

Chapter 2 – Threat Management & Cybersecurity Resources

Objectives

1. Describe how vulnerabilities are defined.
2. List the two main sites with vulnerability libraries.
3. List the steps required to ensure any testing or scanning is performed in a legal manner
4. Perform a basic vulnerability scan
5. Use the results of a vulnerability scan to mitigate any vulnerabilities
6. Describe how TCP/IP addresses and ports are used
7. Identify commonly used port numbers
8. Perform a network scan and identify open ports on a device
9. Explain what a penetration test is
10. Identify the rules of engagement and how to perform a pen test
11. Compare and contrast vulnerability scans and pen tests
12. Describe different cybersecurity resources
13. Define the relationship between updates, patches, and vulnerabilities.
14. Describe the different methods for ensuring patches and updates are installed
15. Check an OS or application for update/patch status
16. Describe the purpose of a cyber security framework
17. Identify common cyber security frameworks
18. List the major steps in a cyber security framework
19. Apply what you've learned to your home computers, tablets, phones, routers, and other devices.

What this section is about – what you should learn

When you start working in cybersecurity you'll find that it's different than most other areas of Computer Science or Information Technology in that you won't be given a specific task to work on, you'll be responsible for security. But what does being in charge of cybersecurity mean on a day to day basis or hour to hour basis? It's not like programming where you need to write a program to meet specific needs, or network administration where you'll be tasked with configuring and maintaining computers and network devices. You won't be given a specific set of tasks, but you'll be the person responsible for ensuring that the organization's data and devices are protected. So, how do you move from the vague notion of providing security to a specific set of tasks you can perform?

In this section you'll learn the basics of how to do this by asking, and finding the answers to, two questions. The first question is "What are the current security problems?" The second is "What problems need to be fixed right now, and which ones can wait for later?" You'll then learn how to build a process where you continuously improve security by repeatedly ask these questions.

A good analogy to help you understand these concepts is to compare working as a cyber security specialist with working as the person in charge of physical security for a hotel chain, or apartment complex, or shopping mall. When you initially start your job, you'll need to have some way to evaluate the current security for the building, and then some process to use to ensure that you're fixing any big problems first, while not losing site of smaller problems, and constantly updating the list of issues that need your attention to catch any new issues big or small, that may arise.

Or, just think about security for your home, not cybersecurity, but the physical security like your locks and doors. Hopefully you live in a safe area where you don't have to give this any thought, somewhere where you can leave your house open and unlocked without any worry. But if you've ever lived in the big city or a high crime area, or even when you move into a new place, you need to give your physical security some thought. For example, you might go through the following checklist.

1. Doors have working locks. Reinforced frames and locks in high crime areas.
2. Garage door(s) have locks, or powered openers use secure codes
3. Windows have working latches. May have bars on windows in high crime areas.
4. Doorbell or security cameras may be installed and tested.
5. Motion detector lights are installed and tested
6. Cars parked outside are secure
7. Spare house key is well hidden
8. Foliage around house is placed as to not hide attackers
9. Home security system is installed and tested
10. Large, protective dog that barks at strangers, lives in house

If any of the items are missing, or broken, or need batteries, it will give you a list of things to do. If there are multiple issues you'll have to make a judgment call regarding which one is the most important. Sometimes the most important task is obvious, like if the garage door is broken or the lock on the back door doesn't work. But there may be times where you've taken care of the big things and you don't have any issues at the current time.

Now let's jump back and look at the problem of providing security to multiple buildings, like the shopping mall or apartment complex. When you deal with multiple buildings the process for checking the current security profile to find any problems becomes more complex. It's the same general process as checking the security for your home, but there are a lot more things to check. This is the same type of problem that you face in cybersecurity, where you have multiple computers and devices to secure.

Which brings us back to the two questions that can be used to decide what tasks need to be done.

With cybersecurity there are two main processes used for answering the question “What are the current security problems”. These two processes are called Penetration Testing, or Pen Testing, and Vulnerability Scanning. They are both used for evaluating the security posture of a computer, network, or organization, and building a list of issues that need to be addressed, but there are a couple of significant differences. For example, vulnerability scans use an automated process that use a program to check systems against a predefined list of vulnerabilities, and they’re run by someone inside an organization. You can think of this as someone assessing the physical security of building using a checklist, like we discussed above. A pen test on the other hand, would be like hiring someone to check your physical security by actually trying to break in. They might use the same check list to start with, but they don’t have to just stick to the items on the list. With computers and networks, a pen tester might start with a vulnerability scan, but good pen testers will have many more “tricks up their sleeves”, and might do things like use phishing attacks or drop USB drives infected with malware on a sidewalk or in the parking lot near the business.

The book covers pen testing first, and then vulnerability scans or vulnerability assessments, but I’m going to talk about vulnerability assessments first. Another related item, that’s very important is the list of vulnerabilities used in vulnerability scans and pen tests. You’ll learn about where this list comes from, who maintains, and what type of information it contains. The book doesn’t talk a lot about this, but you will have an exercise where you look at it in more detail. The last thing this chapter covers is something called frameworks, which are the important, overall process used in Cybersecurity and Information Assurance (CSIA) to continually evaluate and improve security and ensure that all aspects of CSIA are being addressed and nothing is overlooked.

As always in this class, you’ll learn a lot of new terminology. You’ll also get a brief glimpse at the programs and processes used in port scanning, vulnerability assessment, and penetration testing. These are all very interesting subjects but once again there’s not enough time in the class to do much more than give you a small taste of each. If you find them interesting, you’re in luck as you can look forward to learning more about them in later classes.

Vulnerability Assessments

In this section you’ll learn about Vulnerability Scans or Vulnerability Assessments, and we’ll break it down into the following:

1. Background
2. General steps
3. Scanning a single computer
4. Scanning an organization

Background

You’re being told that a vulnerability scan will check a system against a list of all known possible vulnerabilities, but what exactly is a vulnerability, and has somebody really built a list of **all** the

known vulnerabilities? And if they have, how do you get your hands on and use a copy of the list?

Let's start by defining the term vulnerability. In the previous chapter you learned that a vulnerability is a weakness that an attacker could use to gain unauthorized access to data or a system. Every device and every OS have a list of vulnerabilities, and new vulnerabilities are found every day. That's the dictionary definition, the problem for you, as a cybersecurity professional, is keeping track of all the different vulnerabilities on all the different systems. Luckily there are a few groups that track vulnerabilities and have built databases that you can use to check for problems on a specific system. One of these is the Common Vulnerabilities and Exposures (CVE) database run by the Mitre Corporation, and another is the National Vulnerability Database (NVD) run by the NIST. You'll take a detailed look at these in one of your homework assignments, but for now you just need to know that there are a metric crap ton of vulnerabilities. There are way too many for any one person to keep track of. It would be like a home security checklist with 200,000 items to check. You can think of the CVE and NVD databases as being like Wikipedia in the sense that they're huge central silos of information that anyone can access. But in this case, they're only used to track vulnerabilities, and unlike Wikipedia not just anyone can add or edit the database entries. Another key point about the CVE and NVD database is that also list the fix, update or patch that can be installed to mitigate the problem.

The following figure shows an example of the database entry for a single NVD entry. Note that it says what it affects, in this case an application called Geyser that's associated Minecraft, and how to mediate the issue, in this case by upgrading the application.

CVE-2021-39177 Detail

Current Description

Geyser is a bridge between Minecraft: Bedrock Edition and Minecraft: Java Edition. Versions of Geyser prior to 1.4.2-SNAPSHOT allow anyone that can connect to the server to forge a LoginPacket with manipulated JWT token allowing impersonation as any user. Version 1.4.2-SNAPSHOT contains a patch for the issue. There are no known workarounds aside from upgrading.

[+View Analysis Description](#)

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

	NIST: NVD	Base Score: 9.8 CRITICAL
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
	CNA: GitHub, Inc.	Base Score: 7.4 HIGH
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N		

The following figure shows the CVE database entry for the same vulnerability. Notice that it includes a link to the NVD database entry.

CVE-ID	
CVE-2021-39177	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Geysers is a bridge between Minecraft: Bedrock Edition and Minecraft: Java Edition. Versions of Geysers prior to 1.4.2-SNAPSHOT allow anyone that can connect to the server to forge a LoginPacket with manipulated JWT token allowing impersonation as any user. Version 1.4.2-SNAPSHOT contains a patch for the issue. There are no known workarounds aside from upgrading.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• CONFIRM:https://github.com/GeysersMC/Geysers/security/advisories/GHSA-h77f-xxx7-4858• URL:https://github.com/GeysersMC/Geysers/security/advisories/GHSA-h77f-xxx7-4858• MISC:https://github.com/GeysersMC/Geysers/commit/b9541505af68ac7b7c093206ac7b1ba88957a5a6• URL:https://github.com/GeysersMC/Geysers/commit/b9541505af68ac7b7c093206ac7b1ba88957a5a6• MISC:https://updates.playhive.com/weekend-maintenance-disclosure-2kJMaY• URL:https://updates.playhive.com/weekend-maintenance-disclosure-2kJMaY	
Assigning CNA	
GitHub (maintainer security advisories)	
Date Record Created	
20210816	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20210816)	
Votes (Legacy)	

Both databases have been around for many years and contain hundreds of thousands of entries, with new ones being added as new vulnerabilities are found, which means almost constantly. The databases are very complete and contain vulnerabilities for all kinds of devices and Operating Systems including computers, mobile devices, networking devices such as routers, even vehicles. You may not realize it at the moment, but the fact that this data has all been captured and is free for use is nothing short of amazing. Can you imagine how much work it would be if you had to create and maintain your own list of vulnerabilities for every device you might have to support. It would be impossible. And the fact that these databases are free to use is even more amazing, although in reality they are supported by the US government, so they are supported using our tax dollars.

You'll look into these databases more in an exercise for this chapter, but for now the important thing to take away from this is that when we say we're checking a device for vulnerabilities we mean that we're checking it against the vulnerabilities stored in these databases. If you want to know more about the CVE and NVD database entries you can also try the following links. If these links don't work you should try searching on your own, or you can check out the videos I made for you.

<https://www.cvedetails.com/browse-by-date.php> - You can use this if you want to see what a CVE looks like, and how many are issued.

<https://cve.mitre.org/> - This is where you would go to download the entire CVE database, or report new vulnerabilities.

<https://nvd.nist.gov/vuln-metrics/cvss#> - NIST database of CVEs. This page tells you how to read the CVSS scores which range from 1-10.

The next thing to learn about is how a vulnerability scan is performed. If you were going to do the scan manually you'd have to first check a system and determine what hardware it uses, what the OS is and what patches and upgrades have been installed, what services it may be running, and finally what applications are installed and the version of every application. You'd next have to query the CVE and NVD databases and see if there are any vulnerabilities associated with all of hardware or software items on your list. Building the list and making the database queries wouldn't be an impossible task, it'd would take a lot of time, but it could be done. But, luckily for us, someone wrote a program to automate the process, and now there are several good vulnerability scanning programs available.

The following sites have list of tools. If these links no longer work, you can find similar sites by searching for something like "vulnerability scan tools".

<https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/>
<https://www.softwaretestinghelp.com/vulnerability-assessment-tools/>

So, when someone says they're doing a vulnerability scan they mean that they're running one of these applications. The application will do what you'd do manually, build a list of everything on a computer and then check the CVE and NVD databases for any known vulnerabilities. It's also important to note that a vulnerability scan is much more than simply checking that all OS and browser updates are installed. Checking the OS and browser for updates are a good start, but a vulnerability scan checks ALL applications.

Vulnerability Scan/Assessment - General steps

Now that you know what is meant by vulnerability and vulnerability scan, let's look the general steps in installing and running a vulnerability scan application. A lot of this will be the normal download and install process, but there are a couple steps that are specific to vulnerability scan programs.

1. Download, and install. This is just like downloading and installing any program.
2. Configure the application. This step is different than most programs as most vulnerability scan applications require you to create an account. This is because when you run the program it will connect to a server that will provide the most current list of CVEs and NVDs to check. This is done new because new vulnerabilities are being found every day and this way you'll always be scanning against the most current list.

3. Configure a scan. This will tell the program things like what device(s) you want to scan, and what types of things you want to check or not check, such as connected USB drives, etc.
4. Run the scan. The only thing about this step that may be out of the ordinary is how long it can take to complete. Of course, this depends on the speed of the system being checked and the network connection, but typically there are a lot of vulnerabilities to check and it can take several minutes to finish.
5. Generate a report and interpret the results. A vulnerability scan will produce a list of any vulnerabilities found during the scan. These will use the information from the NVD database to let you know how critical the vulnerability is, and whether you need to deal with it right away, or if it may not be a big deal. Looking at the list of results and deciding what to do about them is the vulnerability assessment, so it's a little more involved than running a scan. Doing the assessment takes more experience and knowledge than just running a scan, as you need to be able to recognize how critical each vulnerability may be and what they mean to your organization. Note that the terms *Vulnerability Scan* and *Vulnerability Assessment* refer to two slightly different things, but they're often used interchangeably. *Vulnerability Scan* refers to the process that will build a list of vulnerabilities, while *Vulnerability Assessment* refers to doing a scan, and then assessing the results of the scan and deciding what to do about any vulnerabilities found in the scan. Most people don't make this distinction between vulnerability scan and vulnerability assessment, and the terms are often used interchangeably. In reality, and in the workplace, anyone can run a scan as the only thing it requires is running a program, but performing an assessment requires a professional who knows how to interpret the results of the scan, decide whether any vulnerabilities that were found are important or not, and what to do if something needs to be done.

Let's use the shopping mall security as an example. Assume you hire someone to do a safety scan and the results of the scan report the door at the rear of Noah's Pet Store doesn't have a lock. This would be a critical security issue if the door opened to the outside of the mall. However, you know that this door leads to the dog grooming area, and the dog grooming area has no other doors in or out, which means the door doesn't need a lock.

Running a scan on a typical home computer might seem like it should be a relatively simple and quick process, but it's actually a little complicated, complicated enough that it's not something a typical home user is going to do. The typical home user can do things like check to make sure the OS and browser are updated, and run an anti-virus scan, but checking for all the possible vulnerabilities in the hardware, OS, and applications requires installing and running a vulnerability assessment program, which is beyond the skill set of the typical home user.

Demo of scanning a single computer

If you want to see the complete process for installing a vulnerability scan program, and running the scan on a Windows Home computer using a program called Nessus there's one in the following YouTube video. It's not necessary that you watch this, as you aren't required to do a scan in this class, and you'll get plenty of experience in a later class. But watching the video or even trying it yourself should give you a better idea of what a vulnerability scan is and what it can show you. Just be warned that if you do try this yourself it will require you to create an account at Nessus.

<https://www.youtube.com/watch?v=H2ajE4KoqL4>

Scanning an entire network or organization

Now that you have a better idea of what a vulnerability scan is, and how to perform it on a single computer, it's time to look at scanning all the devices in an entire organization. You could do this by going to each device in the organization and performing a scan, but this would not only be time consuming, it would mean you'd need to know the location of every device. The developers behind the vulnerability scanning programs realized that that this would be a problem and found ways to automate the process. That is, they've designed their programs so you can first use them to discover every device connected to a network, scan each of those devices, and build a report for each device.

You might think that this is only applicable to a business or large organization, but you can also use it on your home network. You might think the only thing connected to your network is your computer, but it's also possible that your network is being used by your printers, your phone(s) and tablet, game consoles, smart appliances, etc. And, if you haven't set up good security on your home router, it's even possible that your neighbors are leaching off your home network.

I'm going to explain how this works, but this is another optional subject. Understanding the process requires learning some background on TCP/IP, which is advanced enough that you'll spend the better portion of an entire class to learn about it. I'm going to try and explain it in a few paragraphs, but you don't need to know all the details for this class. For this class you just need to know that most programs you'll use for vulnerability scanning are capable of scanning all the devices on a network.

1. Background on TCP/IP
2. Discovering devices – network mapping
3. Discovering open ports on devices – port mapping
4. Configuring the scan
5. Run the scan
6. Generate report and interpret the results

Background on TCP/IP

The first network concept to learn about is how computers communicate on the Internet. This is accomplished by the following:

- The information is placed in something called a packet, which is like a package. You can think of the packet like a snail mail letter. The packet has the address of the computer the package is being sent to (destination), the address of the computer sending the package (source), and the actual information (data) stuffed inside the packet.
- The source and destination addresses are called IP addresses. (IP stands for Internet Protocol, but no one ever spells it out. It's always just IP.) Every computer or device on the Internet has a unique IP address. The IP addresses perform the same general function as a phone number as they uniquely identify a computer. IP addresses consist of 4 numbers separated by a dot or period. For example, 192.168.2.14. And like phone numbers, part of each IP address determines which network the device is on, and part of it identifies the specific device on the network.

Let's illustrate this with the phone number 1-509-547-0511. The leading 1 is the country code for the United States, 509 is the area code for Eastern Washington state, 547 is a prefix used in Pasco Washington, and 0511 identifies the specific phone. The first numbers in the IP address tell us which network the number is associated with, and the last numbers tell us a specific computer on a network. For example, in the IP number 212.69.159.108 the numbers 212.69.159 identify the CBC network, and the number 108 identifies the specific computer on the CBC network. In this case the 212.69.159 is called the network portion of the IP address and the 108 is called the host portion.

- A network packet sent to an IP address will get it to the correct computer.

Ok ... I know that's a large chunk of information to process if it's the first time you've been exposed to it. But the main thing to take away is that network packets sent to an IP address will get the packets to the correct computer on the Internet. (If you know about TCP/IP networking you might know that I'm simplifying how things work a bit. But I want to keep this brief while still providing enough information so you understand the basics of network vulnerability scans. If you don't know a lot about TCP/IP, don't worry about learning more at this point. You'll learn all about this in your networking classes.)

Network Ports and Port Mapping

The next network concept to learn about is how computers determine which program should be given an incoming network packet. This is necessary because a single computer can be running several different programs that could be expecting a delivery of network packets. Sending network packets to an IP address gets the packets to the correct computer, but we need something more to get the packets to the correct program on that computer. For example, you could be running a web browser, a music player like Spotify or Pandora etc., and maybe even hosting your own Minecraft server. And most companies run things like mail

servers, database servers, web servers etc.; and they could all be running on the same computer. Network packets sent to a computer's IP address will get those packets to the computer, but now the computer needs to decide which program should receive the packets. This is accomplished by the following:

- Each program on a computer that sends or receives network packets is assigned something called a port number. You can think of the port number as being like a phone extension. That is, large organizations such as CBC use a single phone number, (509) 547-0511, even though there are thousands of phones at the college. Calling the main number will get your phone call to CBC, just like sending a packet to an IP address will get it to a computer. But once your call is received at CBC it has to be routed to the correct extension to get it to the correct person. This is what port numbers do on a computer, provide a means to get the incoming packets to the correct program.
- When a network packet is sent, the port number of the program on the destination computer is included along with destination IP address. This way when the packet arrives at the destination it will be passed to the correct program.
- There are lists of standard port numbers that are almost always used for services like web servers or email servers. When packets are sent to standard services, like a web server or an email server, they will be sent to something called a "well-known" service. For example, HTTP packets are almost always sent to port 80 and HTTPS packets are almost always sent to port 443. If you set up your own server for something like Minecraft you'll have to assign it a port number, and then let anyone you want to connect to the server know what the port number is. Using the phone number extension analogy, this is like saying there's a set of standard extensions that almost everyone uses. For example, the operator will probably use extension 0, and the HR Department will use extension 666 LOL. We don't actually use these standard extensions for phones, other than 0 for the operator, but hopefully you get the idea.

The next concept to understand is what port-mapping is, and what it accomplishes.

- Port mapping consists of two steps. The first step is building a map of a network, or specifically building a list of all the computers or devices connected to a network. Technically this is called network mapping, and it is done by checking all of the IP addresses on a network to see if that address is currently in use. Going back to the phone analogy, this would be like calling an entire set of phone numbers to see if anyone answers. If someone answers then you know the phone is being used. For example, an attacker might call all 10,000 phone numbers that start with (509) 547. That is, they will start by calling (509) 547-0000, then call (509) 547-0001, (509) 547-0002 ... and end by calling (509) 547-9999.
- Once you have a map showing all of the active IP addresses, the next step is to determine which ports are open at each IP active IP address. This is done by sending

packets to different ports and see if there is any response. For example, if you send packets to port 80 and get a response then you know there's a good chance the device at that IP address is running a web server. When this is complete, you will have a map, or list of all the devices on the network, and what network programs each device is running.

- After the port mapping is complete, you can begin the network vulnerability scan. When a vulnerability scan is run it's set to target each computer or device on the network, and check all of the vulnerabilities for that type of computer or device, and for each open port found in the port mapping step. For example, if the port mapping reveals that the computer at an IP address is a Windows based computer running a web server and an email server, the vulnerability scan program will check all the vulnerabilities in Windows web servers and Windows email servers. This process is fairly automated as you can just point the vulnerability analysis program at a computer or device and let it run. When the program is finished it will produce a report that contains a list of open vulnerabilities on the device that was scanned.
- After you've finished running the vulnerability scan on all of your devices you'll have a list of all the open vulnerabilities. At this point you need to do the part of the process that can't be automated as it requires analyzing the findings of the vulnerability scan. The vulnerability assessment or analysis phase requires looking at all list of problems returned by the vulnerability scan and deciding:
 - A. Whether everything on the list really is a problem. The vulnerability scanning programs are very easy to run, but it takes some experience to decipher what the actual vulnerabilities are, what they mean, and whether or not you actually need to deal with each vulnerability. For example, the scan might find problems with a web server on one of your computers, but you know that the computer in question is only being used by other security analysts at the company as a testbed, and that they require the vulnerability to remain open to do their work.
 - B. What to do about each vulnerability. It might be as simple as installing a patch, but it might be as complicated as writing new database code to sanitize queries or writing new program code.
 - C. How to prioritize any actions you decide to take. Typically, you want to mitigate the most serious problems first, and then deal with any minor issues. But it takes experience with both cyber security and with the specific business you're working with to decide what makes a problem more or less serious. Going back to the house analogy, you might find an exterior door that doesn't lock. If this door is the front door to your home you should get it fixed immediately. But if this is the door to your garden shed, and all you store in the shed is an old shovel and a rake, then this probably isn't your most pressing issue.

Pen Testing

The other process to learn about is penetration testing, or pen testing as it's usually called. Pen testing is meant to provide a more complete picture of a company's security than can be shown from a vulnerability scan. While a vulnerability assessment will report potential problems, the person running the scan doesn't actually try to break in. In a Pen Test, the security analyst will try to make use of any vulnerabilities and break into a system.

A pen tester may start by running a vulnerability scan, but they would then take the next step and try to leverage any vulnerabilities to try and gain access. A good way to understand the difference between a vulnerability scan and a penetration test is go back to the physical building security analogy. As pointed out earlier, you can run a vulnerability scan and check all your doors and locks for problems. If you find any problems with the hardware during the vulnerability scan you can add the item to your list of things that need to be fixed, but you won't actually try to break in. In a pen test, the tester will also look for vulnerable locks and doors, but if any are found the tester will try and exploit the weakness and gain access to the building.

A good pen tester can also chain together attacks on vulnerabilities to penetrate deeper into a network than they would be able to by exploiting a single weakness. For example, they may be able to use a weakness in a network router to gain a foothold inside a network, and from there exploit a weakness in a server to gain unauthorized access to user account. The pen tester may then be able to use that user account to run an attack that would give them administrative access to a different system. Using the physical security analogy, this would be like finding a broken lock which provides access to a store room. From the store room the pen tester might be able to access the ventilation system, and crawl through the vents to gain access to an office that contains the keys that will unlock every room in the building.

Another way to make the distinction between a vulnerability scan and a pen test is to think of a vulnerability scan as a checklist someone inside the company runs through, while the pen test is similar to what someone outside the organization, like an attacker, would do. This analogy is not quite correct, as often pen testers are given inside access to an organization, but it should help you visualize the difference.

The last difference between pen tests and vulnerability assessments, at least the last difference I'm going to bring up, is that a vulnerability scan is great for finding weaknesses in hardware and software, but it completely fails to test what's been proven to be the biggest source of security problems which is wetware or people. Remember that most attackers succeed by taking advantage of mistakes made by a company's users. The users fall for phishing attacks, they use weak passwords or use the same password on multiple systems, or they feel lucky when they find a thumb drive in the parking lot, etc. A good penetration test will include a vulnerability scan, but it will also test the users to see how well they respond to things like phishing attempts, etc.

Hopefully this all makes sense, but I realize it's a lot to take in. And once again, don't worry about learning all the details or even becoming an expert on TCP/IP, or at running vulnerability scans or pen tests. If you get the BAS in Cybersecurity you'll have entire classes devoted to these subjects.

For now, here are some of the main points you should take away:

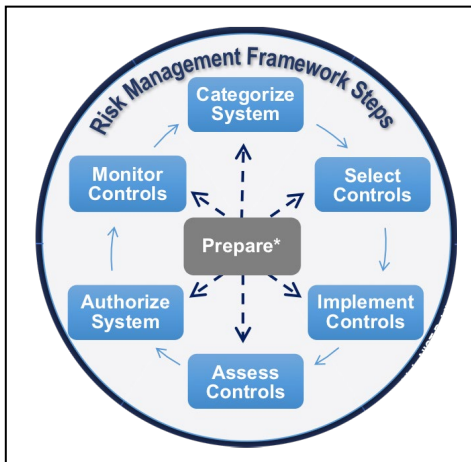
1. A vulnerability analysis provides you with a list of vulnerabilities that should be addressed. It can be run against a single device, multiple devices, or all the devices on a network. These are the same vulnerabilities that attackers use, which means you need to mitigate any problems before an attacker is able to exploit it. Running a scan is relative simple, but interpreting the results and knowing how to mitigate any issues requires more knowledge and experience.
2. The network and port mapping performed when you run a scan of a network may reveal devices on your network that you didn't know were in existence or in place.
3. In addition to just checking for missing updates and patches, a pen test should reveal things like poorly configured security on different services like a web server, database server, mail server, etc. Rather than just supplying a list of vulnerabilities, the pen test tries to attack a device or network by exploiting weaknesses in hardware, software, and possibly with the company's employees. The pen test will also provide a list of problems that need to be mitigated.
4. Vulnerability assessments and pen tests provide you with perspective on the overall security of a device, network, or organization, which allows you to prioritize the work to be done moving forward.

The Pledge

Oh ... and let me emphasize one important item about cyber security. That is the fact that you're learning how to do things, like port mapping and vulnerability scans, which can get you in serious trouble. You'll learn more about the specific laws covering computer crimes in other classes, but for now it should suffice to say that running these types of scans against computers or networks where you do not have prior authorization is a violation of the law. The programs for doing these types of scans and assessments are easy to find and use, but you should only use them to test systems after you have written permission from the proper authority. If you run these types of scans against a system or network it will almost certainly be detected and logged, and this information can be used to easily trace the attack back to your computer. If you do a scan or pen test with the company's permission it's called an assessment and you get paid to do it. If you do a scan or pen test without permission it's called an attack and you get to go to jail. So, make sure and use your powers only for good, and not for evil. I know this may sound like a joke but it's very serious. Never do a port scan, vulnerability analysis, or pen test against a system or network unless you have prior written authorization to protect you.

Frameworks

The chapter closes with a discussion of frameworks. To understand what a framework is, you need to understand that taking care of Cybersecurity issues is a repetitive process, as shown in the following figures. It's not something that you do once and say you're finished. When you view Cybersecurity from this perspective it's often referred to as Information Assurance.



The specific steps defined in each of the frameworks illustrated above have different names or labels, but they basically do the same things. Generally speaking, the process followed in most frameworks is to first define the risks for a system, check for vulnerabilities, and then mitigate or fix any vulnerabilities that you find. You also have a step in the process where you address any security breaches or failures. You start the process with the biggest and most obvious risks, but after they're addressed you repeat the process for any remaining risks or check for new risks. It's kind of like going to the doctor to check your health. Say you visit the doctor and you have a great checkup, and the doctor says you have no health issues. That's great and I hope

you are in great health. But one good checkup isn't a free pass to never visit the doctor again. Even if you have a great checkup this year, you'll need to go back next year for another checkup.

But let's look at a different outcome and instead say you have a checkup and the doctor finds you have a broken leg, acne, and you fall asleep when you watch the videos I've made for you. The doctor will triage your symptoms and treat your leg first, since that's the most serious ailment. (Just make sure and go to the doctor and not my Grandpa Dee. Grandpa Dee is an old school veterinarian and if you break your leg you get to "go live on the farm" with your old dogs Allie and Ellie.) After your leg is fixed, the doctor process will repeat the process and treat the acne, which is your next most important issue. In other words, it's a cyclical process where you address the biggest problems first, but continually look for and address any problems that may crop up. The important thing to understand is that cyber security isn't a one-and-done job, it's a process of continuous evaluation and improvement, and the frameworks provide a defined way to perform the process.

Utilizing a framework also allows you to move from a reactive position to a proactive position. That is, without a framework you'll probably end up running around, responding to problems as they pop up. You'll be reacting to problems as they occur, instead of taking an organized approach to stop the problems before they occur which is what a framework is designed to do.

This should help you understand the Information Assurance process in general. The different frameworks that the book references define the same general steps in the process, but they will differ in the specifics. For example, all the frameworks address password security, but some of them require passwords to be changed more frequently than others. Using a framework is important, as it provides a step-by-step process for validating your current security posture, and then addressing any weaknesses. If implemented properly this allows you to improve an organization's security as time goes by. And on the other hand, I've seen highly skilled individuals work without a framework. These were people that were obviously technically competent, but they always seemed to be putting out fires. This prevented them from making any overall progress and resulted in a lot of security issues.

Hopefully this helps provides with a better understanding of frameworks. Remember at this point you just need to understand the general concept. You'll learn all about the specifics in a later Cyber Security class.

Applying What You've Learned to Your Home System(s)

Background & Basic Security Steps

One of the things I like to do in this class is to take the things you learn about protecting devices and networks for an organization, and show you how to apply them to your home devices and network. I think that this will not only help with absorb new terms and processes, but it may also help you improve your own security. With that in mind, in this set of videos you'll learn

how to apply what you've learned about the basic process for checking for and mitigating vulnerabilities to your home system(s).

Before we do that, let's back up one step and look at a few basic, fundamental things all cyber security experts agree you can do that will help prevent most malware and attacks, and possibly save you if you fall for a social engineering attack and your computer is encrypted by ransomware. These are considered basic because they're relatively simple to do, and if done, will protect you against a vast majority of security issues. If you're not doing these things then you're asking for trouble. It would be like walking around town, pulling a wagon full of money, and wearing a sign that says "Rob Me".

The basic things you can do include:

1. Run an Anti-Virus program, and keep the definitions up to date.
2. Install updates for the OS and any applications.
3. Create regular backups.
4. Use strong passwords.

Hopefully these seem super basic to you, and I also hope that you're already doing all of them.

But, now let's look in more go back to what you just learned about doing a vulnerability scan, and using it to check for problems that may need your attention. You can do a vulnerability scan on the devices on your home network, which you'll learn about in a later video, but what I really want to talk about now is doing a check for vulnerabilities that could be caused if you're not doing step #2, keeping up with the updates and patches for your OS and applications. You might *think* everything's up to date, but how do you know for sure?

The network vulnerability scans described in the book aren't really designed to show you this information, but there is a way to get it, which is what you're going to learn about in this section. You'll first learn how to check the Windows OS to ensure it's up to date, and then learn how to check your other applications.

Checking Windows Updates

Here's the process for checking Windows to ensure it's current with security patches and updates. If it's not up to date I also suggest that you configure the OS so that it automatically installs updates when they become available. The process is explained in good detail at the following web site. The web site says Windows 7 in the URL, but it also has information for later versions including Windows 10. If this web page no longer exists If this URL no longer works you can do your own search for something like "How to update Windows".

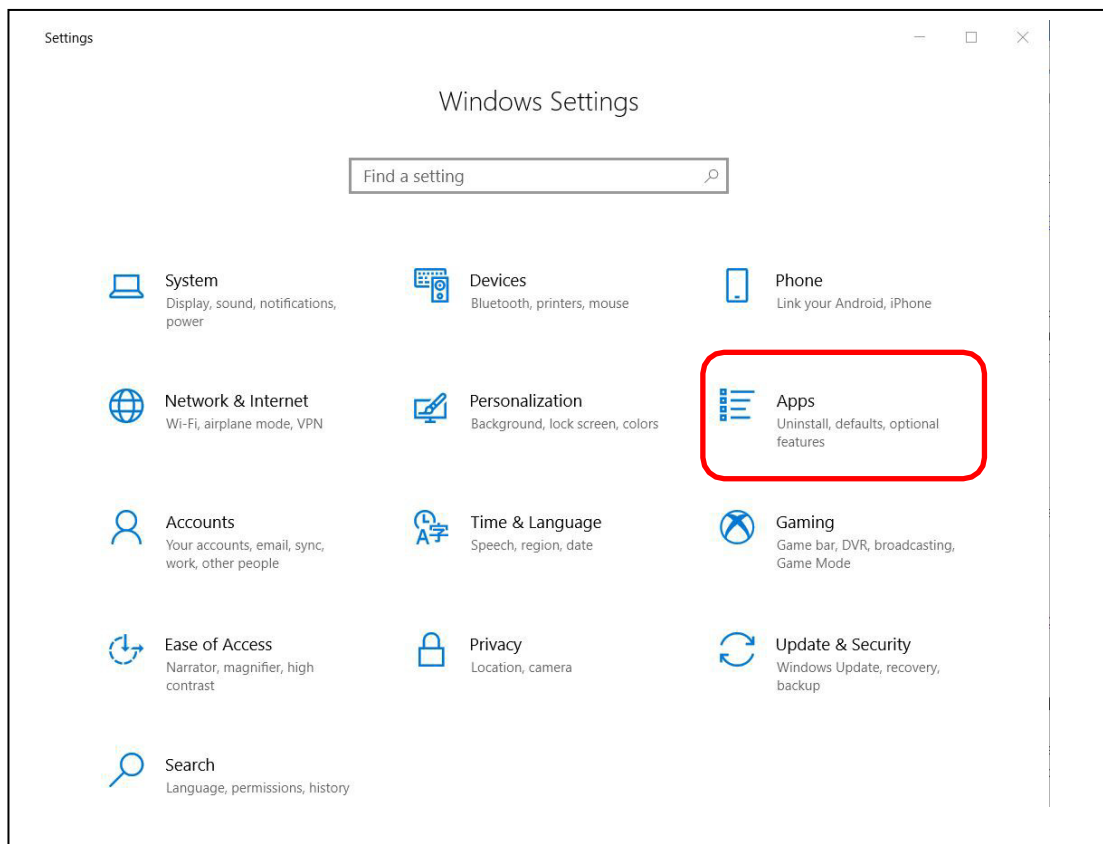
<https://www.howtogeek.com/howto/5529/how-to-keep-your-new-windows-7-computer-updated-and-secure/>

Application Patches and Updates

In addition to keeping the OS up to date, you also need to keep your applications and programs up to date. This is a little harder, as each program has to be updated separately, and they are different ways that the upgrades are performed. Here's a link to a video on checking your applications for updates.

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-checking-all-applications-for-updates/> - Ensuring application programs are up to date.

Or, you can read the following text. The first thing you should do is take inventory of your applications. You can find a list of the major installed programs on your system by opening **Windows Settings**, and then selecting **Apps**. You should go through your applications and ensure that it's running the latest version. This list will contain a lot of applications, but typically some of them will be part of a suite of applications that can all be updated at one time.

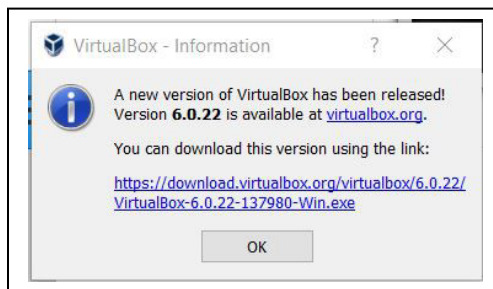


Oh ... there will probably be several programs listed that you don't recognize. You may be tempted to delete them, but be very, very careful before doing this. There are typically several applications installed to run things like the computer's sound or video, or handle the keyboard and mouse, or the touchpad. These often have strange sounding names, and you might think that they're some type of malware since you never installed them. But, they are critical for

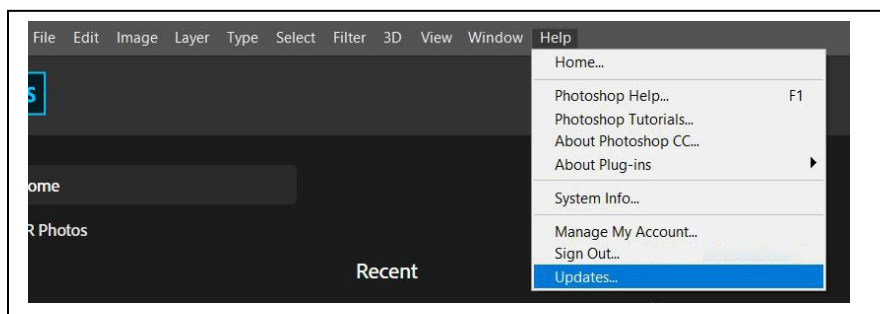
running your system, and if you delete them you may “break” your computer to the point that you need to completely reinstall Windows. So, if you see a program that you don’t recognize, do an Internet search and determine what it is before deleting the application.

Once you have a list of your applications, the next step is to ensure that you have the latest version of each application, or installing any patches. This can be handled in a few different ways including:

- A. Some applications include an “updater”, which is a small program that always runs, and automatically checks for updates for you. For example, if you install most Microsoft, Apple or Adobe applications, you’ll also install a program that checks for updates for you. You can configure these applications so when an update is found they either install it automatically, or prompt you to do the install. Some applications are built so they will check for updates each time you start the program. They will either ask if you want to check for updates, or check for updates automatically and prompt you if an update is found.



- B. Some applications make you manually check for updates. Many programs have an option for doing this that can be accessed once the program is started. To do this, start the program, then select the **Help** menu, and then look for something like **Updates**. Some applications don’t provide any help with upgrades. If that’s the case you’ll need to figure out what version of the program you’re currently running, and then manually go to the applications web site and check to see if a new version is available.



- C. A third way is to use an application to check for you. These applications all do what you would do manually, figure out which applications are installed and then see if any of the applications are out of date, but all you need to do is install and start the program. While there are some good options available, I haven't found one I really like yet. The problem as I see it is that there's no way for any single program to track updates and current versions for every other program you might possibly load onto your computer. Most the applications I've tried check against a specific list of the most popular applications, but I've never found one that was able to provide information for all of my installed programs. But in any case, I've made videos that show you how to use a couple of these programs in case you're interested.

Scanning Your Home Network and Ports

Another thing you can do to check your home security is to scan your home network. If you're going to run a full vulnerability scan on your network using Nessus the network and port scan can be done as part of that process. But if you don't to take the time and effort to install and run Nessus you can run a separate network scan to discover the devices connected to your home network. Oh ... and this is another one of the things you don't have to do, but you can do it if you choose. Plus, you'll learn how to do it in the Wireless security class, and by that time you'll have learned more about networking that will make it easier to do and understand. The reason I'm showing you this now is because doing the scans yourself, instead of just reading about them, should help you put what've learned about network and vulnerability scans into context.

If you do scan your network there hopefully won't be any surprises. But who knows ... if you haven't secured your wireless router you might find that a neighbor or a stranger connected to your network, sucking up your precious bandwidth.

To do this you'll first learn how to use a program called nmap to perform a port scan. There's a lot you need to know to make sense of what's going on with nmap, so in addition to the Lecture Notes I've made a couple of videos to provide some background and help you. Remember that this is all optional, but if you want to try it yourself I strongly suggest that you watch the videos on nmap before starting as they provide an explanation of what you'll be doing and how to interpret the results of the port scan.

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-network-ports-background-for-nmap/> - nmap – Background on Network Ports

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-using-nmap/> - Tips for using Nmap

Scanning Your Home Router for Ports Open to the Internet

Running nmap on your home network shows you the ports that are open on the side of your router that serves your home network, not the side that's exposed to the Internet. In most

cases having open ports and services on the private side of your network isn't an issue as the only devices that will be able to access them must be connected to your home network. So, if you have your home network password protected, you probably don't have to worry about an attacker getting into your router from your home network. But your router is most likely also connected to the larger Internet, and running nmap from inside your home network won't show you what ports are open and exposed to the outside world. If you want to check for open ports and vulnerabilities on the public side of the router that anyone on the Internet can access, you can use the following process. Once again, this is totally optional.

A. The first step in checking your router is to determine the outside IP address. This is typically assigned to the router by your ISP, unless you've paid extra to receive what's called a static IP address. Your IP address can also change periodically, so even if you've checked this before it may be different at this time. In any case, there are a few different ways to find your router's outside IP address including the following. Note that you only need to do one of these, as they all should have the same result.

- The simplest way is to connect to one of the following web sites:

<http://whatsmyrouterip.com/> - this site also has an explanation of the difference between your public or outer facing IP address, and your private or internal network IP address. It also contains other instructions for a few other methods for finding your router's IP in the off chance this doesn't work.

<https://www.whatismyip.com/>



- Connect to your router through the web interface. To do this you'll need to know your router's internal IP address, which is typically 192.168.1.1, but may vary.

- Use one of the manual methods described at the following web page. If this page is no longer available try searching for something like “how to find my router’s ip address”.

<https://www.businessinsider.com/how-to-find-ip-address-of-router>

- B. After you have the Public IP address for your router, you can run a port scan against it. The following links will take you to two sites that will do this scan for you. If these links no longer work you can do a search using a term like “scan home router”.

<http://www.t1shopper.com/tools/port-scan/result/>

<https://pentest-tools.com/network-vulnerability-scanning/network-security-scanner-online-openvas#>

If you use the t1shopper site, it will load what it thinks your router’s IP is for you. Be aware that scanning the ports can take a long time. It really doesn’t take all that long, but they’re slowed the process down for two reasons. The first is that they don’t want attackers to use their site to perform their port mapping. By slowing the process way down t1shopper makes they’re portmapper much less attractive to an attacker who would be better off running their own port mapper. The second reason for the slowdown is that it prevents the site being scanned from going into panic alert mode and blocking all of the traffic from the scanner. Network firewalls and routers can detect when they’re being scanned, and automatically block all of the network traffic from the suspect computer, which essentially blocks the scan. But if the scanning is done slowly, it’s much harder to see the pattern of scans and determine that an attack is underway.

- C. The hope is that the scan will not show any open ports, unless you’ve opened some yourself. We often open ports on our home router for my sons, when they want to run something like a Minecraft server or Garry’s Mod server, and play games with their friends. Or maybe you’re running a VPN, which will also require an open port. If you do find some open ports you should do some detective work and see what service is running and why it’s open.

Ways to Check Your Comprehension

The test over this chapter won’t be for a few weeks, so I suggest that you use the review questions at the end of the chapter to check your comprehension. I don’t have the review questions loaded in Canvas, so you’ll have to just read them and figure out your answers on your own. Or you could try and connect with some other students in the class and drill each other using these questions.

The material in this section will be included in Test 1, which isn't due for a few weeks. If you look in the Test 1 Canvas Module you'll see it contains a link to a Practice Test. You can take the Practice Test as few or as many times as you want. You're not required to take the practice test, but it's also a good way to check your comprehension and prepare for the "real" test.

The Activities for This Section

There are two sets of activities for this section, the Hands-On Projects and the Case Projects (writing assignments).

Hands-On Projects

The required homework for this section includes two Hands-On Projects from the book, **2-1 Exploring Common Vulnerabilities and Exposures (CVE)** and **2-2 Exploring the National Vulnerability Database**. Make sure and complete both of these assignments. Read the following notes carefully, as they explain exactly what you need to submit to receive credit.

Before submitting your work, add all of the information for your submission into a single document. Make sure that this document has the proper header information (your name, project number, date) and well as the project and step number for each item in the document. That is, if you are submitting a screen shot for Project 2-1, step 16, make sure and add some text that says "Project 2-1 #16", or something to that effect.

What to submit for Project 2-1:

Well, somebody moved your cheese again. That is, the CVE web site has web site has changed significantly since the book was published and the instructions in the book won't work. **You'll need to view the following videos on CVEs in Canvas for help completing the project.**

Viewing the old CVE web site (Video)

Viewing the new CVE web site (Video)

These videos will show you how to access the CVE web site so you can complete the project. Watch the videos and then do the following:

- Answer the questions for #4, 6, 7, 8, and 11
- Create a screen shot after steps #11 and 13. To get a screen shot use the Windows Snipping Tool or hit the <ALT> + <Print Screen> keys at the same time. The screen shot will then be on your clipboard and you can paste it into your word document. If you need help creating a screen shot there are many videos on Youtube that will provide further instruction and details. Do NOT take a picture of your screen with your camera/phone. If you submit a photo you score will be 0 for the assignment.

What to submit for Project 2-2:

- Answer the questions for #5, 8, 9, and 16
- Create a screen shot after steps #16 and 24.

Case Project (Writing Assignment)

For the writing assignment for this section you need to do one of the following **Case Projects** which are located at the end of the chapter. Note that your book makes a distinction between "Projects" and "Case Projects". For this assignment you want to be working on the *Case Projects*. Choose from one of the following:

- Case Project 2-1 False Positives & False Negatives
- Case Project 2-2 Pen Test Products
- Case Project 2-3 Vulnerability Scanners

If you do 2-2 or 2-3 you will need to take extra care to not copy and paste information when you create your tables as this impact the Turn-In-Score. And, even though the main task is to create a table you need to ensure that you answer the questions and include the required references. I'm going to repeat this last instruction to make sure you don't miss it. You need to include references unless otherwise noted.

If you haven't already read the [Guidelines for Writing Assignments](#), now would be a good time. The document explains what you'll need to do for the paper and provides details on how your paper/report will be graded. Also, remember if you need help creating your references the Citation Machine web site will be your new best friend.

When your project is complete, turn it in by opening the Assignment in Canvas, and clicking the **Submit Assignment** button.

Also, remember to check your TurnItIn score. If it is higher than 30% your submission will NOT be graded. You will need to either edit your material and put more of it in your own words, or add more original material. Once you have made your changes, you can resubmit your work. There is no way to check your TurnItIn score prior to submitting your work. This is because your work must be submitted for the TurnItIn program to be able to access it and check it. Don't worry about making multiple submissions, as it has no impact on your grade..

<https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-checking-your-turnitin-score/> - How to check your TurnItIn score

Optional Extra Credit Activities

The following exercises are optional, but if you do choose to do them you can earn up to 10 extra credit points. Note that you can only earn a maximum of 10 points, but there are more

than 10 points available. This means that if you complete the Nessus scan, which is worth 10 points, you won't get any additional points for completing any of the other items.

1. [10 Points] Use Nessus to run a vulnerability scan your home computer or the class VM. The steps and instructions for doing this can be found above. Note that this will take some time and effort on your part, and you will be required to create an account at Nessus.

To get the extra credit points you must create the following screenshots and email them to me through Canvas. The subject of the email must be Extra Credit Nessus.

- A screenshot showing the list of vulnerabilities found by Nessus. There may not be any urgent issues, but there should be a long list of things that Nessus checked.
 - A screenshot showing the details of one of the items in the Nessus report.
2. [5 Points] Use nmap to run a scan on your home network and display all of the connected devices. The steps and instructions for doing this can be found above. Note that you must do this on your home network, not the class VM. The class VM network won't show you anything other than the VM itself, so it's pretty boring and not too helpful. To get the extra credit points you must create a screenshot showing the network map or list of devices found by nmap, and email the screenshot to me through Canvas. The subject of the email must be Extra Credit nmap.
 3. [5 Points] Run a scan on your home router and display the ports that are open to the Internet. The steps and instructions for doing this can be found above. Note that you must do this on your home network, not the class VM. To get the extra credit points you must create a screenshot showing the website you used to perform the port scan and a list of any open ports, and email the screenshot to me through Canvas. The subject of the email must be Extra Credit Router Ports.