Chapter 5 – Networking and Server Attacks

What this section is about – what you should learn

In this chapter you will learn about another big category of attacks called Network attacks. Network attacks as the name implies, are attacks that come from the network. Or it might be more precise to say your computer must be connected to the network for the attack to occur. This distinguishes network attacks from Malware attacks and social engineering attacks, as the latter two can happen to computers that aren't necessarily connected to a network. The distinction between networking attacks and malware attacks might seem a little strange since most people always have their computers connected to the Internet. But really, it's just a way of categorizing the attacks, a way of organizing them into different boxes, so you don't have to learn about all of the different types of attacks at the same time.

Another distinction is that since these attacks originate or occur "somewhere" out on the network, traditional Anti-virus programs won't be able to detect them. Some of these attacks start with an attacker running something called a vulnerability scan, which as the name implies, checks a network and any exposed devices for potential vulnerabilities. If any vulnerabilities are found, the attacker can then run another set of programs aimed at exploiting each specific vulnerability. With modern tools this can all be done with the click of a mouse, much like the hacking shows you see on TV. (Note – you'll learn a little more about vulnerability scanning later in this class, and a lot more about it in the CSIA 440 Cyber Testing and Penetration class.) Other network attacks occur when you visit a rogue web site where they take advantage of weaknesses in your browser or browser plugins/add-ons.

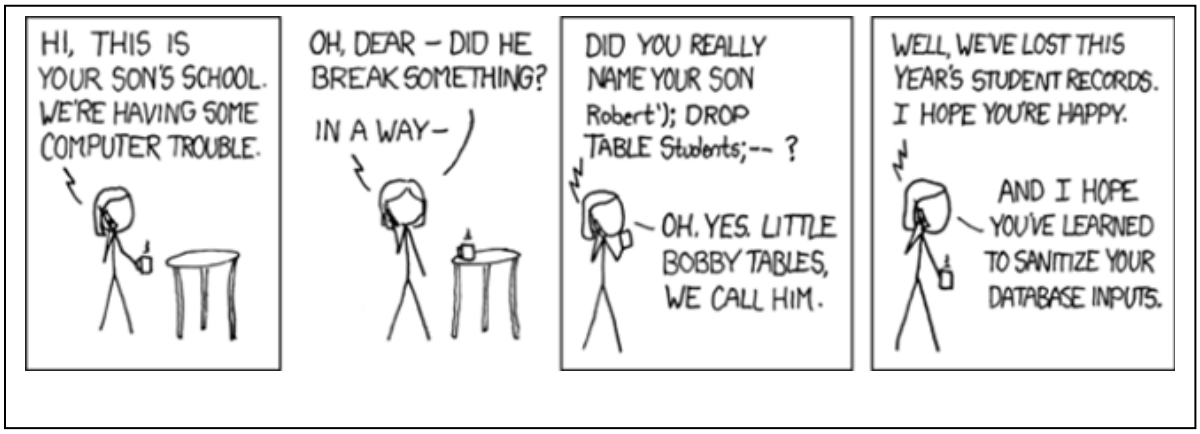
A third difference is that some of these attacks aren't typically aimed at home systems, they're aimed at large organizations. That is, most home users aren't running a large database containing credit card information so you'll probably never personally be the target of a SQL Injection attack. Of course you or other individuals will be the ultimate victims of these types of attacks, if the personal data on some corporation's computer is compromised. But the attack won't be against you and your home computer, the attack will be aimed at databases used by large businesses or institutions.

But before you start feeling too safe, you should be aware there are some network attacks that are aimed at home systems. These are attacks on your home router, if you have one.

In any case network(ing) attacks are another category of attacks and as you read the chapter you will see that there are dozens of different specific types of networking attacks. And once again you're given a pretty large brain dump of information regarding all of the attacks. There are details on things like injection attacks or cross server scripting attacks that only SQL and JavaScript coders will understand, or DNS and ARP poisoning attacks that you will understand after you learn the details of network communication. So don't worry if some of the explanations don't make a lot of sense at this point. Remember this class is an introductory

class, and the expectation is that you'll get a general sense of what network attacks are, as well as start to learn some of the terminology. To really understand how the attacks occur and the weaknesses they exploit requires taking several other classes where you'll learn about the underlying technologies, and months or years of experience. At this point you're just dipping you toes in the ocean, but soon you'll be in the water up to your neck, or over your head, or floating your boat … however that saying goes.

Many of the things you would do to prevent network attacks have to be done at the application level, by the people writing the programs, or at the network level by the organizations like your Internet Service Provider or your Local Area Network administrator. For example, the way to prevent a SQL Injection Attack is for the database programmer to check for bad queries before executing them. Or the network administrator must configure the firewall correctly to prevent attackers from gaining access to your network traffic.



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

In other words, for most of the attacks described in this chapter, there are not many new things you can personally do to directly protect your devices and your home systems. However, there are a few things you can do, which are really the basic security actions or tasks, but with emphasis on a few specific items:

1. Ensure that your anti-virus and anti-malware programs are running and up to date.

2. Ensure that all OS and application patches and updates have been installed. The two things to emphasize in this case are:
    a. Ensure that your browser and all of the plug-in/helper/extensions (programs automatically started by the browser to display different types of data) are up to date.
    b. Ensure that the firmware on your home router is up to date, if you have a router.

3. Use strong passwords. The thing to emphasize in this case is to ensure there is a strong password for the administration account on your home router, if you have a router.

Besides the basic actions, there are a couple of new things you can do:

4. Don't log in to any sensitive sites when you're using free wireless to prevent Man in the Middle attacks, especially if you do any mobile computing. For example, don't log in to your bank account when you're in Starbucks or travelling and waiting around in some airport. You never know who is really controlling the router you're using in your connection. I'm sure you've heard this advice before. And it can easy to forget or ignore. In our always connected society it can really hard for some people to be offline. And what could it hurt to connect to the "FreeStarbucks" wireless network?

5. Make sure you are using a strong authentication protocol on your wireless router, if you have a wireless router. WEP, which is the original protocol, is very easy to crack. It's been replaced by WPA-2, which is what you should select if given a choice. The issues with WEP have been known for years, so the chances of your router using it are very small, unless you have an older router. (Note – you'll learn all about this in the CSIA 330 Wireless Security class.)

If you are curious, and want to know more about how some of the attacks work, I highly suggest going to the lessons section of HackSplaining web site at:
https://www.hacksplaining.com/lessons

This site contains dozens of interactive lessons that 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.

Ok … There's always more to learn about all of the various attacks, but there's one group I'd like to discuss further, which are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. As the book says, these are nuisance attacks that prevent a site from processing valid traffic. A good analogy for a DoS attack would be your phone. Say someone keeps calling you and hanging up when you answer. This will be annoying, but the bigger problem is it will also prevent you from answering valid calls. If you get attacked on your phone this way, you can simply block the number and the attack will stop. To get around this, the attacker can recruit thousands of other people to also make nuisance calls to your number, or in other words distribute the attack. This is very similar to what happens with DoS and DDoS attacks. But instead of making a phone call, in a DoS or DDoS attack the attacking computer starts the process of opening a network connection with the target computer. The target computer will respond, but the attacking computer never completes the network connection. The target computer only has a limited number of network connections it can open at any time, so by tying them up, even briefly, the attacker is able to prevent valid users from connecting. Like a phone call from a single phone number, a DoS attack is relatively easy to block, which stops the

attack. This is why the attackers evolved to using thousands of computers to all attack at the same time in a Distributed Denial of Service attack. In a DDoS attack it's very difficult, maybe even impossible, to block all of the devices involved in the attack.

Hopefully this explanation makes sense. But the main point of this is, and the thing that should be of interest to you and anyone who owns a computer or smart device, is where do these thousands of attacking devices come from? The devices used in the attack are devices that are owned by unsuspecting members of the general public, people like you and me. We don't know our devices are being used, and certainly wouldn't explicitly agree to let them be used as part of an attack. But if you don't take some basic security precautions it's quite possible for an attacker to plant some code on your device. This code allows the attacker to take control of your device at any time, and have it participate in the attack. You might not even notice when this occurs as each individual device only generates a relatively small amount of network traffic during the DDoS attack.

If an attacker is able to compromise a device and plant the DDoS code, the device is called a zombie. The network they make up is called a zombie net and it is controlled by the attacker. The DDoS code lies dormant until it receives a message from the controller, telling it which computer to attack. At this point all of the zombies perform a DoS attack, typically overwhelming the target.

Another interesting fact about DDoS attacks is that any smart device connected to the Internet can become a zombie. This has been a problem because many smart devices aren't secured, and there may be no way to secure them. The people making the smart devices want to make them easy to use, and often don't even take security into consideration during early development. Sooner or later they realize that they'll need to add some security, but it's much easier to make sure things are secure from the start and can be much more difficult to retrofit once a product is built.

So … How do you protect your devices from becoming zombies? Just do the normal basic security items listed above, stay away from sketchy web sites, don't reply to texts from people you don't know, etc. If you are attacked with a DoS or DDoS attack there's not much you can do, but you can prevent your computer or any other devices you own from being part of the attack. You might find articles on the Internet that promote methods for protecting networks from DDoS attacks, but it's not really possible at this time.

Here's one last question, and then I promise I'll be done on this subject. I have a friend, Troy Thompson, who used to be the Director of Cyber Security at PNNL/Battelle, and this was his idea. He thought that if your device was converted to a zombie and used in a DDoS attack you should have to pay a fine. After all it's pretty simple to protect your devices, all you need to do is run anti-virus software and keep your OS and applications up to date. So if you're not taking the basic security precautions and your device is used in an attack you should pay a fine. There are already similar laws for other devices that set the precedent. For example, several states have laws that allow you to be ticketed if you leave your car running and unattended. Part of

the reason for these laws is environmental, but another reason for the law is it makes it too easy for someone to steal the car.

https://www.goodhousekeeping.com/life/news/a41993/car-idling-laws/

In any case, what do you think? Should you be fined if a device you own is used in DDoS attack, and you failed to perform even the basic security tasks? You don't have to answer this formally, or upload your answer anywhere. It's just food for thought.

The Activities for This Section

There are three sets of activities for this section, the required hands-on assignments, the required writing project, and some optional activities.

1. Required Hands-On Projects Homework

The required homework for this section consists of two hands-on projects from the book. You need to complete Hands-On Projects 5-1 **Testing Browser Security** and **5-2 Configuring Microsoft Windows DEP**. 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 5-1:

- The instructions for this assignment no longer work as written. I've made a few videos showing you how to use the Qualys site to check your browser to see if it needs updating, plus how to check to see if any of the browser plugins/add-ons need an update. Watch the videos, and at a minimum create a screenshot showing the result of the online browser check. I also suggest that you use one of the other tools to check your browser's plugins/add-ons. You don't have to do this, but this is one of the real world skills you can use to improve the security of your own computer(s).

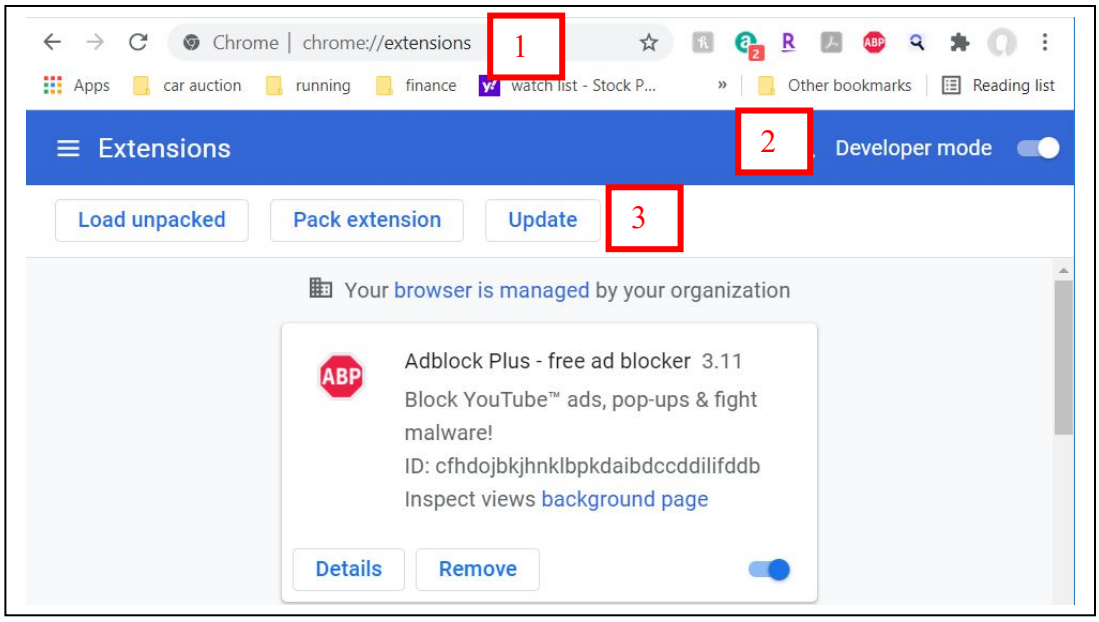
  https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-checking-browser-add-on-security/ - This explains the problem with Hands-On 5-1 and how to deal with it.

  [OPTIONAL] https://tonysako.com/cs150-various-methods-for-checking-browser-plugin-extensions-for-updates/ - Alternative methods for checking your browser's plugins/add-ons to see if they need updating. You're not required to do this for the

class, but I suggest that you do something like this to keep your personal devices up to date.

And here's one more method for checking Chrome for updates.

1. Start Chrome and type **chrome://extensions** in the location dialog box
2. Turn **Develop mode** on
3. Click the **Update** button



[OPTIONAL] https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-checking-all-applications-for-updates/ - This video demonstrates some methods for checking *all* of your applications for updates, not just the browser plugins. Once again, this not required for the class, but it's something that I suggest you do to improve the security on your personal computer.

- Answer the following question. Did the scan(s) report any issues that you need to fix? That is, is your browser up to date? And if you use any of the other tools, are your plugin/add-ons up to date?

What to submit for Project 5-2:

- Take a screen shot after steps 2 and 7. 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.)

- Answer the following question. Does your computer support NX?

2. Required Case Project Homework (Writing Assignment)

The writing assignment for this section requires you to do some research and write a paper. You can select any of the subjects described in Case Project 5-1, 5-2, 5-3, 5-4, or 5-5. You only need to write one paper, but it must be on one of these subjects. All of the papers require you to do some research, so make sure and keep track of the papers or web sites you use for research, and include them as references in your paper.

Hopefully you remember how your paper must be formatted, and the other guidelines for writing papers. But if not, you can refer to the Written Project Guidelines document for details on how your paper/report will be graded. You can find the document at:

https://tonysako.com/writingprojectguidelines2021/

Also, remember to check your TurnItIn score. If the score 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 before submitting your work. But don't worry about making multiple submissions, everyone does it and 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

3. Optional Activities

If you continue taking Cyber Security or Network Administration classes you'll learn quite a bit more about some of the attacks described in this chapter. But there are also a couple of quick exercises you can do that should shed a little more light on several of the attacks you learned about in the book. These exercises are completely optional. There's no to turn them in and they will not be graded. However, they don't take much time and I think you'll find them interesting.

A. Do Hands-On Project 5-3 in your book. As you may know, most Internet traffic is based on TCP/IP. With TCP/IP every computer is assigned an IP address, which is a 4 part number similar to 104.56.72.78. To send packets to another device you must know the recipient's IP address. It's almost like phones, where every phone needs a number, and you need to know the recipient's number to call them. And just like with phone numbers, it's much easier for humans to remember names than it is to remember numbers. If you're old enough you might remember the phone book, it provided this service for phone numbers. That is, it's easier to remember a person's name than their phone number. But to call someone you need to know their phone number. With the white pages phone book, or the old 411 service, you could

"resolve" a person's name to their phone number. DNS does this exact same thing for IP addresses. The difference is that DNS is built into most network applications. All you need to do is type a URL or email address with an easy to remember DNS name, and the network will automatically query the DNS system and resolve this to an IP address. But imagine what would happen if an attacker could change the DNS system so that when you asked for IP address of a legitimate site, it returned the IP address of their fake site.

You'll learn the details about the DNS system in a later networking class. And you'll see that the DNS system itself is pretty trustworthy as it's relatively difficult for someone to hijack the entire system. But a key part of the DNS configuration is done on each computer. This is the part where you have a list of DNS servers that will be queried any time you need an IP address, or a small local "phonebook" that can be used like the contacts list on your phone. If an attacker can change either of these two files, they can fool your computer into using a fake IP addresses, and redirect some of your network traffic to computers they control.

In this exercise, you'll learn how to edit the file on your computer that acts like your phone's contact list. This will give you an idea of what big DNS does, that is, you give it a name and it returns an IP address. Plus, you'll get an idea of how it can be attacked. You can also use your knowledge to pull stupid computer tricks on your friends. But be careful if you do this, as it's actually a Federal crime. That is, changing the file so that your friend is redirected to their CBC Canvas account when they try to access Facebook would be a funny trick, as long as you are there to laugh and then help them fix it. But changing the file so that your friend goes to your fake site when they try to access the government's Social Security site will land you in jail.

Once again, this exercise is optional and there's nothing to turn in. You'll learn more about DNS and these types of attacks in a later class. But I believe it's relatively short and easy, and will give you a better idea of what's going on with the DNS Poisoning attack.

B. The second optional activity is to check the log on your home router, if you have one. The reason for doing this is that it can show you all of the attempted connections coming from outside of your network. Usually you initiate every network connection from inside your network. That is, when you ask for a web page, that network request starts on your home computer, inside your network. The router makes the connection to the web server for you, and knows that the data being sent back is in response to your request. So, any requests from outside your network, that aren't initiated by a device inside your network, are an indication that someone is trying to gain access to your network. These attempts are typically blocked by the router to protect you, as the router also acts as a firewall. The attempts are also typically logged by your router.

Of course, it's possible that you have a device inside your network that people can access. Maybe you've set up your own VPN, or maybe you or your kids are running a Minecraft server. In this case, you must typically configure the firewall portion of the router to allow these requests into your network. You'll learn all about routers, firewall, and network traffic in a later class. But for now I thought it would be interesting for you to check your router to see how many attacks are being performed against your home router. Every time I've checked my router the log is full of evidence of attempted network attacks, and I imagine your is probably the same.

The specific steps for checking your router log will vary, depending on the make and model of router, but the general steps will be the same, and they include:

i. Start your web browser.
ii. Log in to your router.
iii. Find the command in the router's Control Panel to display the logs

I've made a video that demonstrates the process, and has some guidance on figuring out what to do if the steps for your specific router are different.

Here is the link to the video, plus links to a couple other videos that show you the same thing, and links to some of the sites referenced in the video:

https://tonysako.com/cs150-viewing-wireless-router-logs/ - My Video on viewing router logs, with troubleshooting tips. Every router follows the same general process, but the specifics will be different.

https://www.techwalla.com/articles/how-to-check-a-routers-log - Techwallas video on checking router logs

https://www.howtogeek.com/233952/how-to-find-your-routers-ip-address-on-any-computer-smartphone-or-tablet/

https://www.quora.com/How-can-you-know-router-admin-password-without-reset

Ways to Check Your Comprehension

The test over this chapter won't be for a few weeks, so if you want check your comprehension you can use the review questions at the end of the chapter or the Practice Test. 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.

If you want to use the Practice Test, look in the Test 2 Canvas Module for the 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.