CWL
CyberWarFare Labs

CWL CERTIFIED CYBER SECURITY ANALYST [C3SA] MODULE - 1

Course Primer :

- ➢ C3SA is a **100%** hands-on course with **exercises** aimed to upskill **beginners** about emerging & job-aligned **cyber security** domains

- ➢ To benefit the maximum from the course, try **hands-on** of each & every exercise & demo present in the modules

- ➢ All the available videos are **ONLY** the **DEMONSTRATION (or instructions)** to keep you align with the self-paced course

Course Primer :

- Keep your virtual environment ready & make sure to always reach out to our technical support at support@cyberwarfare.live

- Candidates are free to follow the sequence, however if you pick up a module, please complete it & then move to the other one

- If the computing resources are not enough, please turn-on only the machines that are required for the exercises.

- Always **TRY** instead of making assumptions in any case. Think, look in the internet & make-up possible use cases, this will expand your visibility about the topic

- We are in **Cyber-Age**, **recon** as much as you can. Collect & Document about any topic that you feel is of your interest

- It is always better to **write down / map** things (**in pointers**) of position in case you get stuck anywhere in any scenario.

- **Take as much time** you require to go through the **curated content** but be **engaged** in the **demos / exercises**. We hope the above **suggestions** will help you in progressing through the course

Course Expectations :

- **CWL** is aimed at spreading cyber security knowledge with best-ever practical learning scenarios for better causes

- We need candidates with developed interest in **Cyber Security** domains & eager to serve & better protect organization assets

- Always eager to **learn / implement** & create productive applications of the information.

COURSE CONTENT

1. Introduction to Cyber Security:

1.1 Why Cyber Security?

1.2 Introduction

1.3 Career Paths (CICE Mapping - 2 PDFs)

1.4 Scope present in Cyber Security

1.5 Cyber Space Nomenclature

1.6 Guidelines and Recommendations for students

1.7 Cyber Security Scope and Engagement (Corporate culture)

COURSE CONTENT

2. Infrastructure Setup

2.1 Installing Virtualization Software

2.2 Network Configuration

2.3 Parrot OS Setup

2.4 Vulnerable environment setup

2.5 Computing resources allocation

COURSE CONTENT

3. Web Application Exploitation

3.1 Web Fundamentals

3.2 Deep dive into Web

3.3 Common mis-configurations

3.4 Hands-on OWASP Top 10 vulnerabilities

3.5 Automation using Tools

3.6 Case Study (Critical Bugs)

3.7 Web Pentesting Methodology

COURSE CONTENT

4. Network Exploitation

4.1 Basics of Network

4.2 Understanding protocols (TCP/UDP)

4.3 Deep dive into Networking

4.4 Mapping Network Architecture

4.5 Attacking Mapped Architecture

4.6 Network Pivoting

4.7 Network Pentesting Methodology

COURSE CONTENT

5. Operating System Exploitation

5.1 Command Line Basics (Windows & Linux)

5.2 Attacking Windows Machines

5.3 Attacking Linux Machines

COURSE CONTENT

6. Cloud Penetration Testing

6.1 Introduction to Cloud Concepts

6.2 Amazon Web Services Cloud

6.3 Google Cloud Platform

6.4 Microsoft Azure

COURSE CONTENT

7. Security Operations

7.1 Basics of Security Operations

7.2 Host based Defence

7.3 Network based Defence

7.4 Threat Intelligence

7.5 Threat Hunting

7.6 Incident Response

CWL
CyberWarFare Labs

Introduction To CyberSecurity

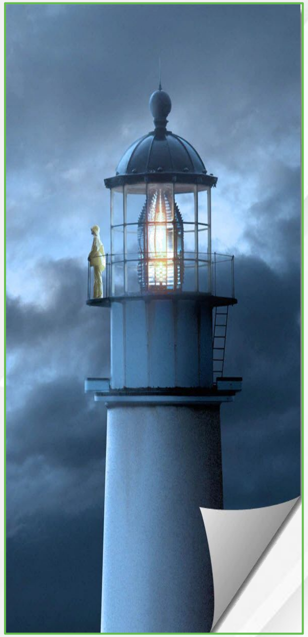
1. Introduction To CyberSecurity

1. **WHO ARE YOU?**

2. **WHAT SHOULD YOU HAVE ACCESS TO?**

1.1 CYBER SECURITY

- Cybersecurity is the action(s) taken to protect sensitive information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Cyber Criminals are actively targeting the following sectors:
  - Healthcare
  - Retailers
  - Nuclear Facility
  - ATM Networks
  - Corporate enterprises
  - Financial firms (banks etc.)



- ➢ With increase in data breaches in **2020-2021**, various sectors are actively looking for security professionals to secure their environment

- ➢ When we call it a data breach / hacking ?
  - ■ Critical information leaked (Personal, financial, personal to company etc)
  - ■ Irregularities in organization functioning
  - ■ Technology information, which includes both classified & unclassified
  - ■ Can be difficult to identify
  - ■ Weak/Default Passwords

- How are organizations breached?
  - Variety of mis-configurations in servers, routers, applications, cloud
  - Insider Threat
  - Unpatched software / applications
  - Outdated operating systems
  - Malicious Thumb drives / hard-disks
  - Phishing

- Who are the real hackers?
  - Insiders
  - Hackers
  - Cyber Criminals
  - Terrorists
  - Organized Criminals
  - Foreign Intelligence Entities
- Organization require support from various intelligence and cyber operators / professionals that can handle cyber threats and attacks.
- Today’s students / graduates are nations assets and organizations will rely on you to be their eyes and ear.

INFO : The Indian Electrical Power Grid is probed 5 million times each day, informing us of targeted cyber attacks.

- Major fields in Cyber Security:
  - Critical Infrastructure Security
    - ATM Networks
    - Power Grids
    - Critical Healthcare Infrastructure
    - Nuclear Facility
    - Large Manufacturing units
    - Oil / Gas factories
    - Financial assets etc
  - Network Security
  - Cloud Security

- Iot Security
- Application Security
- Mobile Security
- Security Operations Centre (SOC)

REMINDER :

YOU ARE THE FIRST **LINE OF DEFENSE** AGAINST THESE TARGETED **CYBER ATTACKS**

Exercise - 1

What would be your response upon receiving the below email?

To: Employees
From: IT Department
Subject: Project strategy placement

Dear employees,

Project strategy requires its data to be stored separately on a secure server. To secure the process, the IT department is adding all users. Please provide your user name and password: **www.strategyalpha@456.com**

1.2 CYBER SECURITY CAREER PATHS

- CyberWarFare Labs course focuses on enhancing skills, knowledge and strategic mindset of individuals to test themselves against practical cyber security workforce
- Our team have compiled a list of **high demand skills/competencies** mapped with various **Cyber Security roles** that are required by employers of global organizations which we call “**CyberWarFare Labs Initiative for Cybersecurity Framework”**

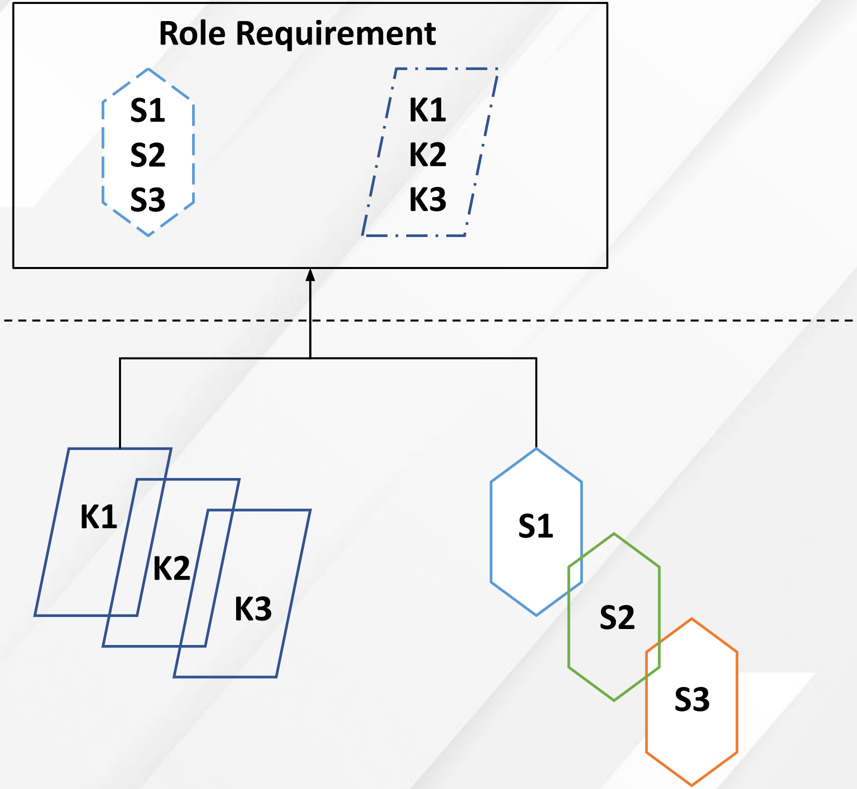
In-demand Industry focused skills

MAPPED WITH

Cyber Security Roles (Global)

INFO : The framework will adapt based on the ever changing Cyber Security ecosystem (agile)

Employer Requirement



Role Requirement

S1
S2
S3

K1
K2
K3

K1
K2
K3

S1
S2
S3

Learner Skillset

S = Skill

K = Knowledge

CWL
CyberWarFare Labs

ADDITIONAL MATERIAL :

Explore PDF mapped with **Cyber Security** job roles & **job description** by reputed companies

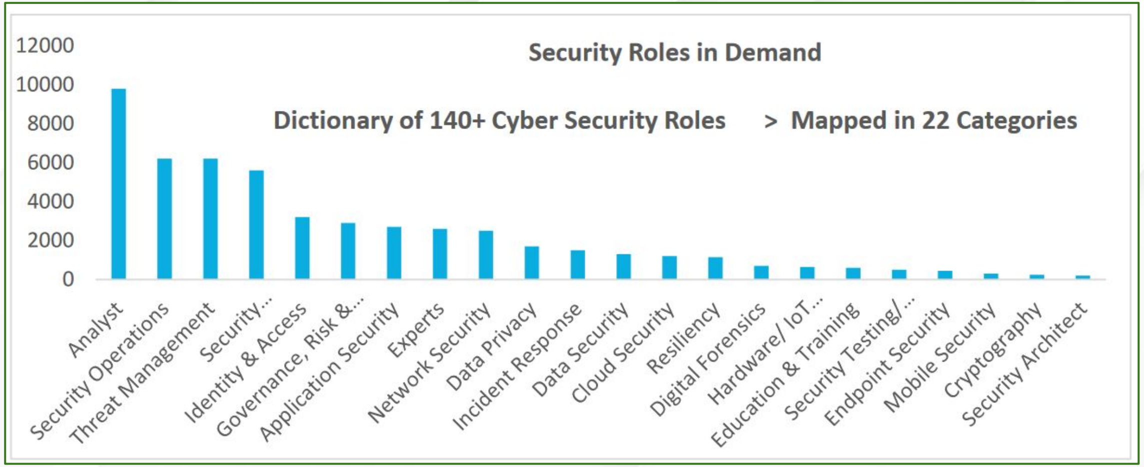
https://cyberwarfare-labs-website.s3.ap-south-1.amazonaws.com/Job_Profile.pdf

INFO : The framework will adapt based on the ever changing Cyber Security ecosystem (agile)

1.3 SCOPE PRESENT IN CYBER SECURITY

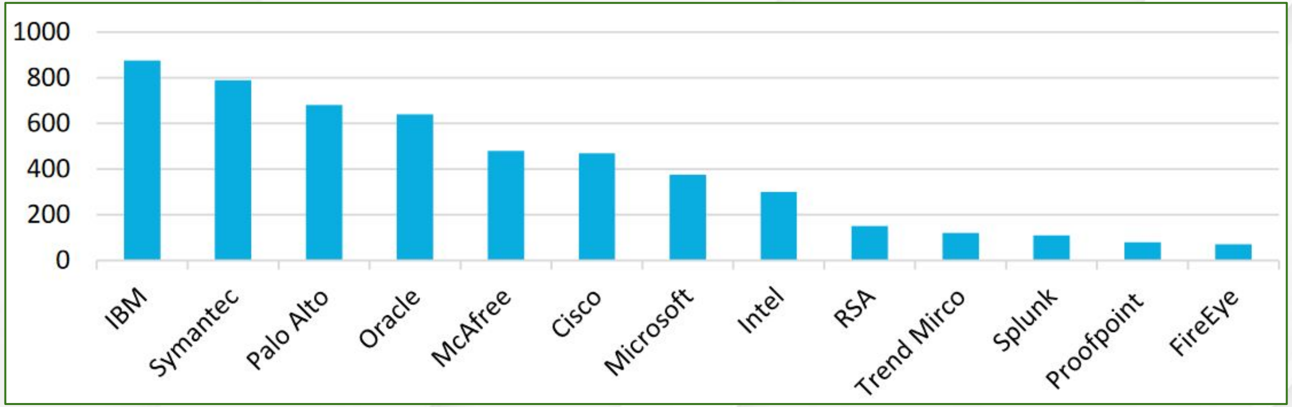
- Cyber Security field possess huge potential in not only the IT fields but with any industry that is using IT facilities including Healthcare, Nuclear, Retailers, financial firms etc.

- The field is very diverse with a potential to cover each & every networking devices present in human race.



In-Demand Cyber Security Roles

Top-Tier MNCs hiring freshers / professionals



1.4 CYBER SECURITY NOMENCLATURE

- **Reconnaissance** : Attackers research and identify valuable information about their target through openly available information
- **Initial Access (intrusion into network)** : Getting initial foothold into the target devices (can be Server, computer, mobile device, cloud platform etc)
- **Backdooring** : Attackers installs malicious software's for future and continued exploitation

- **Elevating privileges** : They escalate to users possessing highest power in the environment so that they can control all the devices.

- **Data Exfiltration** : Attackers collect and gather critical information from the target network

- **Covering Tracks & maintaining persistence**

- **APT :** Also called advanced persistent threats or threat groups are sponsored (financially & intuitively) by nation state governments, powerful agencies etc.

- **Vulnerability** : Mis-configuration or outdated versions in any software, application (web or mobile), Operating System, hardware etc.
- **Payload :** Generally controls the resource as crafted by attacker
- **Exploit**: Attackers leverages (abuse) such vulnerabilities to get control of the resource
- **Cyber Warfare :** Attacking a nation, causing comparable harm to actual warfare for strategic or military purposes
- **Fileless Attacks :** Attacks that do not involve files and is often stealth comparatively

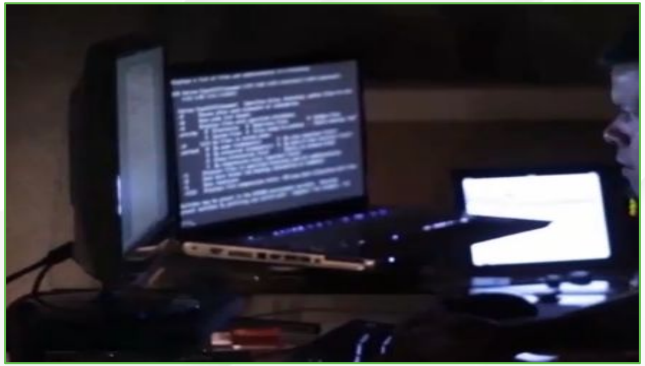
- **Social Engineering** : Manipulating a person which results in performing actions or divulging confidential information

- **Cyber Kill Chain :** Kill chain depicts the full-fledge compromise cycle used by the threat groups (i.e reconnaissance to data exfiltration).

- **Unauthorized access** : Any access that violates the stated security policy.

- **Espionage** : The act of obtaining, delivering, transmitting, communicating or receiving TOP SECRET information with an intent to the advantage of any foreign nation.

Exercise - 1



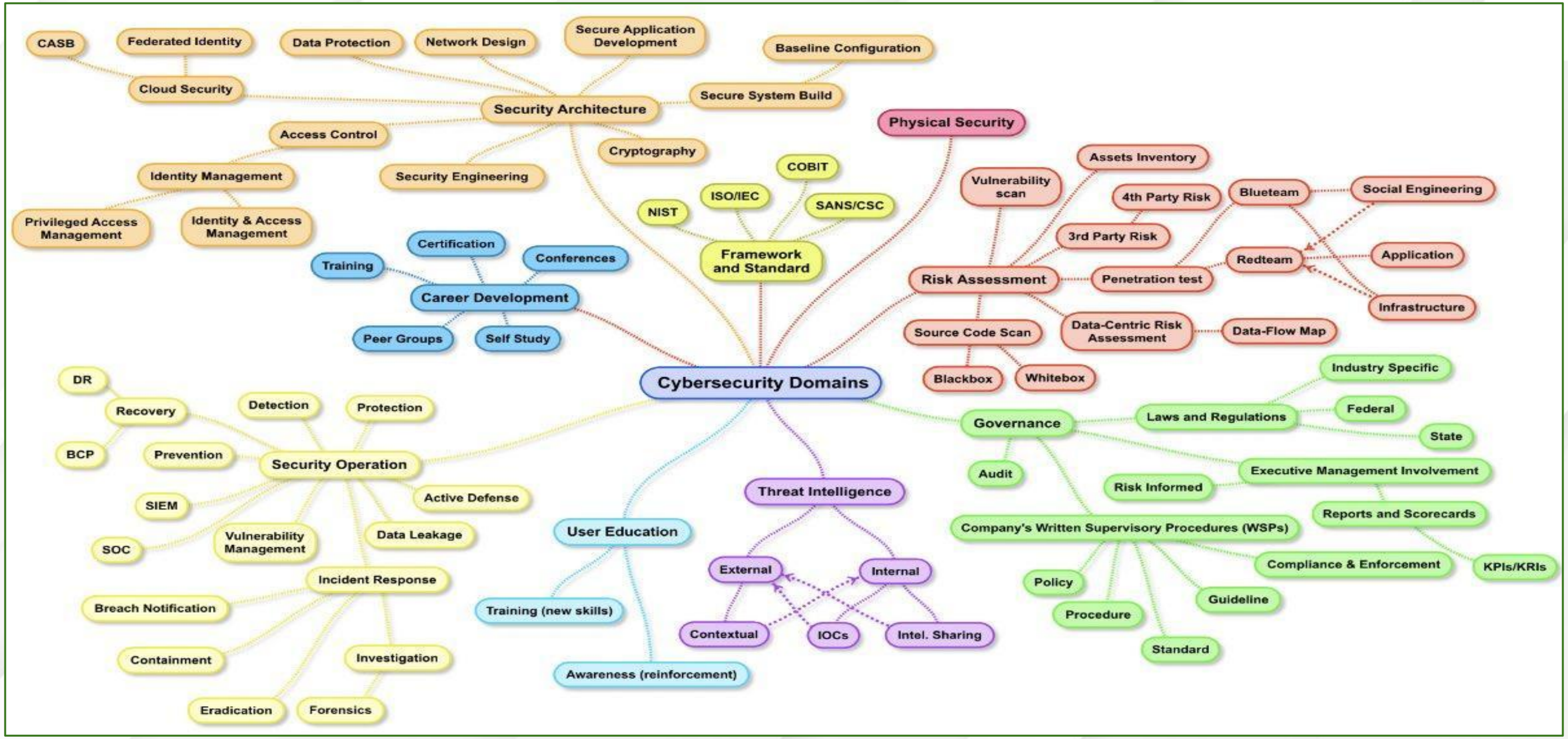
Based on your past events what do you recall when creating passwords?

a. I use the same, very secure password for everything. It’s 8 characters and includes lower and upper case letters, numbers, and special characters. There’s no way a password cracker is getting my information.

b. I change passwords frequently and always use a combination of numbers, letters, and special characters. I’m fairly confident my passwords are secure.

c. I don’t worry about my password; my organization’s security is strong enough to defeat a hacker. I make sure to use something I can remember like a significant date or name.

1.5 GUIDELINES & RECOMMENDATIONS



Credits : @AlyssaM_InfoSec

1.6 CYBERSECURITY CORPORATE CULTURE

- Cyber Security domains are ever-evolving with latest research from individuals, groups etc.

- Student willing to make career, have to be updated about the recent on-going in the cyber space whether it is related to a crime, a new technique or anything etc.

- ➢ Most of the renowned researchers are generally active on social media platforms like : LinkedIn, Twitter, mastodon and publish their research in form of posts

- ➢ Attending Talks / workshops / trainings in conferences is a very good way to increase the knowledge as well as connectivity with the like-minded peoples

- ➢ Coping up with the recent happenings in industry with good soft skills is one of the factor to really excel and be unique among others.

INFO : Following renowned researchers have a benefit. They regularly posts various good opportunities / links for students

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live