BLACK TOWER ACADEMY

How to start and build a CyberSecurity Career

Pace & Space (5 min Q&A @ End)
45 Min / 31 Slides = 1:45m Per slide

Starting a Cybersecurity career

01 What does it take?

02 What does it look like?

03 The job titles are so confusing?

04 What do the roles mean?

05 What are the paths?

06 Where do I start?

Why is it called Breaking in?

How it was done over a decade ago, isn’t something we can keep doing today.

The need is too high, too strong, and we simply need more people than the old way can support.

Neckbeards

Grouchy Computer People (so angry)

- Can be seen as pedantic, overly focused on niche interests, condescending, or antisocial.

The way it used to be (10+ years)

System Administrator

Sysadmins understand operating systems, networks, software applications, and hardware configurations. This foundational knowledge is crucial for understanding attack vectors and vulnerabilities.

Network Engineer

Having deep knowledge about network configurations, protocols, and services allows for better understanding of network-based threats and how to mitigate them.

Software Developer

Developers understand the intricacies of software design, data structures, algorithms, and system architecture, which are vital when evaluating vulnerabilities or designing secure software.

No longer works

We have to change

With the increasing number and sophistication of cyber threats, the demand for skilled cybersecurity professionals has skyrocketed.

Recruiters

Don’t really know enough, or understand the industry enough to find the right candidate.

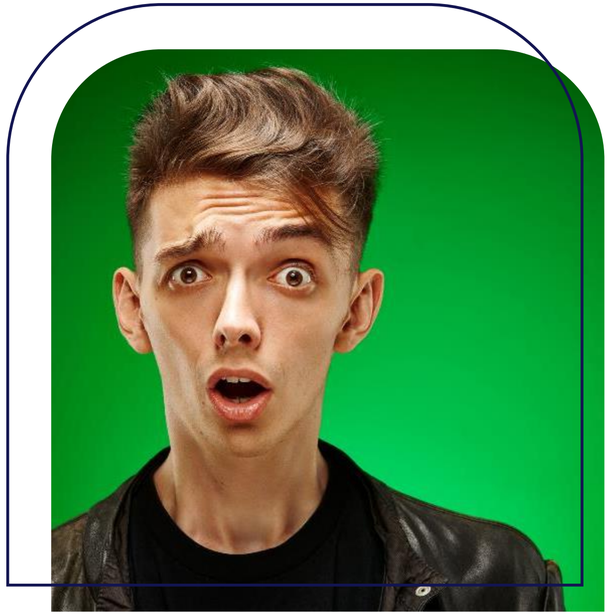
Applicants

Don’t understand “the game”, what it takes, and how long it takes to obtain a position.

Where are the jobs?

Why are they only looking for EXPERTS!?>

Looking for a job ‘be like’



Confusing

Overwhelming

Vague Job Descriptions

Multiple Tracking Systems

Lack of Feedback

Frustrating

Rejection

Inconsistent Responses

Long and Disparate processes

Impersonal

Painful

Vulnerable

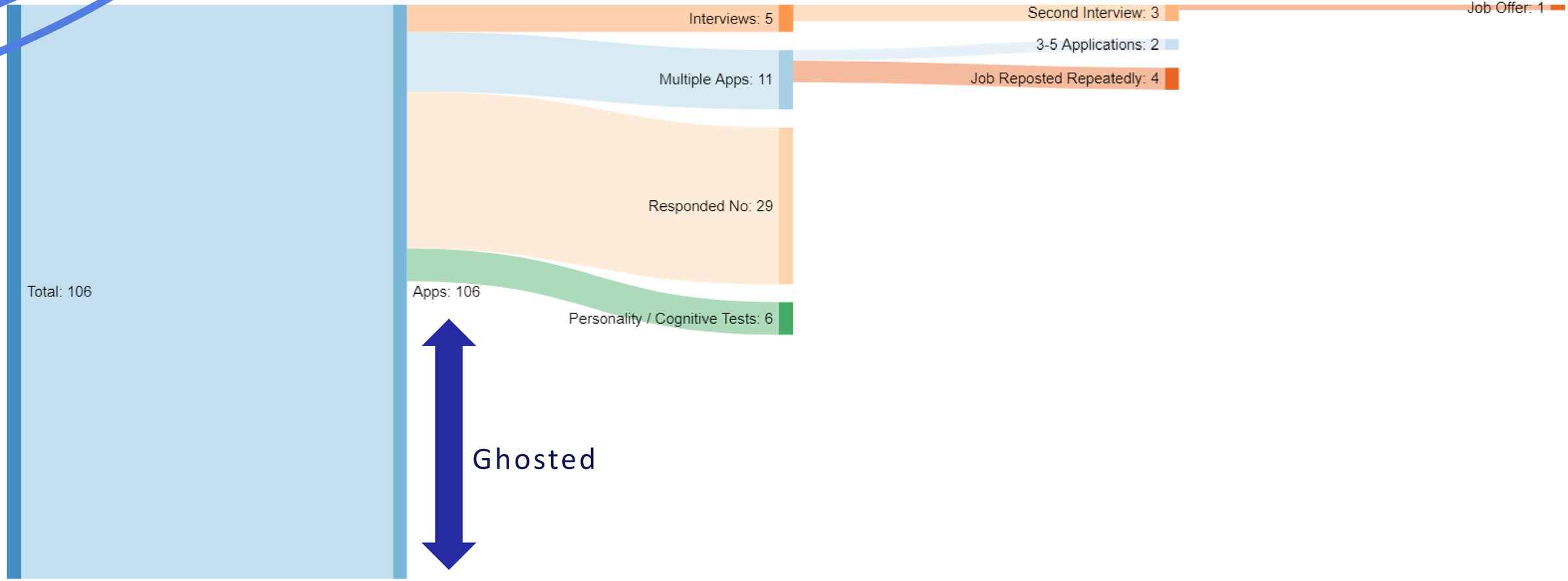
Uncertainty

Identity

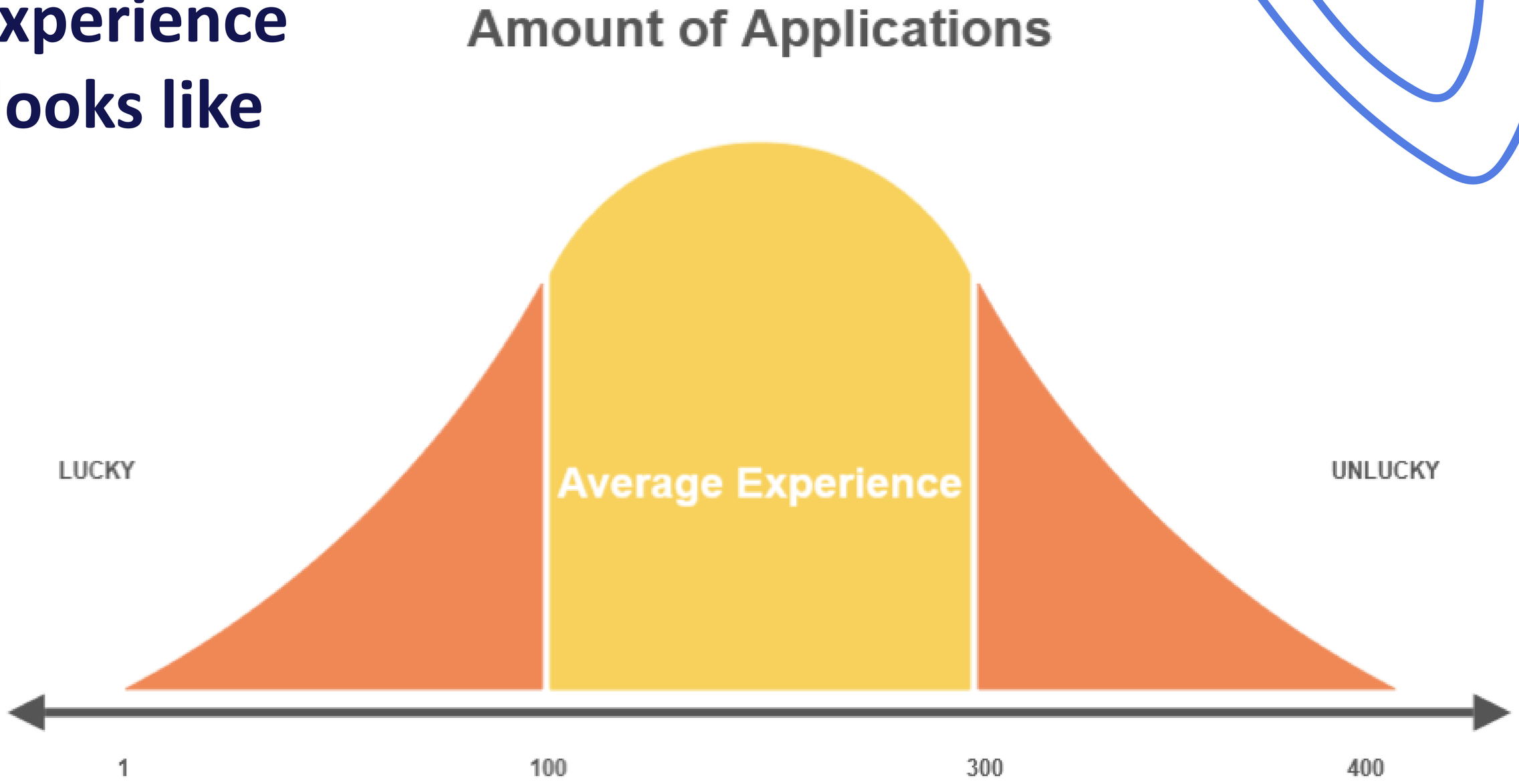
Self Worth

What a easy job hunt look like

Actual Experience



What the full experience looks like



How long? (It is just maths)

		Number of applications needed (Worst Case)	400
		Number of applications per week	7
400	/	7	
		Time to Success in weeks	57.1
		Time to Success in Months	14.3

How long? (It is just maths)

Number of applications needed (Worst Case)			400
Number of applications per week			14
400	/	14	
Time to Success in weeks			28.6
Time to Success in Months			7.14


"A journey of a
thousand miles begins
with a single step.“
~Tao Te Ching

Effort and Time

- Perseverance
- Fierce interest
- Understanding the Game
- NOT giving up

In person / Relocate?

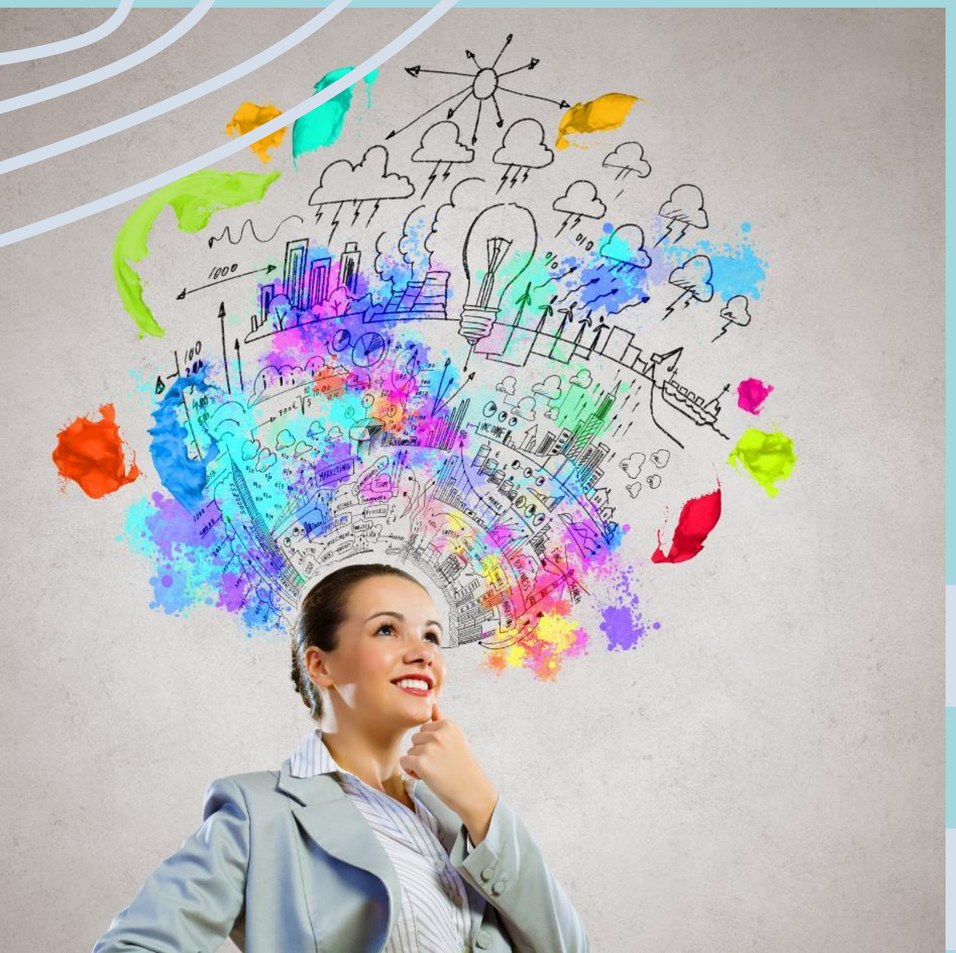
Remote?

Balance in all things

- Emotional Management
- Understanding your feelings
- Strive for calmness
- Understand how feelings come and go
- Observe the emotional storms instead of getting caught up in them.

“A goal without a plan is only a dream.”

- Brian Tracy



Having a Plan

HAVE TARGETS

Identify 1-3 Work Roles

“I don’t care; I’ll take any job just won’t do.”

CONDUCT RESEARCH

Understand clearly what it takes to become attractive for those work roles

PROFESSIONAL ASSOCIATIONS

Identify, select, and join relevant associations

SOCIAL NETWORKING

Build & Nurture LinkedIn

Attend local cybersecurity events and build your social connections

IMPROVE ONESELF

Develop your Skills

Obtain Certifications

Improve your Abilities

HEALTH ENGAGEMENT

Physical Health

Mental Health

Emotional Health

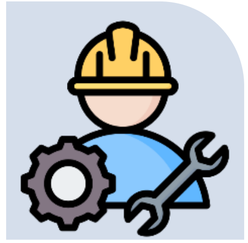
Major Work Roles

ANALYST

Primarily focused on Detection and Response.

ARCHITECT

Designs the overarching security infrastructure and strategy.



ENGINEER

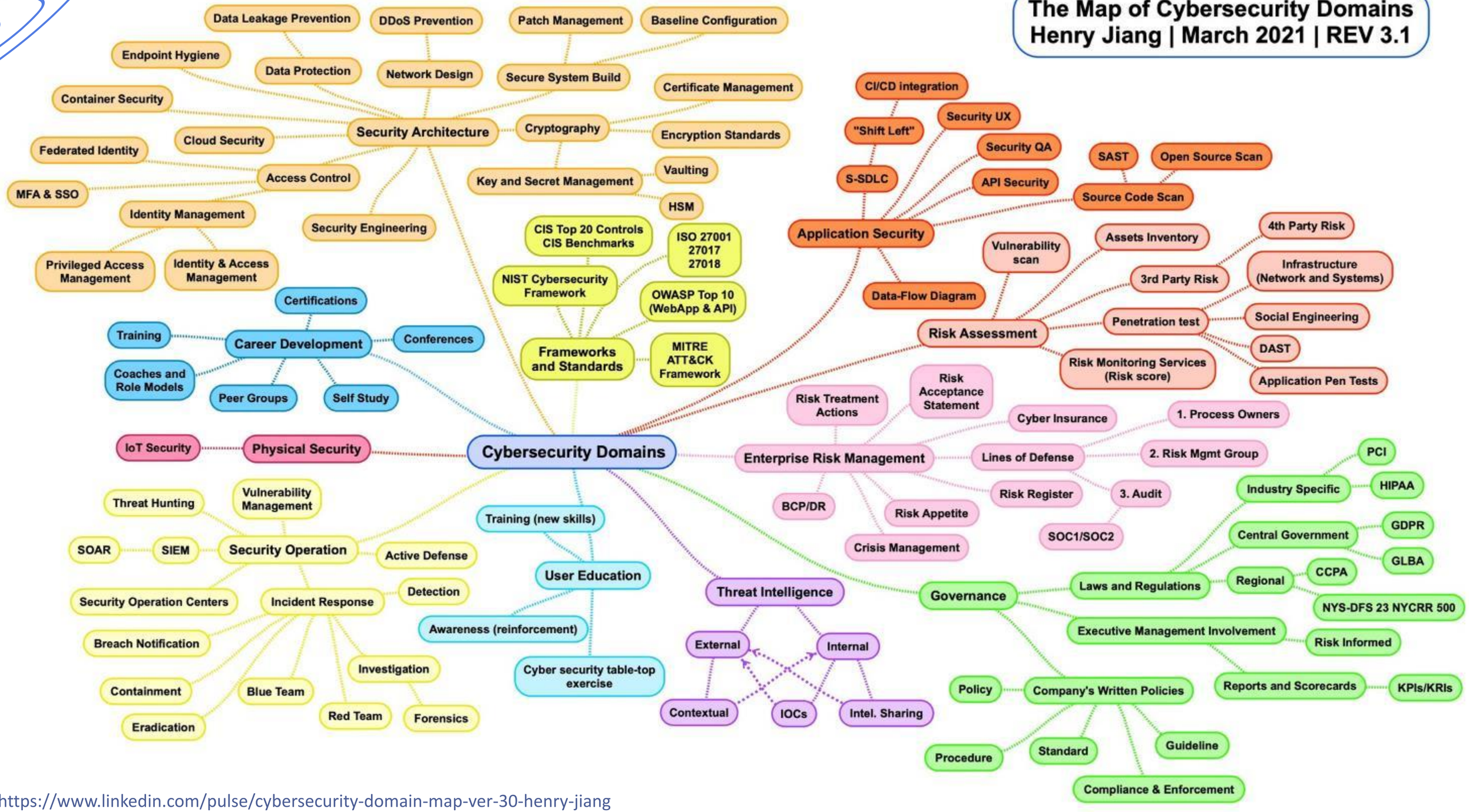
Designs, implements and maintains security solutions.

CONSULTANT

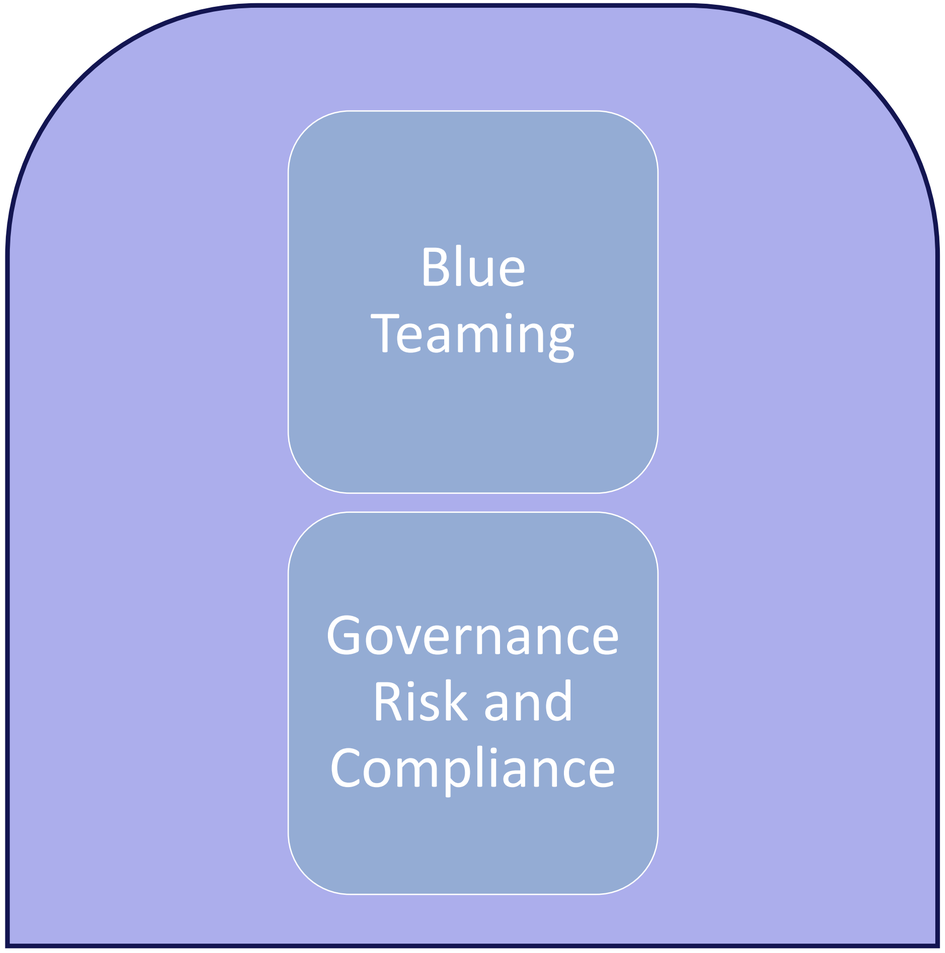
Provides expert guidance and advance on cybersecurity to organizations.

www.flaticon.com/free-icons/business-analyst
https://www.flaticon.com/free-icons/engineer
https://www.flaticon.com/free-icons/architect"
https://www.flaticon.com/free-icons/consulting

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1



https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang



Entry Level Zones

Have to start SOMEWHERE

Most CyberSecurity Roles are not directly accessible from Entry Level.

It is clear what CISOs want

PICK a ROLE

After years of first-person engagement with CISOs and hiring managers across the cybersecurity industry, they don’t want to see your name on every application they get across the company.

PICK A ROLE

Modern Resumes

SKILLS

- Windows Systems
- Python
- Networking
- Linux Systems
- Teamwork
- Project Management
- Budget Planning & Management
- Metrics-Based Operations Management
- Risk Mitigation

INTERESTS

Cybersecurity Operations Management, Leadership, Machine Learning & Automation

Cybersecurity Analyst

Marine Corps Veteran that is passionate about cybersecurity transitioning to a more hands-on technical role.

el
408-
Hi
linke
Ur
a3a6

WORK EXPERIENCE

Technical Recruiter
Palo Alto Networks and Okta
01/2014 - Present
Achievements/Tasks
- 7 years cybersecurity industry experience. Over 20 years professional experience. Additional information available upon request.

EDUCATION

08/2022 - Present

Cybersecurity
Arapahoe Community College
05/2020 - Present *4.0 GPA*

San Jose State University
07/2001 - 12/2003 *3.4 GPA*

CERTIFICATES

CompTIA Security+
COMP0

CompTIA Network+
COMP001

Project Management Professional
PMP Number 13

PROJECTS

Hashcat Rig (04/2022 - 05/2022)
- Converted one of my old Ethereum mining rigs into a Hashcat rig to perform dictionary, brute force, mask, and combinator attacks on password hashes.

OPNSense VMWare Lab (05/2022 - Present)
- Created a VMWare lab for testing OPNSense virtual firewalls.

27@gmail.com
31
linkedin.com
a

SKILLS

- IAM
- Risk Management
- Active Directory
- Audit
- Windows Administration
- Security Administration
- Regulatory Compliance
- Securities Regulation

CERTIFICATES

CompTia Security+
(04/2022 - 04/2025)
Candidate ID#COMPC

FINRA Series 7 (General Securities Representative)
(10/2020 - Present)

NOTABLE PROJECTS

Processing Automation SME
(03/2018 - 04/2019)
- Subject matter expert on automation project for brokerage transactions.
- Provided the documentation matrix to facilitate documentation requirements.
- The insight provided influenced executive management and application developers to update policy and procedures. This increased processing productivity and improved brokerage operations SLA KPI's.

Cybersecurity Professional

An Innovative technical professional with over 10 years in the Brokerage/Financial industry. Seeking to pivot into another role in cybersecurity to support Risk Management.

WORK EXPERIENCE

Information Security Specialist
U.S. Bank
02/2021 - Present
Achievements/Tasks
- Ensure IAM Quality Assurance by confirming access rights and approvals.
- Developed and Maintain procedures for systems access and quality assurance.
- Performed Weekly, Monthly and Quarterly IAM Reviews to ensure Risk Management Policies are followed.
- Assisted with onboarding and decommissioning web based applications.

WIM QA Analyst
Wells Fargo Advisors
04/2019 - 01/2021
Achievements/Tasks
- Daily reviewed brokerage customer complaint program practices and resolutions.
- Followed FINRA Policy and Risk Management practices.
- Ensured complaint resolutions were documented and filed according to FINRA requirements.

Securities Operations Specialist
Wells Fargo Advisors
06/2012 - 04/2019
Achievements/Tasks
- Resolved complex Brokerage account transactions.
- Provided coaching, training and feedback to new and existing staff.
- Acted as Subject Matter Expert for software testing and automation projects.

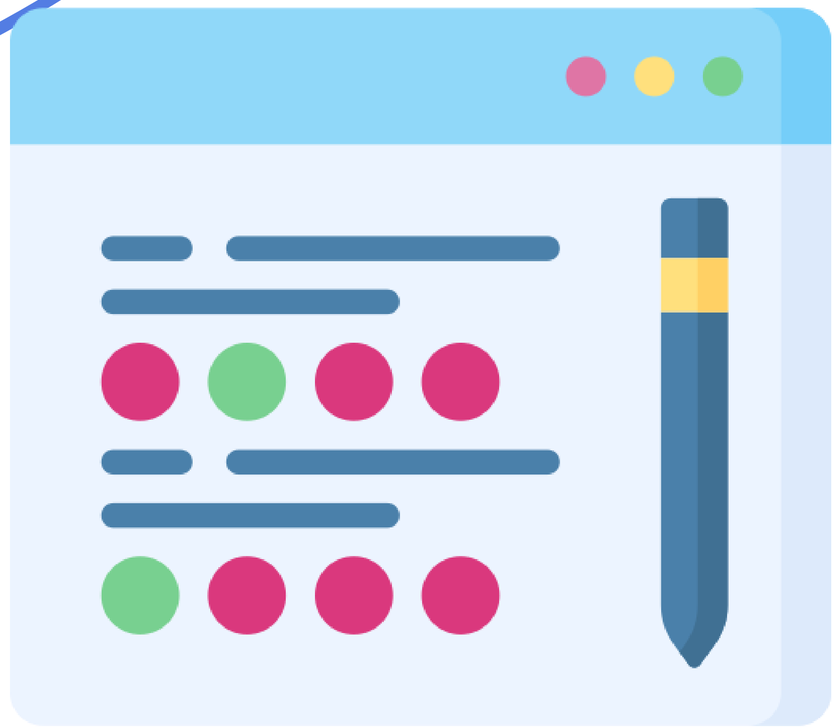
Technical Support Analyst
Connectria Hosting
09/2008 - 05/2012
Achievements/Tasks
- Monitored managed hosting environment in a NOC(Network Operations Center).
- Added and removed users in Active Directory.
- Added and removed firewall rules for customer environments via Cisco ASDM.
- Escalated level 2 and 3 Network and Security Issues to on-call engineers.

EDUCATION

Telecom/Networking Essentials Certificate
Pace University
09/2013 - 09/2014

General Studies
High School
09/2001 - 05/2005

Psycho metrics are so hot right now



PERSONALITY TEST

Employee Personality Profile

The EPP is a personality assessment that measures twelve traits. Scores for each trait are expressed as a percentile ranking, which reflects how a person scored on that trait relative to other test-takers. There are no "high" or "low" scores on the EPP; rather, people with certain traits tend to be a better fit for certain jobs. The EPP contains a series of job families that assess how good a fit a person's personality is for a given position.

Results Summary

No Job Family Selected

Score Details

Achievement	Impulsive	24	Goal-Oriented
Assertiveness	Deferential	72	Forceful, Dominant
Competitiveness	Relaxed	72	Competitive
Conscientiousness	Spontaneous, Laid-Back	44	Dependable, Self-Disciplined
Cooperativeness	Aggressive, Independent	68	Accommodating
Extroversion	Introverted, Low-Key	87	Extroverted, Sociable
Managerial	Follower	81	Leader
Motivation	Mellow	93	Committed, Driven
Openness	Conventional, Traditional	83	Experimental, Creative
Patience	Impatient	75	Patient
Self-Confidence	Timid, Lacks Self-Assurance	81	Self-Confident
Stress Tolerance	Excitable	21	Calm, Even-Tempered

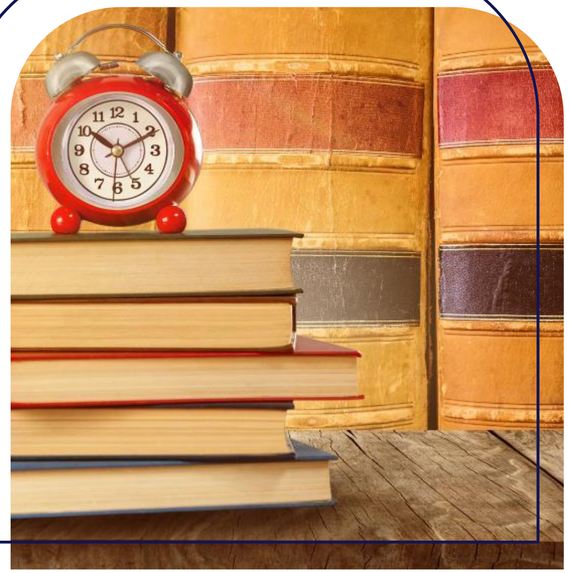
https://www.flaticon.com/free-icons/quiz

Do what you can do

Control what you can
And let go of the rest

While we cannot control the job market, company hiring timelines, or the preferences of recruiters, we can control our preparation, mindset, and approach.

The many paths one can take.



SELF TAUGHT

Skill Development

Flexible

Portfolio Building

Social Networking

Problem Solving

EDUCATION

Academia

Boot Camps

Certifications

Badges

Self-Taught

CERTIFICATIONS

CompTIA Sec+

CompTIA Net+

CompTIA CYSA+

Cloud+ / CCSK

How I’m working to disrupt Education

In development

Building an entire cybersecurity program from zero to HERO coming out in the next year.

Comprehensive Program

- Economically Viable
- Textbooks
- Videos
- Hands on Labs
- Tutoring & Mentorship

Notable Graduate Destinations

BLACK TOWER ACADEMY

Unique and high-quality textbooks

BLACK TOWER ACADEMY

Types of IOCs

IOCs can be categorized into various types, each providing different insights into potential security incidents:

1. **IP Addresses:** Malicious IP addresses associated with known threat actors or compromised systems that are communicating with internal assets.
2. **Domain Names:** Domains known to host malware, phishing sites, or command and control (C2) servers.
3. **URLs:** Specific URLs that may deliver malware or redirect users to malicious sites.
4. **File Hashes:** Unique hashes (e.g., MD5, SHA-1, SHA-256) of known malicious files. Since hashes are unique to specific file contents, they are effective in identifying malware samples.
5. **Email Addresses:** Email addresses used in phishing campaigns or associated with spear-phishing attacks.
6. **Registry Keys:** Specific Windows Registry keys that are often modified or used by malware.
7. **File Paths:** Unusual or suspicious file paths and names where malware is typically located or installed.
8. Malware Artifacts**:** Specific characteristics or behaviors of malware, such as mutex names, command-line arguments, or persistence mechanisms.
9. **Anomalous Network Traffic:** Unusual patterns of network traffic that indicate data exfiltration, lateral movement, or communication with C2 servers.
10. **Anomalous System or User Behavior:** Behavioral anomalies that deviate from normal baseline activity, such as sudden increases in data access or export, unusual login times, or geographic irregularities.

So... It begins...

After achieving an initial breach and securing persistence within a target environment, threat actors typically proceed with scanning, discovery, enumeration, and vulnerability assessment for several strategic reasons. These actions are critical for understanding the environment, identifying valuable assets, and planning subsequent stages of the attack.

Next Steps After Breach

1. **Establish Persistence:** The first goal for many attackers is to ensure they can maintain access to the compromised environment, even if the initial entry point is discovered and closed. This might involve creating backdoor accounts, exploiting vulnerabilities to escalate privileges, or installing malware that automatically reconnects at intervals.
2. **Conduct Reconnaissance:** Once inside, attackers often spend time understanding the environment, identifying valuable assets, data stores, and understanding the network topology. This reconnaissance helps them plan subsequent actions, such as data exfiltration or further compromise.
3. **Expand Access:** With knowledge of the environment, attackers may attempt to move laterally across the network, compromising additional systems to gain access to specific valuable or strategic assets.

Conduct Reconnaissance – Sneaky Style

Mapping the Environment

What is in a packet?

Packets, the fundamental units of data transmission in network communications, are structured into multiple layers, each serving specific purposes in the encapsulation, transmission, and interpretation of data. A packet typically consists of two main parts: the header(s) and the payload. Here's a detailed overview of the data contained in these components:

Headers

Headers precede the payload and contain metadata necessary for routing and managing the data as it moves across networks. Headers are added at each layer of the OSI (Open Systems Interconnection) model or the TCP/IP stack when a data packet is prepared for transmission. The information in headers varies by protocol and layer but generally includes:

- **Source and Destination Addresses**: Identifiers for the sender and receiver of the packet. At the Internet layer (IP), this is the IP address; at the transport layer (TCP/UDP), this includes port numbers.
- **Protocol Type**: Information about the protocol being used (e.g., TCP, UDP, ICMP) that tells the receiving system how to process the packet.
- **Packet Length**: The size of the packet or the payload, which helps in the reassembly of segmented data and ensures integrity.
- **Sequence and Acknowledgment Numbers** (TCP): Used in establishing connections and ensuring the ordered and reliable delivery of packets.
- **Flags** (TCP): Control flags (e.g., SYN, ACK, FIN) indicating the state of a communication or specific requests between sender and receiver.
- **Time-to-Live (TTL)**: A counter that decrements at each hop; when it reaches zero, the packet is discarded, preventing it from looping indefinitely.
- **Checksum**: A form of error checking that allows the receiver to verify that the packet arrived intact.

Payload

The payload is the actual data that the packet is transporting. This can be anything from a segment of a web page, a portion of an email, or data from a file being transferred over the

7. MIMO (Multiple Input, Multiple Output)

MIMO technology uses multiple antennas at both the transmitter and receiver ends to improve communication performance. MIMO technology enables higher data rates, increased capacity, and more reliable transmission, which is essential for wireless communication standards like Wi-Fi and LTE.

8. SDMA (Space Division Multiple Access)

SDMA uses physical separation between users to provide multiple access pathways. In wireless communications, SDMA refers to using directional antennas to spatially separate signals, allowing multiple users to be in the same frequency band simultaneously.

9. TDMA (Time Division Multiple Access)

TDMA divides the channel into several time slots and allocates each user a specific slot during which they can transmit or receive data. This method reduces interference and increases channel capacity.

10. FDM (Frequency Division Multiplexing)

FDM works by dividing the available bandwidth into a series of frequency bands, each used by a different signal. Each channel is separated by a frequency guard band to avoid interference, allowing simultaneous transmission of multiple signals.

11. TDM (Time Division Multiplexing)

TDM assigns different time slots in a set sequence to multiple data streams, allowing several transmissions to share the same transmission medium while using the full channel bandwidth during their allotted time slot.

The Transport Layer plays a pivotal role in determining the quality and reliability of communication between host computers over a network. It acts as a mediator between the network and the application layers, ensuring that application data is sent and received as intended.

TCP / UDP

TCP (Transmission Control Protocol) and **UDP (User Datagram Protocol)** are two key protocols used at Layer 4 (the Transport Layer) of the OSI model. Each serves different needs in data transmission across a network. Here's a detailed comparison:

1. Connection Orientation

- **TCP** is connection-oriented.
  - It establishes a connection between the sender and receiver before data transmission begins. This ensures a reliable path for data exchange.
- **UDP** is connectionless.
  - It sends data without establishing a prior connection, making it faster but less reliable than TCP.

2. Reliability

- **TCP** provides reliable data transfer. It ensures that data packets are delivered in order, without duplicates, and verifies data integrity. If a packet is lost, TCP retransmits it.
- **UDP** does not guarantee reliable delivery. Packets may arrive out of order, be duplicated, or get lost without notice.

Examples of hands-on keyboard labs

Exercise 6

Using `grep` with logical operators

To use `grep` for searching two different patterns (variables) within files, you have a few options, depending on whether you want to find lines that match both patterns (logical AND) or either of the patterns (logical OR).

Logical OR (`pattern1` OR `pattern2`)

If you want to find lines that contain either `pattern1` or `pattern2`, you can use the `-E` option with `grep` and separate the patterns with a pipe `|`

Example:

```
grep -E 'pattern1|pattern2' filename
```

Task 1

Find any logs with User2 AND open file and then redirect it to a file called log1.txt

For example, to search for lines containing either "apple" or "banana" in `file.txt`:

```
grep -E 'apple|banana' file.txt
```

The basic syntax of the `scp` command is:

```
scp [options] [source] [destination]
```

- `[options]`: Optional flags that modify the behavior of the command.
- `[source]`: Specifies the path of the file or directory you want to copy.
- `[destination]`: Specifies the destination path where the file or directory will be copied.

For example, to copy a local file to a remote server, you would use:

```
scp /path/to/local/file username@remote_host:/path/to/destination
```

PROTIP if you don't provide /path/to/destination, so you just end in : it drops it in your home folder.

To copy a file from a remote server to your local machine:

```
scp -r /path/to/local/directory username@remote_host:/path/to/destination
```

The `scp` command prompts for the password if SSH key-based authentication is not set up. Additionally, it supports various options like `-P` for specifying a custom SSH port, `-i` for specifying the identity file, and `-C` for enabling compression during transfer, among others. You can explore more options and details in the `scp` command's manual page by running `man scp` in your terminal.

nmap syntax in this context

<command> <option1> <option2> <argument>

```
nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org
```

You will see a long/large output as it identifies all the vulnerabilities on `scanme.nmap.org`

```
ajay@server1:/usr/share/nmap/scripts/scipag_vulscan$ cd
ajay@server1:~$
ajay@server1:~$
ajay@server1:~$ nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 00:32 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.058s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-5975] The SSH USERAUTH CHANGE REQUEST feature in SSH Tectia Server 6.0.4 through 6.0.20, 6.1.0 through 6.1.1
2, 6.2.0 through 6.2.5, and 6.3.0 through 6.3.2 on UNIX and Linux, when old-style password authentication is enabled, al
lows remote attackers to bypass authentication via a crafted session involving entry of blank passwords, as demonstrated
 by a root login session from a modified OpenSSH client with an added input_userauth_passwd_changereq call in sshconnect
2.c.
| [CVE-2012-5536] A certain Red Hat build of the pam_ssh_agent_auth module on Red Hat Enterprise Linux (RHEL) 6 and Fedo
ra Rawhide calls the glibc error function instead of the error function in the OpenSSH codebase, which allows local user
s to obtain sensitive information from process memory or possibly gain privileges via crafted use of an application that
 relies on this module, as demonstrated by su and sudo.
| [CVE-2010-5107] The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TC
P connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection
-slot exhaustion) by periodically making many new TCP connections.
| [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by ca
```

Task 3

```
echo This is evil naughty naughty malware > malware.txt
```

This redirects the output of the echo to a file. No error or feedback means that it completed successfully.

Validate that it worked by:

```
cat malware.txt
```

The output should be exactly what you put in the echo but it's saved to the file.

Now lets encode the output of the file and then save the encoded output to a different file.

```
cat malware.txt | base64 > notmalwarenoreally.txt
```

The encoded output should be exactly what you put in the echo but it's saved to the file.

Validate that it worked by:

```
cat notmalwarenoreally.txt
```

It should be encoded and NOT human readable.

"If you want something done right, do it yourself"

BLACK TOWER ACADEMY

Connect with me on LinkedIn:

https://www.linkedin.com/in/ajaymenendez/