Chapter 3 – Threats & Attacks on Endpoints
What this section is about – what you should learn

In the previous section you learned about using pen tests and vulnerability scans to check a system or network for vulnerabilities, how the CVE and NVD databases provide a list of vulnerabilities, and how frameworks define a process for improving security in a proactive and continuous way. In this section we're going to change perspective on security and instead of looking at vulnerabilities, you'll look at different types of threats and types attacks on endpoints.

To explain this change in perspective, where we begin looking at threats and attacks on endpoints, let's go back to the analogy with physically securing something like a shopping mall. The cybersecurity vulnerability scan is like checking a list of all the different types of locks, doors, windows, etc. and the pen test is like hiring someone to try and break in the mall. The main point is that both of these tests are done without any people in the mall, either people that work in the shops, customers, or thieves. Now, consider everything that could go wrong once you let people in the mall. Once this happens you're going to face all kinds of threats, such as thieves, scam artists, or even malicious employees, etc. Worrying about what the people might do in the mall is analogous to the threats and attacks that could happen to the computers and networks you're responsible for protecting.

What do you need to know about all of these possible threats and attacks? Just like the mall, do you really need to know the details about every possible type of threat posed by thieves, scam artists, embezzlers, organized crime, or wayward teen mallrats amped up on too many Cinnabons? I've never been a mall cop, but my guess is what you probably need to know about is the general categories of threats you're facing to ensure you know what to do if they occur. If you try to memorize the details of every single possible threat posed by humans, of which there must be hundreds of thousands[1], you'll get buried in the details, and it won't help you towards your main goal which is protecting the mall. That is, you probably need to know what to do in case of armed robbery, but you don't need to make the distinction between attacks with a Charter Bulldog .38 special revolver, versus an attack with a Beretta 12-gauge shotgun, versus an attack with a Sako Finnlight rifle (no relation), etc.

We have the same problem with possible threats and attacks on endpoints, there are so many that you would quickly get overwhelmed if you try to understand the details of each specific attack. The count of virus variations alone is literally in the millions, with new ones being introduced on a daily basis. You need to know enough about the general categories of attacks to help you towards the main goal which is providing security. Knowing the difference between the Trojan.Win32.WHISPERGATE.YXCAX and Backdoor.Win64.CARBANAK.A isn't going to help you reach your goal.

---

[1] https://www.law.cornell.edu/uscode/text/18/part-I

If you want to view the details of a specific attack you can use the following resources. The Trend Micro Threat Encyclopedia provides information on many different malware threats, which can be helpful if you are attacked and are able to identify the malware. It will also provide an idea of the number of different types of attacks.
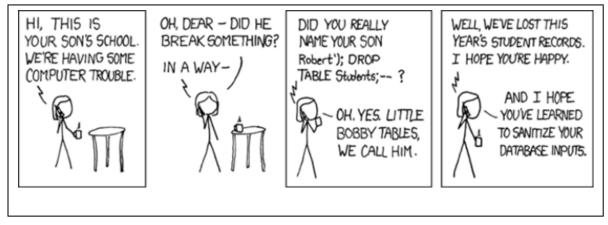
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/page/1

The Trend Micro Threat Encyclopedia doesn't list every possible piece of malware, as it only lists the last 500 most recent. If for some reason you want to see a more complete list, you can check the FortiGuard Labs Threat Encyclopedia. As of April 2022, it held entries for over 8 million threats, organized by name and by year.

https://www.fortiguard.com/encyclopedia

Once again, don't worry that you'll have to memorize the details about any specific attack. If I were a good teacher I'd make you memorize the details of every piece of malware and regurgitate the details on a timed test. But lucky for you I'm not that kind of teacher. The lists of malware are just for your information, and meant to illustrate the point that there are a lot of possible threats and attacks.

While there are too many threats to count many attacks are very similar and they can be broken up into categories of similar attacks such as malware or ransomware attacks. The book does a good job of explaining the main characteristics of each category of attacks. I say these are "good" explanations, not great ones, because many of the explanations require that you have some specialized knowledge to understand what the book is saying. For example, if you don't know anything about databases and SQL queries, the explanation of the SQL injections attacks probably won't make much sense to you. Or if you don't know much about programming and how a process is loaded into memory, the buffer overflow explanation probably won't make much sense. To be fair to the book's author, since this book covers almost every aspect of cybersecurity he has limited space to explain any single subject, like injection attacks or buffer overflow attacks, and the explanations he does provide are excellent considering he has to do it in a page or two at most. But, there's just not enough content in the book to completely explain most of these attacks if you don't already have experience and knowledge.

(This cartoon from XKCD is hilarious if you know about SQL)

And this is one of the problems with any introduction and overview class, like this one. It's the old forest versus the trees problem. That is, if the goal is to explain that a forest is a collection of plants and animals, plus maybe a little geology and geography, that concept can get lost if you're shown every possible species of plant and animal in the forest. So, once again, don't worry too much if you don't get the details on all the attack types and do not try to memorize all the acronyms and types of threats. At this point the objective is to simply introduce you to the terminology and help you learn the big picture of what threats and attacks on endpoints are. As you progress through the Cybersecurity program you'll get further exposure to things like SQL, and hardware, and programming; all things that should help you better understand the various types of attacks and threats.

Next, we'll go over some demonstrations that should provide you with a little more insight into a few of the attacks. But before we start the demos let me say that while this chapter of the book has a lot of information about the various threats and attacks you might be surprised that it doesn't discuss what to do about them. If you are surprised, don't worry, the information about things you can do to prevent attacks is coming in the next chapter.

Ok … let's jump in and see if we can't help you make better sense of what some of these attacks look like and how they work.

Macro Viruses

The first thing you'll learn more about are macro viruses. We're starting with macro viruses because they're relatively simple, and you should be able to see how it's possible to turn a useful tool into something malicious. So, what is a macro? A macro is a program or chunk of programming code that is attached to an application file, like a Word document or Excel spreadsheet. Macros are great for automating repetitive tasks inside a document, making it possible to do things like add a big block of text, like your address block, by pushing a single key. Or they can be used in a spreadsheet to tell Excel to perform a series of calculations.

This explanation makes perfect sense, right? Of course, it does, if you already understand what a macro is. But if you don't I doubt that this explanation will be much help, which is why you're going to learn how to create your own macros. I'm not going to show you how to create a macro that will do anything malicious. But if you follow the steps in these videos you'll learn how to create macros that will run automatically when a document is opened, and it's a small step to go from the macros you'll create to a macro that could be destructive. The links to the videos are also provided in Canvas.

https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-threats-attacks-creating-a-macro/

https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-threats-attacks-autorun-macros/

Ransomware
The next thing you'll learn a bit more about is ransomware. I'm sure you know that this attack works by encrypting files on a computer, but how does an attacker actually perform the encryption. In this set of videos, you'll learn how to use a command line encryption tool called OpenSSL to encrypt and decrypt files.

https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-threats-attacks-ransomware-background-with-openssl-pt-1/

https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-threats-attacks-ransomware-background-with-openssl-pt-2/

SQL Injection Attacks
The last type of attack we'll look at in more detail is the SQL injection attack. The following two videos provide background on database and SQL queries, and how information that should be restricted can be read from poorly secured databases using SQL injection. The first video provides background and demonstration of an actual attack. The second video, from Computerphile, is optional. It contains a deep dive into the complete SQL injection attack process, so it might be too much if you don't have good background in database technology, but might be too much if you don't.

https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-threats-attacks-sql-injection-background-demonstration/

[OPTIONAL] Running an SQL Injection Attack - Computerphile
https://www.youtube.com/watch?v=ciNHn38EyRc

[OPTIONAL] The SQL lesson at the HackSplaining web site
https://www.hacksplaining.com/lessons

[OPTIONAL] Other Attacks

Some of the remaining attacks, such as buffer overflow attacks or cross site scripting attacks, require quite a bit of technical background to even begin to understand. If you already have extensive background in programming or web programming you might find the following videos interesting as they explain how certain flawed programming methods can be a threat. These videos are optional as they require a good amount of knowledge and experience to understand.

The interactive lessons at the HackSplaining web site provide a hands-on way to learn about of the some of the attacks you've learned about in this section. The details of the attacks may not make sense until you take a few more classes, but you'll be able to see the attacks in action, which I believe will help you understand why they are a problem.
https://www.hacksplaining.com/lessons

Running a Buffer Overflow Attack – Computerphile (YouTube)
https://www.youtube.com/watch?v=1S0aBV-Waeo

Background on Cross Site Scripting (XSS) Attacks (Video)
https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-threats-attacks-cross-site-scripting-xss-background/

Cracking Websites with Cross Site Scripting – Computerphile (YouTube)
https://www.youtube.com/watch?v=L5l9lSnNMxg

Web sites with vulnerabilities, that allow you to practice
https://www.acunetix.com/blog/web-security-zone/test-xss-skills-vulnerable-sites/

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

Normally at this point we discuss applying what you've learned about protecting an organization's devices to protecting your personal devices. However, this chapter is a little unique as it describes attacks and threats but doesn't get into protection at all. Protecting endpoints from the attacks and threats you learn about in this chapter isn't discussed at all in this chapter, that's what the next chapter is about. This means there's nothing in this chapter that we'll apply to your personal devices … but there will be a lot in the next chapter.

Ways to Check Your Comprehension

This is the last chapter to be included in the first test. Even though there's no delay between this chapter and the test, I still suggest that you use the review questions at the end of the chapter, and the practice test, to check your comprehension before taking test 1.

For the test itself, make sure that you leave yourself adequate time to complete it by the due date. Remember that the test must be completed on time to receive any points. The test will lock at midnight on the due date, so if you haven't finished it by then you will be locked out. If you do happen to miss it, don't panic. You can always miss one test as there's an optional 4th test you can take to make up for any missed tests. But let me just warn you that the 4th test is much harder than the first 3, so it would be much wiser to just complete all of the tests on time.

Also remember that the test is open book and open note, but you must do your own work.

The Activities for This Section

There are two sets of activities for this section, the required homework, and an optional extra credit activity.

Required Homework

The required homework for this section consists of two Hands-On projects from the book. 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. There are no Case Projects (writing projects) for this section.

The Hands-On Projects are:

- **3-1 Analyze File and URL for File-Based Viruses Using VirusTotal Part 1**
- **3-3 Explore Ransomware Sites**.

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 3-1, step 6, make sure and add some text that says "Project 3-1 #6", or something to that effect.

What to submit for Project 3-1:
- Take a screen shot after step 11, showing the results of the analysis. (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.)
- Take a screen shot after step 17, showing the results of the analysis.
- Answer all the questions in step #20.

What to submit for Project 3-3:

- Answer questions #4 and #11
- Take a screen shot after step #6, showing a list of the Decryption Tools. You do NOT have to download any of the tools, unless you have some files you would like to try and decrypt.

In addition, answer these questions:

- What is your greatest protection against ransomware? That is, if your computer is attacked by ransomware, what will save you from paying the ransom regardless of the type of ransomware?
- Assume you are asked for assistance by someone who works in your local city government. The city computer and network systems have been attacked by ransomware and are not functioning, bringing several critical systems to a stop. The last backups were performed 3 months ago, so there's no way to use the backups to restore the systems. The attackers are demanding $250,000 to decrypt the systems. Would you recommend the city pay the ransom? Do you feel that not having viable backups is a fireable offense for the city's current IT director, or do you feel that this isn't serious enough to cost someone their job?

Optional Extra Credit Activities

The following exercise is optional, but if you do choose to do it you can earn up to 5 extra credit points.

[5 Points] Create a Word Macro that will draw a white cloud with a blue outline, similar to the one shown below. To get the extra credit points you must ensure that you do everything on the following checklist. That is, there will be no partial credit for this activity.

- The macro must execute automatically any time the document is loaded
- The cloud must be 200 pixels x 200 pixels. The upper left corner of the cloud should be at pixel coordinates (50, 50)
- The cloud must have a white background with a blue outline. The colors must be set in the VBA code
- You must copy and paste the VBA code into the document you submit in Canvas. Do NOT attach the macro to the document you submit in Canvas.
- You must label the section of the document containing VBA code with bold text that reads **Extra Credit Macro**.

- You must also include a screenshot showing the result of running the macro.