Introduction To Cybersecurity

Isaac Gray-Christensen

2022-09-03

Contents

1 Introduction

In the modern world, cybersecurity is now one of the most sought after positions and is highly in demand. Especially with the SolarWinds hack that occured in late-2019/early-2020, then the Log4Shell application vulnerabilities that is still fresh in everyones mind from late-2021/early-2022, cybersecurity has started drastically more weight. These major events have even lead to new legislation that introduced policies and laws that now extends between geopolitical boundaries.

But however glorious cybersecurity may seem, especially with it being the shiny thing everyone wants to be doing, it is often less glamorous than it seems. Cybersecurity ranges from exploit development and pentesting, all the way to creating filters for events in logging systems or writing policies/standards. It also comes with its challenges, with the most notable encountered being constantly educating non-technical end-users, executives, or potentially even customers. Regardless of one's job position, it is absolutely imperative and unfortunately under-represented in many company's cybersecurity staffing's that individuals in cybersecurity positions that are non-technical (managerial, compliance, documentation/policies) lack even the most fundamental cybersecurity understandings.

These labs will help build a base that you can carry forward and use to understand the basics of cybersecurity that you will use throughout your career. The labs are broken up into sections that will continintroduceduously build upon the previous sections.

1.1 Lab Environment

To get started with the lab environment, you first must install Docker.

Docker is a tool that setups up containers locally and allows for the ability to create reproducible environments between computers, even Operating Systems (OS's).

Once docker is installed on your platform of choice, you'll need to open up a CLI interface.

WINDOWS:

1. Click on the start menu

2. Type in `Powershell.exe`
3. When a blue window opens up, run `docker run -it --rm <container:image>`

---

2 Cryptography

At its core, cryptography is one of the most critical elements that is used and implemented in nearly every system that could be encountered in one's daily life.

However, before we jump into how encryption is used, it is important to understand the methods for applying the encryption. This will be the first step we will focus on here.

2.1 Basic Cryptography

Cryptography has a very long history that extends from even before the Roman era, over 2000 years ago. Essentially, since written communication has been used, various methods of cryptography have been applied to hide the message from plain view so that only the intended recepient is able to read it. It involves creating a message, known as plaintext, then applying some sort of encryption scheme to then produce what is referred to as cipher text, which contains the now hidden message.

2.1.1 ROT13

ROT13 a rotational cipher that uses an alphabet with all letters transposed left or right 13 letters. The below table shows what ROT13 looks like in comparison with the normal flow of the alphabet.

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	X	Z
Cipher	N	O	P	Q	R	S	T	U	V	W	Y	X	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

An Example of this in practice:

```
Plaintext: Apple

Ciphertext: Nccxr
```

While the characters are rotated and obfuscates the text from immediately being able to tell what the word/phrase is, modern computers renders this form of encryption useless.

2.1.1.1 ROT13 Lab

Run the `rot13` command in the lab for hands-on practice

2.1.2 Caeser Cipher

As the name hints, this type of cipher is from the Roman era where Julius Caeser used it. While it has a fancy name, it is nothing more than a modified version of the ROT13 cipher.

In essence, all the Caeser Cipher does is modify how far the Alphabet is shifted left or right. This can be just one character or up to 25 characters in a given direction. It is important to note that like the ROT13 cipher, the ***whole*** alphabet needs to be shifted over the given number of characters.

2.1.2.1 Caeser Cipher Lab

To see this in practice, run the `caeser_cipher` command.