Introduction to Cybersecurity

The introductory course for those who want to explore the world of cybersecurity.

Table of Contents

Welcome

When you were a child, did you ever imagine yourself as a Masterful Defender of the Universe — recognizing a threat, protecting the innocent, seeking out the evildoers, and bringing them to justice?

Did you know you can make a career out of that?

- Cybersecurity Guru
- Cybersecurity Forensic Expert
- Information Security Expert
- Ethical Hacker

All of these roles can be part of your work in the exciting, ever-changing, high-demand field of cybersecurity.

The Student Support page includes a link to the NetAcad Facebook page and our LinkedIn page. It also contains Additional Resources and Activities for each chapter.

Course Overview

As the course title states, the focus of this course is to explore the field of cybersecurity. In this course, you will do the following:

- Learn the basics of being safe online.
- Learn about different types of malware and attacks, and how organizations are protecting themselves against these attacks.
- Explore the career options in cybersecurity.

By the end of this course, you will be more aware of the importance of being safe online, the potential consequences of cyberattacks, and possible career options in cybersecurity.

Chapter 1: The Need for Cybersecurity

This chapter explains what cybersecurity is and why the demand for cybersecurity professionals is growing. It explains what your online identity and data is, where it is, and why it is of interest to cyber criminals.

This chapter also discusses what organizational data is, and why it must be protected. It discusses who the cyber attackers are and what they want. Cybersecurity professionals must have the same skills as the cyber attackers, but cybersecurity professionals must work within the bounds of the local, national and international law. Cybersecurity professionals must also use their skills ethically.

Also included in this chapter is content that briefly explains cyber warfare and why nations and governments need cybersecurity professionals to help protect their citizens and infrastructure.

Personal Data

What is Cybersecurity?

The connected electronic information network has become an integral part of our daily lives. All types of organizations, such as medical, financial, and education institutions, use this network to operate effectively. They utilize the network by collecting, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

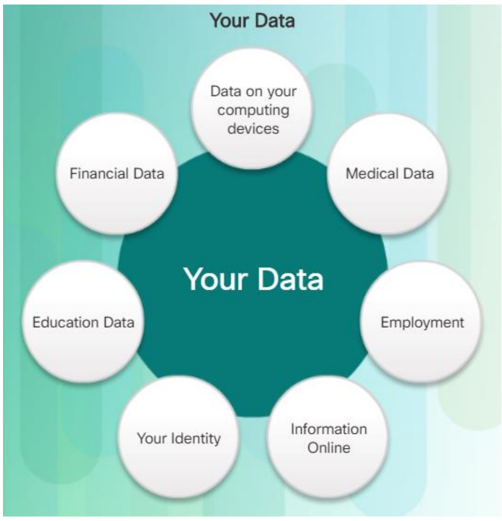
Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, you need to safeguard your identity, your data, and your computing devices. At the corporate level, it is everyone's responsibility to protect the organization's reputation, data, and customers. At the state level, national security, and the safety and well-being of the citizens are at stake.

Your Online and Offline Identity

As more time is spent online, your identity, both online and offline, can affect your life. Your offline identity is the person who your friends and family interact with on a daily basis at home, at school, or work. They know your personal information, such as your name, age, or where you live. Your online identity is who you are in cyberspace. Your online identity is how you present yourself to others online. This online identity should only reveal a limited amount of information about you.

You should take care when choosing a username or alias for your online identity. The username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.

Your Data



Any information about you can be considered to be your data. This personal information can uniquely identify you as an individual. This data includes the pictures and messages that you exchange with your family and friends online. Other information, such as name, social security number, date and place of birth, or mother's maiden name, is known by you and used to identify you. Information such as medical, educational, financial, and employment information, can also be used to identify you online.

Medical Records

Every time you go to the doctor's office, more information is added to your electronic health records (EHRs). The prescription from your family doctor becomes part of your EHR. Your EHR includes your physical health, mental health, and other personal information that may not be medically-related. For example, if you had counseling as a child when there were major changes in the family, this will be somewhere in your medical records. Besides your medical history and personal information, the EHR may also include information about your family.

Medical devices, such as fitness bands, use the cloud platform to enable wireless transfer, storage and display of clinical data like heart rates, blood pressures and blood sugars. These devices can generate an enormous amount of clinical data that could become part of your medical records.

Education Records

As you progress through your education, information about your grades and test scores, your attendance, courses taken, awards and degrees rewarded, and any disciplinary reports may be in your education record. This record may also include contact information, health and immunization records, and special education records including individualized education programs (IEPs).

Employment and Financial Records

Your financial record may include information about your income and expenditures. Tax records could include paycheck stubs, credit card statements, your credit rating and other banking information. Your employment information can include your past employment and your performance.

Where is Your Data?

All of this information is about you. There are different laws that protect your privacy and data in your country. But do you know where your data is?

When you are at the doctor's office, the conversation you have with the doctor is recorded in your medical chart. For billing purposes, this information may be shared with the insurance company to ensure appropriate billing and quality. Now, a part of your medical record for the visit is also at the insurance company.

The store loyalty cards maybe a convenient way to save money for your purchases. However, the store is compiling a profile of your purchases and using that information for its own use. The profile shows a buyer purchases a certain brand and flavor of toothpaste regularly. The store uses this information to target the buyer with special offers from the marketing partner. By using the loyalty card, the store and the marketing partner have a profile for the purchasing behavior of a customer.

When you share your pictures online with your friends, do you know who may have a copy of the pictures? Copies of the pictures are on your own devices. Your friends may have copies of those pictures downloaded onto their devices. If the pictures are shared publicly, strangers may have copies of them, too. They could download those pictures or take screenshots of those pictures. Because the pictures were posted online, they are also saved on servers located in different parts of the world. Now the pictures are no longer only found on your computing devices.

Our Computing Devices

Your computing devices do not just store your data. Now these devices have become the portal to your data and generate information about you.

Unless you have chosen to receive paper statements for all of your accounts, you use your computing devices to access the data. If you want a digital copy of the most recent credit card statement, you use your computing devices to access the website of the credit card issuer. If you want to pay your credit card bill online, you access the website of your bank to transfer the funds using your computing devices. Besides allowing you to access your information, the computing devices can also generate information about you.

With all this information about you available online, your personal data has become profitable to hackers.

They Want Your Money

If you have anything of value, the criminals want it.

Your online credentials are valuable. These credentials give the thieves access to your accounts. You may think the frequent flyer miles you have earned are not valuable to cybercriminals. Think again. After approximately 10,000 American Airlines and United accounts were hacked, cybercriminals booked free flights and upgrades using these stolen credentials. Even though the frequent flyer miles were returned to the customers by the airlines, this demonstrates the value of login credentials. A criminal could also take advantage of your relationships. They could access your online accounts and your reputation to trick you into wiring money to your friends or family. The criminal can send messages stating that your family or friends need you to wire them money so they can get home from abroad after losing their wallets.

The criminals are very imaginative when they are trying to trick you into giving them money. They do not just steal your money; they could also steal your identity and ruin your life.

They Want Your Identity

Besides stealing your money for a short-term monetary gain, the criminals want long-term profits by stealing your identity.

As medical costs rise, medical identity theft is also on the rise. The identity thieves can steal your medical insurance and use your medical benefits for themselves, and these medical procedures are now in your medical records.

The annual tax filing procedures may vary from country to country; however, cybercriminals see this time as an opportunity. For example, the people of the United States need to file their taxes by April 15 of each year. The Internal Revenue Service (IRS) does not check the tax return against the information from the employer until July. An identity thief can file a fake tax return and collect the refund. The legitimate filers will notice when their returns are rejected by IRS. With the stolen identity, they can also open credit card accounts and run up debts in your name. This will cause damage to your credit rating and make it more difficult for you to obtain loans.

Personal credentials can also lead to corporate data and government data access.

Organizational Data

Types of Organizational Data

Traditional Data

Corporate data includes personnel information, intellectual properties, and financial data. The personnel information includes application materials, payroll, offer letters, employee agreements, and any information used in making employment decisions. Intellectual property, such as patents, trademarks and new product plans, allows a business to gain economic advantage over its competitors. This intellectual property can be considered a trade secret; losing this information can be disastrous for the future of the company. The financial data, such as income statements, balance sheets, and cash flow statements of a company gives insight into the health of the company.

Internet of Things and Big Data

With the emergence of the Internet of Things (IoT), there is a lot more data to manage and secure. IoT is a large network of physical objects, such as sensors and equipment that extend beyond the traditional computer network. All these connections, plus the fact that we have expanded storage capacity and storage services through the cloud and virtualization, lead to the exponential growth of data. This data has created a new area of interest in technology and business called “Big Data". With the velocity, volume, and variety of data generated by the IoT and the daily operations of business, the confidentiality, integrity and availability of this data is vital to the survival of the organization.

Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability, known as the CIA triad, is a guideline for information security for an organization. Confidentiality ensures the privacy of data by restricting access through authentication encryption. Integrity assures that the information is accurate and trustworthy. Availability ensures that the information is accessible to authorized people.

Availability
Confidentiality
Integrity

CIA TRIAD

Confidentiality

Another term for confidentiality would be privacy. Company policies should restrict access to the information to authorized personnel and ensure that only those authorized individuals view this data. The data may be compartmentalized according to the security or sensitivity level of the information. For example, a Java program developer should not have to access to the personal information of all employees. Furthermore, employees should receive training to understand the best practices in safeguarding sensitive information to protect themselves and the company from attacks. Methods to ensure confidentiality include data encryption, username ID and password, two factor authentication, and minimizing exposure of sensitive information.

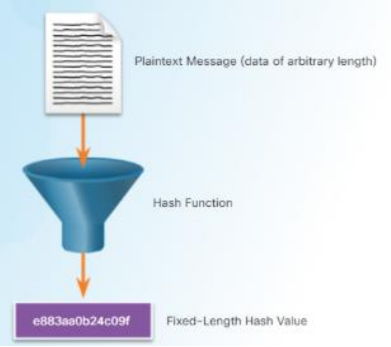
Integrity

Integrity is accuracy, consistency, and trustworthiness of the data during its entire life cycle. Data must be unaltered during transit and not changed by unauthorized entities. File permissions and user access control can prevent unauthorized access. Version control can be used to prevent accidental changes by authorized users. Backups must be available to restore any corrupted data, and checksum hashing can be used to verify integrity of the data during transfer.

A checksum is used to verify the integrity of files, or strings of characters, after they have been transferred from one device to another across your local network or the Internet. Checksums are calculated with hash functions.

Some of the common checksums are MD5, SHA-1, SHA-256, and SHA-512. A hash function uses a mathematical algorithm to transform the data into fixed-length value that represents the data. The hashed value is simply there for comparison. From the hashed value, the original data cannot be retrieved directly. For example, if you forgot your password, your password cannot be recovered from the hashed value. The password must be reset.

After a file is downloaded, you can verify its integrity by verifying the hash values from the source with the one you generated using any hash calculator. By comparing the hash values, you can ensure that the file has not been tampered with or corrupted during the transfer.



CREATING A HASH

Availability

Maintaining equipment, performing hardware repairs, keeping operating systems and software up to date, and creating backups ensure the availability of the network and data to the authorized users. Plans should be in place to recover quickly from natural or man-made disasters. Security equipment or software, such as firewalls, guard against downtime due to attacks such as denial of service (DoS). Denial of service occurs when an attacker attempts to overwhelm resources so the services are not available to the users.

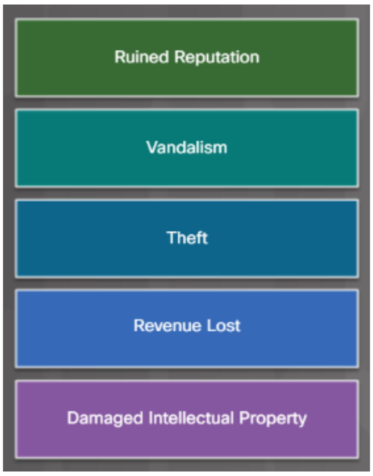
1.2.1.3 Lab – Compare Data with a Hash

In this lab, you will generate a hash for a file and use the hash value to compare the integrity of a file.
Follow instructions on Lab document.

The Consequences of a Security Breach

To protect an organization from every possible cyberattack is not feasible, for a few reasons. The expertise necessary to set up and maintain the secure network can be expensive. Attackers will always continue to find new ways to target networks. Eventually, an advanced and targeted cyberattack will succeed. The priority will then be how quickly your security team can respond to the attack to minimize the loss of data, downtime, and revenue.

By now you know that anything posted online can live online forever, even if you were able to erase all the copies in your possession. If your servers were hacked, the confidential personnel information could be made public. A hacker (or hacking group) may vandalize the company website by posting untrue information and ruin the company's reputation that took years to build. The hackers can also take down the company website causing the company to lose revenue. If the website is down for longer periods of time, the company may appear unreliable and possibly lose credibility. If the company website or network has been breached, this could lead to leaked confidential documents, revealed trade secrets, and stolen intellectual property. The loss of all this information may impede company growth and expansion.



The monetary cost of a breach is much higher than just replacing any lost or stolen devices, investing in existing security and strengthening the building's physical security. The company may be responsible for contacting all the affected customers about the breach and may have to be prepared for litigation. With all this turmoil, employees may choose to leave the company. The company may need to focus less on growing and more on repairing its reputation.

Security Breach Example 1

The online password manager, LastPass, detected unusual activity on its network in July 2015. It turned out that hackers had stolen user email addresses, password reminders, and authentication hashes. Fortunately for the users, the hackers were unable to obtain anyone's encrypted password vaults.

Even though there was a security breach, LastPass could still safeguard the users' account information. LastPass requires email verification or multi-factor authentication whenever there is a new login from an unknown device or IP address. The hackers would also need the master password to access the account.

LastPass users also have some responsibility in safeguarding their own accounts. The users should always use complex master passwords and change the master passwords periodically. The users should always beware of Phishing attacks. An example of a Phishing attack would be if an attacker sent fake emails claiming to be from LastPass. The emails ask the users to click an embedded link and change the password. The link in the email goes to a fraudulent version of the website used to steal the master password. The users should never click the embedded links in an email. The users should also be careful with their password reminder. The password reminder should not give away your passwords. Most importantly, the users should enable multi-factor authentication when available for any website that offers it.

If the users and service providers both utilize the proper tools and procedures to safeguard the users' information, the users' data could still be protected, even in the event of security breach.

Security Breach Example 2

The high tech toy maker for children, Vtech, suffered a security breach to its database in November 2015. This breach could affect millions of customers around the world, including children. The data breach exposed sensitive information including customer names, email addresses, passwords, pictures, and chat logs.

A toy tablet had become a new target for hackers. The customers had shared photos and used the chat features through the toy tablets. The information was not secured properly, and the company website did not support secure SSL communication. Even though the breach did not expose any credit card information and personal identification data, the company was suspended on the stock exchange because the concern over the hack was so great.

Vtech did not safeguard the customers' information properly and it was exposed during the breach. Even though the company informed its customers that their passwords had been hashed, it was still possible for the hackers to decipher them. The passwords in the database were scrambled using MD5 hash function, but the security questions and answers were stored in plaintext. Unfortunately, MD5 hash function has known vulnerabilities. The hackers can determine the original passwords by comparing millions of pre-calculated hash values.

With the information exposed in this data breach, cybercriminals could use it to create email accounts, apply for credits, and commit crimes before the children were old enough to go to school. For the parents of these children, the cybercriminals could take over the online accounts because many people reuse their passwords on different websites and accounts.

The security breach not only impacted the privacy of the customers, it ruined the company's reputation, as indicated by the company when its presence on the stock exchange was suspended.

For parents, it is a wake-up call to be more vigilant about their children's privacy online and demand better security for children's products. For the manufacturers of network-connected products, they need to be more aggressive in the protection of customer data and privacy now and in the future, as the cyberattack landscape evolves.

Security Breach Example 3

Equifax Inc. is one of the nationwide consumer credit reporting agencies in the United States. This company collects information on millions of individual customers and businesses worldwide. Based on the collected information, credit scores and credit reports are created about the customers. This information could affect the customers when they apply for loans and when they are looking for employment.

In September 2017, Equifax publicly announced a data breach event. The attackers exploited a vulnerability in the Apache Struts web application software. The company believes that millions of U.S. consumers' sensitive personal data were accessed by the cyber criminals between May and July of 2017. The personal data includes the customers' full names, Social Security numbers, birth dates, addresses and other personally identifiable information. There is evidence that the breach may have affected customers in United Kingdom and Canada.

Equifax established a dedicated web site that allows the consumers to determine if their information was compromised, and to sign up for credit monitoring and identity theft protection. Using a new domain name, instead of using a subdomain of equifax.com, this allowed nefarious parties to create unauthorized websites with similar names. These websites can be used as part of a phishing scheme to trick you into providing personal information. Furthermore, an employee from Equifax provided an incorrect web link in social media for worried customers. Fortunately, this web site was taken down within 24 hours. It was created by an individual who use it as an educational opportunity to expose the vulnerabilities that exists in Equifax's response page.

As a concerned consumer, you may want to quickly verify if your information was compromised, so you can minimize the impact. In a time of crisis, you may be tricked into using unauthorized websites. You should be cautious about providing personal information so you do not become a victim again. Furthermore, companies are responsible for keeping our information safe from unauthorized access. Companies need to regularly patch and update their software to mitigate exploitation of known vulnerabilities. Their employees should be educated and informed about the procedures to safeguard the information and what to do in the event of a breach.

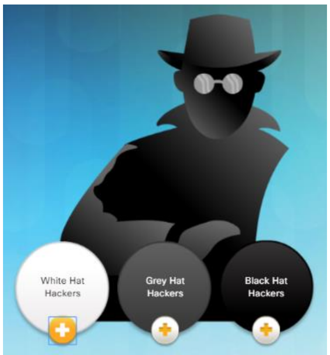
Unfortunately, the real victims of this breach are the individuals whose data may have been compromised. In this case, Equifax has the burden of protecting the collected consumer data while conducting credit checks because the customers did not choose to use the services provided by Equifax. The consumer has to trust the company to safeguard the collected information. Furthermore, the attackers can use this data to assume your identity, and it is very difficult to prove otherwise because both the attacker and the victim know the same information. In these situations, the most you can do is be vigilant when you are providing personally identifiable information over the Internet. Check your credit reports regularly (once per month or once per quarter). Immediately report any false information, such as applications for credit that you did not initiate, or purchases on your credit cards that you did not make.

1.2.2.5 Lab – What Was Taken?

In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.
Follow instructions on Lab document.

Attackers and Cybersecurity Professionals

Types of Attackers



Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. Attackers are interested in everything, from credit cards to product designs and anything with value.

Amateurs – These people are sometimes called Script Kiddies. They are usually attackers with little or no skill, often using existing tools or instructions found on the Internet to launch attacks. Some of them are just curious, while others are trying to demonstrate their skills and cause harm. They may be using basic tools, but the results can still be devastating.

Hackers – This group of attackers break into computers or networks to gain access. Depending on the intent of the break-in, these attackers are classified as white, gray, or black hats. The white hat attackers break into networks or computer systems to discover weaknesses so that the security of these systems can be improved. These break-ins are done with prior permission and any results are reported back to the owner. On the other hand, black hat attackers take advantage of any vulnerability for illegal personal, financial or political gain. Gray hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability in a system. Gray hat hackers may report the vulnerability to the owners of the system if that action coincides with their agenda. Some gray hat hackers publish the facts about the vulnerability on the Internet so that other attackers can exploit it.

> **White Hat Hacker** – These are ethical hackers who use their programming skills for good, ethical and legal purposes. White-Hat hackers may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be threatened. Some organizations award prizes or bounties to white hat hackers when they inform them of a vulnerability.
>
> **Grey Hat Hacker** – These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage.an example would be someone who compromises a network without permission and then discloses the vulnerability publicly. A grey hat hacker may disclose a vulnerability to the affected organization after having compromised their network. This allows the organization to fix the problem.
>
> **Black Hat Hacker** – These are unethical criminals who violate computer and network security for personal gain, or for malicious reasons such as attacking networks. Black-hat hackers exploit vulnerabilities to compromise computer and network systems.

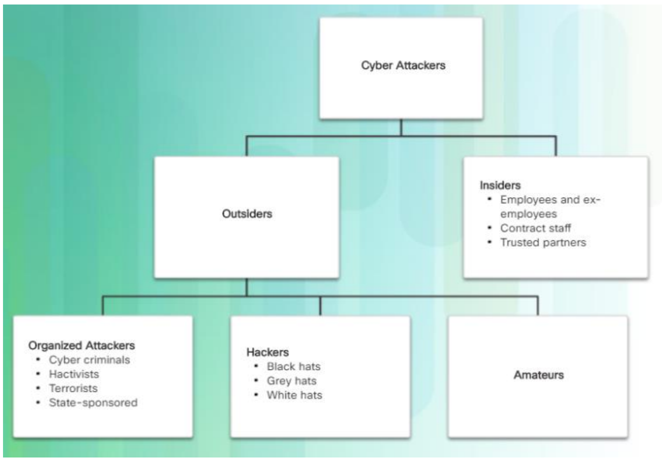
Organized Hackers – These hackers include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are usually groups of professional criminals focused on control, power, and wealth. The criminals are highly sophisticated and organized, and they may even provide cybercrime as a service to other criminals. Hacktivists make political statements to create awareness to issues that are important to them. State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.

Internal and External Threats

Internal Security Threats

Attacks can be originated from within an organization or from outside of the organization, as shown in the figure. An internal user, such as an employee or contract partner, can accidently or intentionally:

- Mishandle confidential data
- Threaten the operations of internal servers or network infrastructure devices
- Facilitate outside attacks by connecting infected USB media into the corporate computer system
- Accidentally invite malware onto the network through malicious email or websites



Internal threats also have the potential to cause greater damage than external threats, because internal users have direct access to the building and its infrastructure devices. Employees also have knowledge of the corporate network, its resources, and its confidential data, as well as different levels of user or administrative privileges.

External Security Threats

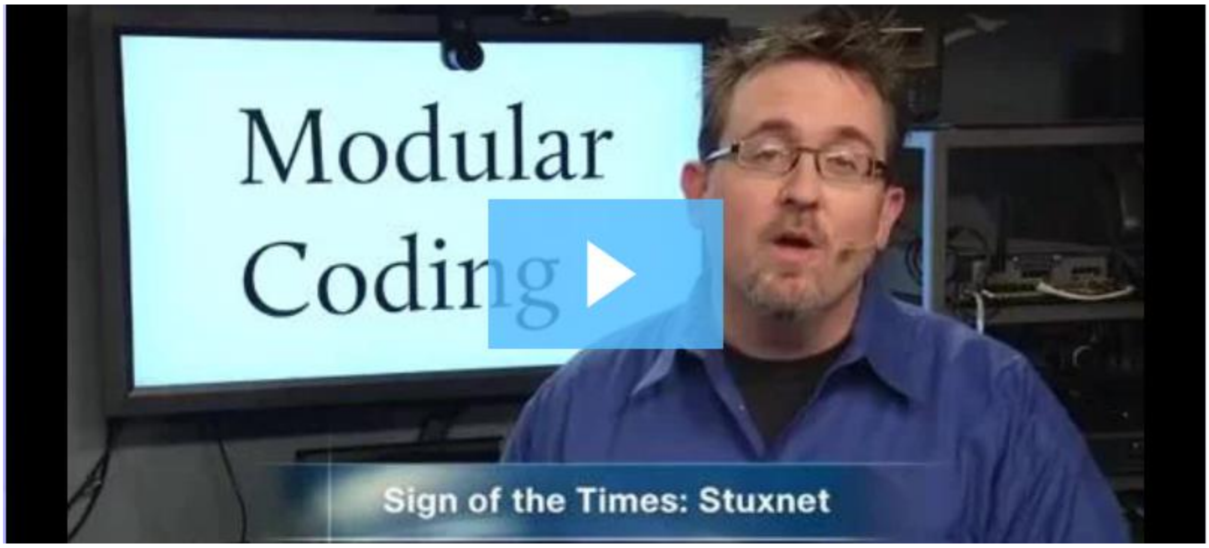
External threats from amateurs or skilled attackers can exploit vulnerabilities in network or computing devices, or use social engineering to gain access.

Cyberwarfare

What is Cyberwarfare?

Cyberspace has become another important dimension of warfare, where nations can carry out conflicts without the clashes of traditional troops and machines. This allows countries with minimal military presence to be as strong as other nations in cyberspace. Cyberwarfare is an Internet-based conflict that involves the penetration of computer systems and networks of other nations. These attackers have the resources and expertise to launch massive Internet-based attacks against other nations to cause damage or disrupt services, such as shutting down a power grid.

An example of a state-sponsored attack involved the Stuxnet malware that was designed to damage Iran's nuclear enrichment plant. Stuxnet malware did not hijack targeted computers to steal information. It was designed to damage physical equipment that was controlled by computers. It used modular coding that was programmed to perform a specific task within the malware. It used stolen digital certificates so the attack appeared legitimate to the system. Click Play to view a video about Stuxnet.



Breaking Down Stuxnet (Video Transcript)

You know when it comes to security news, It's always puzzling what gets reported. As viewers of this show, you know there's a very regular rhythm of security issues that are always bubbling just below the surface and it takes something truly profound to grab the public's attention. Well one new threat making the rounds did have the right mix of ingredients last summer. Stuxnet. I mean it makes sense, right? Computer attacks, nuclear power. Foreign governments, sabotage. Spy versus spy, but how much of it is real? Enough to say it's a sign of the times. Now as all good threats, the details will continue to evolve, but I do think that there are five items worth paying attention to here. the first one, non-trivial distribution. Primarily spread via USB sticks. Think non-internet connected systems that then propagate by escalating privilege levels through zero day exploits, notable for the fact that true zeros are special and they're only valuable for a short period of time. Very expensive, very hard to come by. The next one, sophistication. This is an intelligent worm. Initially targeting Windows computers, where it even installs its own drivers using a stolen but legitimate certificate. The offending certificate gets revoked of course, but then another one gets added within 24 hours. Our third point, modular coding. This thing can get new tires while still on the road. Multiple control servers. First in Malaysia, then Denmark, now more, including peer-to-peer. In fact, when two run into each other, they compare versions and make sure that they're both updated. Fourth point, unique targeting. Windows is just the intermediary, the friend of the friend. Stuxnet is looking for a particular model of PLC. That's programmable logic controller, which is technically not SCADA as it's often reported. These are small imbedded condustrial control systems that run all sorts of automated processes, from factories to oil refineries to nuclear power plants. Stuxnet will leverage the vulnerability in the controller software to reach in and change very specific bits of data. Shut things off. Don't grease a bearing for 10 minutes. Don't sound an alarm. This is really unique knowledge. Respectable coding skills that imply a higher level of patience of good funding resources. Our final point, motive. Stuxnet does not perform... Excuse me. It does not threaten. It performs sabotage. Really has no criminal focus. Does not spread indiscriminately or steal credit card information or login credentials. It does not recruit systems into a botnet. It targets infrastructure, our most essential necessities like power, water, safety and much, much more. You know these are older systems. Very established. Generally run with the mentality of hey, if it ain't broke, don't fix it. These things don't get watched over and patched by technical handlers who understand these kind of things. Not yet anyway. So stay tuned. This one is not done. We all have a lot to learn and somebody is working hard to teach us.

The Purpose of Cyberwarfare

The main purpose of cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

A nation can continuously invade other nation’s infrastructure, steal defense secrets, and gather information about technology to narrow the gaps in its industries and military. Besides industrial and militaristic espionage, cyberwar can sabotage the infrastructure of other nations and cost lives in the targeted nations. For example, an attack can disrupt the power grid of a major city. Traffic would be disrupted. The exchange of goods and services is halted. Patients cannot get the care needed in emergency situations. Access to the Internet may also be disrupted. By affecting the power grid, the attack can affect the everyday life of ordinary citizens.

Furthermore, compromised sensitive data can give the attackers the ability to blackmail personnel within the government. The information may allow an attacker to pretend to be an authorized user to access sensitive information or equipment.

If the government cannot defend against the cyberattacks, the citizens may lose confidence in the government’s ability to protect them. Cyberwarfare can destabilize a nation, disrupt commerce, and affect the citizens’ faith in their government without ever physically invading the targeted nation.

Summary: The Need for Cybersecurity

This chapter explained the features and characteristics of cybersecurity. It explained why the demand for cybersecurity professionals will only continue to increase. The content explains why your personal online identity and data is vulnerable to cyber criminals. It gives some tips on how you can protect your personal online identity and data.

This chapter also discussed organizational data: what it is, where it is, and why it must be protected. It explained who the cyber attackers are and what they want. Cybersecurity professionals must have the same skills as the cyber attackers. Cybersecurity professionals must work within the bounds of the local, national and international law. Cybersecurity professionals must also use their skills ethically.

Finally, this chapter briefly explained cyberwarfare and why nations and governments need cybersecurity professionals to help protect their citizens and infrastructure.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

Chapter 2: Attacks, Concepts and Techniques

This chapter covers the ways that cybersecurity professionals analyze what has happened after a cyberattack. It explains security software and hardware vulnerabilities and the different categories of security vulnerabilities.

The different types of malicious software (known as malware) and the symptoms of malware are discussed. The different ways that attackers can infiltrate a system is covered, as well as denial of service attacks.

Most modern cyberattacks are considered to be blended attacks. Blended attacks use multiple techniques to infiltrate and attack a system. When an attack cannot be prevented, it is the job of a cybersecurity professional to reduce the impact of that attack.

Analyzing a Cyberattack

Finding Security Vulnerabilities

Security vulnerabilities are any kind of software or hardware defect. After gaining knowledge of a vulnerability, malicious users attempt to exploit it. An *exploit* is the term used to describe a program written to take advantage of a known vulnerability. The act of using an exploit against a vulnerability is referred to as an attack. The goal of the attack is to gain access to a system, the data it hosts or to a specific resource.

Software vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code, despite all the effort companies put into finding and patching software vulnerabilities, it is common for new vulnerabilities to surface. Microsoft, Apple, and other operating system producers release patches and updates almost every day. Application updates are also common. Applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.

In 2015, a major vulnerability, called SYNful Knock, was discovered in Cisco IOS. This vulnerability allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco 1841, 2811, and 3825 routers. The attackers could then monitor all network communication and had the ability to infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed in the routers. To avoid this, always verify the integrity of the downloaded IOS image and limit the physical access of the equipment to authorized personnel only.

The goal of software updates is to stay current and avoid exploitation of vulnerabilities. While some companies have penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited, third party security researchers also specialize in finding vulnerabilities in software.

Google's Project Zero is a great example of such practice. After discovering a number of vulnerabilities in various software used by end-users, Google formed a permanent team dedicated to finding software vulnerabilities.

Hardware vulnerabilities

Hardware vulnerabilities are often introduced by hardware design flaws. RAM memory for example, is essentially capacitors installed very close to one another. It was discovered that, due to proximity, constant changes applied to one of these capacitors could influence neighbor capacitors. Based on that design flaw, an exploit called Rowhammer was created. By repeatedly rewriting memory in the same addresses, the Rowhammer exploit allows data to be retrieved from nearby address memory cells, even if the cells are protected.

Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and a physical security are sufficient protection for the everyday user.

Categorizing Security Vulnerabilities

Most software security vulnerabilities fall into one of the following categories:

Buffer overflow – This vulnerability occurs when data is written beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

Non-validated input – Programs often work with data input. This data coming into the program could have malicious content, designed to force the program to behave in an unintended way. Consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

Race conditions – This vulnerability is when the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or proper timing.

Weaknesses in security practices – Systems and sensitive data can be protected through techniques such as authentication, authorization, and encryption. Developers should not attempt to create their own security algorithms because it will likely introduce vulnerabilities. It is strongly advised that developers use security libraries that have already created, tested, and verified.

Access-control problems – Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.

Nearly all access controls and security practices can be overcome if the attacker has physical access to target equipment. For example, no matter what you set a file's permissions to, the operating system cannot prevent someone from bypassing the operating system and reading the data directly off the disk. To protect the machine and the data it contains, physical access must be restricted and encryption techniques must be used to protect data from being stolen or corrupted.

Types of Malware

Short for Malicious Software, malware is any code that can be used to steal data, bypass access controls, or cause harm to, or compromise a system. Below are a few common types of malware:

Spyware – This malware is design to track and spy on the user. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses.

Adware – Advertising supported software is designed to automatically deliver advertisements. Adware is often installed with some versions of software. Some adware is designed to only deliver advertisements but it is also common for adware to come with spyware.

Bot – From the word robot, a bot is malware designed to automatically perform action, usually online. While most bots are harmless, one increasing use of malicious bots are botnets. Several computers are infected with bots which are programmed to quietly wait for commands provided by the attacker.

Ransomware – This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting data in the computer with a key unknown to the user. Some other versions of ransomware can take advantage of specific system vulnerabilities to lock down the system. Ransomware is spread by a downloaded file or some software vulnerability.

Scareware – This is a type of malware designed to persuade the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating the system is at risk or needs the execution of a specific program to return to normal operation. In reality, no problems were assessed or detected and if the user agrees and clears the mentioned program to execute, his or her system will be infected with malware.

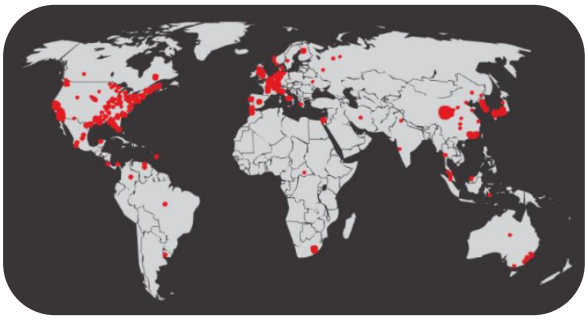
Rootkit – This malware is designed to modify the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. Most rootkits take advantage of software vulnerabilities to perform privilege escalation and modify system files. It is also common for rootkits to modify system forensics and monitoring tools, making them very hard to detect. Often, a computer infected by a rootkit must be wiped and reinstalled.

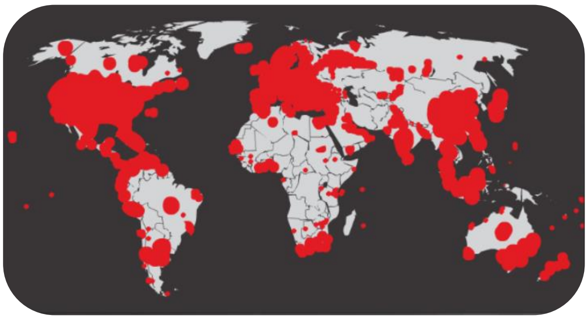
Virus - A virus is malicious executable code that is attached to other executable files, often legitimate programs. Most viruses require end-user activation and can activate at a specific time or date. Viruses can be harmless and simply display a picture or they can be destructive, such as those that modify or delete data. Viruses can also be programmed to mutate to avoid detection. Most viruses are now spread by USB drives, optical disks, network shares, or email.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation. This malicious code exploits the privileges of the user that runs it. Often, Trojans are found in image files, audio files or games. A Trojan horse differs from a virus because it binds itself to non-executable files.

Worms – Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network. Worms share similar patterns. They all have an enabling vulnerability, a way to propagate themselves, and they all contain a payload.

Worms are responsible for some of the most devastating attacks on the Internet. As shown in Figure 1, in 2001 the Code Red worm had infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers as shown in Figure 2.





Man-In-The-Middle (MitM) – MitM allows the attacker to take control over a device without the user's knowledge. With that level of access, the attacker can intercept and capture user information before relaying it to its intended destination. MitM attacks are widely used to steal financial information. Many malware and techniques exist to provide attackers with MitM capabilities.

Man-In-The-Mobile (MitMo) – A variation of man-in-middle, MitMo is a type of attack used to take control over a mobile device. When infected, the mobile device can be instructed to exfiltrate user-sensitive information and send it to the attackers. ZeuS, an example of an exploit with MitMo capabilities, allows attackers quietly to capture 2-step verification SMS messages sent to users.

Symptoms of Malware

Regardless of the type of malware a system has been infected with, these are common malware symptoms:

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.

Social Engineering

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. For example, an attacker could call an authorized employee with an urgent problem that requires immediate network access. The attacker could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

These are some types of social engineering attacks:

- **Pretexting** - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
- **Tailgating** - This is when an attacker quickly follows an authorized person into a secure location.
- **Something for Something (Quid pro quo)** - This is when an attacker requests personal information from a party in exchange for something, like a free gift.

Wi-Fi Password Cracking

Wi-Fi password cracking is the process of discovering the password used to protect a wireless network. These are some techniques used in password cracking:

Social engineering – The attacker manipulates a person who knows the password into providing it.

Brute-force attacks – The attacker tries several possible passwords in an attempt to guess the password. If the password is a 4-digit number, for example, the attacker would have to try every one of the 10000 combinations. Brute-force attacks usually involve a word-list file. This is a text file containing a list of words taken from a dictionary. A program then tries each word and common combinations. Because brute-force attacks take time, complex passwords take much longer to guess. A few password brute-force tools include Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

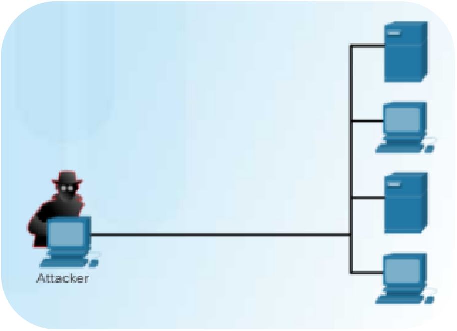
Network sniffing – By listening and capturing packets sent on the network, an attacker may be able to discover the password if the password is being sent unencrypted (in plain text). If the password is encrypted, the attacker may still be able to reveal it by using a password cracking tool.

Phishing

Phishing is when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on their device, or into sharing personal or financial information. An example of phishing is an email forged to look like it was sent by a retail store asking the user to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing emails are customized to a specific person. The attacker researches the target's interests before sending the email. For example, an attacker learns the target is interested in cars, and has been looking to buy a specific model of car. The attacker joins the same car discussion forum where the target is a member, forges a car sale offering and sends email to the target. The email contains a link for pictures of the car. When the target clicks on the link, malware is installed on the target's computer.

Vulnerability Exploitation



Exploiting vulnerabilities is another common method of infiltration. Attackers will scan computers to gain information about them. Below is a common method for exploiting vulnerabilities:

Step 1. Gather information about the target system. This could be done in many different ways such as a port scanner or social engineering. The goal is to learn as much as possible about the target computer.

Step 2.One of the pieces of relevant information learned in step 1 might be the operating system, its version, and a list of services running on it.

Step 3. When the target's operating system and version is known, the attacker looks for any known vulnerabilities specific to that version of OS or other OS services.

Step 4. When a vulnerability is found, the attacker looks for a previously written exploit to use. If no exploits have been written, the attacker may consider writing an exploit.

Figure 1 portrays an attacker using **whois**, a public Internet database containing information about domain names and their registrants. Figure 2 portrays an attacker using the **nmap** tool, a popular port scanner. With a port scanner, an attacker can probe ports of a target computer to learn about which services are running on that computer.

Advanced Persistent Threats

One way in which infiltration is achieved is through advanced persistent threats (APTs). They consist of a multi-phase, long term, stealthy and advanced operation against a specific target. Due to its complexity and skill level required, an APT is usually well funded. An APT targets organizations or nations for business or political reasons.

Usually related to network-based espionage, APT's purpose is to deploy customized malware on one or multiple of the target's systems and remain undetected. With multiple phases of operation and several customized types of malware that affect different devices and perform specific functions, an individual attacker often lacks the skill-set, resources or persistence to carry out APTs.

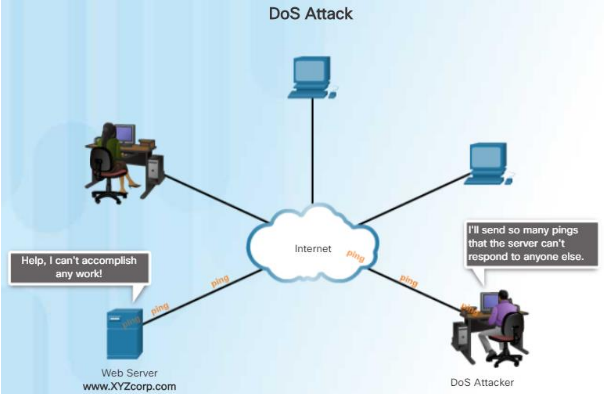
DoS

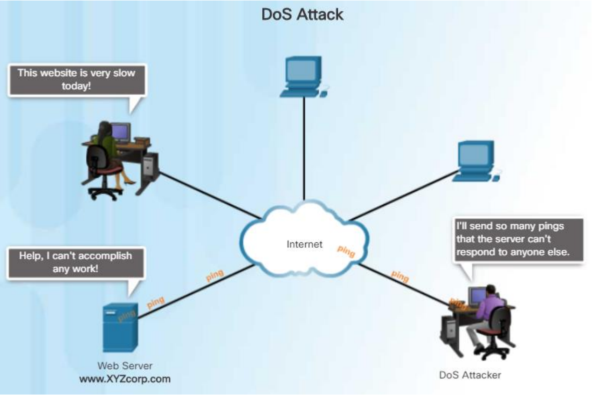
Denial-of-Service (DoS) attacks are a type of network attack. A DoS attack results in some sort of interruption of network service to users, devices, or applications. There are two major types of DoS attacks:

Overwhelming Quantity of Traffic - This is when a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle. This causes a slowdown in transmission or response, or a crash of a device or service.

Maliciously Formatted Packets - This is when a maliciously formatted packet is sent to a host or application and the receiver is unable to handle it. For example, an attacker forwards packets containing errors that cannot be identified by the application, or forwards improperly formatted packets. This causes the receiving device to run very slowly or crash.

DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.


DoS Attack
Help, I can't accomplish any work!
Internet
ping
I'll send so many pings that the server can't respond to anyone else.
Web Server
www.XYZcorp.com
DoS Attacker

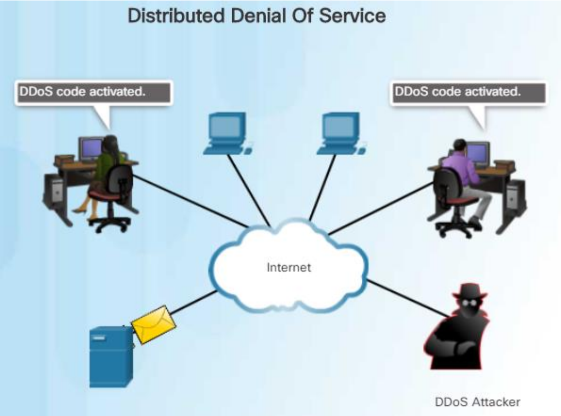

DoS Attack
This website is very slow today!
Help, I can't accomplish any work!
Internet
ping
I'll send so many pings that the server can't respond to anyone else.
Web Server
www.XYZcorp.com
DoS Attacker

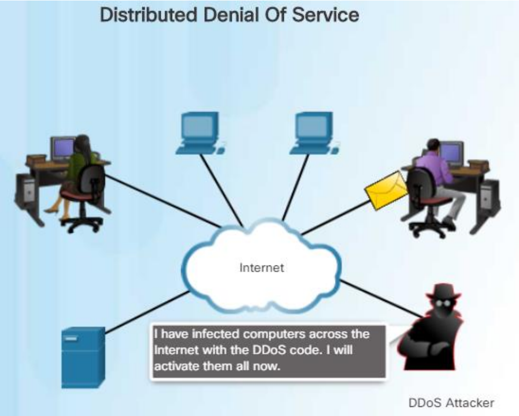
DDoS

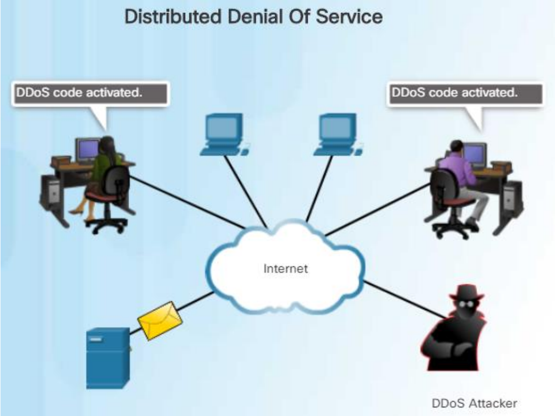
A Distributed DoS Attack (DDoS) is similar to a DoS attack but originates from multiple, coordinated sources. As an example, a DDoS attack could proceed as follows:

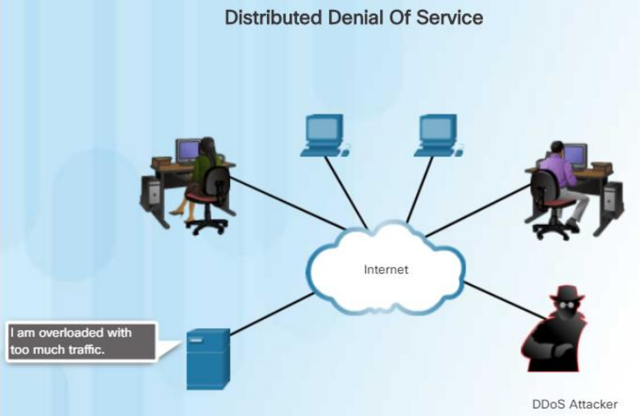
An attacker builds a network of infected hosts, called a botnet. The infected hosts are called zombies. The zombies are controlled by handler systems.

The zombie computers constantly scan and infect more hosts, creating more zombies. When ready, the hacker instructs handler systems to make the botnet of zombies carry out a DDoS attack.




Distributed Denial Of Service
Internet
I have infected computers across the Internet with the DDoS code. I will activate them all now.
DDoS Attacker




Distributed Denial Of Service
Internet
I am overloaded with too much traffic.
DDoS Attacker

SEO Poisoning

Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, a malicious user could use SEO to make a malicious website appear higher in search results. This technique is called SEO poisoning.

The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or perform social engineering. To force a malicious site to rank higher in search results, attackers take advantage of popular search terms.

The Cybersecurity Landscape

What is a Blended Attack?

Blended attacks are attacks that use multiple techniques to compromise a target. By using several different attack techniques at once, attackers have malware that are a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes. This trend of blended attacks is revealing more complex malware and placing user data at great risk.

The most common type of blended attack uses spam email messages, instant messages or legitimate websites to distribute links where malware or spyware is secretly downloaded to the computer. Another common blended attack uses DDoS combined with phishing emails. First, DDoS is used to take down a popular bank website and send emails to the bank's customers, apologizing for the inconvenience. The email also directs the users to a forged emergency site where their real login information can be stolen.

Many of the most damaging computer worms like Nimbda, CodeRed, BugBear, Klez and Slammer are better categorized as blended attacks, as shown below:

- Some Nimbda variants used email attachments; file downloads from a compromised web server; and Microsoft file sharing (e.g., anonymous shares) as propagation methods.

- Other Nimbda variants were able to modify the system’s guest accounts to provide the attacker or malicious code with administrative privileges.

The recent Conficker and ZeuS/LICAT worms were also blended attacks. Conficker used all the traditional distribution methods.

What is Impact Reduction?

While the majority of successful companies today are aware of common security issues and put considerable effort towards preventing them, no set of security practices is 100% efficient. Because a breach is likely to happen if the prize is big, companies and organizations must also be prepared to contain the damage.

It is important to understand that the impact of a breach is not only related to the technical aspect of it, stolen data, damaged databases, or damage to intellectual property, the damage also extends to the company’s reputation. Responding to a data breach is a very dynamic process.

Below are some important measures a company should take when a security breach is identified, according to many security experts:

- Communicate the issue. Internally employees should be informed of the problem and called to action. Externally, clients should be informed through direct communication and official announcements. Communication creates transparency, which is crucial in this type of situation.
- Be sincere and accountable in case the company is at fault.

- Provide details. Explain why the situation took place and what was compromised. It is also expected that the company take care of the costs of identity theft protection services for affected customers.
- Understand what caused and facilitated the breach. If necessary, hire forensics experts to research and learn the details.
- Apply what was learned from the forensics investigation to ensure similar breaches do not happen in the future.
- Ensure all systems are clean, no backdoors were installed, and nothing else has been compromised. Attackers will often attempt to leave a backdoor to facilitate future breaches. Make sure this does not happen.
- Educate employees, partners, and customers on how to prevent future breaches.

Summary: Attacks, Concepts and Techniques

This chapter covered the ways that cybersecurity professionals analyze what has happened after a cyberattack. It explains security software and hardware vulnerabilities and the different categories of security vulnerabilities.

The different types of malicious software (known as malware) and the symptoms of malware explained. Some of the malware that was discussed included viruses, worms, Trojan horses, spyware, adware, and others.

The different ways that attackers can infiltrate a system was covered, including social engineering, Wi-Fi Password Cracking, Phishing, and vulnerability exploitation. The different types of denial of service attacks were also explained.

Blended attacks use multiple techniques to infiltrate and attack a system. Many of the most damaging computer worms like Nimbda, CodeRed, BugBear, Klez and slammer are better categorized as blended attacks. When an attack cannot be prevented, it is the job of a cybersecurity professional is to reduce the impact of that attack.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

Chapter 3: Protecting Your Data and Privacy

This chapter focuses on your personal devices and your personal data. It includes tips for protecting your devices, creating strong passwords and safely using wireless networks. It also discusses maintaining your data securely.

Your online data is worth something to cyber criminals. This chapter briefly covers authentication techniques to help you maintain your data securely. It also covers ways to enhance the security of your online data with tips about what to do and what not to do online.

Protecting your Data

Protect Your Computing Devices

Your computing devices store your data and are the portal to your online life. Below is a short list of steps you can take to protect your computing devices from intrusion:

- **Keep the Firewall On** – Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your personal or company data. Turn on your firewall:

  Windows 7 or 8.1: http://windows.microsoft.com/en-us/windows/turn-windows-firewall-on-off
  Windows 10: http://windows.microsoft.com/en-us/windows-10/turn-windows-firewall-on-or-off
  Mac OS X: https://support.apple.com/en-us/HT201642

- **Use Antivirus and Antispyware** – Malicious software, such as viruses, Trojan horses, worms, ransomware and spyware, are installed on your computing devices without your permission, in order to gain access to your computer and your data. Viruses can destroy your data, slow down your computer, or take over your computer. One way viruses can take over your computer is by allowing spammers to broadcast emails using your account. Spyware can monitor your online activities, collect your personal information, or produce unwanted pop-up ads on your web browser while you are online. A good rule is to only download software from trusted websites to avoid getting spyware in the first place. Antivirus software is designed to scan your computer and incoming email for viruses and delete them. Sometimes antivirus software also includes antispyware. Keep your software up to date to protect your computer from the newest malicious software.

- **Manage Your Operating System and Browser** – Hackers are always trying to take advantage of vulnerabilities in your operating systems and your web browsers. To protect your computer and your data, set the security settings on your computer and browser at medium or higher. Update your computer's operating system including your web browsers and regularly download and install the latest software patches and security updates from the vendors.

- **Protect All Your Devices** – Your computing devices, whether they are PCs, laptops, tablets, or smartphones, should be password protected to prevent unauthorized access. The stored information should be encrypted, especially for sensitive or confidential data. For mobile devices, only store necessary information, in case these devices are stolen or lost when you are away from your home. If any one of your devices is compromised, the criminals may have access to all your data through your cloud-storage service provider, such as iCloud or Google drive.

IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most of the IoT devices still have their original firmware. If vulnerabilities are found in the firmware, the IoT device is likely to stay vulnerable. To make the problem worse, IoT devices are often designed to call home and require Internet access. To reach the Internet, most IoT devices manufacturers rely on the customer's local network. The result is that IoT devices are very likely to be comprised and when they are, they allow access to the customer's local network and data. The best way to protect yourself from this scenario is to have IoT devices using an isolated network, sharing it only with other IoT devices.

Visit Shodan at https://www.shodan.io/, a web-based IoT device scanner.

Use Wireless Networks Safely

Wireless networks allow Wi-Fi enabled devices, such as laptops and tablets, to connect to the network by way of the network identifier, known as the Service Set Identifier (SSID). To prevent intruders from entering your home wireless network, the pre-set SSID and default password for the browser-based administrative interface should be changed. Hackers will be aware of this kind of default access information. Optionally, the wireless router can also be configured to not broadcast the SSID, which adds an additional barrier to discovering the

network. However, this should not be considered adequate security for a wireless network. Furthermore, you should encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on the wireless router. Even with WPA2 encryption enabled, the wireless network can still be vulnerable.

In October 2017, a security flaw in the WPA2 protocol was discovered. This flaw allows an intruder to break the encryption between the wireless router and the wireless client, and allow the intruder to access and manipulate the network traffic. This vulnerability can be exploited using **K**ey **R**einstallation **A**tta**ck**s (KRACK). It affects all modern, protected Wi-Fi networks. To mitigate an attacker, a user should update all affected products: wireless routers and any wireless capable devices, such as laptops and mobile devices, as soon as security updates become available. For laptops or other devices with wired NIC, a wired connection could mitigate this vulnerability. Furthermore, you can also use a trusted VPN service to prevent the unauthorized access to your data while you are using the wireless network.

Visit https://www.krackattacks.com/, to learn more about KRACK.

When you are away from home, a public Wi-Fi hot spot allows you to access your online information and surf the Internet. However, it is best to not access or send any sensitive personal information over a public wireless network. Verify whether your computer is configured with file and media sharing and that it requires user authentication with encryption. To prevent someone from intercepting your information (known as "eavesdropping") while using a public wireless network, use encrypted VPN tunnels and services. The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable.

Visit https://www.fcc.gov/consumers/guides/protecting-your-wireless-network, to learn more about protecting yourself when using wireless networks.

Many mobile devices, such as smartphones and tablets, come with the Bluetooth wireless protocol. This capability allows Bluetooth-enabled devices to connect to each other and share information. Unfortunately, Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth turned off when you are not using it.

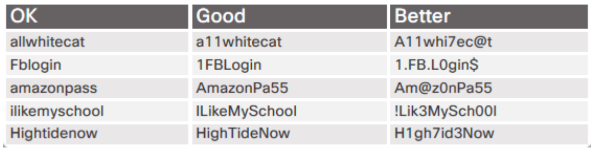
Use Unique Passwords for Each Online Account

You probably have more than one online account, and each account should have a unique password. That is a lot of passwords to remember. However, the consequence of not using strong and unique passwords leaves you and your data vulnerable to cyber criminals. Using the same password for all your online accounts is like using the same key for all your locked doors, if an attacker was to get your key, he would have the ability to access everything you own. If criminals get your password through phishing for example, they will try to get into your other online accounts. If you only use one password for all accounts, they can get into all your accounts, steal or erase all your data, or decide to impersonate you.

We use so many online accounts that need passwords that is becomes too much to remember. One solution to avoid reusing passwords or using weak passwords is to use a password manager. A password manager stores and encrypts all of your different and complex passwords. The manager can then help you to log into your online accounts automatically. You only need to remember your master password to access the password manager and manage all of your accounts and passwords.

Tips for choosing a good password:

- Do not use dictionary words or names in any languages
- Do not use common misspellings of dictionary words
- Do not use computer names or account names
- If possible use special characters, such as: ! @ # $ % ^ & * ( )
- Use a password with ten or more characters



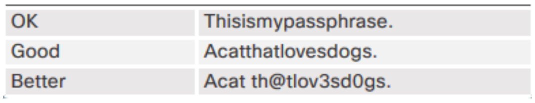
OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

Use Passphrase Rather Than a Password

To prevent unauthorized physical access to your computing devices, use passphrases, rather than passwords. It is easier to create a long passphrase than a password, because it is generally in the form of a sentence rather than a word. The longer length makes passphrases less vulnerable to dictionary or brute force attacks. Furthermore, a passphrase maybe easier to remember, especially if you are required to change your password frequently. Here are some tips in choosing good passwords or passphrases:

Tips in choosing a good passphrase:

- Choose a meaningful statement to you
- Add special characters, such as ! @ # $ % ^ & * ( )
- The longer the better
- Avoid common or famous statements, for example, lyrics from a popular song



OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

Recently, United States National Institute for Standards and Technology (NIST) published improved password requirements. NIST standards are intended for government application but can also serve as a standard for others as well. The new guidelines aim to provide better user experience and put the burden of user verification on the providers.

Summary of the new guidelines:

- 8 characters minimum in length, but no more than 64 characters
- No common, easily guessed passwords, such as password, abc123
- No composition rules, such as having to include lowercase and uppercase letters and numbers
- Improve typing accuracy by allowing the user to see the password while typing
- All printing characters and spaces are allowed
- No password hints
- No periodical or arbitrary password expiration
- No knowledge-based authentication, such as information from shared secret questions, marketing data, transaction history

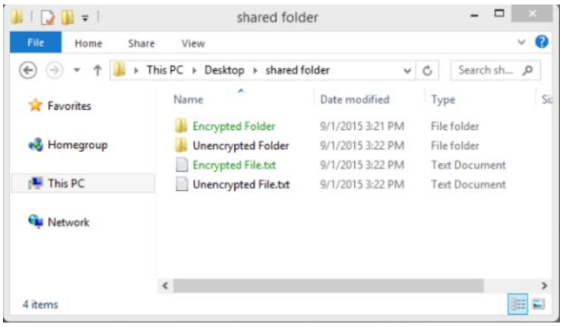
Visit https://pages.nist.gov/800-63-3/, to learn more about the improved NIST password requirement.

Even with access to your computers and network devices secured, it is also important to protect and preserve your data.

3.1.1.5 Lab – Create and Store Strong Passwords

In this lab, you will explore the concepts to create strong passwords and how to store it securely.
Follow instructions on Lab document

Encrypt Your Data



Name	Date modified	Type
Encrypted Folder	9/1/2015 3:21 PM	File folder
Unencrypted Folder	9/1/2015 3:22 PM	File folder
Encrypted File.txt	9/1/2015 3:22 PM	Text Document
Unencrypted File.txt	9/1/2015 3:22 PM	Text Document

Your data should always be encrypted. You may think you have no secrets and nothing to hide so why use encryption? Maybe you think that nobody wants your data. Most likely, this is probably not true.

Are you ready to show all of your photos and documents to strangers? Are you ready to share financial information stored on your computer to your friends? Do you want to give out your emails and account passwords to the general public?

This can be even more troublesome if a malicious application infects your computer or mobile device and steals potentially valuable information, such as account numbers and passwords, and other official documents. That kind of information can lead to identity theft, fraud, or ransom. Criminals may decide to simply encrypt your data and make it unusable until you pay the ransom.

What is encryption? Encryption is the process of converting the information into a form where an unauthorized party cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form. The encryption itself does not prevent someone from intercepting the data. Encryption can only prevent an unauthorized person from viewing or accessing the content.

Software programs are used to encrypt files, folders, and even entire drives.

Encrypting File System (EFS) is a Windows feature that can encrypt data. EFS is directly linked to a specific user account. Only the user that encrypted the data will be able to access it after it has been encrypted using EFS. To encrypt data using EFS in all Windows versions, follow these steps:

Step 1. Select one or more files or folders.

Step 2. Right-click the selected data **>Properties**.

Step 3. Click **Advanced…**

Step 4. Select the **Encrypt contents to secure data** check box.

Step 5. Files and folders that have been encrypted with EFS are displayed in green, as shown in the figure.

Back up Your Data

Your hard drive may fail. Your laptop could be lost. Your smart phone stolen. Maybe you erased the original version of an important document. Having a backup may prevent the loss of irreplaceable data, such as family photos. To back up data properly, you will need an additional storage location for the data and you must copy the data to that location regularly and automatically.

The additional location for your backed up files can be on your home network, secondary location, or in the cloud. By storing the backup of the data locally, you have total control of the data. You can decide to copy all of your data to a network attached storage device (NAS), a simple external hard drive, or maybe select only a few important folders for backup on thumb drives, CDs/DVDs, or even tapes. In that scenario, you are the owner and you are totally responsible for the cost and maintenance of the storage device equipment. If you subscribe to a cloud storage service, the cost depends on the amount storage space needed. With a cloud storage service like Amazon Web Services (AWS), you have access to your backup data as long as you have access to your account. When you subscribe to online storage services, you may need to be more selective about the data being backed up due to the cost of the storage and the constant online data transfers. One of the benefits of storing a backup at an alternate location is that it is safe in the event of fire, theft or other catastrophes other than storage device failure.

3.1.2.3 Lab – Back up Data to External Storage

In this lab, you will use an external disk and a remote disk to back up your data.
Follow instruction on the lab document.

Deleting Your Data Permanently

When you move a file to the recycle bin or trash and delete it permanently, the file is only inaccessible from the operating system. Anyone with the right forensic tools can still recover the file due to a magnetic trace left on the hard drive.

In order to erase data so that it is no longer recoverable, the data must be overwritten with ones and zeroes multiple times. To prevent the recovery of deleted files, you may need to use tools specifically designed to do just that. The program SDelete from Microsoft (for Vista and higher), claims to have the ability to remove sensitive files completely. Shred for Linux and Secure Empty Trash for Mac OSX are some tools that claim to provide a similar service.

The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device. It has been the folly of many criminals in thinking their files were impenetrable or irrecoverable.

Besides storing data on your local hard drives, your data may also be stored online in the cloud. Those copies will also need to be deleted. Take a moment to ask yourself, “Where do I save my data? Is it backed up somewhere? Is it encrypted? When you need to delete your data or get rid of a hard drive or computer, ask yourself, “Have I safeguarded the data to keep it from falling into the wrong hands?”

3.1.2.5 Lab – Who Owns Your Data?

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.
Follow instructions on the lab document.

Safeguarding Your Online Privacy

Two Factor Authentication

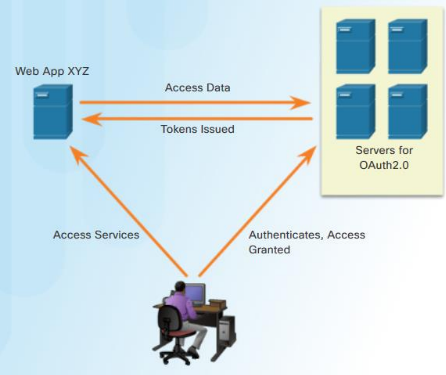
Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentication to add an extra layer of security for account logins. Besides the username and password, or personal identification number (PIN) or pattern, two factor authentication requires a second token, such as a:

- **Physical object** - credit card, ATM card, phone, or fob
- **Biometric scan** - fingerprint, palm print, as well as facial or voice recognition

Even with two factor authentication, hackers can still gain access to your online accounts through attacks such as phishing attacks, malware, and social engineering.

Visit https://twofactorauth.org/, to find out if websites you visit use two factor authentication.

OAuth 2.0



Open Authorization (OAuth) is an open standard protocol that allows an end user's credentials to access third party applications without exposing the user's password. OAuth acts as the middle man to decide whether to allow end users access to third party applications. For example, say you want to access web application XYZ, and you do not have a user account for accessing this web application. However, XYZ has the option to allow you to log in using the credentials from a social media website ABC. So you access the website using the social media login.

For this to work, the application 'XYZ' is registered with 'ABC' and is an approved application. When you access XYZ, you use your user credentials for ABC. Then XYZ requests an access token from ABC on your behalf. Now you have access to XYZ. XYZ knows nothing about you and your user credentials, and this interaction is totally seamless for the user. Using secret tokens prevents a malicious application from getting your information and your data.

Do Not Share Too Much on Social Media

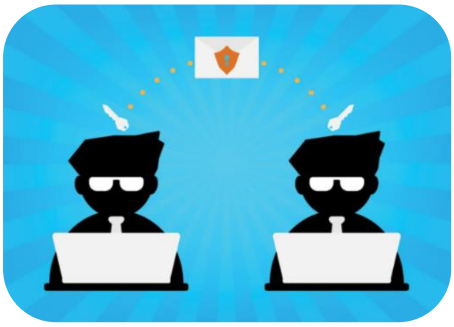
If you want to keep your privacy on social media, share as little information as possible. You should not share information like your birth date, email address, or your phone number on your profile. The people who need to know your personal information probably already know it. Do not fill out your social media profile completely, only provide the minimum required information. Furthermore, check your social media settings to allow only people you know to see your activities or engage in your conversations.

The more personal information you share online, the easier it is for someone to create a profile about you and take advantage of you offline.

Have you ever forgotten the username and password for an online account? Security questions like "What is your mother's maiden name?" or "In what city were you born?" are supposed to help keep your account safe from intruders. However, anyone who wants to access your accounts can search for the answers on the Internet.

You can answer these questions with false information, as long as you can remember the false answers. If you have a problem remembering them, you can use password manager to manage them for you.

Email and Web Browser Privacy



Every day, millions of email messages are used to communicate with friends and conduct business. Email is a convenient way to communicate with each other quickly. When you send an email, it is similar to sending a message using a postcard. The postcard message is transmitted in plain sight of anyone who has access to look, and the email message is transmitted in plain text, and is readable by anyone who has access. These communications are also passed among different servers while in route to the destination. Even when you erase your email messages, the messages can be archived on the mail servers for some time.

Anyone with physical access to your computer, or your router, can view which websites you have visited using web browser history, cache, and possibly log files. This problem can be minimized by enabling the in-private browsing mode on the web browser. Most of the popular web browsers have their own name for private browser mode:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab / private window
- **Safari**: Private: Private browsing

With private mode enabled, cookies are disabled, and temporary Internet files and browsing history are removed after closing the window or program.

Keeping your Internet browsing history private may prevent others from gathering information about your online activities and enticing you to buy something with targeted ads. Even with private browsing enabled and cookies disabled, companies are developing different ways of fingerprinting users in order to gather information and track user behavior. For example, the intermediary devices, such as routers, can have information about a user’s web surfing history.

Ultimately, it is your responsibility to safeguard your data, your identity, and your computing devices. When you send an email, should you include your medical records? The next time you browse the Internet, is your transmission secure? Just a few simple precautions may save you problems later.

This figure shows two businessmen with computer laptop send email data with protection shield and key decryption.

3.2.2.3 Lab – Discover Your Own Risky Online Behavior

In this lab, you will identify risky online behavior and explore some tips on how to become safer online.
Follow instructions on lab document.

Summary: Protecting Your Data and Privacy

This chapter focused on your personal devices, your personal data. It included tips for protecting your devices, creating strong passwords and safely using wireless networks. It covered data backups, data storage and deleting your data permanently.

Authentication techniques were discussed to help you maintain your data securely. It briefly covered how easy it is to share too much information on social media and how to avoid this security risk.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

Chapter 4: Protecting the Organization

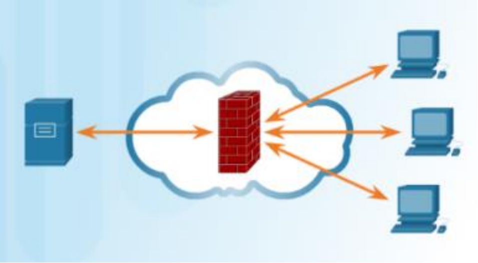
This chapter covers some of the technology and processes used by cybersecurity professionals when protecting an organization's network, equipment and data. First, it briefly covers the many types of firewalls, security appliances, and software that are currently used, including best practices.

Next, this chapter explains botnets, the kill chain, behavior-based security, and using NetFlow to monitor a network.

The third section discusses Cisco's approach to cybersecurity, including the CSIRT team and the security playbook. It briefly covers the tools that cybersecurity professionals use to detect and prevent network attacks.

Firewalls

Firewall Types

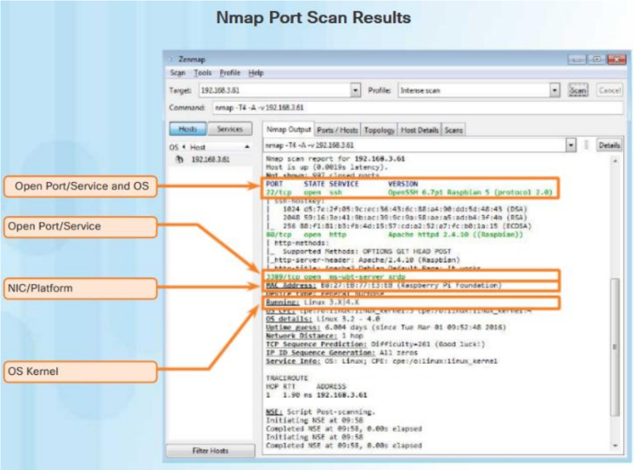


A firewall is a wall or partition that is designed to prevent fire from spreading from one part of a building to another. In computer networking, a firewall is designed to control, or filter, which communications are allowed in and which are allowed out of a device or network, as shown in the figure. A firewall can be installed on a single computer with the purpose of protecting that one computer (host-based firewall), or it can be a stand-alone network device that protects an entire network of computers and all of the host devices on that network (network-based firewall).

Over the years, as computer and network attacks have become more sophisticated, new types of firewalls have been developed which serve different purposes in protecting a network. Here is a list of common firewall types:

- **Network Layer Firewall** – filtering based on source and destination IP addresses
- **Transport Layer Firewall** –filtering based on source and destination data ports, and filtering based on connection states
- **Application Layer Firewall** –filtering based on application, program or service
- **Context Aware Application Firewall** – filtering based on the user, device, role, application type, and threat profile
- **Proxy Server** – filtering of web content requests like URL, domain, media, etc.
- **Reverse Proxy Server** – placed in front of web servers, reverse proxy servers protect, hide, offload, and distribute access to web servers
- **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
- **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system

Port Scanning



Nmap Port Scan Results

Target: 192.168.3.61

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.3.61

```
nmap -T4 -A -v 192.168.3.61
Nmap scan report for 192.168.3.61
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH 6.7p1 Raspbian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 d5:7e:2f:05:9c:ec:36:43:6c:88:a4:90:dd:5d:48:43 (DSA)
|   2048 59:16:3e:41:9b:ac:39:9c:9a:58:ae:a5:ad:b4:3f:4b (RSA)
|_  256 88:f1:81:b3:fb:4d:15:57:cd:a2:52:a7:fc:b0:1a:15 (ECDSA)
80/tcp    open  http          Apache httpd 2.4.10 ((Raspbian))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.10 (Raspbian)
|_http-title: Apache2 Debian Default Page: It works
3389/tcp open  ms-wbt-server xrdp
MAC Address: B8:27:EB:77:E3:EB (Raspberry Pi Foundation)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Uptime guess: 6.004 days (since Tue Mar 01 09:52:48 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.90 ms 192.168.3.61

NSE: Script Post-scanning.
Initiating NSE at 09:58
Completed NSE at 09:58, 0.00s elapsed
Initiating NSE at 09:58
Completed NSE at 09:58, 0.00s elapsed
```

Port-scanning is a process of probing a computer, server or other network host for open ports. In networking, each application running on a device is assigned an identifier called a port number. This port number is used on both ends of the transmission so that the right data is passed to the correct application. Port-scanning can be used maliciously as a reconnaissance tool to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to verify network security policies on the network.

For the purposes of evaluating your own computer network's firewall and port security, you can use a port-scanning tool like Nmap to find all the open ports on your network. Port-scanning can be seen as a precursor to a network attack and therefore should not be done on public servers on the Internet, or on a company network without permission.

To execute an Nmap port-scan of a computer on your local home network, download and launch a program such as Zenmap, provide the target IP address of the computer you would like to scan, choose a default scanning profile, and press scan. The Nmap scan will report any services that are running (e.g., web services, mail services, etc.) and port numbers. The scanning of a port generally results in one of three responses:

- **Open or Accepted** – The host replied indicating a service is listening on the port.

- **Closed, Denied, or Not Listening** – The host replied indicating that connections will be denied to the port.
- **Filtered, Dropped, or Blocked** – There was no reply from the host.

To execute a port-scan of your network from outside of the network, you will need to initiate the scan from outside of the network. This will involve running an Nmap port-scan against your firewall or router's public IP address. To discover your public IP address, use a search engine such as Google with the query "what is my ip address". The search engine will return your public IP address.

To run a port-scan for six common ports against your home router or firewall, go to the Nmap Online Port Scanner at https://hackertarget.com/nmap-online-port-scanner/ and enter your public IP address in the input box*: IP address to scan…* and press *Quick Nmap Scan*. If the response is *open* for any of the ports: 21, 22, 25, 80, 443, or 3389 then most likely, port forwarding has been enabled on your router or firewall, and you are running servers on your private network, as shown in the figure.

Security Appliances

Today there is no single security appliance or piece of technology that will solve all network security needs. Because there is a variety of security appliances and tools that need to be implemented, it is important that they all work together. Security appliances are most effective when they are part of a system.

Security appliances can be stand-alone devices, like a router or firewall, a card that can be installed into a network device, or a module with its own processor and cached memory. Security appliances can also be software tools that are run on a network device. Security appliances fall into these general categories:

Routers - Cisco Integrated Services Router (ISR) routers, shown in Figure 1, have many firewall capabilities besides just routing functions, including traffic filtering, the ability to run an Intrusion Prevention System (IPS), encryption, and VPN capabilities for secure encrypted tunneling.

FIGURE 1

FIGURE 2

Firewalls - Cisco Next Generation Firewalls have all the capabilities of an ISR router, as well as, advanced network management and analytics. Cisco Adaptive Security Appliance (ASA) with firewall capabilities are shown in Figure 2.

IPS - Cisco Next Generation IPS devices, shown in Figure 3, are dedicated to intrusion prevention.

FIGURE 3

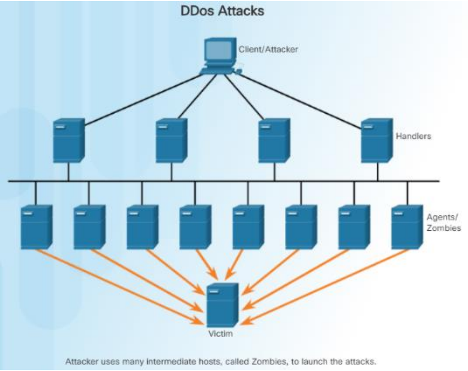
VPN - Cisco security appliances are equipped with a Virtual Private Network (VPN) server and client technologies. It is designed for secure encrypted tunneling.

Malware/Antivirus - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.

Other Security Devices – This category includes web and email security appliances, decryption devices, client access control servers, and security management systems.

Detecting Attacks in Real Time

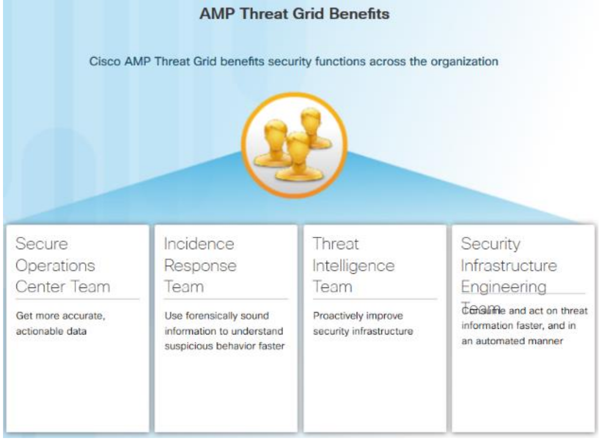
Software is not perfect. When a hacker exploits a flaw in a piece of software before the creator can fix it, it is known as a zero-day attack. Due to the sophistication and enormity of zero-day attacks found today, it is becoming common that network attacks will succeed and that a successful defense is now measured in how quickly a network can respond to an attack. The ability to detect attacks as they happen in real-time, as well as stopping the attacks immediately, or within minutes of occurring, is the ideal goal. Unfortunately, many companies and organizations today are unable to detect attacks until days or even months after they have occurred.


DDos Attacks
Client/Attacker
Handlers
Agents/
Zombies
Victim
Attacker uses many intermediate hosts, called Zombies, to launch the attacks.

- **Real Time Scanning from Edge to Endpoint** - Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices. Next generation client/server malware detection with connections to online global threat centers must also be used. Today, active scanning devices and software must detect network anomalies using context-based analysis and behavior detection.

- **DDoS Attacks and Real Time Response** - DDoS is one of the biggest attack threats requiring real-time response and detection. DDoS attacks are extremely difficult to defend against because the attacks originate from hundreds, or thousands of zombie hosts, and the attacks appear as legitimate traffic, as shown in the figure. For many companies and organizations, regularly occurring DDoS attacks cripple Internet servers and network availability. The ability to detect and respond to DDoS attacks in real-time is crucial.

Protecting Against Malware


AMP Threat Grid Benefits
Cisco AMP Threat Grid benefits security functions across the organization
Secure Operations Center Team
Get more accurate, actionable data
Incidence Response Team
Use forensically sound information to understand suspicious behavior faster
Threat Intelligence Team
Proactively improve security infrastructure
Security Infrastructure Engineering Team
Consume and act on threat information faster, and in an automated manner

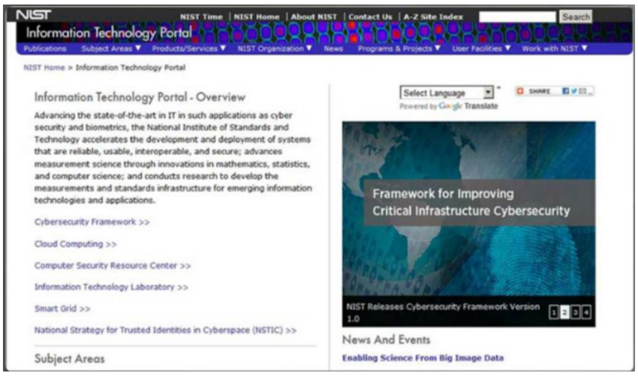
How do you provide defense against the constant presence of zero-day attacks, as well as advanced persistent threats (APT) that steal data over long periods of time? One solution is to use an enterprise-level advanced malware detection solution that offers real-time malware detection.

Network administrators must constantly monitor the network for signs of malware or behaviors that reveal the presence of an APT. Cisco has an Advanced Malware Protection (AMP) Threat Grid that analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts. This provides a global view of malware attacks, campaigns, and their distribution. AMP is client/server software deployed on host endpoints, as a standalone server, or on other network security devices. The figure shows the benefits of the AMP Threat Grid.

Security Best Practices

Many national and professional organizations have published lists of security best practices. The following is a list of some security best practices:

- **Perform Risk Assessment** – Knowing the value of what you are protecting will help in justifying security expenditures.
- **Create a Security Policy** – Create a policy that clearly outlines company rules, job duties, and expectations.


NIST
NIST Time | NIST Home | About NIST | Contact Us | A-Z Site Index
Search
Information Technology Portal
Publications
Subject Areas ▼
Products/Services ▼
NIST Organization ▼
News
Programs & Projects ▼
User Facilities ▼
Work with NIST ▼
NIST Home > Information Technology Portal
Select Language
Powered by Google Translate
SHARE

Information Technology Portal - Overview

Advancing the state-of-the-art in IT in such applications as cyber security and biometrics, the National Institute of Standards and Technology accelerates the development and deployment of systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

Cybersecurity Framework >>

Cloud Computing >>

Computer Security Resource Center >>

Information Technology Laboratory >>

Smart Grid >>

National Strategy for Trusted Identities in Cyberspace (NSTIC) >>

Subject Areas

Framework for Improving Critical Infrastructure Cybersecurity

NIST Releases Cybersecurity Framework Version 1.0

News And Events

Enabling Science From Big Image Data

- **Physical Security Measures** – Restrict access to networking closets, server locations, as well as fire suppression.
- **Human Resource Security Measures** – Employees should be properly researched with background checks.
- **Perform and Test Backups** – Perform regular backups and test data recovery from backups.
- **Maintain Security Patches and Updates** – Regularly update server, client, and network device operating systems and programs.
- **Employ Access Controls** – Configure user roles and privilege levels as well as strong user authentication.
- **Regularly Test Incident Response** – Employ an incident response team and test emergency response scenarios.
- **Implement a Network Monitoring, Analytics and Management Tool** - Choose a security monitoring solution that integrates with other technologies.
- **Implement Network Security Devices** – Use next generation routers, firewalls, and other security appliances.
- **Implement a Comprehensive Endpoint Security Solution** – Use enterprise level antimalware and antivirus software.
- **Educate Users** – Educate users and employees in secure procedures.
- **Encrypt data** – Encrypt all sensitive company data including email.

Some of the most helpful guidelines are found in organizational repositories such as the National Institute of Standards and Technology (NIST) Computer Security Resource Center, as shown in the figure.

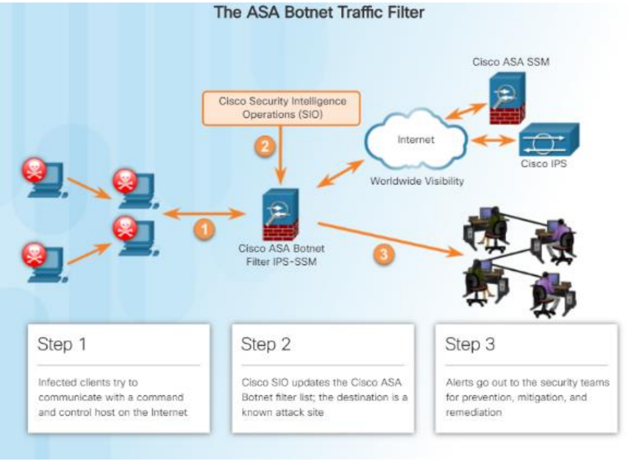
One of the most widely known and respected organizations for cybersecurity training is the SANS Institute. Visit https://www.sans.org/about/, to learn more about SANS and the types of training and certifications they offer.

Behavior Approach to Cybersecurity

Botnet

A botnet is a group of bots, connected through the Internet, with the ability to be controlled by a malicious individual or group. A bot computer is typically infected by visiting a website, opening an email attachment, or opening an infected media file.

A botnet can have tens of thousands, or even hundreds of thousands of bots. These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute force password attacks. Botnets are typically controlled through a command and control server.


The ASA Botnet Traffic Filter
Cisco Security Intelligence Operations (SIO)
Cisco ASA SSM
Internet
Worldwide Visibility
Cisco IPS
Cisco ASA Botnet Filter IPS-SSM
1
2
3

Step 1

Infected clients try to communicate with a command and control host on the Internet

Step 2

Cisco SIO updates the Cisco ASA Botnet filter list; the destination is a known attack site

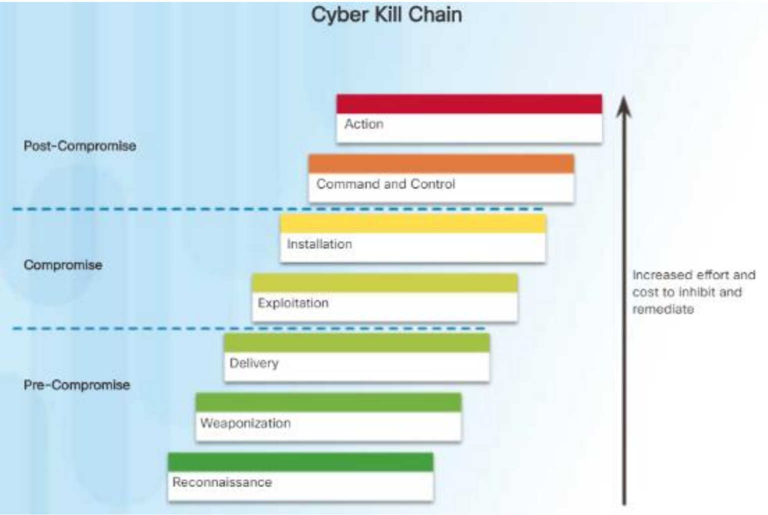
Step 3

Alerts go out to the security teams for prevention, mitigation, and remediation

Cyber criminals will often rent out Botnets, for a fee, to third parties for nefarious purposes.

The figure shows how a botnet traffic filter is used to inform the worldwide security community of botnet locations.

The Kill Chain in Cyberdefense



In cybersecurity, the Kill Chain is the stages of an information systems attack. Developed by Lockheed Martin as a security framework for incident detection and response, the Cyber Kill Chain is comprised of the following stages:

Stage 1. Reconnaissance - The attacker gathers information about the target.

Stage 2. Weaponization - The attacker creates an exploit and malicious payload to send to the target.

Stage 3. Delivery - The attacker sends the exploit and malicious payload to the target by email or other method.

Stage 4. Exploitation - The exploit is executed.

Stage 5 Installation - Malware and backdoors are installed on the target.

Stage 6. Command and Control - Remote control of the target is gained through a command and control channel or server.

Stage 7. Action - The attacker performs malicious actions like information theft, or executes additional attacks on other devices from within the network by working through the Kill Chain stages again.

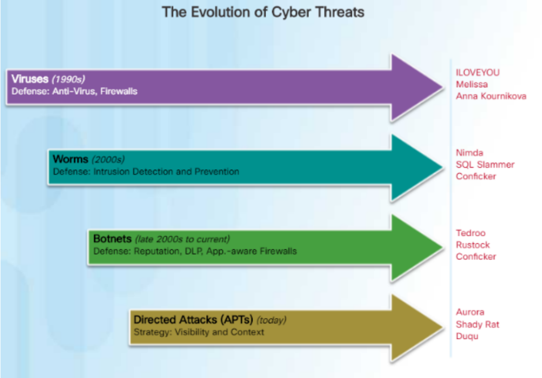
To defend against the Kill Chain, network security defenses are designed around the stages of the Kill Chain. These are some questions about a company's security defenses, based on the Cyber Kill Chain:

- What are the attack indicators at each stage of the Kill Chain?
- Which security tools are needed to detect the attack indicators at each of the stages?

- Are there gaps in the company's ability to detect an attack?

According to Lockheed Martin, understanding the stages of Kill Chain allowed them to put up defensive obstacles, slow down the attack, and ultimately prevent the loss of data. The figure shows how each stage of the Kill Chain equates to an increase in the amount of effort and cost to inhibit and remediate attacks.

Behavior-Based Security

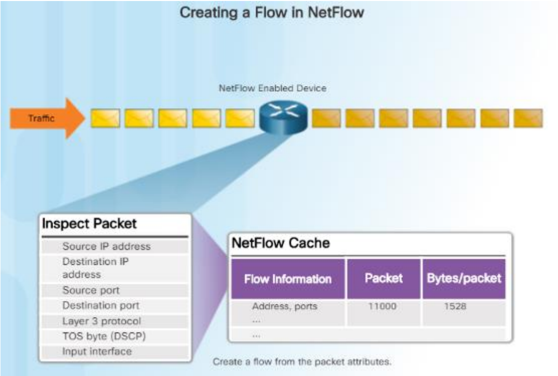

The Evolution of Cyber Threats
Viruses (1990s)
Defense: Anti-Virus, Firewalls
ILOVEYOU
Melissa
Anna Kournikova
Worms (2000s)
Defense: Intrusion Detection and Prevention
Nimda
SQL Slammer
Conficker
Botnets (late 2000s to current)
Defense: Reputation, DLP, App.-aware Firewalls
Tedroo
Rustock
Conficker
Directed Attacks (APTs) (today)
Strategy: Visibility and Context
Aurora
Shady Rat
Duqu

Behavior-based security is a form of threat detection that does not rely on known malicious signatures, but instead uses informational context to detect anomalies in the network. Behavior-based detection involves capturing and analyzing the flow of communication between a user on the local network and a local, or remote destination. These communications, when captured and analyzed, reveal context and patterns of behavior which can be used to detect anomalies. Behavior-based detection can discover the presence of an attack by a change from normal behavior.

- **Honeypots** - A Honeypot is a behavior-based detection tool that first lures the attacker in by appealing to the attacker's predicted pattern of malicious behavior, and then, when inside the honeypot, the network administrator can capture, log, and analyze the attacker's behavior. This allows an administrator to gain more knowledge and build a better defense.

- **Cisco's Cyber Threat Defense Solution Architecture** - This is a security architecture that uses behavior-based detection and indicators, to provide greater visibility, context, and control. The goal is to know who, what, where, when, and how an attack is taking place. This security architecture uses many security technologies to achieve this goal.

NetFlow



Flow Information	Packet	Bytes/packet
Address, ports	11000	1528
...		
...		

NetFlow technology is used to gather information about data flowing through a network. NetFlow information can be likened to a phone bill for your network traffic. It shows you who and what devices are in your network, as well as when and how users and devices accessed your network. NetFlow is an important component in behavior-based detection and analysis. Switches, routers, and firewalls equipped with NetFlow can report information about data entering, leaving, and travelling through the network. Information is sent to NetFlow Collectors that collect, store, and analyze NetFlow records.

NetFlow is able to collect information on usage through many different characteristics of how data is moved through the network, as shown in the figure. By collecting information about network data flows, NetFlow is able to establish baseline behaviors on more than 90 different attributes.

Cisco's Approach to Cybersecurity

CSIRT

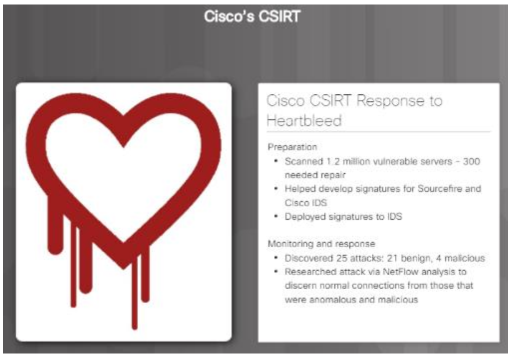
CSIRT Organizations

US-CERT
APCERT
FIRST
Improving Security Together
CERT-EU
Software Engineering Institute
Carnegie Mellon University

Many large organizations have a Computer Security Incident Response Team (CSIRT) to receive, review, and respond to computer security incident reports, as shown in Figure 1. The primary mission of CSIRT is to help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents. To prevent security incidents, Cisco CSIRT provides proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review.

Cisco's CSIRT collaborates with Forum of Incident Response and Security Teams (FIRST), the National Safety Information Exchange (NSIE), the Defense Security Information Exchange (DSIE), and the DNS Operations Analysis and Research Center (DNS-OARC).

There are national and public CSIRT organizations like the CERT Division of the Software Engineering Institute at Carnegie Mellon University, that are available to help organizations, and national CSIRTs, develop, operate, and improve their incident management capabilities.


Cisco's CSIRT

Cisco CSIRT Response to Heartbleed

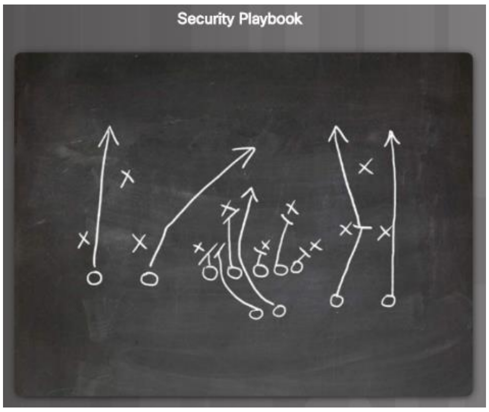
Preparation

- Scanned 1.2 million vulnerable servers - 300 needed repair
- Helped develop signatures for Sourcefire and Cisco IDS
- Deployed signatures to IDS

Monitoring and response

- Discovered 25 attacks: 21 benign, 4 malicious
- Researched attack via NetFlow analysis to discern normal connections from those that were anomalous and malicious

Security Playbook


Security Playbook

Technology is constantly changing. That means cyberattacks are evolving too. New vulnerabilities and attack methods are discovered continuously. Security is becoming a significant business concern because of the resulting reputation and financial impact from security breaches. Attacks are targeting critical networks and sensitive data. Organizations should have plans to prepare for, deal with, and recover from a breach.

One of the best way to prepare for a security breach is to prevent one. There should be guidance on identifying the cybersecurity risk to systems, assets, data, and capabilities, protecting the system by the implementation of safeguards and personnel training, and detecting cybersecurity event as soon as possible. When a security breach is detected, appropriate actions should be taken to minimize its impact and damage. The response plan should be flexible with multiple action options during the breach. After the breach is contained and the compromised systems and services are restored, security measures and processes should be updated to include the lessons learned during the breach.

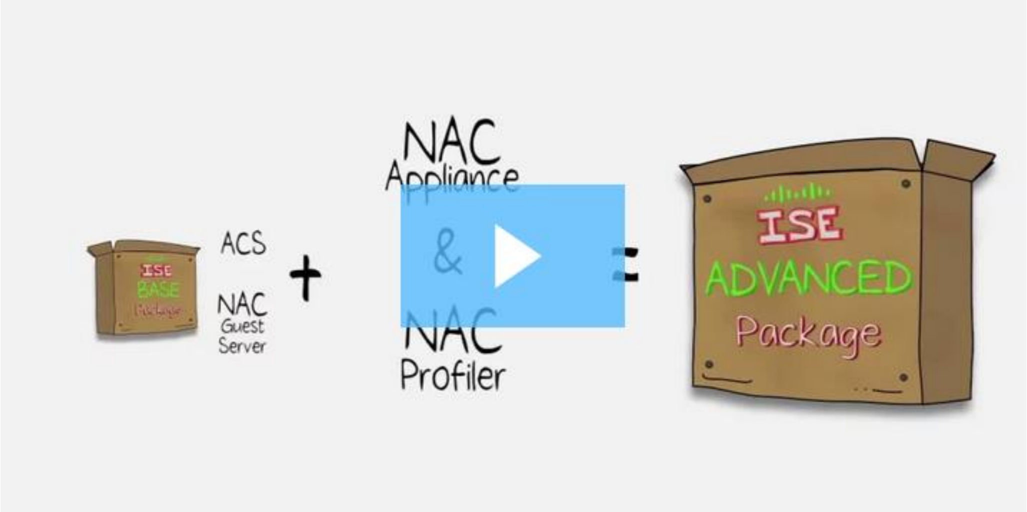
All this information should be compiled into a security playbook. A security playbook is a collection of repeatable queries (reports) against security event data sources that lead to incident detection and response. Ideally the security playbook must accomplish the following actions:

- Detect malware infected machines.
- Detect suspicious network activity.
- Detect irregular authentication attempts.
- Describe and understand inbound and outbound traffic.
- Provide summary information including trends, statistics, and counts.
- Provide usable and quick access to statistics and metrics.
- Correlate events across all relevant data sources.

Tools for Incident Prevention and Detection

These are some of the tools used to detect and prevent security incidents:

- **SIEM** – A Security Information and Event Management (SIEM) system is software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network.
- **DLP** – Data Loss Prevention Software (DLP) is a software or hardware system designed to stop sensitive data from being stolen from or escaping a network. A DLP system may focus on file access authorization, data exchange, data copying, user activity monitoring, and more. DLP systems are designed to monitor and protect data in three different states: data in-use, data in-motion and data at-rest. Data in-use is focused on the client, data in-motion refers to data as it travels through the network, and data at-rest refers to data storage.
- **Cisco ISE and TrustSec** – Cisco Identity Services Engine (Cisco ISE) and Cisco TrustSec enforce access to network resources by creating role-based access control policies that segment access to the network (guests, mobile users, employees) without added complexity. Traffic classification is based on user or device identity. Click play in the figure to learn more about ISE.



Fundamentals of ISE – Video Transcript

I remember my first security policy. So simple. Good stuff on, bad stuff off. Over the years, however, defining good and bad as gotten really difficult. So one policy quickly became two, then 10, then more and forget about just defining these policies, I need to enforce them as well. Now there's compliance and the need to prove I'm secure. On top of all that, everyone's bringing in his or her favorite Wi-Fi device and expecting full network access. Keeping up with this stuff takes time, people, and money, not to mention how I translate policy terms like location, users, devices, and applications into geek speak like IPs, MACs, ACLs, ports, and 802.1x. Enough! An answer for us. The Cisco Identity Servers Engine or ISE is an identity-based policy platform that enables compliance, enhances security, and streamlines operations. Its unique architecture lets you gather real-time contextual information about users and devices to proactively enforce governance policy across the entire network infrastructure. When you think about it, how could all this be attempted otherwise? As the central policy component for Cisco's TrustSec Solution, ISE is the single source for policy definition, control, and reporting. So, you want to be on my network? Let me show you the tool set. Triple A. Authentication, authorization, and accounting. Hey, what's your username and your password? Cool. Now let me give you access to just what you need and by the way, I'm logging this whole session just in case. Posture. Is this device clean? Carrying any suspicious applications or viruses? No? Profiler. You say you're a printer, but now you act like a web camera? I'm going to show you the door. Out! And now, guest management. Just need temporary access? No problem. You get just enough access, but when your time is up, it's up. And automatically. Nice thing for me, I don't even have to set you up as a guest. All that's handled by the person who wanted you to visit Now many of you are saying to yourself right now, self, this sounds just like Cisco NAC and ACS. And you're right. That's where it starts. ISE combines the functionality of both, but with simpler deployment and common management. Moving forward, ISE will extend more deeply into the network, into the data center, and the application stack. The Cisco Identity Services Engine is the single source of truth for end points all across the network. Now, there are really just two packages to understand here. The base package is all about authentication, ID, and guest services like what you find in Cisco ACS and NAC Guest Server. The advanced package adds profiling and posture services into the mix. A deeper more intelligent analysis of anything requesting access. NAC Appliance and Profiler, they'd be your reference points here. And anticipating your next logical question, no, this does not mean end of life for NAC or ACS. Every network is different. ICS is for those of us who want to consolidate policies in an 802.1x framework. If that's not you because say you want a choke point that's in line, or maybe you're just looking to authenticate a network device admins or something. Well, existing NAC or ACS products? They're going to be a better fit. Now speaking of fit, you have three different hardware appliances to choose from, as well as a VMwarebased and virtualized appliance. And because Cisco's shipping on the same hardware used by NAC and ACS today, there's a built-in level of investment protection. Always a good point to make to the bean counters, right? Now unlike other solutions, Cisco ISE has the ability to run specific functions at critical points in the network. For example, a pair of ISE appliances for administration, maintenance, and troubleshooting, and logging, and a high availability configuration. This could be located centrally, but with distributed appliances for making policy decisions as close to the user or device as possible communicating to your Cisco network infrastructure for enforcement. This is a really important design point to call out here. Cisco ISE works with your existing network devices, switches, wireless controllers, VPN concentrators, to balance the workload and keep enforcement as close to the end point as possible. If you have legacy gear in your network, no worries. ISE can make enforcement work with these as well. Now this example was a large network design simply to illustrate the flexibility available. You can still get tremendous value from just two of these things. Redundancy, right? Start small, add capacity through additional appliances or extra licenses whenever needed. All right. Our assault on complexity continues now with a simple interface including things like a centralized dashboard with hotlinks to more Video - Fundamentals of ISE Cisco and/or its affiliates. All rights reserved. Cisco Confidential Page 2 of 2 www.netacad.com details, flexible filtering of your active session, drag and drop re-ordering of rules, reusable objects. ISE uses state of the art widgets to make page-hopping and crazy scrolling a thing of the past. You're just going to love the clarity ISE provides here. Visibility into what just happened, when it happened, who or what was involved and how it was taken care of. We all know that complexity is the enemy of good security. This is why the ISE dashboard and the reporting tools, the live logs, are so robust and valuable. So there you have it. Cisco Identity Services Engine. Single point of truth restoring visbility and control to the edge of your network. Enough already, huh? Why don't you check it out for yourself? For more information, visit cisco.com/go/ise.

IDS and IPS

An Intrusion Detection System (IDS), shown in the figure, is either a dedicated network device, or one of several tools in a server or firewall that scans data against a database of rules or attack signatures, looking for malicious traffic. If a match is detected, the IDS will log the detection, and create an alert for a network administrator. The Intrusion Detection System does not take action when a match is detected so it does not prevent attacks from happening. The job of the IDS is merely to detect, log and report.

The scanning performed by the IDS slows down the network (known as latency). To prevent against network delay, an IDS is usually placed offline, separate from regular network traffic. Data is copied or mirrored by a switch and then forwarded to the IDS for offline detection. There are also IDS tools that can be installed on top of a host computer operating system, like Linux or Windows.

An Intrusion Prevention System (IPS) has the ability to block or deny traffic based on a positive rule or signature match. One of the most well-known IPS/IDS systems is Snort. The commercial version of Snort is Cisco's Sourcefire. Sourcefire has the ability to perform real-time traffic and port analysis, logging, content searching and matching, and can detect probes, attacks, and port scans. It also integrates with other third party tools for reporting, performance and log analysis.

Summary: Protecting the Organization

This chapter began by discussing some of the technology and processes used by cybersecurity professionals when protecting an organization's network, equipment and data. This included types of firewalls, security appliances, and software.

Botnets, the kill chain, behavior-based security, and using NetFlow to monitor a network were covered.

Finally, Cisco's approach to cybersecurity, including the CSIRT team and the security playbook were explained. It briefly covers the tools that cybersecurity professionals use to detect and prevent network attacks, including SIEM, DLP, Cisco ISE and TrustSec, as well as IDS and IPS systems.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

Chapter 5: Will Your Future Be in Cybersecurity

This chapter covers the legal and ethical issues that arise when working in cybersecurity. It also discusses educational and career paths for cybersecurity. There are educational paths towards certifications that you may wish to pursue with the Cisco Networking Academy. Some of these certifications are prerequisites to Specialization Certificates in many areas of networking, including cybersecurity.

The Networking Academy Talent Bridge page (netacad.com under Resources) provides good information to help you write a great résumé and prepare for a job interview. It also contains listings for Cisco and Cisco Partner jobs. Three external Internet job search engines are presented for you to explore.

Cybersecurity Legal and Ethical Issues, Education and Careers

Legal Issues in Cybersecurity

Cybersecurity professionals must have the same skills as hackers, especially black hat hackers, in order to protect against attacks. One difference between a hacker and a cybersecurity professional is that the cybersecurity professional must work within legal boundaries.

IMPACT

152 NATIONS

HAVE JOINED THE COALITION.

ITU-IMPACT IS TODAY, THE LARGEST GLOBAL CYBERSECURITY ALLIANCE

Personal Legal Issues

You do not even have to be an employee to be subject to cybersecurity laws. In your private life, you may have the opportunity and skills to hack another person's computer or network. There is an old saying, "Just because you can does not mean you should." Keep this in mind. Most hackers leave tracks, whether they know it or not, and these tracks can be followed back to the hacker.

Cybersecurity professionals develop many skills which can be used for good or evil. Those who use their skills within the legal system, to protect infrastructure, networks, and privacy are always in high demand.

Corporate Legal Issues

Most countries have some cybersecurity laws in place. They may have to do with critical infrastructure, networks, and corporate and individual privacy. Businesses are required to abide by these laws.

In some cases, if you break cybersecurity laws while doing your job, it is the company that may be punished and you could lose your job. In other cases, you could be prosecuted, fined, and possibly sentenced.

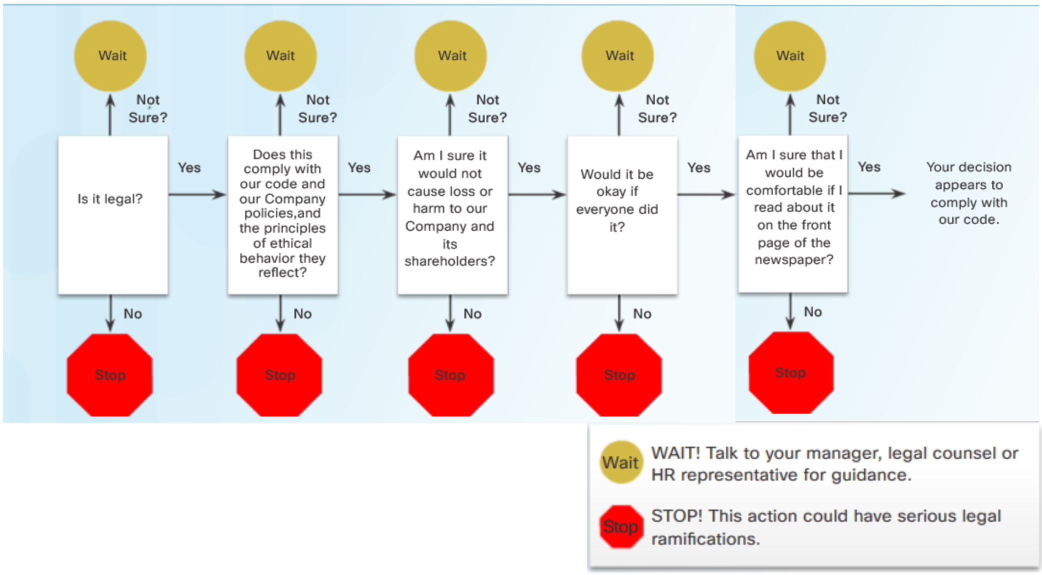
In general, if you are confused about whether an action or behavior might be illegal, assume that it is illegal and do not do it. Your company may have a legal department or someone in the human resources department who can answer your questions before you do something illegal.

International Law and Cybersecurity

The area of cybersecurity law is much newer than cybersecurity itself. As mentioned before, most countries have some laws in place, and there will be more laws to come.

Ethical Issues in Cybersecurity

In addition to working within the confines of the law, cybersecurity professionals must also demonstrate ethical behavior.


Wait
Not Sure?
Is it legal?
Yes
No
Stop
Wait
Not Sure?
Does this comply with our code and our Company policies,and the principles of ethical behavior they reflect?
Yes
No
Stop
Wait
Not Sure?
Am I sure it would not cause loss or harm to our Company and its shareholders?
Yes
No
Stop
Wait
Not Sure?
Would it be okay if everyone did it?
Yes
No
Stop
Wait
Not Sure?
Am I sure that I would be comfortable if I read about it on the front page of the newspaper?
Yes
No
Stop
Your decision appears to comply with our code.
Wait
WAIT! Talk to your manager, legal counsel or HR representative for guidance.
Stop
STOP! This action could have serious legal ramifications.

Personal Ethical Issues

A person may act unethically and not be subject to prosecution, fines or imprisonment. This is because the action may not have been technically illegal. But that does not mean that the behavior is acceptable. Ethical behavior is fairly easy to ascertain. It is impossible to list all of the various unethical behaviors that can be exhibited by someone with cybersecurity skills. Below are just two. Ask yourself:

- Would I want to discover that someone has hacked into my computer and altered images in my social network sites?
- Would I want to discover that an IT technician whom I trusted to fix my network, told colleagues personal information about me that was gained while working on my network?

If your answer to any of these questions was 'no', then do not do such things to others.

Corporate Ethical Issues

Ethics are codes of behavior that are sometimes enforced by laws. There are many areas in cybersecurity that are not covered by laws. This means that doing something that is technically legal still may not be the ethical thing to do. Because so many areas of cybersecurity are not (or not yet) covered by laws, many IT professional organizations have created codes of ethics for persons in the industry. Below is a list of three organizations with Codes of Ethics:

- The CyberSecurity Institute (CSI) has published a code of ethics that you can read here http://csisite.net/training/ethicsconduct.htm
- The Information Systems Security Association (ISSA) has a code of ethics found here http://www.issa.org/?page=CodeofEthics
- The Association of Information Technology Professionals (AITP) has both a code of ethics and a standard of conduct found here http://www.aitp.org/?page=EthicsConduct

Cisco has a team devoted exclusively to ethical business conduct. Visit http://csr.cisco.com/pages/governance-and-ethics, to read more about it. This site, http://investor.cisco.com/investor-relations/governance/code-of-conduct/default.aspx, contains an eBook about Cisco's Code of Business Conduct, and a pdf file. In both files is an "Ethics Decision Tree", as shown in the figure. Even if you do not work for Cisco, the questions and answers found in this decision tree can easily be applied to your place of work. As with legal questions, in general, if you are confused about whether an action or behavior might be unethical, assume that it is unethical and do not do it. There may be someone in your company's human resources or legal department who can clarify your situation before you do something that would be considered unethical.

Search online to find other IT-related organizations with codes of ethics. Try to find what they all have in common.

Cybersecurity Jobs

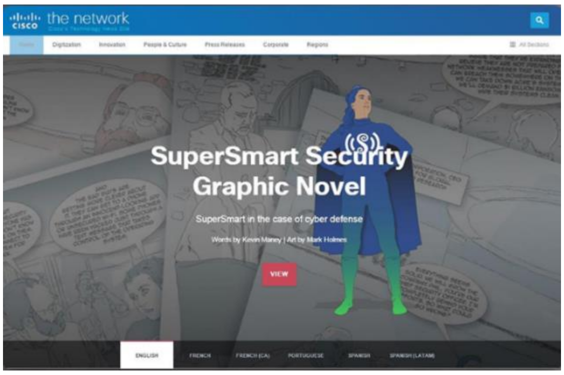
Many other businesses and industries are hiring cybersecurity professionals. There are several online search engines to help you find the right job in cybersecurity:

- ITJobMatch – The ITJobMatch search engine specializes in IT jobs of every kind, all over the globe. https://itjobmatch.com/
- Monster – Monster is a search engine for all types of jobs. The link provided goes directly to cybersecurity jobs. http://jobs.monster.com/search/?q=cybersecurity
- CareerBuilder – CareerBuilder is also a search engine for all types of jobs. The link provided goes directly to cybersecurity jobs. http://www.careerbuilder.com/jobs/keyword/cyber-security

These are just three of many different online job search sites. Even if you are just starting your education in IT and cybersecurity, looking at job search engines is a good way to see what kinds of jobs are available, all over the world.

Depending on your interest in cybersecurity, different types of jobs can be available to you, and they can require specialized skills certifications. For example, a penetration tester, also known as an ethical hacker, searches and exploits security vulnerabilities in applications, networks and systems. To become a penetration tester, you will need to gain experience in other IT jobs, such as security administrator, network administrator, and system administrator. Each one of these jobs requires its own set of skills that will help you become a valuable asset to an organization.

Our hope is that this course has peaked your interest in pursuing an education in IT and cybersecurity and then continuing on to an exciting career! The Cisco Networking Academy provides many courses for you to continue your education in Cybersecurity. We encourage you to enroll in the next course, Cybersecurity Essentials, to continue to build strong foundational knowledge in Cybersecurity. Check out the Cisco Networking Academy and see a list of courses that are available. Furthermore, you can also access career resources available in Cisco Networking Academy.



Just for fun, go to http://newsroom.cisco.com/supersmartsecurity to read a graphic novel about a cybersecurity superhero!

Before You Go

Congratulations! You are nearly done with this course. Before you go, have a look at all the ways that NetAcad can support your education and your career!

- **Cisco Cert Exams and Discount Vouchers** – You have worked so hard to complete this course. Now it is time to think about how your new skills and knowledge can help when taking industry-recocognized certification exams, Not only that, netacad.com might also be able to help save you money on the cost of exams!
- **Talent Bridge** – Is It time to find a GREAT job? Talent Bridge can help. Register today at https://www.netacad.com/careers/employment-opportunities/learn-about-talent-bridge, and start your search. Talent Bridge can match your skills and experience with jobs at Cisco and Cisco Partners. They are always looking for NetAcad Alumni!
- **Career Resources** – Is this your first job search? Maybe it's been a long time since you've looked for a job. Click **Careers** at the top of netacad.com. You'll find great information on employment opportunities, webinars, career advice, pathways, certifications and success stories. While you're here, click **Courses** at the top of the page. At the bottom of the drop down menu, click **All Courses** to see what else Netacad has to offer.

Summary: Will Your Future Be in Cybersecurity?

This chapter began by discussing the legal and ethical issues that professionals in cybersecurity commonly face. It also presented educational and career paths for those who wish to become cybersecurity professionals. Three external Internet job search engines are presented for you to explore.

If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.