Introduction

Anish Goyal

Yubo Cao

September 2, 2022

Contents

1 Motivation

- The goal of Cybersecurity department is to offer a symposium for research, enrichment, and sharing for anyone with an interest in Cybersecurity .
- Ignite, sustain, and increase awareness of K-12 Cybersecurity content and Cybersecurity postsecondary and career opportunities.
- Strives to be a part of the solution to the Nation's shortfall of skilled Cybersecurity professionals.

In addition to the above goals, you are expected to *have fun* here. Cybersecurity department will attract peers who share your interests.

2 Goal

After this lecture, you should have a good understanding of the following:

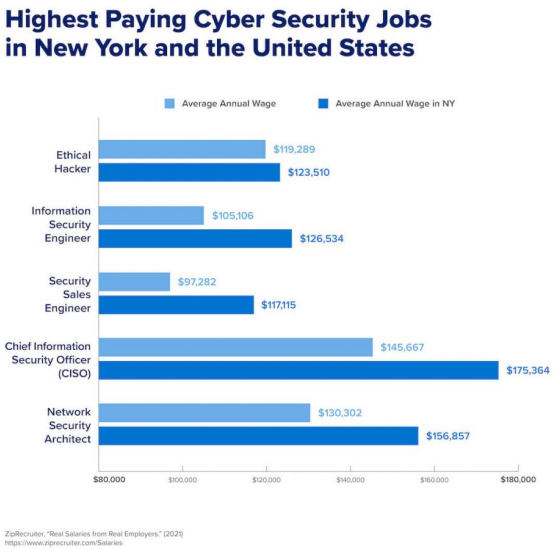
- Basic Cybersecurity principles
- Basic Cybersecurity terminology, concepts, tools, and techniques.
- Be able to distinguish ethical behavior and unethical behavior.
- Virtualization technique and lab setup.

3 Cybersecurity

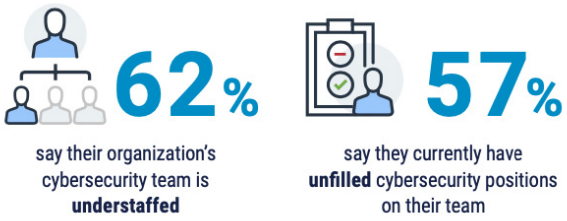
Cybersecurity is the field responsible for protecting and securing digital assets and data. The Cybersecurity field encompasses different jobs that require varying skill sets.

3.1 Jobs

It appears that Cybersecurity , among biology, physics, and chemistry, cannot for some reason presume that the participants in the class are interested in this topic. Therefore, a brief explanation of why Cybersecurity could be of interest to you is provided below.



(a) Cybersecurity and payment data



(b) Cybersecurity hiring challenge

First, Cybersecurity is a field that makes a lot of money. The people in this field with decent amount of intelligence and experience are able to make $ 175,364 per year, as shown in figure 1a.

Second, there is not a lot of people in Cybersecurity yet. About 62% of organizations claims that they don't got enough Cybersecurity professionals, as shown in figure 1b.

3.2 Workflow

The Cybersecurity workflow may be expressed as follows:

Algorithm 0: Cybersecurity workflow

```
while true do
    Research and understand the system and its vulnerabilities;
    Protect the system and its assets;
    if Attack detected then
        Identify the attack;
        Mitigate the attack;
    end
end
```

The protection of the system is a dead-loop. The weakness is continuously discovered and so as the attack. In short, this is an endless battle between you and the attacker.

3.3 Ethics

Let's talk about something exciting, *hacking*. Cybersecurity department will teach you how to hack, but you are not allowed to hack beyond the competition, unless you are authorized, i.e., become a penetration tester.

- 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, describes such illegal activities in detail:

  > Whoever …intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— …information from any protected computer …shall be punished as provided in subsection (c) of this section.

  In case one are interested in knowing more, refer to U.S. Code § 1030.

- USA Patriot Act, Homeland Security Act, and the DoD Cybersecurity Act are the laws that govern the Cybersecurity field.

- `https://www.justice.gov/criminal-ccips` is another website which has information about the laws that govern the Cybersecurity field.

Put it in plain English

- Unauthorized access or use of a computer or network system is illegal
- Unintentional attacks are illegal too

3.4 Common Hacker

- Operator/user blunders.
- Hackers driven by intellectual challenge or boredom.

- Insiders: employees or customers seeking revenge or gain.
- Criminals seeking financial gain.
- Organized crime seeking gain or hiding criminal activities.
- Organized terrorist groups or nation states trying to influence national policy.
- Foreign agents seeking information for economic, political, or military purposes.
- Tactical countermeasures intended to disrupt military capability.
- Large organized terrorist groups or nation-states intent on overthrowing the US government.

3.5 Vulnerability

Vulnerability, is a potential occurrence, malicious or otherwise, that might damage or compromise assets.

Interception asset is diverted

Interruption asset is delayed

Modification asset is altered

Fabrication asset is manufactured

3.5.1 Common Vulnerabilities

- Poorly chosen passwords
- Software bugs
- unchecked array access (buffer overflow attacks)
- Automatically running active content: macros, scripts, Java programs
- Incorrect configuration

- Untrained users/system administrators
- Trap doors (intentional security holes)
- Unencrypted communication
- Limited Resources (i.e. TCP connections)

3.6 Assets

Asset is any data, device, or other component of the environment that supports information-related activities.

- Hardware
- Software
- People
- Data

3.7 Principles

3.7.1 CIA Triads

Figure 2: CIA Triads

The CIA triad is a common model that forms the basis for the development of security systems, demonstrated in figure 2.

Confidentiality asset is not visible to unauthorized users

Integrity asset is not altered or modified by unauthorized users

Availability asset is available to authorized users

3.7.2 Common Concepts

Defense in Depth

- A strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited
- This helps ensure that you are protecting your assets as effectively as possible
- Often called the castle approach

For example,

- Padlock on GSMST's doors
- Anti-virus software on GSMST's computers
- Student don't have Admin access
- Firewall on GSMST's computers, routers, and DNS spoofing in local DNS server

Confidentiality Ensures that only authorized users may view the information. Applies whether data is in storage, transit or processing, i.e., in the entire life cycle of the assets.

For example,

- Encryption
- Manage data access
- Passwords
- Physically secure devices

Integrity Goal is to protect data from modification from any unauthorized party, hence, one may trust the data he received.

For example,

- Checksum in IP packets
- md5, sha1, sha256, sha512 hash in files
- Logging software, audit software

Availability Just unplug your server, and you have the *safest* server in the world. Nobody will have access to your server, not even you.

Therefore, the availability of the system is a critical component of the security of the system. The system must respond to valid requests of data.

For example,

- DDoS (Distributed Denial of Service)
- Computational redundancy (i.e. multiple servers, backup systems, redundant array of independent disks)
- Physical protections (i.e. secure server rooms)

Think Like an Adversary *Hacking*! YaY! If you are over-excited, read 3.3 one more time.

The strategy of putting yourself inside the mindset of a potential attacker that allows you to anticipate attack strategies and defend your systems accordingly. This allows you to be proactive rather than reactive.

Put it in plain English, you ask someone or hack your system by yourself, in order to figure weakness in the system. Only in such situation, one may hack without legal implications.

Keep it Simple, Stupid

- The lack of complexity allows system designers and programmers to identify unwanted access paths

- Easier to understand, maintain, and test – so more secure
- Users can easily translate their general protection goals to appropriate system security configurations
- The simpler it is, the less that can go wrong

A counter example would be requiring a user to devise a 40-character password. That kind of security measurement is almost always bypassed, as user would simply store their password in plain text file somewhere in their computer.

4 Setup Virtual Machines

Virtual machine (VM) is the virtualization/emulation of a computer system, i.e., use software to emulate some hardware and install system inside.

Several reasons you don't want to install a Windows™ Server, Linux, or Cisco™ in your own computer.

- It helps distribution of computing resources, i.e., a server may to host multiple web servers, mail servers, and other applications simultaneously. Hence, when you work in a company later, more than likely you will be working with them.
- It prevents the physical computer from potential damage of virus and other malicious software, as any modification happened inside the virtual machine does not affect the physical computer. You might crash the system due to your own fault, and you definitely don't want to crash your own computer. In a virtual machine, you can reset it back to the most recent snapshot in 5 s.
- Linux is **shit**. I strongly suggest you not to use it in your own computer. You will see it crash every hour if not used properly.
- It gives you ability to practice in a lot of different environment. For example, when we study `dhcpcd` or `RAID` later, you don't need to by 10 extra computers or 4 extra disks in order to practice.

We will use VMWare™ Workstation to install our virtual machine. It is a commercial product; however, the player version is free. We are currently working with Tech-Triage to install it on school laptop. Since this is still in progress, you need to follow the following procedure in a Windows™ 10 system with VT-x support. We will setup an Ubuntu™ 22.04 LTS system.

Some other alternatives exist; however, VMWare Workstation is what will be used during CyberPatriot competition.

Virtual Box `https://www.virtualbox.org/wiki/Downloads`

Hyper-V `https://www.microsoft.com/en-us/virtualization/hyper-v`

Qemu `https://www.qemu.org/`

4.1 Download

Ubuntu™ 22.04 LTS `https://www.ubuntu.com/download/desktop`

VMWare™ Workstation `https://www.vmware.com/products/workstation/`

After the image and player are downloaded, click next on the installation wizard for VMware Workstation. Hopefully, you got it installed and can try it for 30 days. Obviously, people with certain extent of experience know how to use it for free and forever, but for the sake of ethics, we will not disclose such methods here.

4.2 Installation