Colby Heilner

Professor Torres

8/24

IT-120

Lab 1

Part A

What does it take to work in Cyber Security? What education, certification, experience, and knowledge are required for what you want to do?

I found a Good looking red team job with this title: Cyber Security Cloud Threat Modeling Analyst. When looking through some of the requirements for this job here are some of the more important ones. First off certs, CompTIA CASP+, CompTIA PenTest+, AWS, Google Cloud Architect, ISACA, GIAC. The list could go on! They also want you to have a bachelor's degree/University degree or equivalent experience, master's degree is preferred.

List 10 different types of Cyber Security jobs

Cloud Engineer

Cybersecurity Engineer

Cyber Threat Analyst

Cybersecurity Business Analyst

FT or PT Cybersecurity AI Instructor

Senior Principal, Information Security Architect

Product Cybersecurity Engineer

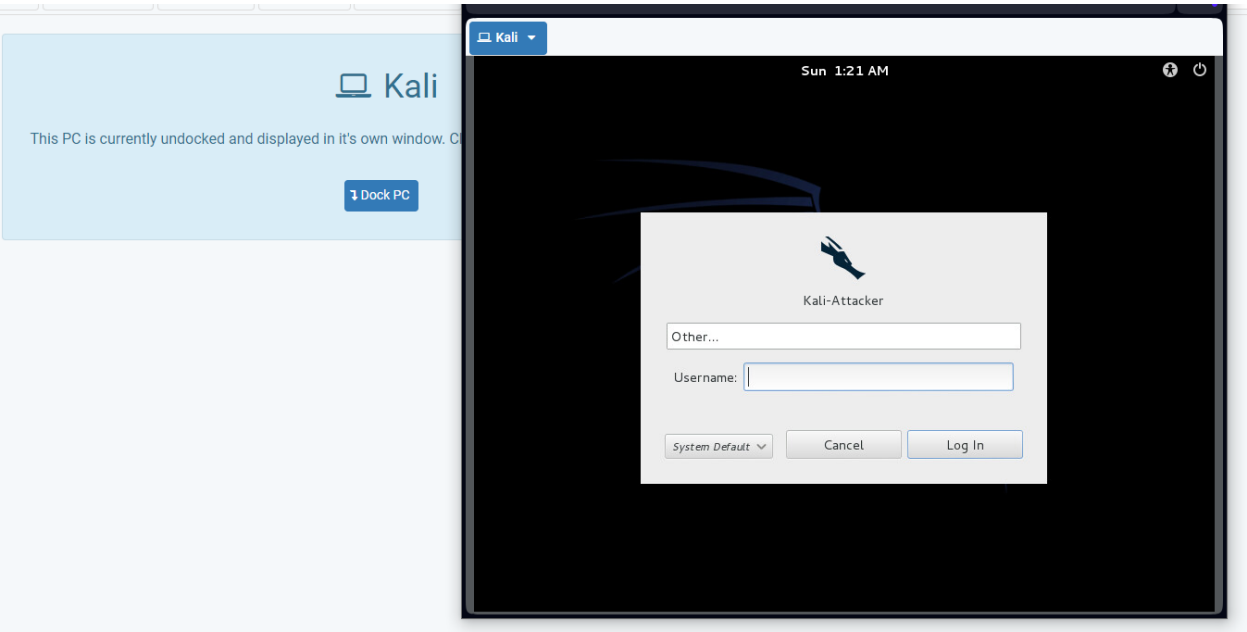
Staff IAM Engineer

Information Assurance/Insider Threat User Activity (UAM) Analyst

Cyber Triage Analyst

PART B

Un-dock the Kali Linux system



I then logged onto all the systems and had them Ping all other systems.

Here is Kali pinging one DMZ and Internal

```
root@Kali-Attacker:~# ping 10.1.1.10
PING 10.1.1.10 (10.1.1.10) 56(84) bytes of data.
64 bytes from 10.1.1.10: icmp_req=1 ttl=63 time=0.827 ms
64 bytes from 10.1.1.10: icmp_req=2 ttl=63 time=0.716 ms
64 bytes from 10.1.1.10: icmp_req=3 ttl=63 time=0.650 ms
^C
```

```
root@Kali-Attacker:~# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_req=1 ttl=127 time=1.13 ms
64 bytes from 192.168.1.100: icmp_req=2 ttl=127 time=0.671 ms
64 bytes from 192.168.1.100: icmp_req=3 ttl=127 time=0.834 ms
64 bytes from 192.168.1.100: icmp_req=4 ttl=127 time=0.817 ms
^C
```

Here is Ubuntu Pings (One Kali and DMZ)

```
PING 10.1.1.12 (10.1.1.12) 56(84) bytes of data.
64 bytes from 10.1.1.12: icmp_req=1 ttl=127 time=0.942 ms
64 bytes from 10.1.1.12: icmp_req=2 ttl=127 time=0.773 ms
64 bytes from 10.1.1.12: icmp_req=3 ttl=127 time=0.888 ms
^C
```

```
PING 203.0.113.2 (203.0.113.2) 56(84) bytes of data.
64 bytes from 203.0.113.2: icmp_req=1 ttl=63 time=1.98 ms
64 bytes from 203.0.113.2: icmp_req=2 ttl=63 time=0.844 ms
64 bytes from 203.0.113.2: icmp_req=3 ttl=63 time=2.00 ms
^C
```

Here is DVL ping One kali and Internal

```
bt ~ # ping 203.0.113.2
PING 203.0.113.2 (203.0.113.2) 56(84) bytes of data.
64 bytes from 203.0.113.2: icmp_seq=1 ttl=63 time=0.850 ms
64 bytes from 203.0.113.2: icmp_seq=2 ttl=63 time=0.808 ms
64 bytes from 203.0.113.2: icmp_seq=3 ttl=63 time=0.611 ms
```

```
bt ~ # ping 192.168.1.50
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_seq=1 ttl=63 time=0.999 ms
64 bytes from 192.168.1.50: icmp_seq=2 ttl=63 time=0.642 ms
64 bytes from 192.168.1.50: icmp_seq=3 ttl=63 time=0.749 ms
64 bytes from 192.168.1.50: icmp_seq=4 ttl=63 time=0.847 ms
```

Finally, I had pfSense firewall ping all areas of the network even though it should work regardless because it is in-between all of them.

Internal

```
PING 192.168.1.50 (192.168.1.50): 56 data bytes
64 bytes from 192.168.1.50: icmp_seq=0 ttl=64 time=0.502 ms
64 bytes from 192.168.1.50: icmp_seq=1 ttl=64 time=0.443 ms
64 bytes from 192.168.1.50: icmp_seq=2 ttl=64 time=0.328 ms
```

DMZ

```
PING 10.1.1.12 (10.1.1.12): 56 data bytes
64 bytes from 10.1.1.12: icmp_seq=0 ttl=128 time=3.085 ms
64 bytes from 10.1.1.12: icmp_seq=1 ttl=128 time=0.557 ms
64 bytes from 10.1.1.12: icmp_seq=2 ttl=128 time=0.627 ms
```

Kali

```
PING 203.0.113.2 (203.0.113.2): 56 data bytes
64 bytes from 203.0.113.2: icmp_seq=0 ttl=64 time=0.481 ms
64 bytes from 203.0.113.2: icmp_seq=1 ttl=64 time=0.951 ms
64 bytes from 203.0.113.2: icmp_seq=2 ttl=64 time=0.363 ms
```

Just to test something as well I went into shell in the pfsense and nuked all rules.

pfctl –F rules

I could no longer ping from kali.

```
root@Kali-Attacker:~# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
^C
--- 192.168.1.100 ping statistics ---
59 packets transmitted, 0 received, 100% packet loss, time 58463ms
```

PART C

What is your opinion/view about these documents?

CIS Controls Implementation Guide

This seems like a useful tool for small business owners to get educated on cybersecurity practices. I am going to dive into the first page in this document in depth. These three points in the first paragraph stand out to me.

Do you know what is connected to your network?
- Do you know what software is installed?
- Do you know if your administrators and users are using strong passwords?

All of these I fall under the “know what your environment contains and what you need to secure and where to look for vulnerabilities.” This seems like a topic we WILL get to cover in the class. I feel that other than the actual securing of assets, devices and data, this step is the most important.

This does deserve an honorable mention:

Do you know which online platforms are being used by your employees (i.e., work productivity or chat tools)?

Knowing what applications and tools are being used on the network is super important. Imagine an employee using an outdated version of zoom comprising the entire subnet, maybe even network. EX: CVE-2023-39213.

Now looking at the NIST document seems to follow the same flow. It aims to set itself as a standard for small to medium size business to help them establish strong cybersecurity. The 6 sections are Govern, Identify, Protect, Detect, Respond and Recover. Again, I think we will be able to get to all of these in this class. The only one I think we may skip/ not go into full depth is govern. This is because this may differ depending on the business that is implementing this Framework. Something to add is that I feel it is a little funny that they must add this line: **Antivirus software alerts when it detects that a host is infected with malware.** To me this seems like a no brainer, but some people are uneducated on any cybersecurity at all.