. Processes should not use unnecessary jargon or be written in an ambiguous fashion.
- They are accessible or well known. All users who could follow a process at any stage, should know how to access the process. A good example of this commonly being done well is with fire evacuations in buildings. Most people know where the nearest evacuation points are because of good signage.

- They are consistent. Processes should not contradict each other, if possible. If a process has a lot of exceptions or deviations, it increases complexity. Later, you will learn about how cyber attackers can exploit this during their attacks.

Technology

Technology is all of the underlying infrastructure.

Within cybersecurity, this commonly covers elements such as device encryption, network perimeter defenses, and anti-malware technologies.

Within business, good uses of technology solve problems without creating new ones for their users.

An example of good technical security is device management software, which can track software patch statuses and apply updates. This is often an essential tool for large organizations. If this is done correctly, then the technology is non-intrusive and users will be secured in a passive manner. If this is done poorly, then users might try to disable the software entirely. As users of devices, you encounter this too.

The following table shows some technological leaps for security, their perceived drawbacks, and some downsides to their introduction from the user perspective

Technological leap	Business benefit	Perceived drawback	Undesirable user responses
Automated patch management	All software is up-to-date	Interruptions to use of device	User does not power down devices
High complexity mandatory passwords	Harder for attackers to guess passwords	Tedious to use	P@ssw0rd!
Mandatory passwords expire after 30 days	Passwords cannot be compromised for long periods of time	Predictably repetitive	PasswordJan to then PasswordFeb
Encrypted emails	Attackers cannot read emails in transit	Additional configuration and complexity	Disable encryption feature

You can see it is important for organizations to educate users as to why exactly the technology has been introduced and why perceived drawbacks might be necessary.

Controls

To meet each objective of the CIA triad, you need controls. In cybersecurity, controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical, tangible, or digital property.

Let's explore examples of controls for preserving confidentiality, integrity, and availability.

Controls for confidentiality

Consider these standard controls for preserving confidentiality.

- **Encryption** converts your data into a form that only someone with the decryption key can understand.
- **Access controls** are measures designed to ensure that only the correct people can view, modify, or share data. If you use password protection, you're using an access control. Access controls also include biometrics, such as fingerprints or retinal scans, that ensure that only authorized people can access the data.
- **Patch management** involves updating system software. Regularly updating system software fixes potential security weak points that attackers can exploit.

Controls for integrity

Consider these standard controls for preserving integrity.

- **Checksums** are mathematical algorithms that generate a unique value for a data set. If the data changes, the checksum will also change, alerting you to the alteration.
- **Access controls** and **user permissions** can limit who can change data and what changes they can make.
- **Data backups** can help restore data to its correct state if changes occur.
- **Audit trails** can track and record all changes made to data. They give you a clear record of who made a change and when they made it.

Controls for availability

Consider these standard controls for preserving availability.

- **Redundant systems** and **data backup procedures** help protect against data loss or system failure. You might use multiple servers or store data in multiple locations.

- **Antimalware software** and **firewalls** protect systems from attacks that can disrupt services.
- **Disaster recovery** and **business continuity plans** lay out the steps needed to restore services quickly and efficiently in case a disruption occurs, minimizing downtime.

Technological leap	Business benefit	Perceived drawback	Undesirable user response
Automated patch management	All software is up to date	Interruptions to use of device	User does not power down devices
High complexity mandatory passwords	Harder for attackers to guess passwords	Tedious to use	P@ssw0rd!
Mandatory passwords expire after 30 days	Passwords cannot be compromised for long periods	Predictably repetitive	PasswordJan to then PasswordFeb
Encrypted emails	Attackers cannot read emails in transit	Additional configuration and complexity	Disable encryption feature

Risks Management

Introduction

Risks are part of everyday life and something that we are all instinctively familiar with. A **risk** is the possibility of something happening with a negative consequence.

Managing risk is at the heart of most businesses and the core of many industries. For example, think of the insurance industry. An insurance company assesses the risk associated with insuring a person or entity. First, it determines the likelihood of an incident and the probability of someone making a claim if the incident occurs. Then, it sets premiums accordingly. It absorbs the potential financial risk from its clients in return for these regular premium payments.

Good businesses understand and manage risks effectively to give them a competitive advantage. In this module, you'll explore some key concepts about risk and how they apply to cybersecurity.

Learning objectives

After completing this module, you should be able to:

- Choose the best questions to answer when determining risk value
- Describe the four responses that organizations can choose to address risk
- Contrast high and low risk appetites

Risk Valuation

All risks are not equally important. Some risks require urgent attention, while others can be ignored. More significant risks are known as **high risks**. You can use this basic equation to calculate the value of a risk:

Risk value = Consequence × Likelihood

- **Consequence** is the impact and associated damages.
- **Likelihood** is how often the risk impact occurs.

The risk value equation quantifies the significance of a risk. It's the product of the potential consequence of a risk occurring and the probability of its occurrence. If the consequence of a risk is high (severe impact) and its likelihood is also high (very probable), then the risk value will be significant. This high risk would require immediate attention and mitigation. A risk with a low consequence or likelihood wouldn't require such immediate attention.

Ideally, for mathematical reasons, it would be great if good statistical information existed for every risk. If, for example, you know that one in 10 cars will experience a flat tire in a given year, then you can easily work out the associated risk value.

Example

An example of the risk value equation applied to the previous flat tire scenario might be as follows. Someone might lose a day's productivity because they got a flat tire on the way to work. The **consequence** of this risk is the loss of one day of work. Though this consequence is annoying, remember that the **likelihood** of the risk is low: one in 10 cars a year. Thus, you might assess the overall risk value to be low.

In cybersecurity, likelihood is hard to measure directly because of the constant evolution of technology and the involvement of outside attackers. Generally, the likelihood of an organization experiencing an attack depends partly on three attributes:

Likelihood = Adversary capability × Adversary motivation × Vulnerability severity

Adversary is a general term for an entity that wishes to compromise an information system.

Adversary capability includes the attacker's resources, technology access, and expertise. High adversary capability indicates that the attacker has the tools, means, and proficiency to exploit vulnerabilities, thus posing a greater risk. Conversely, an attacker with low capability might not be able to exploit complex vulnerabilities, thus posing a lesser risk.

Adversary motivation is the incentive or reason that drives an adversary to attempt a cyberattack. This motivation can come in various forms, such as financial gain, desire for information, political influence, or simply the thrill of disruption.

Vulnerabilities are potential weaknesses within a system that someone can exploit to compromise it. For example, a vulnerability can be a login process that does not authenticate a user accurately.

Example

Let's consider an example to demonstrate how the equation for likelihood works. Imagine that a recently formed hacking group targets a bank. The malicious group is interested in stealing users' banking login details and passwords.

- You might assess the **adversary capability** as *low* because their organization is new and might not have the latest technology or resources to develop their own tools, if required.
- You might assess their **motivation** as *high* because they can attempt multiple attacks over a period of time.
- You might assess an identified **vulnerability** as *high* because it is comparatively easy to exploit. For example, some vulnerabilities have published descriptions online, enabling attackers to mirror attacks easily.

Note: Using the rating terms *low*, *medium*, and *high* is an example of qualitative risk analysis. In an ideal world, you would use exact numbers or percentages. However, finding them can be challenging, so estimates are often all you have.

Activity: Choose the best questions to answer when determining risk value

You've learned about risk valuation. Now, you'll apply your knowledge to perform the initial steps in a risk assessment.

In this activity, you'll read about Harper Family Care, a small healthcare clinic, and review a list of the clinic's cybersecurity risks identified during a risk assessment. Then, you'll choose one relevant question to answer for each risk to determine the risk's significance or value.

Background information

Harper Family Care is a small doctor's office that has served the local community for 40 years. The founder, Orlando Harper, is also the head doctor. His daughter, Heidi, is his office manager. Orlando is an excellent and well-respected doctor, but he doesn't keep up with the latest trends in technology, including those that impact his practice. Particularly concerning is that he doesn't keep up with cybersecurity trends and the measures needed to safeguard patients' data. But Heidi explains why the clinic should undergo a cybersecurity risk assessment. He reluctantly agrees to it.

Heidi hires Data Defense, a cybersecurity consulting firm, to perform the assessment. You are the Data Defense representative handling Harper Family Care's case. First, you review the organization's cybersecurity infrastructure. You identify the following areas of risk.

1. Outdated operating system
2. Single-factor authentication for email accounts
3. Antimalware software isn't updated regularly
4. Important files aren't backed up
5. Old hardware

Questions for determining risk value

Now, you'll consider each area of risk. You'll choose one relevant question to consider for determining the risk's significance or value.

Risk 1: Outdated operating system

The clinic's computers run on an outdated operating system (OS). The vendor of the OS no longer supports it and doesn't provide security updates for it.

Which question is relevant for determining the value of this risk?

Would updating the OS disrupt any currently running applications or services?

What is the total cost associated with updating the operating system?

What technical support is available for migrating to a more secure OS?

What negative impact can this outdated OS have on system and data security?

Risk 2: Single-factor authentication for email accounts

The clinic's email system uses single-factor authentication. Users need only one form of authentication, a password, for access. The current industry standard for authentication is **multifactor authentication**, which is when a login requires at least two types of credentials. For example, logging into your bank account from a new device might require a password and the answer to a security question.

Which question is relevant for determining the value of this risk?

How can single-factor authentication compromise the clinic's email security?

How burdensome is providing multiple types of credentials for users?

How much do users trust the provider of the multifactor authentication service?

How compatible is multifactor authentication with all company devices?

Risk 3: Antimalware software isn't updated regularly

The organization's antimalware software isn't updated regularly. The software isn't configured to update automatically, and the system administrator, Heidi, updates the software manually on an irregular basis.

Which question is relevant for determining the value of this risk?

How inconvenient is the process of updating the antimalware software?

What is the probability of a virus or other malware attacking this system?

How reluctant is Heidi to pay for regularly updating the antimalware software?

Would other antimalware software provide better technical support?

Risk 4: Important files aren't backed up

The organization has no regular backup routine for important data files.

Which question is relevant for determining the value of this risk?

How time-consuming is the backup process?

How often should the clinic back up patients' data?

What damages can result from losing patients' data?

Is the backup process efficient enough for the clinic?

Risk 5: Old hardware

The clinic relies on old hardware. Some computers are quite old and don't support the latest updates or software. Employees use these computers only for basic tasks that don't require high processing power, and the computers don't hold sensitive data.

Which question is relevant for determining the value of this risk?

Are the old computers accessible through the clinic's network?

Does maintaining these older machines cost more than replacing them?

How much do users prefer using the old computers because of familiarity?

Are these computers older on average than those in other clinics?

Risk response

After an organization assesses all its risks, it starts risk management or response. Generally, organizations can choose from the following four responses to a risk.

Acceptance

The organization **accepts** the risk in its current form. It acknowledges the potential consequences of the risk and is prepared to deal with them if they occur. A senior person within the organization, referred to as a risk owner, makes the decision to accept a risk.

Reduction

The organization decides a risk is too large to accept and aims to **reduce** it in some fashion. To reduce the risk, the organization can reduce either its likelihood or consequence. It does so by implementing security controls or patching system vulnerabilities.

Transference

The organization chooses to **transfer** the risk. It can have a third party accept part or all of the risk instead of accepting the risk itself. Transfer typically occurs through insurance or outsourcing. Though the risk remains, another entity manages its impact, reducing the direct threat to the organization.

Rejection

The organization decides a risk is too high and **rejects** it, meaning that the organization withdraws from being affected by it. Rejecting the risk can significantly change business

operations. For example, rejection might involve shutting down sites, avoiding markets, or avoiding activities that lead to the risk.

Example

Let's illustrate these four responses to a risk. Imagine that you are considering starting an at-home bakery business. One risk in any bakery is a fire, which can cause extensive damage. Consider the following responses to this risk.

- **Acceptance:** You examine the risk and, with faith in your baking skills, take the chance that it is unlikely anything will go wrong. Should your baking go wrong, you can repair your kitchen and are prepared to do so.
- **Reduction:** You decide that you prefer not to put your kitchen and oven at a high level of risk, and you decide to reduce the risk. You can reduce the likelihood of fire-related incidents by installing a smoke detector to provide early warning. You can reduce the consequence of a fire by having a fire suppression system installed. Both options will incur a small cost, but you believe that they are worth it.
- **Transference:** You go to your insurance company and upgrade your insurance to cover home cooking-related fires. The company performs its own assessment of the risk. Together, you agree on a cost to pay the company to cover the risk. Should your oven catch fire, the company will cover the costs. This arrangement incurs a cost initially but limits your liability.
- **Rejection:** You decide that the oven-related fire risk is too high. You can change recipes to make cakes without using an oven or not start your business in the first place.

This example shows that even in simple situations, you have many factors to consider. Businesses with rapidly changing IT technology face many continually evolving risks. Risk management is a full-time job in many companies and guides a lot of both strategic and tactical decision-making.

Risk appetite

A **risk appetite** is the level of risk that an organization is willing to accept.

- An organization has a *high* risk appetite if it is willing to accept a high level of risk.
- An organization has a *low* risk appetite if it does not like accepting risk.

In cybersecurity, risk appetite refers to an organization's willingness to accept the potential consequences of cyberattacks. Organizations with a high risk appetite might take bold initiatives, using the latest technologies and potentially vulnerable systems, to pursue significant competitive advantages. They accept the risk of potential cyberattacks, but also have robust contingencies for when breaches occur.

Conversely, organizations with a low risk appetite are more cautious in their approach to cybersecurity. They might prioritize stability and reliability over competitive advantage, focusing more on protective measures such as firewalls, encryption, and regular system updates. These organizations aim to minimize the risk of cyberattacks as much as possible, even if doing so means missing out on certain opportunities.

Note that neither approach is better. An organization's level of risk appetite should align with its overall strategic goals and resources. It should also vary by the potential impact of cyberattacks on its operations and reputation.

Types of cyberattacks

Introduction

Attackers can use various methods to enter and exploit systems. Some attacks target vulnerabilities in technology. Others exploit vulnerabilities in humans, specifically the flawed ways in which humans interact with systems.

In this module, you'll explore some of the most common types of cyberattacks:

- Denial-of-service (DoS) attack
- Distributed denial-of-service (DDoS) attack
- Phishing
- Spear phishing
- Malware
- Man-in-the-middle (MitM) attack
- Domain Name System (DNS) attack

Learning objectives

After completing this module, you should be able to:

- Describe common types of cyberattacks
- List ways that artificial intelligence (AI) can enhance the structure and sophistication of cyberattacks

- Examine cyberthreat real-time maps

Denial-of-service (DoS) attack

- A **denial-of-service (DoS) attack** is any attack that causes a complete or partial system outage.
- DoS can occur when a person or system floods a website or online service with too much network traffic, much like a traffic jam on a road. This traffic overflow makes the website or service slow down or shut down completely, denying access to legitimate users.
- DoS can also occur when traffic consumes enough system resources to slow down or crash the system.

Example

An attacker uses a billion laughs attack, also known as an XML bomb, where the attacker creates a small, seemingly harmless piece of code in an Extensible Markup Language (XML) document. The attacker then submits this document to the target organization's system. When the system processes the code, the code continually replicates. The replications consume more and more system resources, eventually slowing down or even crashing the system.

Distributed denial-of-service (DDoS) attack

A **distributed denial-of-service (DDoS) attack** is an attack that comes from multiple sources simultaneously to cause a complete or partial system outage.

To perform DDoS attacks, attackers use bots. A **bot**, or **zombie**, is an internet-connected device infected with malware that enables the attacker to control the device remotely. For DDoS attacks, attackers manipulate multiple bots under the same instance, forming a network of bots called a **botnet**. A botnet can include hundreds or even thousands of bots, each sending data or requesting access from the target server simultaneously. This sudden traffic surge overwhelms the server, causing a denial of service to its users.

Attackers can use AI to analyze patterns and predict the optimal number of bots needed to effectively overwhelm a target's server without wasting resources. AI also helps attackers monitor each bot's performance in real time to maximize effectiveness.

Example

An attacker can send many page requests to a web server over a brief period, overloading the server. Similarly, spikes in user demand on ticket sale websites can overload systems.

Phishing

Phishing is the practice of sending messages, seemingly from a trusted source, to trick users into taking a specific action.

It combines social engineering and technical trickery.

After opening the message, unsuspecting users might install malware, enable remote access, or divulge confidential information.

Example

An attacker might send an email with a file attachment or link to a fake website. When the recipient clicks the attachment or link, they unwittingly install malware on their computer.

Spear phishing

Spear phishing is a type of phishing that targets a specific person, group, or organization.

Attackers take time to research targets. Attackers use this research to create personal and relevant messages, making them more effective.

Some attackers use AI to automate the email creation process. They generate personalized and convincing emails that are more likely to deceive users into revealing sensitive information.

Example

An attacker collects a target's details from social media and then calls the target, pretending to be a bank representative. The attacker claims that the target's account is compromised and asks them to transfer money to a *safe* bank account. The attack is convincing because the attacker uses legitimate knowledge about the client.

Malware

Malware is a catch-all term for malicious software. **Malware** is software designed to harm data or systems without the user's informed consent.

It often triggers secretly when a user runs a program or downloads a file. This user action is often unintentional.

Once active, malware can block access to data and programs, steal information, and make systems inoperable.

AI can help malware adapt to evade detection, enabling them to cause more damage within an infected system.

Example

Many types of malware exist and often, the malware's name indicates its function. For example, **keyloggers** capture a victim's keystrokes, and **ransomware** holds a victim's files captive in exchange for a ransom payment.

Man-in-the-middle (MitM) attack

A **man-in-the-middle (MitM) attack** occurs when attackers insert themselves into communications between a client and server.

With this attack, attackers can view everything that both sides send and receive.

Example

An attacker might set up a free wifi hotspot in a popular public location. If someone connects to that network, the attacker can examine their communications. In turn, the attacker can redirect the victim to a fake login screen or insert advertisements over web pages.

Domain Name System (DNS) attack

The **Domain Name System (DNS)** is one of the core protocols used on the internet. With the DNS protocol, a computer can resolve a domain to an IP address. For example, imagine a user types **bmw.com** into a browser's search bar and then presses **Enter**. The DNS protocol resolves this domain name to the IP address for the main BMW website, taking the user to the site. This function is convenient because domain names are far easier to remember than IP addresses!

A **DNS attack** targets the DNS by manipulating or disrupting the resolution of domain names and possibly redirecting users or hindering access to websites. It involves tactics such as domain hijacking and cache poisoning.

Example

Attackers associated with the Roaming Mantis criminal gang have compromised wireless routers so that entering the URL for a valid website redirects the user to a malicious website. This site delivers malware called Wroba to the user's device. When the device is infected, the attackers can use it as a bot, and then use it to compromise other wireless routers.[1]

Structured query language (SQL) injection

Structured query language (SQL) is a programming language for accessing, managing, and querying databases.

SQL injection is the placement of malicious code in SQL queries, usually via web page input. With a successful attack, attackers can run common commands, including commands to delete the database itself!

SQL injection is one of the most common web hacking techniques.

Attackers can use AI to automate the process of discovering and exploiting vulnerabilities in a database's security.

Example

In the UK, two teenagers managed to target TalkTalk's website in 2015. Using SQL injection, they stole hundreds of thousands of customer records from a database that was remotely accessible.

AI in cyberattacks

Attackers are increasingly turning to AI. With AI, attackers can enhance the structure and sophistication of their attacks in several ways.

Task automation

AI can automate repetitive tasks, enabling attackers to launch attacks at a speed and scale otherwise impossible. For example, AI can automate the creation and dissemination of phishing emails, increasing the likelihood of success.

Detection evasion

AI can help attackers create malware that changes and adapts to evade detection by traditional antivirus solutions. To do so, attackers often use machine learning (ML) algorithms that can learn from each detection attempt and alter the malware's code to avoid future detections.

Target identification

AI can help attackers identify optimal targets for attacks. Sophisticated algorithms can analyze vast amounts of data to identify vulnerable systems or high-value targets, thus increasing the effectiveness of attacks.

Social engineering

Attackers can use AI technologies, such as deep learning, to enhance the effectiveness of social engineering attacks with convincing fake audio and video content. One notable

example is deepfakes, which are fake images, videos, or audio created through deep learning. For example, an attacker might call a victim and use an audio deepfake to impersonate someone that the victim knows and trusts.

AI has introduced a new challenge for cyberdefense systems. The cybersecurity landscape must continually evolve, incorporating AI in its strategies to effectively counter these advanced threats.

Knowledge check

Question 1

Your company's website experiences a sudden influx of traffic. At this time of day, the site usually receives a dozen or so visits. Instead, the site is receiving hundreds of connection requests. This traffic is causing the website to load very slowly if it loads at all.

Which type of cyberattack might be occurring?

Denial-of-service (DoS) attack

Structured query language (SQL) injection

Man-in-the-middle (MitM) attack

Spear phishing

Question 2

Rinaldo receives an email that seems to be from a company that he's done business with many times. The email informs him that his invoice is ready and that he should click the attached file to view it. But the file is malware in disguise, and by clicking it, Rinaldo installs the malware on his computer.

Which type of cyberattack does this scenario represent?

Man-in-the-middle (MitM) attack

Domain Name System (DNS) attack

Structured query language (SQL) injection

Phishing

Question 3

ByteWave Innovations is a small but growing technology company. A competitor obtained copies of the company's research and development plans. Cordelia, the head of the company's cybersecurity division, suspects corporate espionage. The leaked information contained details that an outsider can obtain only by monitoring the keystrokes of certain employees.

Which type of cyberattack did the attacker most likely use to collect this information?

Structured query language (SQL) injection

Malware

Domain Name System (DNS) attack

Denial of Service (DoS) attack

Social engineering

Introduction

When you think of cybersecurity threats, you probably think of digital threats, such as malware, that exploit vulnerabilities in technology. But attackers can also exploit vulnerabilities in **people** to get what they want.

In this module, you'll learn about social engineering and the techniques that attackers use to hack people, not technology.

Learning objectives

After completing this module, you should be able to:

- Define social engineering
- Explain the reasons that social engineering works
- List key aspects of a good social engineering attack
- List ways to defend against social engineering
- Identify common signs of a phishing email

What is social engineering?

Social engineering is the art of making someone do what you want them to do. It overlaps heavily with academic fields involving psychology, biology, and even mathematics.

In cybersecurity, **social engineering** is the use of deception to manipulate individuals into divulging confidential or personal information for fraudulent purposes. Basically, how can someone trick another person into giving up something private? Social engineering attacks are the dark art of using social interactions to trick people into making security mistakes.

Attackers can employ social engineering tactics in person, over the phone, or online through websites, email, and social media.

When an attacker makes someone perform a certain action, the attacker can gain access to sensitive systems, steal assets, or advance a more complex attack. This notion of focusing on persuading or tricking people might sound unreliable. However, many case studies show that social engineering is an incredibly powerful technique.

Example

Effective social engineering tactics can result in defrauding vulnerable people of their savings through **scams and confidence tricks**. For organizations with physical buildings, social engineering also includes **tailgating**, which is when a person enters a secure area without authorization by closely following an authorized person.

Why social engineering works

Social engineering works because humans are imperfect. In short, attackers exploit people's propensity to take shortcuts and make quick decisions based on false promises.

Let's explore the specific reasons why social engineering works so well.

Human nature and social norms

Social engineering takes advantage of human psychology and our natural inclination to trust and help others. Attackers exploit social norms and expectations to manipulate people into divulging information or performing actions that they wouldn't perform otherwise.

For example, an attacker might pose as a coworker in distress, urgently needing access to a particular system to meet a deadline. The target, driven by the desire to be helpful, provides the requested information without second-guessing the authenticity of the request.

Trust and authority

Attackers often exploit people's trust in authority figures or institutions. They can gain credibility and deceive targets by impersonating someone in a position of power or using official-sounding language.

For example, an employee might receive an email from someone claiming to be the company's chief executive officer (CEO). The supposed CEO demands immediate action on a sensitive issue, such as providing access to a client's records. Because the email seemingly comes from the top executive, the employee hastily complies without verifying the authenticity of the request. As a result, the employee provides confidential client data to the attacker.

Emotional manipulation

Social engineering often uses emotions such as fear, curiosity, or excitement to influence decision-making. Attackers create a sense of urgency or exploit personal vulnerabilities to manipulate targets.

For example, someone might receive a phone call from an attacker posing as a representative for the lottery. The attacker congratulates the person for winning the grand prize. The excitement and lure of a large monetary reward cloud the victim's judgment. In turn, they share their bank account information to ensure the lottery company can transfer the supposed prize into their account.

Lack of awareness

Social engineering works well on people less informed about common security and potential risks. And people unfamiliar with social engineering tactics are especially susceptible to manipulation.

For example, a person might receive an email that seems to be from a trusted banking institution instructing them to update their password because of a security breach. Unaware of standard social engineering tactics such as this one, the person promptly follows the instructions and unknowingly gives their login details to the attacker.

All these factors impact a target's ability to make a good decision or even notice that they are being manipulated in the first place.

Key aspects of a social engineering attack

1. It is **well-researched**. If an attacker is trying to impersonate a member of a company, then they will use the company's letterhead, jargon, or format to help build credibility. Not all methods are equally effective against everyone. Cyberattackers research to determine the best driver for their target.
2. It is **delivered confidently**. In-person, good social engineers are prepared and confident, and they reassure targets. Knowing when to launch an attack and how to develop a rapport with the target is essential. Usually, attackers build up a high-value social engineering attack over a series of exchanges, lending

credibility and reducing inhibitions with each exchange. Rushing the attack can backfire and lead to attackers revealing themselves through desperation.

3. It is **plausible and realistic**. The best social engineering attacks are often the ones where the victim doesn't even know that they've been tricked.

How can you defend against social engineering?

Everyone should be aware of and guard against common social engineering attacks.

Aside from never trusting anyone, you should follow this simple rule to defend against social engineering attacks designed to trick people like you.

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

So, if you ever face a financial windfall unexpectedly, a head-hunting request, or a prize from a competition you did not enter, then be aware and inquisitive. Don't let the benefits cloud your judgment.

In addition, don't be afraid to challenge others who make unusual requests or appear out of place. Imagine that an unknown colleague makes a strange request or you see someone loitering in a restricted area. In most such situations, you can ask for details or report your suspicions. Don't comply just because someone claims that an executive from the head office sent them, and they're in a hurry to get by you into a building. You can pause to check. Often, verification costs far less than letting an imposter into your office!

But how do organizations defend against social engineering? They should focus on the three key elements of cybersecurity: process, education, and technology.

Process

They should implement policies that outline the acceptable use of corporate resources and procedures for handling sensitive information.

Education

They should hold regular cybersecurity training sessions to ensure that every employee understands the policies and the risks associated with violating them.

Technology

They should invest in security software, such as spam filters and antimalware software, that can detect and thwart social engineering attacks.

When implemented together, these measures can significantly boost an organization's defenses against social engineering.

Beware of phishing

Phishing emails are one of the most common forms of social engineering, and if you let your guard down, you can fall prey to this tactic. Follow these tips to detect phishing emails, whether personal or business-related. Note that no single phishing email will contain all the signs of phishing mentioned in this list. But the more of these clues that you find in an email, the more likely that it is a phishing attempt.

- Consider if you were expecting the email. Does it make sense that the sender chose to contact you? Is the message too good to be true, or does it pressure you to act quickly?
- Check the sender's email address. Is the email from someone or a company that you recognize?
- Look for the salutation. Does it address you with a generic greeting such as "Dear valued member" instead of your name?
- Search for any language or grammar errors. Does it have poor grammar or a lot of spelling errors?
- Determine what the email is requesting. Does it ask you to visit a fake or "spoof" website? Does it ask you to call a fake customer service number or open attachments that you did not request?
- Look for the red flags of a fake request that are typically part of the phishing email. For example, does it ask for your bank information or password?
- Note any language that is alarming or creates a sense of urgency to act quickly without thinking. Does the email claim that the company will delete your account if you don't act now? Does it state that a virus has been detected on your system, so you should download and install an attached security patch immediately?
- Don't click a link without verifying the URL it points to.
    - Does the URL include a non-secure link? To know if the link is secure, check that the URL begins with "https".
    - Does the URL direct you to a completely different website? Some attackers use URLs that look like legitimate ones. For example, examine this fake URL for PayPal: www.paypall.accountlogin.com/signin. Notice the misspelling of "PayPal".

Important note

If you receive an email that you think might be phishing, don't respond in any way, click any links, or open any attachments. Most email services have a method to report an email as spam.

When in doubt, you can contact the sender via a trusted channel, such as a previously saved contact phone number. You can also access the service web address from your records.

An overview of computer networking

Activities you do every day are part of networking. When you're watching a streaming video through a service like YouTube or TikTok, have you ever thought about how the video makes its way through the internet to your phone, tablet, or laptop? You know that when you click on an online video, you instantly start watching it. And you know that thousands of other people might watch the same video at the same time. The process seems so simple that it's easy to take it for granted. But what makes it possible?

When groups of computers and devices are connected to each other in a way that lets them share data and resources between each other, they form a computer network. A network might be small with only a few devices, or it might be large with a building full of connected servers. And through their network, they send, receive, and share data, including streaming videos.

Computers work mainly with digital data—many ones and zeros—to process documents, videos, images, and other types of files. Even without being connected to the internet or other computers, your phone or laptop works with data. You save, edit, and delete data on your device without a network connection. You can even transfer data physically from one device to another without using a network if you use thumb drives, floppy disks, or writable CD-ROM disks.

But as soon as you transfer data through the internet you are using a network. Your email, text messages, and even YouTube and TikTok content are data. You're using a real-time, online networked connection between resources like computers. Computer networks share data.

Being connected to the network requires more than just two computers. You also need special equipment like a modem to talk to the internet and a router to help manage the **traffic,** the data that is moving. Computer networks share resources such as computers, modems, and routers.

Network. A computer network is a group of computing devices that share data and resources. The technologies that connect the devices can use physical wires, wireless

electromagnetic signals, optical waves, or radio waves. Networked devices are sometimes called network nodes or endpoints.

Network (shared) resources. Network resources are data, information, computing devices, and peripherals that you might access through your network connection.

Computing devices process increasingly large amounts of data. The amount of data they send over a network can be extremely large. Where data (not code) has repetitive information (for example the clear sky in a photo, which is a large area made up of the same shade of blue), an algorithm will account for that more efficiently—like writing a sentence once and adding x100 next to it instead of writing a sentence 100 times on a sheet of paper.

The units you need to use to measure network traffic data account for different sizes.

Modem

The modem is a computer part that connects to an internet service. A modem might be an external box or an internal card.

Router

A router is a box that manages network traffic between your devices and the internet.

Gateway

A gateway is a box that contains both a modem and a router.

The network router transfers data between computers on a network or over the internet.

Routers route data. A router box has an access point with at least one antenna. Although most routers support wireless networking, they are not truly wireless. They need to be plugged into a power outlet with a power cord.

You might have watched a sporting event on television and seen that the broadcast company provided a small window showing a person doing sign language. The interpreter was listening to the sportscaster’s words and signing them for those who understand sign language. In a way, the interpreter was routing information from a source (the sportscaster) to the intended audience (the viewer).

Routers do something similar: They transmit traffic from one side of a network or device (the sender) to the other side of the network or device (the receiver)

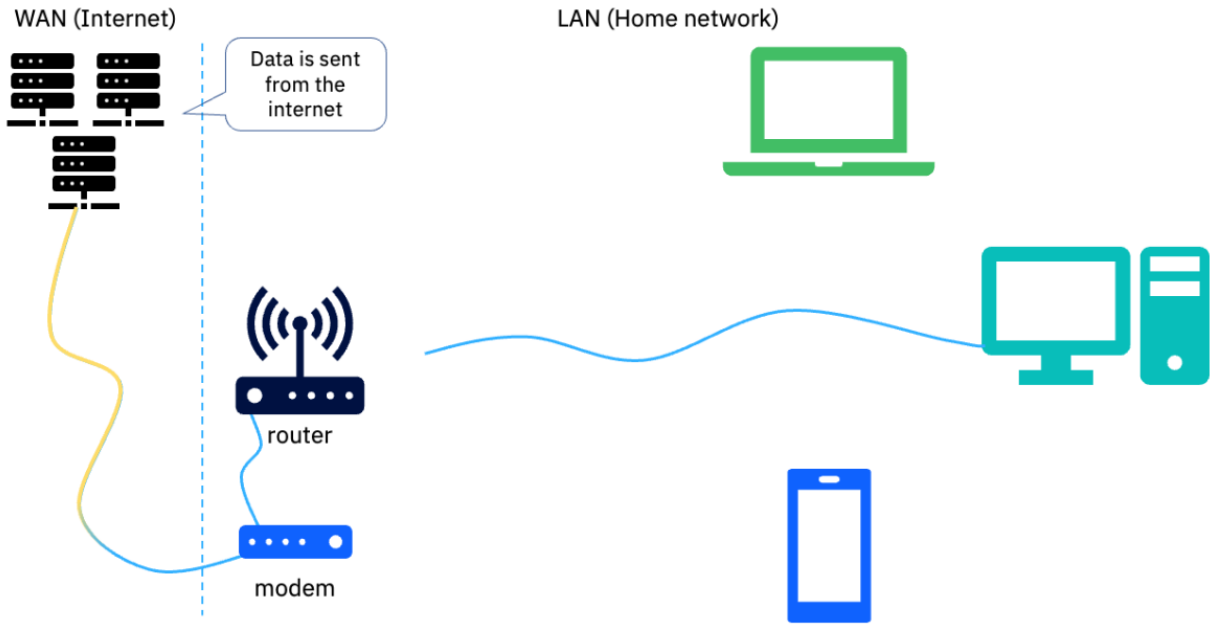
Routing. The router’s task is to choose the path for data traffic.

Routers use MAC addresses, which are given to devices at the factory, and IP addresses, which are assigned to the devices by the internet service provider (ISP), to route data properly. The combination of MAC address and IP address gives each device

a unique ID that routers understand. Because of this, routers play an essential role in getting data to where it needs to go.

How these devices connect and transmit data

The following animation shows how data flows in a network. Internet servers send the data to a modem. The modem then sends the data to a router. The router sends the data to devices on the network. Notice that the router can send data with either wired or wireless networking.



Question 1:

Which of the following devices is a type of hardware that manages network traffic between your devices and the internet?

- Router
- Radio
- Modem
- Gateway

Question 2:

To identify a particular device on your home network, which type of ID would your router have assigned?

Mac address

Username

IP address

Network address

Question 3:

You are watching a new cat video on YouTube on your mobile device while you are traveling. The video is playing mostly without interruption. What accounts for the video's stability?

The video is somewhere on the internet, and somehow it makes it to your device.

A megabyte contains 2^{20} bits and is large enough to contain about a minute of music.

YouTube delivered it intact all at once.

The video is delivered in packets allowing hardware to adjust for missing or misplaced data.

Question 4:

Computer networking is the transfer of data between computers and devices through which means?

Disk drives

Thumb drives

Wireless and wired connections

Documents, videos, websites, and images

Question 5:

You need to send a message to everyone in your group. You write the message and then send it to the people on your list. In which order does your message travel to the recipients?

The routers of the people in your group, then your router, then the internet

The routers of the people in your group, then the internet, then your router

Your router, then the internet, then the routers of the people in your group

The internet, then your router, then the routers of the people in your group

PAN, LAN, and WAN

Personal area networks (PANs). Many modern devices allow you to pay for products by touching your device to a pad at the store. You can also send files and photos to a friend wirelessly if they're in the same place you are. These technologies use specific networking languages called **protocols** like Bluetooth and near-field communication (NFC). As you can see by the term **near-field**, the networking technology depends on two devices being close together. You are not able to use NFC or Bluetooth to send data to someone in another town or even another block.

These types of networks are called **personal area networks (PANs)**. They have that name because the network really is personal. PAN is also secure. You have to approve any transfer or reception of data. The data can only go between devices that you possess and over which you have control.

Expand for some more thoughts

PANs are popular because they can be low cost, efficient, and portable. When you need a simple connection, a PAN can replace bulky corded connections. Another way PANs can be useful is for quick knowledge transfers. For example, a museum might have a display with an NFC chip to provide additional details about the display to visitors who use their mobile phones.

PANs have very specific applications. They are useful when you need to complete a particular task like sending a single file. Most of the work and play that you perform on your devices involves streaming data, moving a lot of files at a time, getting push notifications for news, weather, and messaging, and similar activities. For this more real-time functionality, you need a full-time connection to a network.

Local area networks (LANs). Networks also need some level of privacy. A corporation, a school, or even a home needs a way to protect data, provide resources just for the people in the home or organization, and have a way to let some people in and keep others out. Your home would be unlivable if anyone is able to walk in the door, sit down at your table, and start eating your dinner any time they wanted! Networks need similar gatekeeping. This is the work a LAN performs for you.

When you set up a router for your home and use your ISP to connect to the internet, you're setting up a LAN. When you enter a wifi password at a coffee shop, you're entering the front door of the shop's LAN. Once inside, you can access special resources or access the wider world of the internet.

Wide area networks (WANs). The internet is what is called a wide area network (WAN). As with PANs and LANs, a WAN mainly refers to how far distance-wise the network extends. WANs can be just as secure as LANs but cover a much wider geographic area. The internet happens to be a public WAN that covers the world (and now, even space). The internet is considered an **open** WAN because devices don't need permission to access it. LANs, PANs, and WANs that require security credentials to access them are considered **closed** networks.

While closed WANs exist, they can get quite expensive because they require a secure way to transmit data between disparate and broad geographic areas. Building transmission lines that a single company will use, for example, is not feasible for many. But what if a company needs the security of a LAN but to allow people from all over the world to access their network. That requires special technology.

Question 1:

If you tried to get on the internet at home and it suddenly stopped working, what technology might you first troubleshoot to identify the issue?

The Bluetooth connection

The VPN

The MAC address

The router

Question 2:

If you wanted to transfer a picture of your friend to another friend who is sitting across the table at a restaurant with you, which type of network would be ideal for this?

VPN

WAN

PAN

LAN

Question 3:

Carol is a college student at a local community college. While on campus, Carol logs into the college wifi network.

When off campus, what remote network connection will Carol use to connect to the college's network?

WAN

PAN

LAN

VPN

Question 4:

What kind of network do you need set up in your home to keep an uninvited person from walking into your house, sitting down at the table, and connecting to the internet through your router?

WAN

LAN

PAN

VPN

Question 5:

How do routers play an essential role in getting data to where it needs to go?

Routers create connections called VPNs because they connect to the internet.

Routers use MAC addresses, which are given to devices at the factory, and IP addresses.

Routers use a small window as a part of a TV broadcast showing an interpreter signing.

Routers choose a path for and then transfer data between computers on a network.

Overview of how the internet functions as a network

Networks can be personal, local, or cover a wide geographic region. The type of network that covers a wide geographic region is called a **wide area network (WAN)**. The internet is a type of WAN. It consists of many computers distributed over geographic areas across the world that communicate. The internet is a really large number of individual computers connected by wires and radio waves communicating with one another.

The internet can seem almost invisible.

You send and receive text messages, emails, watch videos, get the weather report, and pay bills using the internet. You might think about the internet only when something isn't working properly.

A technology that makes it all work as a network is called the domain name system (DNS). The DNS is like a big address book that keeps track of names and addresses. For instance, when you browse to ibm.com, that web address is the name of IBM's network. An IP address is associated with that name. The DNS keeps track of which names go with which IP addresses so you just type "ibm.com" and not have to remember some obscure IP address.

Breaking up data: Packeting makes the internet work

TCP/IP handles data. Data is broken up into packets and sent over the internet in chunks and reassembled at the destination. The technology that enables this type of transmission is called **TCP/IP**. TCP stands for transmission control protocol. The IP in the name is the internet protocol.

Protocol. A protocol is a set of rules or a procedure for how something is be done. Technology professionals apply TCP/IP to ensure that the tools and technologies they're building work with other tools and technology being built for the internet.

The protocols define how data on a network is broken up, how it is transmitted from network to network, and the structure of packets. This basic information, which is called **metadata**, is essential for ensuring that all the data arrives at the proper destination and that the receiving end knows what to do with it. TCP/IP defines how all this is done.

Each packet of data that is sent and received is considered independent from the one that came before it and the one that will follow it. In fact, due to a number of factors, packets can arrive at a destination out of order! The packets themselves contain metadata that enables the routers on the receiving side to assemble the packets in the right order. Imagine what would happen if the router wasn't able to reassemble the data in the right order. You might see the end of a movie streamed over the internet before the beginning!

TCP/IP defines the language that networks use to talk to each other. But that language isn't very friendly for most humans. In fact, engineers who develop internet technology have created systems that make it easier for people who aren't technicians to use.

The domain name system (DNS): The big address book

One technology that makes the internet more user friendly is the **domain name system (DNS)**. The DNS matches domain names with IP addresses. The most common IP

address has a very specific structure. It consists of four sets of numbers separated by a period or dot. An example of an IP address is 192.168.1.1.

What's in an IP address?

In this example IP address, there are two key parts: 192.168.1.1.

Network address

192.168.1.1

The first key part of the IP address is the network ID.

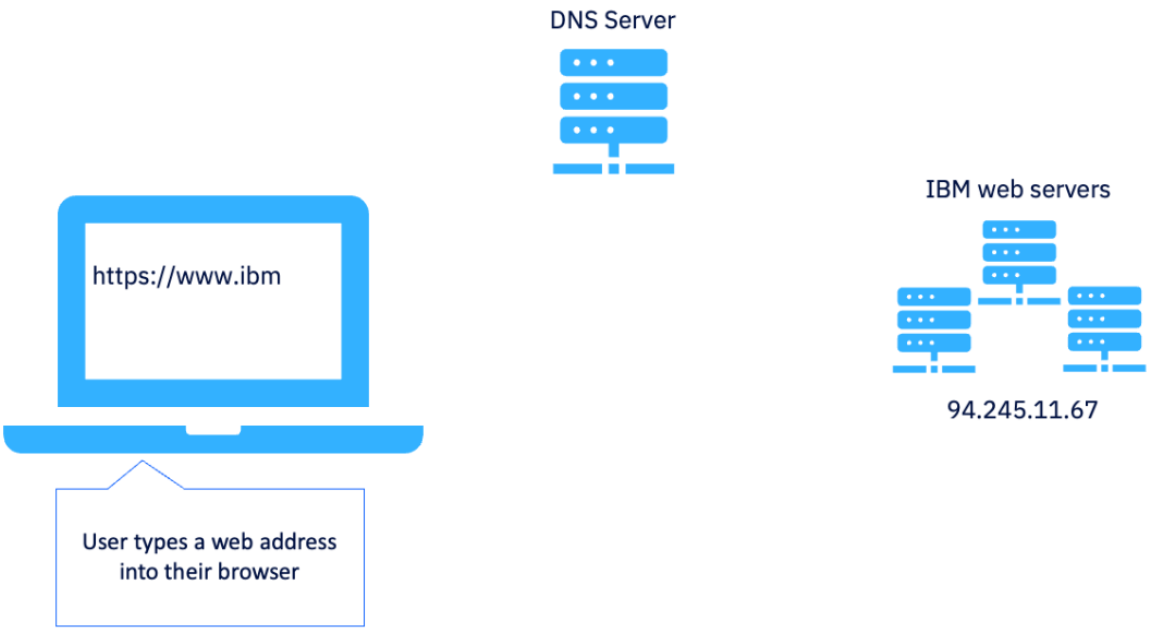
Host address

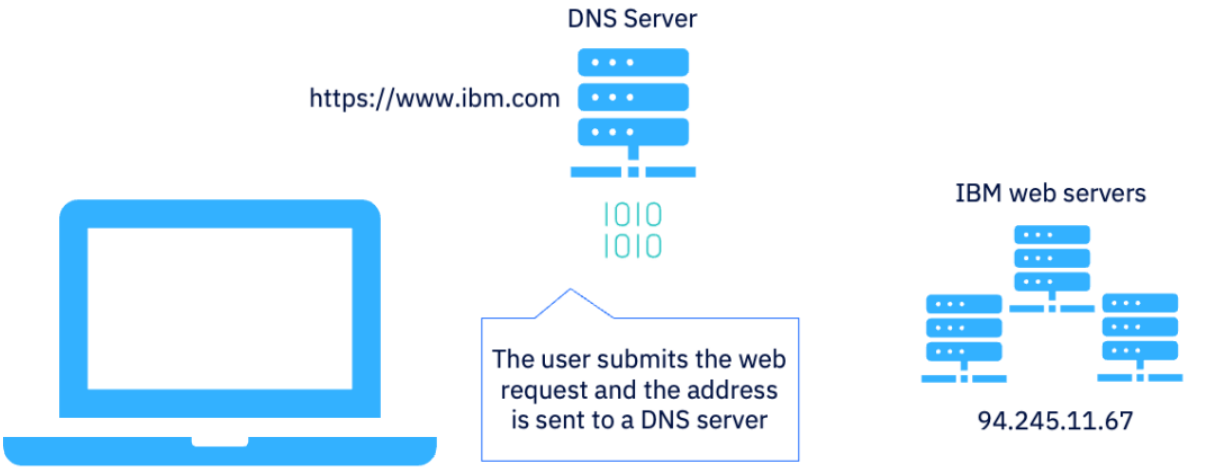
192.168.1.1

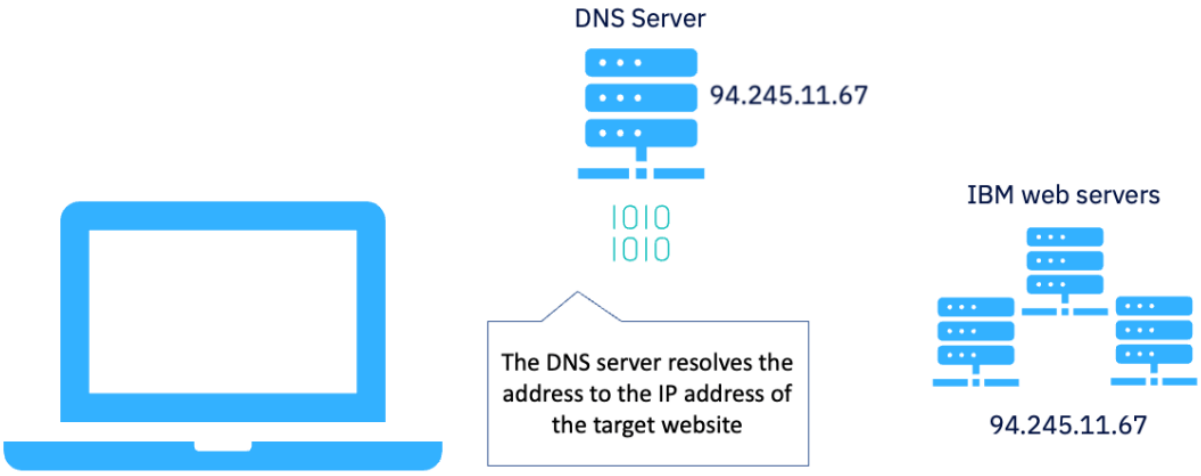
The second key part of the IP address is the host ID.

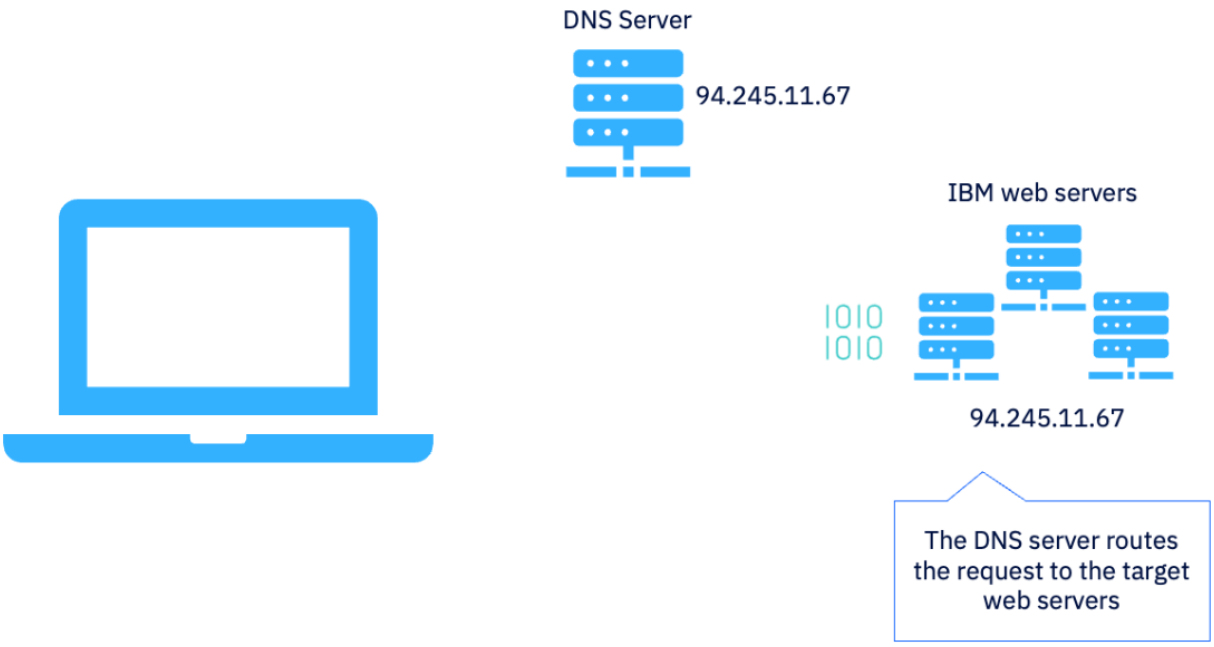
While networks know what to do with that set of numbers, to humans it doesn't mean much. Every place on the internet is located by an IP address. Imagine how inconvenient it would be if in order to visit your favorite social media site like Twitter or Facebook, you had to memorize its IP address and type that in your browser!

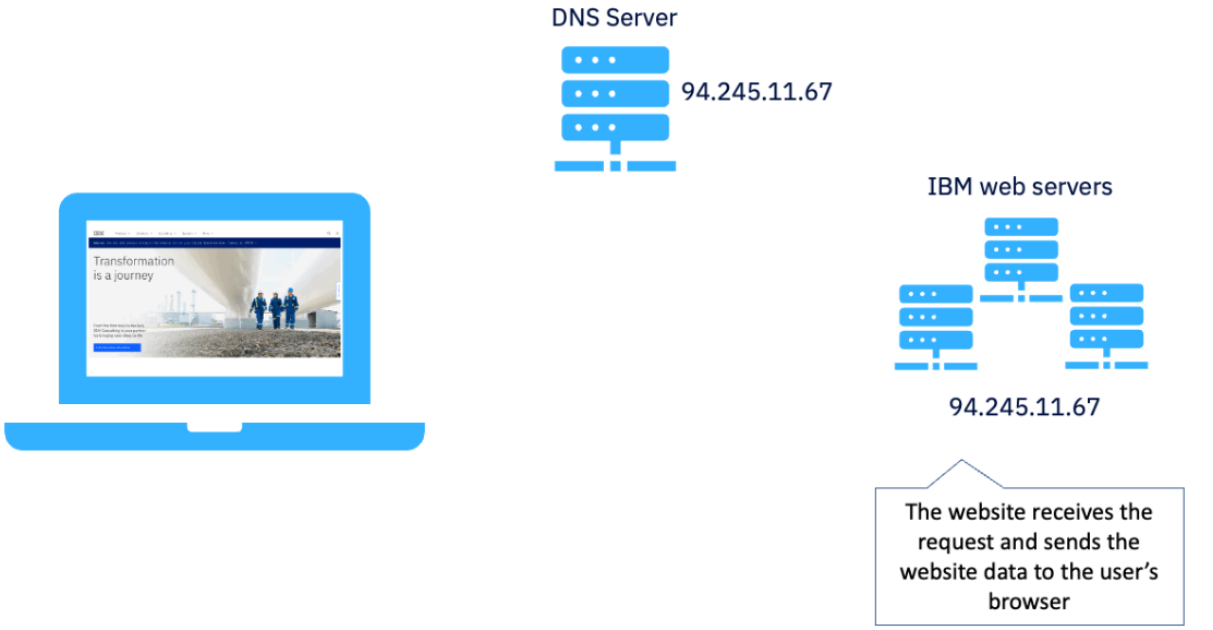
View the following animation to see how the DNS works to find the right address. When the user provides a web address in their browser, the DNS Server receives a request, resolves the IP address, and routes the request to the target web servers. The web servers send the web page to the user's browser.




DNS Server
https://www.ibm.com
1010
1010
IBM web servers
The user submits the web request and the address is sent to a DNS server
94.245.11.67


DNS Server
94.245.11.67
1010
1010
IBM web servers
The DNS server resolves the address to the IP address of the target website
94.245.11.67





Domain names enable you to find places on the internet using friendly natural language names. Consider a domain name like www.ibm.com. This address identifies three domains separated by the dots. The label, com, signifies the top-level domain and is one that many addresses share. The second section, ibm, is considered a subdomain of com. The combination of the subdomain ibm with com creates a unique domain name since only IBM, the company, can use it. The third section, www, is another label

and is a subdomain of ibm.com. A **hostname** refers to domains combined with subdomains that have an IP address associated with them.

Domain name. A domain name refers to the location of a website on the internet.

Hostname. A hostname is the name of the device on the network.

You can think of this system like street addresses in a city. If a friend tells you they live at 123 Cactus Avenue, you can consider avenue as a type of domain (all the streets that are avenues) and a designation that many streets in a city share. The label cactus is for a particular street. The combination of cactus and avenue makes a unique location in a city. While the city might also have a Cactus Lane or a Cactus Boulevard, there can be only one Cactus Avenue in a particular city (which also is a domain). If your friend's house was the only one on Cactus Avenue, they might just say they live on Cactus Avenue. But they say they live at 123 Cactus Ave because there are other houses on that street.

The DNS keeps track of which of these hostnames are associated with which IP addresses. When you type a hostname into your browser, DNS tells your browser which IP address to go to in order to find the right location. All the networking technology does its magic and you are able to get to the website you want.

Common domain types and their meanings

Are you familiar with these common domain types?

Domain type	Meaning
.com	Company
.net	Network
.edu	Education
.org	Organization
.gov	Government
.info	Information

Question 1:

Instead of memorizing a long string of numbers for a web address, what system helps you visit a website without using numbers?

The DNS

The internet

The natural-language address

The IP address

Question 2:

A text message sent from one device in India to another device in Canada travels through a wide digital network.

What is that network called?

Transmission control protocol/internet protocol (TCP/IP)

Packets

The DNS

The internet

Question 3:

The streaming show you are watching spoils the big ending for the series by playing Episode 12 before Episode 11.

What protocol would have helped avoid this issue?

Technology professionals

WAN

TCP/IP

The internet

Question 4:

You are researching advances in artificial intelligence (AI) technology, and you visit the web domain www.ibm.com to find out more about IBM Watson.

The label "ibm" in www.ibm.com designates which type of domain?

Subdomain

Domain name system (DNS)

Top-level domain

IP address

Question 5:

A student taking an online course has a question about one of the lessons. The student writes an email to ask a question, attaches a screenshot of their homework, and sends the email to the instructor.

How does TCP/IP ensure that all of the data arrives and is in the right order?

The internet handles large networks like personal area networks (PANs), local area networks (LANs), and wide area networks (WANs), and can be distributed over geographic areas across the world.

TCP/IP defines the language that networks use to talk to each other.

The DNS keeps track of which names go with which IP addresses so you can just type a domain name in natural language and not have to remember some obscure IP address.

The TCP/IP protocols define how data on a network should be broken up, how it should be transmitted from network to network, and how the contents should be structured.

Network security

Hardware security: Keeping routers, modems, and network adapters safe

Safety in a connected world has become a priority for technologists and users alike. From identity theft to lost revenue, the human toll of data breaches and cyberattacks is enormous.

The average cost to a business for a data breach alone is USD 4.25 million in 2022.

When you hear the term **cybersecurity**, you might immediately think of creating stronger passwords and blocking phishing attacks. These are important. For an IT professional, cybersecurity has to be holistic. This means securing network hardware as well as the software people use to access networks.

Routers and modems can be secured in several ways.

First, the physical devices need to be secured—particularly in environments where many people might access the hardware. Security cameras, cages with locks, and even a door with a lock or a passcode can prevent unauthorized individuals from accessing and installing malware onto a router or modem. Wireless modems, which tend to function better in open spaces, can be made more secure by installing them in hard-to-reach places.

Hardware like routers and modems have a type of operating system called firmware. The firmware controls how the hardware operates and also includes user interface controls to enable technicians to modify how the hardware works. Keeping firmware up to date can help plug security holes and help the hardware perform better to prevent certain types of attacks like denial of service attacks. Using a strong password and the https protocol when accessing routers and modems remotely is another way to keep your network hardware safe.

Unfortunately, many modern security breaches don't happen at the hardware layer. Many attacks happen when people are using the network. But there are several ways to keep yourself safe online.

System security: Passwords and two-factor authentication

How many times have you tried to log into a website and forgotten your password? You have to select the "Forgot password" link and wait for email to reset your password to another one that you hope you'll remember next time.

Passwords have a bad reputation, but they can prevent devastating security breaches. IT professionals sometimes complain about passwords because users tend to create weak ones which open systems up to attack. Users dislike passwords because strong ones can be hard to remember and there tend to be a lot of them to remember.

Using a password manager can solve both problems. Your browser might even have a built-in password manager. Password managers save the many passwords you create. They also will generate strong passwords so that you don't have to come up with them on your own. IT professionals can save themselves and their users a lot of headaches by educating users on (and where appropriate, requiring users to use) password managers.

Password manager. A password manager is a software program for managing, creating, storing, and updating your passwords. A password manager helps you to log in to websites securely.

Two-factor authentication complements password management. A technology that has become commonplace that supplements the tried-and-true password is **two-factor**

authentication (2FA). Two-factor authentication requires that people enter a code, pick an answer from a list, respond to a phone call, or answer a question in order to confirm their identity. This technology helps bolster the strength of usernames and passwords by requiring another form of identity verification.

You probably protect your mobile phone as much as if not more than your wallet. Perhaps you carry your mobile phone at all times. Mobile phones can be deeply personal and individualized. Technologists have recognized this and leveraged mobile devices for security. Two-factor authentication using a mobile device requires that you enter a code sent to your mobile device to confirm your identity. Other implementations use an application on a mobile device that creates a new code every minute, which you must copy and use to confirm your identity in another application.

Regardless of the form it takes, security with passwords and two-factor authentication might seem difficult, but that costs you far less than the impact of lost data, a stolen identity, or financial loss due to a security breach.

Defensive browsing: Ways to stay safe online

Responding to attack vectors. When it comes to online attacks, there are a number of ways—attack vectors—that **threat actors** can attack you or your organization.

Threat actor. A threat actor is someone like a cybercriminal or an organization that is responsible for a threat or malicious impact on the security of an organization or an individual system user.

IT professionals can educate individuals and organizations about staying safe online. Here are some strategies you can use every day to stay safer online. Besides keeping you safer, practicing these strategies can give you background knowledge so you can better help your customers and users.

Email

Spam is unwanted email that wants to sell you things that you don’t need. More nefarious emails come in the form of **phishing** attacks. These types of emails try to make you select a link, call a number, or download a file in order to extract personal information. This information can then be used for bad ends.

An IT professional can warn you to avoid links from sources you don’t know and never to download a file from a source you’re unfamiliar with.

Heuristics

Email tools offer heuristics to help users determine the source of the email. Phishers will disguise an email by using a false name as the sender so it appears to be from a

legitimate source. You hover over or select the sender's name to reveal the actual sender's email address.

For example, if you get an email that appears to be from IBM Support, you can hover over the sender's address. If it shows a personal email address or a non-IBM address, you will be able to tell the email is not actually from IBM support and assume it is a scam.

Browsing

Like email tools, browsers provide ways for you to verify legitimate links. You hover over a link on a web page to see the actual target link in the status bar at the bottom or in a popup over the link. If the link name indicates the target links to a completely different site, you would be unwise to trust it.

Be cautious with any links that don't use the **https** protocol. Your browsers will warn you when a site is unsecure and can prevent you from automatically visiting the site.

Digital awareness

Trust but verify. You might experience many circumstances where the safety of the information you are presented with is unclear. For example, you might get an email from what appears to be your insurance provider. Since you might not get a lot of emails from this source, you might be unsure that the email is valid.

In cases like these, you would do well to verify the information independently. Instead of trusting the email and selecting a link or calling a number in the email, you can browse to your insurance provider's website, log in to your account, and verify the information in the email. You can find the provider's phone number on their website and call that number rather than the number in the email, which is another good way to trust but verify.

Question 1:

In addition to using a password manager, what is another way to make your network software more secure?

Always carry your mobile phone with you.

Ask an IT professional to educate you on how to stay safe online.

Make sure your router firmware is up to date.

Hover over links to make sure they are secure.

Question 2:

Which of the following is an example of two-factor authentication?

Using a phone to receive a verification code

Being asked to fill out a form with your name and address

Use a password manager to solve your problems

Hovering over a link to determine its target

Question 3:

After you have entered your username and your password to log in to a site, you are prompted to enter a code that has been sent to your mobile device.

What is this process called?

Responding to attack vectors

Passwords

Legitimate browser links and HTTPS

Two-factor authentication (2FA)

Question 4:

Which of the following are ways that you can stay safe using a networked device?

Select the two that apply.

- Take a defensive approach to your digital interactions.
- Be aware of your digital surroundings.
- Prevent certain types of attacks like denial of service attacks.
- Bolster the strength of your usernames.

Question 5:

Which of the following is a good way to keep your network hardware secure?

Use a false email name so it appears to be legitimate.

Use a strong password and the https protocol.

There's nothing you can do.

Install your wireless modem in hard-to-reach places.

Network identity

Hardware identity: The media access control (MAC) address

Suppose you want to call a friend in another country. That friend gives you their country code and their phone number. To reach your friend, you simply dial the number with the country code and—out of the billions of phones in the world—theirs will ring. Your friend's phone identification is unique and allows you to reach them simply by dialing a number.

All hardware has a special identification (ID) called a **media access control (MAC) address.** MAC addresses are used to uniquely identify hardware. They are assigned at the factory where the device is manufactured. An interesting fact about MAC addresses is that they (at least theoretically) are unique for every piece of hardware that has ever been created. New products won't share a MAC address with any other products, even ones that get recycled or end up in landfills. The device you're using to take this course has a MAC address that no other device has or will share!

It's a good thing that devices have unique MAC addresses because without them, the data that travels around the internet might not be able to find the right place.

Internet protocol (IP) addresses give computers identity on networks

An IP address is an ID that a router or server assigns to a given device.

This address, along with a MAC address, is how networks find devices. A router on a home network assigns every device that joins it a unique IP address. But IP addresses don't have to be unique in the same way MAC addresses have to be unique.

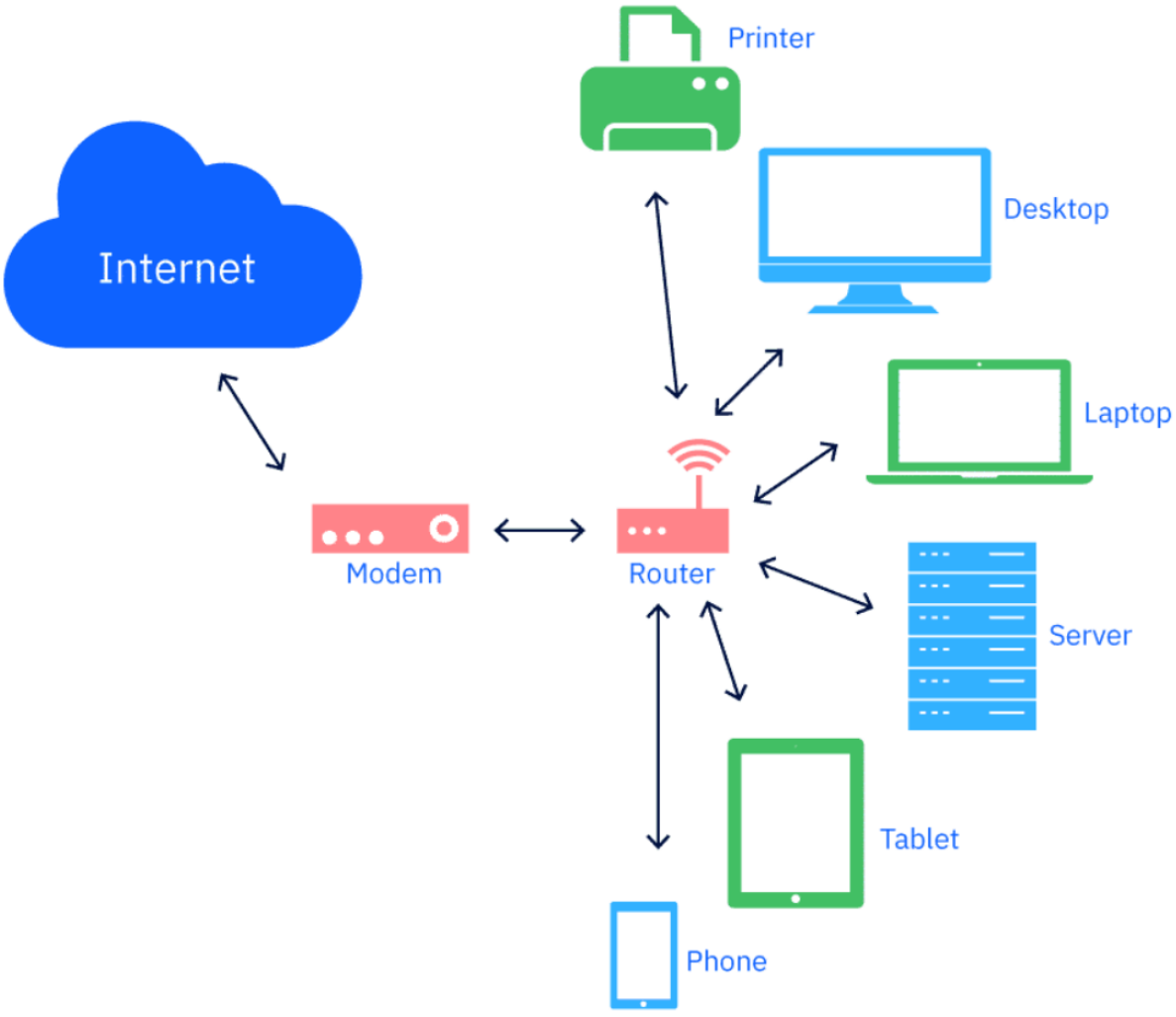
Suppose that a friend's home network has 10 devices connected to it. Each device has a unique IP address for that network. Your friend looks up the IP address for one of the devices (something that they can do from a terminal window or the router's software) and discovers that the device's IP address is 192.168.1.10. You look at all the devices on your home network and discover that you have a device with 192.168.1.10, too. How is this possible? How do two devices on separate networks share an IP address and still get the data they need from the internet?

Routers use subnets. Those devices that share the same IP address are invisible to all other devices outside of your home network. Your router faces in toward your network providing IP addresses for each of your devices. Your network is called a **subnet** because it's a network that is inside another network (the internet).

Subnet. A subnet is an address for a network within a network. The subnet helps your router to sort and send information to its destination.

But your router also faces out toward the internet. Your internet service provider (ISP) provides your router with an IP address, which is unique. So when data is sent to a device on your home network, it gets routed first to your router and your router then sends it to the proper device.

The following diagram shows a network with the router faces in toward six devices and out toward the modem, which communicates with the internet. Notice how the router communicates with the modem and each of the devices.



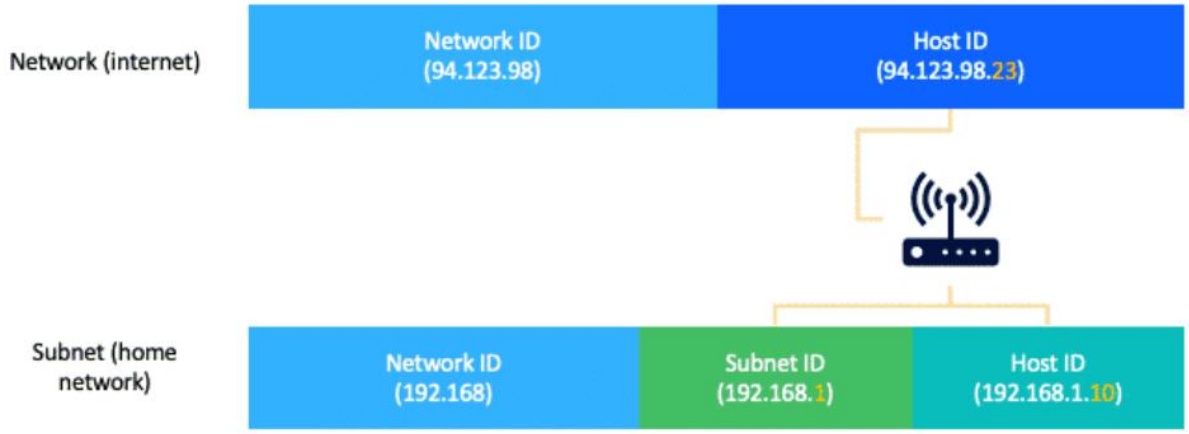
Your friend's devices work the same way. Their router faces in, which provides their subnet addresses. Their router also faces out to the internet with a unique IP address.

So how can two devices on separate networks share an IP address and still get the data they need from the internet? This is because your device and your friend's device are both isolated behind your own routers on your own individual subnets. While the IP address of each of your routers needs to be unique, devices isolated on different subnets can, coincidentally, be assigned the same IP addresses.

In the following diagram, you can see the subnet for your home network that your router has created.

- Data is sent from the internet to your router, which is assigned a unique IP address.

- Your router creates a subnet for your home network.
- Your subnet ID is 192.168.1.
- Each device within your subnet gets an IP address, also called the host ID, based off of your subnet ID.
- The last number in the IP address is how the subnet identifies each device.
- The IP address for your specific device is 192.168.1.10.



Question 1:

How do two devices on separate networks have the same IP address and still get the data they need from the internet?

> Two devices on separate networks do not have the same IP address because each IP address is universally unique.
>
> IP addresses don't have to be unique in the same way MAC addresses have to be unique.

You can identify your IP address from a terminal window or the router's software.

Your router provides an IP address for each device in your subnet, which is unique only within your personal network.

Question 2:

Complete the sentence. Your router is assigned a MAC address. To send and receive messages from the internet it must also have _____.

an IP address

a modem

a password

a domain server name

Question 3:

Which of the following is correct about MAC addresses?

A MAC address routes your data to a unique subnet address.

A network can have 10 devices connected to it.

Using a MAC address is as simple as remembering a phone number.

A MAC address uniquely identifies hardware.

Question 4:

Complete the sentence. A network that is inside another network is called a _____.

subnet

data

denial of service

MAC address

Question 5:

True or false? An IP address and a MAC address share the same address even if they are on different networks.

True

False

Technical scanning

Introduction

In this module, you'll learn about technical scanning techniques and why attackers use them. You'll explore how threat actors use scanning during the reconnaissance, or information gathering, stage of an attack.

Learning objectives

After completing this module, you should be able to:

- Explain the purpose of and information provided by typical technical scanning techniques
- Perform network reconnaissance by using network scanning tools

Why technical scanning?

Technical scanning techniques play an essential part in an organization's network administration and analysis. Think about how attackers collect information about computers and networks. While investigating a target device on a network, an attacker might want to learn more about the device's technical configuration. They might try to find out information such as the following:

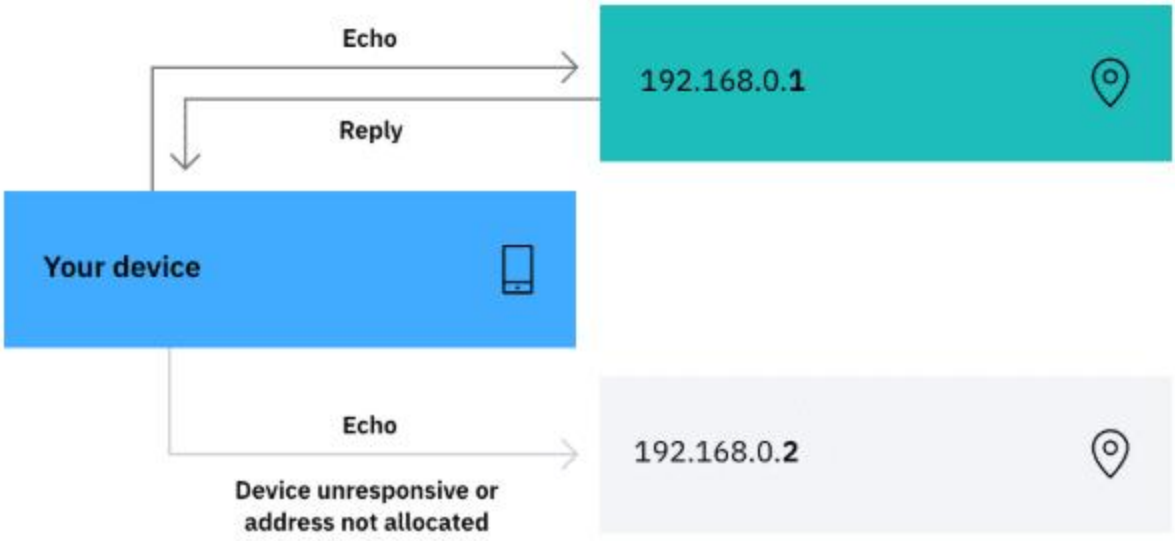
- What operating system is in use?
- What services are running on the device?
- Are any of the services vulnerable to well-known exploits?

Let's explore some typical technical scanning techniques.

- Ping test
- Traceroute
- Port scanning
- Vulnerability scanning
- Search engine for the internet
- Network scanning

Ping test

How does it work?



This diagram shows a phone pinging two IP addresses on its local network and waiting for a response.

A **ping test** measures the time that it takes for a packet to travel from one device or server to another. A **packet**, or ping, is a small amount of formatted data analogous to the digital version of a postcard.

In a ping test, a scanning device sends an Internet Control Message Protocol (ICMP) packet to the target device's Internet Protocol (IP) address. This outbound packet is called an **echo request** packet. If the target device replies with an **echo reply** packet, then the scanning device knows that the target device is most likely active and switched on.

What does it provide?

A ping test indicates if a machine is responsive and when repeated in a sweep, how many devices are on a network.

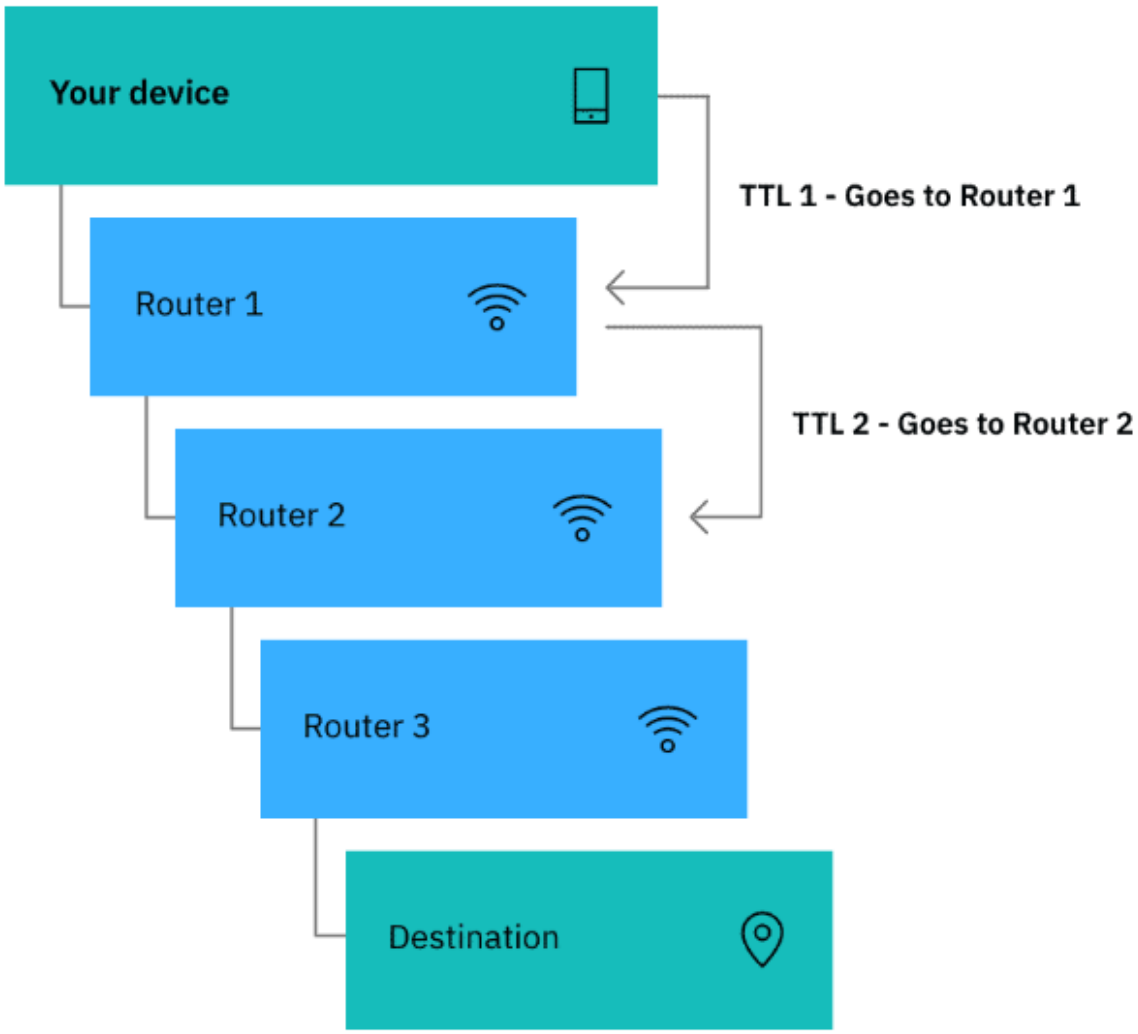
Organizations often use a ping test to debug networking issues. It identifies a device's status. It also indicates how "far" into a network the device is located using a property known as a packet's **time to live (TTL)**. Every router that forwards the packet onwards decreases the time to live by one.

Example

Consider a packet that starts with a TTL of 120. If it reaches the destination with 108 left, then it has gone through 12 stages. You can use this feature in the next scan. On Windows, you can run a ping test from the command prompt by using the following command: **ping target_name**.

Traceroute

How does it work?



This diagram shows a device mapping out its connection between itself and a destination address. A physical analogy for this process is skimming a series of stones on a lake with increasing hops each time.

Traceroute is another network diagnostic tool. When you run a traceroute, the scanning device sends packets to the target device. These packets have either increasing or decreasing TTLs. When a packet is in transit, and its TTL decreases to zero, the device processing the packet sends back an error message to the scanning device indicating that the packet didn't reach its destination.

What does it provide?

You can use a traceroute test to map a network and determine how many routers and switches exist between you and your destination. A router is a network's hardware connection to the internet. A switch integrates all the devices on a network, including the router, allowing for seamless sharing and data transfer among them.

Example

Imagine a target is 12 hops away. If you send a packet with a TTL of 11 toward the target, the packet will fail at the final routing step. The scanning device will receive an error message packet, and this message will reveal the IP address of the device 11 steps away. As the TTL is reduced to one over a few new tests, the traceroute command produces a complete list of the network nodes between the scanner and the target. On Windows, you can run a traceroute by using the following command: **tracert target_name**.

Port scanning

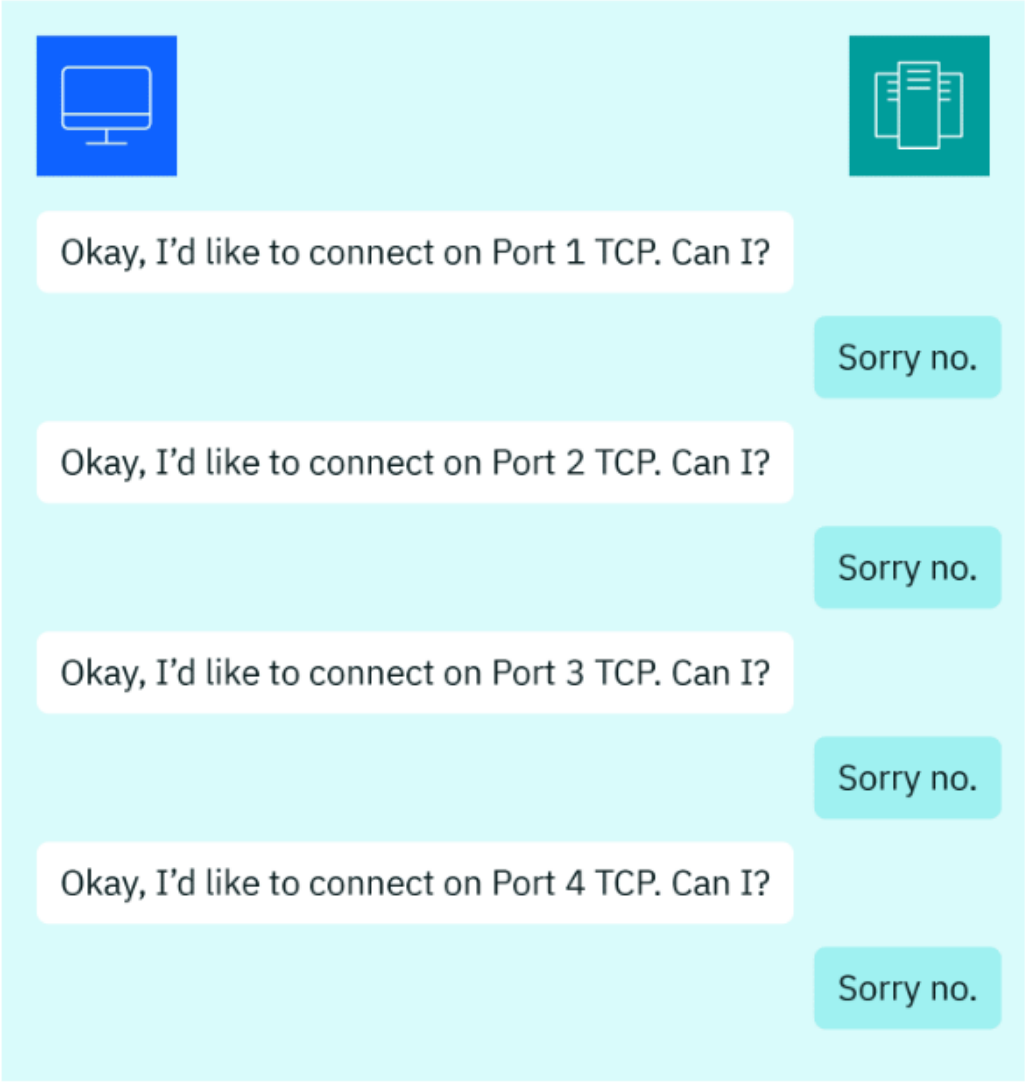
How does it work?

In networking, applications are accessible externally through services on digital ports. A port is a connection point that sends or receives data for a specific network service, such as email. Each port is assigned a number in the **Transmission Control Protocol (TCP)**, a collection of internet protocols that make it possible to create and maintain communication between internet-connected devices. Each port is also associated with an IP address. The relationship between IP addresses and ports is like that between a building and its floors: an IP address is like a building, and port numbers are like different floors in that building.

The usual goal of port scanning is to identify a host's open ports.

- A **host** is a device, such as a server, workstation, laptop, or other smart device, that can communicate with other devices on a network and grant access to devices outside the network.
- An **open** port is one that accepts a connection. Given that a port number is like a floor in a building, an open port is like a floor that you can access through an open door.

Attackers want to find and exploit open ports on hosts. Conversely, network administrators want to close or block these ports while ensuring that legitimate users still have access.



This diagram depicts a port scanner scanning a server. The scanner tests one port at a time to determine if a specific service is available on the port. However, each port rejects the connection, meaning it's a closed port.

The scanner reports that a port is **closed** if the port rejects the connection or **filtered** if the host gives no response to the scan. No response can mean that a package filter, a type of firewall, is blocking access to the port.

What does it provide?

By working through the list of a host's well-known ports, a scanner can often determine what the host's owner uses the device for. The TCP contains 65,536 ports. TCP ports 0 through 1,023 are called **well-known ports**: each has a specific service associated with it, and this association is internationally recognized. Some ports from 1,024 through 49,151 might also have officially registered uses of interest.

Example

HTTP web activity always occurs on TCP port 80. If a scan reveals that port 80 is open, the investigator knows that some web-based application might be using it. For another example, Windows file sharing occurs on TCP port 445. If attackers know this port is open, they might try to exploit it with malware. Famous ransomware attacks, such as the WannaCry attacks, have targeted this port.

A notable port outside the list of well-known ports is TCP port 3389, the default port for the Microsoft Remote Desktop Protocol (RDP). If attackers know this port is open and available, they can try to hack the remote desktop software.

Vulnerability scanning

How does it work?

Another form of testing is vulnerability scanning. One of its features is **dynamic scanning**, which simulates hacking techniques, such as SQL injection, to discover vulnerabilities to exploit.

Other standard vulnerability scanning techniques include version and OS detection:

- **Version detection** reveals the version numbers of software, such as Apache web server, running on the host
- **OS detection** reveals the device's OS, such as macOS.

What does it provide?

Vulnerability scanning is a powerful tool for both organizations to identify vulnerabilities in their network and for attackers to find potential victims. Some organizations run such scans periodically to identify mistakes that need remediation.

Example

A scanner might attempt to connect to a server and check if it is running an outdated version of an application. If the application is out-of-date with a known vulnerability, then the scanner might attempt to exploit the vulnerability to confirm its existence and report this finding.

Important note

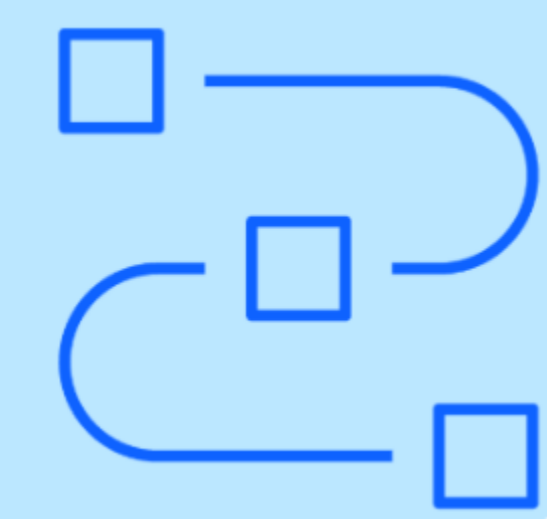
Please be aware that dynamic scanning might automatically perform actions considered illegal in some countries. Scan a target only if the owner has given consent. A network vulnerability scan will often be interpreted as the planning stage of an attack.

Network scanning

Network scans collect information about a network by targeting a host. Network and systems administrators rely on network scans to assess the status and security of their organization's network. Unfortunately, cyberattackers can use these same tools for malicious purposes.

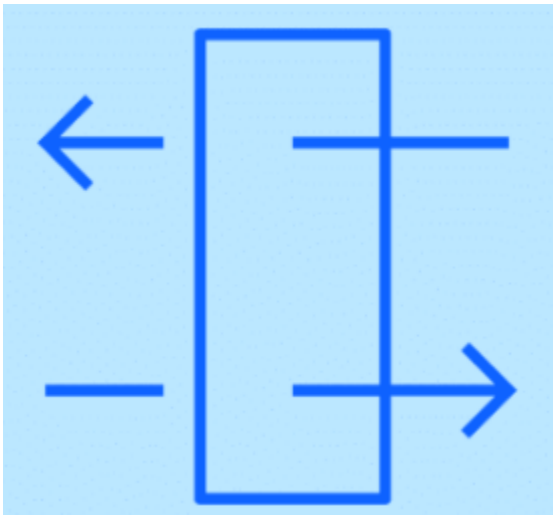
Many network scanning applications exist, but the most well-known scanner is Nmap.

Nmap(opens in a new tab), short for Network Mapper, is a free, open-source network scanner available for Windows, macOS, Linux, and other OSs. Though port scanning is its core feature, Nmap provides other valuable features for investigating networks.



It can reveal the network path from the scanning device to the host, including all other hosts encountered along the way.

It can perform version and OS detection.



It can even identify firewalls in use.

Nmap is a command-line program, but most versions also include Zenmap, the official graphical user interface (GUI) of Nmap. Zenmap(opens in a new tab) makes learning Nmap easier for beginners. With Nmap, you must determine the precise command needed to perform your scan, and the number of options and syntactic requirements can make this challenging. But with Zenmap, you can simply select choices from a user-friendly interface to customize your scan. And if you still want to learn Nmap's command-line options, Zenmap displays the actual Nmap command and options behind your scan.

AI in technical scanning

Artificial intelligence (AI) has become valuable for network scanning. With machine learning (ML) algorithms, network scanners can perform deeper, more helpful analysis.

- Scanners can independently analyze and categorize network vulnerabilities.
- Scanners can prioritize vulnerabilities based on their severity.
- Scanners can learn from past scans and identify patterns and trends to anticipate future threats.

AI can also streamline the scanning process. It can reduce the time needed to scrutinize large networks and reduce the possibility of human error.

An example of an AI-driven network scanning tool is IBM's QRadar® Advisor with Watson™ application. It analyzes security incidents, identifies potential threats, and provides actionable insights. QRadar Advisor uses ML and AI to sift through vast amounts of data, investigating offenses and eliminating false positives. As a result, analysts are free to focus on confirmed threats, optimizing their time and resources.

Cloud security

Cloud services are a tempting target for malicious attackers because there is so much sensitive data store in the cloud.

The collection of practices, technologies and policies designed to make using cloud services safer.

The main goal is to ensure the confidentiality, integrity and availability of cloud-based resources.

Access control. Both onsite and cloud environments need to control access to network resources. However, a cloud environment allows multiple users and applications in different locations to access shared resources, so there's more risks of unauthorized access. In some configurations, cloud environments expose users to more risk of account hijacking to more risk of account hijacking. Attackers might steal could credentials through phishing or brute force attacks, which can provide them with access to an extensive array of resources and information. It's more difficult to protect data that's stored in multiple location. Theis common configuration increases the challenge of securing data in transit as well. Any vulnerability in these system configurations' access control or other measures can result in a compromised system and a dangerous expensive data breach.

Cloud service providers are responsible for managing and maintaining physical and virtual infrastructure and availability of their could services. They also are responsible for implementing network security, data encryption, access restrictions and other security controls in the could environment. So it's important for companies to choose providers carefully. Cloud security is a shared responsibility between the cloud service provider or (CSP), the client company and the cloud user. Companies must create sound security policies and procedures, and users must follow them.

Industry standards: basics of NIST, ISO 27001, SOC 2, GDPR.

NIST (National Institute of Standards and Technology)

- A U.S. agency that publishes widely used cybersecurity frameworks (e.g., NIST Cybersecurity Framework, NIST SP 800-53).
- Focuses on risk management, security controls, and best practices for federal and private organizations.

ISO/IEC 27001

- An international standard for Information Security Management Systems (ISMS).
- Provides a framework for managing sensitive information and continuously improving security practices.
- Certifiable — organizations can get ISO 27001 certified to demonstrate compliance.

SOC 2 (System and Organization Controls 2)

- A U.S. auditing standard for service providers handling customer data, developed by AICPA.
- Focuses on five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.
- Reports provide assurance to clients about how their data is managed.

GDPR (General Data Protection Regulation)

- The EU regulation for protecting personal data and privacy for EU citizens.
- Sets strict rules for how organizations collect, process, store, and share personal data.

- Enforces data subject rights and heavy penalties for non-compliance.

Techniques for Cybersecurity Sales

Why Cybersecurity Sales Is Unique

The cybersecurity market is growing fast but crowded with vendors.

Prospects face complex threats, new regulations, and budget limits — they need trusted advisors, not pushy sellers.

Sales must address both **technical** (features, integrations) and **business** (risk, compliance, ROI) needs.

Example: A company may ask, *"How does your solution help us meet GDPR or NIST CSF?"* — you must be ready.Must-Have Skills for Cybersecurity Sales

Technical Literacy

- Know basic security terms: firewalls, IDS/IPS, SIEM, endpoint protection, zero trust, cloud security.
- Understand common frameworks: NIST, ISO 27001, SOC 2, GDPR — this builds trust with CISOs.

Consultative Selling

- Ask discovery questions to uncover real pain points.
- Tailor solutions instead of "one-size-fits-all."
- Be ready to bring in technical experts when needed.

Building Trust

- Share real success stories and case studies.
- Offer proof of concept (POC) or demos.
- Show you understand their risk profile and compliance needs.

Why Know These Terms?

Cybersecurity buyers are **technical and skeptical** — you must speak their language.

Basic fluency helps you:

- Ask better discovery questions
- Map product features to customer needs

- Build trust with CISOs and IT teams

You don’t need to be an engineer — just know the basics to bring in experts when needed

Effective Techniques & Strategies

Discovery & Qualification

- Who makes the buying decision? Who has budget?
- What are their biggest threats today?
- Any compliance audit coming up?
- How urgent is the risk?

Solution Mapping

- Connect product features to frameworks.
    - E.g., “Our solution supports NIST CSF Identify & Protect functions.”
- Position your solution as risk reduction and business enabler.

Business Value & ROI

- Show cost of a breach vs. cost of prevention.
- Use industry breach statistics to back up the pitch.
- Present clear ROI (Total Cost of Ownership, time savings).

Firewalls

What it is:

- A firewall is a network security device that controls traffic in and out of a network using defined security rules.

Why it matters:

- First line of defense to block unwanted access.
- Firewalls can be hardware or software — many companies have both.

Example Sales Tip:

- “Our solution integrates with your existing firewall to improve threat detection.”

IDS & IPS

IDS: Intrusion Detection System

- Monitors network or system activities for malicious actions.
- Sends alerts but doesn't block automatically.

IPS: Intrusion Prevention System

- Same detection plus automatic blocking of suspicious traffic.
- Often combined with firewalls.

Example Sales Tip:

- "We help you detect and block threats in real-time — like an IPS does for your network."

SIEM (Security Information and Event Management)

What it is:

- A SIEM collects and analyzes logs from multiple sources (firewalls, servers, apps) in one place.
- Correlates events, detects anomalies, and sends alerts.

Why it matters:

- Supports compliance (SOC 2, ISO 27001).
- Helps security teams respond faster.

Example Sales Tip:

- "Our solution feeds logs directly into your SIEM for centralized threat visibility."

Endpoint Protection

What it is:

- Security for individual devices: laptops, phones, servers.
- Includes antivirus, EDR (Endpoint Detection & Response), and device control.

Why it matters:

- Remote work = more endpoints = bigger attack surface.
- Common entry point for malware and ransomware.

Example Sales Tip:

- "Our tool extends protection down to each endpoint, closing common gaps."

Zero Trust

What it is:

- Security model: "Never trust, always verify."
- Every user and device must prove they are authorized — continuously.

Why it matters:

- Reduces impact of breaches.
- Popular with hybrid and remote environments.

Example Sales Tip:

- "We help you implement Zero Trust by enforcing strong authentication and least privilege access."

Cloud Security

What it is:

- Protecting workloads, data, and apps hosted on cloud platforms (AWS, Azure, GCP).

Key concerns:

- Misconfigurations, data leaks, unauthorized access.
- Shared responsibility model: customer + cloud provider.

Example Sales Tip:

- "Our solution helps you monitor cloud assets for compliance gaps and threats."

MFA (Multi-Factor Authentication)

What it is:

- Requires 2+ forms of verification: password + SMS code, or biometrics.

Why it matters:

- Prevents easy credential-based attacks.
- Often required for compliance (GDPR, SOC 2).

Example Sales Tip:

- "Our platform supports MFA to protect user accounts from breaches."

VPN (Virtual Private Network)

What it is:

- Creates a secure, encrypted tunnel for remote access.
- Hides user's IP and protects data in transit.

Why it matters:

- Common for remote work and site-to-site connections.

Example Sales Tip:

- "Our tool works seamlessly with your VPN to secure remote users."

DLP (Data Loss Prevention)

What it is:

- Prevents unauthorized sharing of sensitive data (e.g., credit cards, PII).

Why it matters:

- Helps avoid data breaches and fines.

Example Sales Tip:

- "We integrate with your DLP policies to ensure data stays secure."

SOC (Security Operations Center)

What it is:

- Team and technology that monitors, detects, investigates, and responds to incidents 24/7.

Why it matters:

- Many customers have an in-house or outsourced SOC.
- They need tools that generate actionable alerts — not noise.

Example Sales Tip:

- "We deliver clear, high-fidelity alerts that your SOC can act on immediately."

Staying Updated

Cyber threats change daily — continuous learning is critical.

Attend vendor-specific training & certifications.

Read threat intel reports (e.g., Verizon DBIR, Mandiant, SANS).

Engage with industry bodies: ISACA, ISC², ENISA, NIST.

Follow new laws and frameworks (GDPR updates, CCPA, ISO revisions).

Practical Sales Tips

Speak Their Language

- Use risk and compliance terms they care about: fines, downtime, reputational damage.
- Avoid too much jargon — balance technical depth with business relevance.

Leverage Demos & POCs

- Show exactly how your solution detects threats, responds, and reports.
- Address common objections in real time.

Stay Ethical & Compliant

- Respect customer privacy, don’t overpromise.
- Be transparent about limitations.
- Build long-term relationships, not quick wins.

Final

✅ Be a trusted advisor, not just a vendor.
✅ Know your product, customer needs, and the security landscape.
✅ Connect solutions to frameworks like NIST, ISO 27001, SOC 2, and GDPR.
✅ Keep learning — cybersecurity never stands still!

References

IBM Open e-Learning Ecosystem

Cybersecurity Fundamentals

Cyber Security Tutorial | Cyber Security Training For Beginners | CyberSecurity Course | Simplilearn

Cost of a Data Breach Report 2022(opens in a new tab)