4.4 Computer Crimes & Securing the Web

4.4.1 Computer Crime:

Definition: the act of using a computer to commit an illegal act – Authorized and unauthorized computer access

– **Examples**

• Stealing time on company computers

• Breaking into government Web sites

• Stealing credit card information

- Federal and State Laws

– Stealing or compromising data

– Gaining unauthorized computer access

– Violating data belonging to banks

– Intercepting communications

– Threatening to damage computer systems

– Disseminating viruses

• **Hacking and Cracking**

– Hacker – one who gains unauthorized computer access, but without doing damage – Cracker – one who breaks into computer systems for the purpose of doing damage

4.4.1.1 Types of computer crime:

Data diddling: modifying data

• Salami slicing: skimming small amounts of money

• Phreaking: making free long-distance calls

• Cloning: cellular phone fraud using scanners

• Carding: stealing credit card numbers online

• Piggybacking: stealing credit card numbers by spying
• Social engineering: tricking employees to gain access
• Dumpster diving: finding private info in garbage cans
• Spoofing: stealing passwords through a false login page
• Software piracy – North America – 25%
-Western Europe – 34%
– Asia / Pacific – 51%
– Mid East / Africa – 55%
– Latin America – 58%
– Eastern Europe – 63%

Computer viruses and destructive code
– Virus – a destructive program that disrupts the normal functioning of computer systems
– **Types:**
• Worm: usually does not destroy files; copies itself
• Trojan horses: Activates without being detected; does not copy itself
• Logic or time bombs: A type of Trojan horse that stays dormant for a period of time before activating.

4.4.3 Most Common Computer Crimes:

1. Phishing in San Diego, California

Phishing is when criminals send fraudulent emails pretending to be from legitimate businesses, in an attempt to collect sensitive, personal information. Often, any links in the email will redirect to a website owned by the scammer, so always be careful about what information you give out on the Internet.

2. Harassment

Cyberstalkers use electronic communication, such as email, social media, or websites to stalk and harass people. Forms of online harassment include slander, libel, false accusations, threats, or any other behaviour that demeans or embarrasses someone. Sentences for cyberstalking can include jail time and hefty fines.

3. Ransomware

Cyber criminals can install malicious software on your system that will essentially hold your important information hostage until you meet their demands. A common ransomware attack will shut down a victim's computer or encrypt their files, agreeing to release them only if the victim pays a ransom. All too often, however, the files are never recovered.

4. Prostitution

Many escorts will advertise their services in online classifieds, social media forums, or their own personal websites, making it easy and discreet for people to find them. But since prostitution is illegal in the vast majority of the United States, both the escort and the client are committing a crime.

5. Child Pornography & Solicitation

The National Center for Missing and Exploited Children received over 10 million reports of suspected child sexual exploitation in the last year alone. Perpetrators will use the Internet to gain access to sexually explicit images of children, and sometimes even arrange for a face-to-face meeting.

6. Intellectual Property Theft

More commonly known as piracy, the Internet abounds with books, music, movies, and more that have been illegally obtained and made available for free download. Despite what some people say, piracy is not a victimless crime. Not only do artists and creators lose out, but many illegal downloads also contain hidden malware that can destroy your computer.

7. Account Hacking

We all know how important it is to guard our passwords – think about the damage someone could do if they gained access to your email account containing all your most personal information. If someone logs into your email, social media, or computer without authorization, they could potentially face jail time.

8. Drug Trafficking

With the rise of cryptocurrency, the online drug trade has increased significantly over the past few years. Illegal drugs such as marijuana, cocaine, meth, ecstasy, and heroin are all just a few clicks away – and according to research by the Rand Corporation, over 35% of worldwide revenues from online drug trafficking are based in the United States.

9. Credit Card Fraud

Half of all credit card fraud begins with spyware, malicious software unknowingly installed on a victim's computer or handheld device. Spyware runs in the background, collecting your data and sending it back to the criminal, who then uses your card to make fraudulent purchases.

4.4.4 Securing the Web:

- Web servers are one of the many public faces of an organization and one of the most easily targeted. Web servers represent an interesting paradox namely, how do you share information about your organization without giving away the so-called store? Solving this dilemma can be a tough and thankless job; but it's also one of the most important.
- Before I get too far, though, let's take a look at some of the threats that your server faces by virtue of being one of the "troops" on the front line.
- Now, there are a tremendous number of threats facing a Web server, and many depend on the applications, operating system, and environment you have configured on the system itself. What I have assembled in this section are some of the more generic attacks that your poor server may face.

4.4.4.1 Denial of service:

The denial of service (DoS) attack is one of the real "old-school" attacks that a server can face. The attack is very simple, and nowadays it's carried out by those individuals commonly known as script kiddies, who basically have a low skill level. In a nutshell, a DoS attack is an attack in which one system attacks another with the intent of consuming all the resources on the system (such as bandwidth or processor cycles), leaving nothing behind for legitimate requests. Generally, these attacks have been relegated to the category of annoyance, but don't let that be a reason to lower your guard, because there are plenty of other things to keep you up at night.

4.4.4.2 Distributed denial of service

The distributed DoS (DDoS) attack is the big brother of the DoS attack and as such is meaner and nastier. The goal of the DDoS attack is to do the same thing as the DoS, but on a much grander and more complex scale. In a DDoS attack, instead of one system attacking another, an attacker uses multiple systems to target a server, and by multiple systems I mean not hundreds or thousands, but more on the order of hundreds of thousands. Where DoS is just an annoyance, a DDoS attack can be downright deadly, as it can take a server offline quickly. The good news is that the skill level required to pull a DDoS attack off is fairly high.

Some of the more common DDoS attacks include:

1. **FTP bounce attacks**. A File Transfer Protocol (FTP) bounce attack is enacted when an attacker uploads a specially constructed file to a vulnerable FTP server, which in turn forwards it to another location, which generally is another server inside the organization. The file that is forwarded typically contains some sort of payload designed to make the final server do something that the attacker wants it to do.
2. **Port scanning attack**. A port scanning attack is performed through the structured and systematic scanning of a host. For example, someone may scan your Web server with the intention of finding exposed services or other vulnerabilities that can be exploited. This attack can be fairly easily performed with any one of a number of port scanners available freely on the Internet. It also is one of the more common types of attacks, as it is so simple to pull off that script kiddies attempt it just by dropping the host name or IP address of your server (however, they typically don't know how to interpret the results). Keep in mind that a more advanced attacker will use port scanning to uncover information for a later effort.
3. Ping flooding attack. A ping flooding attack is a simple DDoS attack in which a computer sends a packet (ping) to another system with the intention of uncovering information about services or systems that are up or down. At the low end, a ping flood can be used to uncover information covertly, but throttle up the packets being sent to a target or victim so that now, the system will go offline or suffer slowdowns.

This attack is "old school" but still very effective, as a number of modern operating systems are still susceptible to this attack and can be taken down.

4. Smurf attack. This attack is similar to the ping flood attack but with a clever modification to the process. In a Smurf attack, a ping command is sent to an intermediate network, where it is amplified and forwarded to the victim. What was once a single "drop" now becomes a virtual tsunami of traffic? Luckily, this type of attack is somewhat rare.
5. SYN flooding. This attack requires some knowledge of the TCP/ IP protocol suite—namely, how the whole communication process works. The easiest way to explain this attack is through an analogy. This attack is the networking equivalent of sending a letter to someone that requires a response, but the letter uses a bogus return address. That individual sends your letter back and waits for your response, but the response never comes, because it went into a black hole some place. Enough SYN requests to the system and an attacker can use all the connections on a system so that nothing else can get through.
6. P fragmentation/fragmentation attack. In this attack, an attacker uses advanced knowledge of the TCP/IP protocol to break packets up into smaller pieces, or "fragments", that bypass most intrusion-detection systems. In extreme cases, this type of attack can cause hangs, lock-ups, reboots, blue screens, and other mischief. Luckily, this attack is a tough one to pull off.
7. Simple Network Management Protocol (SNMP) attack. SNMP attacks are specifically designed to exploit the SNMP service, which is used to manage the network and devices on it. Because SNMP is used to manage network devices, exploiting this service can result in an attacker getting detailed intelligence on the structure of the network that he or she can use to attack you later.

4.4.5 Web page defacement

Web page defacement is seen from time to time around the Internet. As the name implies, a Web page defacement results when a Web server is improperly configured, and an attacker uses this flawed configuration to modify Web pages for any number of reasons, such as for fun or to push a political cause.

4.4.6 SQL injection

Structured Query Language (SQL) injections are attacks carried out against databases. In this attack, an attacker uses weaknesses in the design of the database or Web page to extract information or even manipulate information within the database.

4.4.7 Poor coding

Anyone who has been a developer or worked in information technology has seen the problems associated with sloppy or lazy coding practices. Poor coding problems can result from any one of a number of factors, including poor training, new developers, or insufficient quality assurance for an application. At its best, poor coding can be an annoyance, where features don't work as advertised; at its worst, applications can have major security holes.

4.4.8 Shrink-wrapped code

This problem is somewhat related to the above issues with poor coding, but with a twist: Basically, this problem stems from the convenience of obtaining precompiled or pre-written components that can be used as building blocks for your own application, shortening your development cycle. The downside is that the components you're using to help build your application may not have gone through the same vetting process as your in-house code, and applications may have potential problem areas. Additionally, it's not unheard of for developers who don't really know how to analyze the code and understand what it's actually doing to put so-called "shrink-wrapped" components in applications.
In at least one case I can think of, I'm aware of a developer using a piece of shrink-wrapped code to provide an authentication mechanism for an application that was actually authenticating users, but also covertly e-mailing the same credentials to a third-party.

4.4.9 Protecting Web servers

1. Separate Web servers for internal and external use. This sounds like a no-brainer, but it still bears repeating. Most organizations have Web-based applications or sites used internally, as well as applications and sites used externally. In an ideal situation, these two sets of servers and content should be kept separate, with

internal and external sites having their own servers with as little crossover between them as possible. By splitting systems apart like this, you avoid the probability (or at least lessen the risk) of an attacker breaching a server and getting access to data or even internal systems.

2. Separate development and production servers. In my time, I have known several companies that have violated this rule by letting their development team work on production servers to develop their code or tweak existing code. Typically, this is just a case of extreme laziness—one that can lead to catastrophic problems later when an attacker sees your unpolished code and exploits it to his or her own ends. Also, consider that your own developers may compromise security by testing and tweaking code. Do yourself a favor: Implement a development environment.
3. Regular audits. Any Web server or Web application worth its salt will have some method of generating logs of activity on the system. After this information is logged, make it part of your regular routine to scan the logs for problems, such as application failures or suspicious activity. Keep in mind that an audit log is like evidence collected at a crime scene: It's essentially worthless unless you intend to examine it later.
4. Keep your system up to date. Do I really need to go through this one? Yes, I do. Patching a system is an often-overlooked problem when it really shouldn't be. Ideally, you should keep an eye on whether patches, service packs, updates, or other items become available that can help secure your system. Depending on your hosting platform and other factors, you may have the option of having these updates delivered automatically, or you may have to use the old-fashioned manual delivery method. Also keep in mind that many times, updates are the only way to fix problems such as those related to buffer overflows, network client issues, and so on.
5. Vulnerability scanning. In previous articles (see Resources), I covered the topic of vulnerability scanning as a tool for finding problems in your hosting and application infrastructure.Vulnerability scanning can be a very powerful tool in the ongoing struggle to uncover problems relating to software, such as configuration and patching issues. Another advantage is that these scanning tools are regularly

updated, so you can use them to find the latest problems that, in a number of cases, include issues that you may not even be aware of, allowing you to address them before they can be exploited. Tools such as the freeware Nessus (see Resources) can be a great asset to administrators regardless of whether you host on Linux®, UNIX®, or some other platform.

6. Developer training. This one may be a bit more difficult to pull off, but it reaps a tremendous reward, if undertaken. Educating developers on secure coding practices can result in the elimination or reduction of problems associated with sloppy or lazy coding.

****