

**SIX WEEKS SUMMER TRAINING REPORT**

**on**

CompTIA Security+ SY0-601 (Learn+Lab)

Submitted by

**Aditya Raj**

**Registration No : 11905310**

**Programme Name : Btech. CSE**

**School of Computer Science & Engineering**

**Lovely Professional University, Phagwara**

(June-July,2021)

**DECLARATION**

I hereby declare that I have completed my six weeks summer training at Comptia platform from April 30,2021 to June 25,2021 . I have declare that I have worked full dedication during there 8 weeks of training and my learning outcomes fulfill the requirements of training for the award of degree of B.tech. CSE , Lovely Proffesional University, Phagwara.

Date – 29 Sept. 2021 Name Of Student Aditya Raj

Registration no: 11905310

**ACKNOWLEDGEMENT**

I would like to express my gratitude towards my University as well as Comptia for providing me the golden opportunity to do this wonderful summer training regarding Cyber Security, which also helped me in doing a lot of homework and learning. As a result, I came to know about so many new things. So, I am really thank full to them.

Moreover I would like to thank my friends who helped me a lot whenever I got stuck in some problem related to my course. I am really thankfull to have such a good support of them as they always have my back whenever I need.

Also,I would like to mention the support system and consideration of my parents who have always been there in my life to make me choose right thing and oppose the wrong. Without them I could never had learned and became a person who I am now.

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

**Summer Training Certificate By Comptia**



|  |  |  |
| --- | --- | --- |
| **S. No.** | **Title** | **Page No.** |
| 1 | Ìntroduction | 06 |
| 2 | Overview Of Security | 07 - 20 |
| 3 | Reason for choosing Comptia Security + | 21 |
| 4 | Project Work | 22 |
| 5 | Bibliography | 23 |

**INTRODUCTION**

Comptia Security+ course is a complete package that helped me to learn Security measures and Pentesting from Basic to an Intermidiate level. The course curriculm has been divided into 10 weeks, where I practiced questions and I have attempted the assesment tests accordingly. The course offers a wealth of Practical Lab challenges that helped me to learn all about CYber Security .

The course was well Structured and I could join the course anytime and all the content will be avilable to me once I get enrolled. There was video lectures to learn form and multiple choice questions , Practical labs to practice.

I learned lot of security measures to be taken in any organization for their security .This course does not require any prior knowledge of Ethical Hacking but a basic knowledge of Cyber Security will be good.

**Overview Of Security**

**It had 21 units which was further divided into chapters and then topics so during my whole 8 week course I learned the following :**

o Information Security

▪ Act of protecting data and information from unauthorized access,

unlawful modification and disruption, disclosure, corruption, and

destruction

o Information Systems Security

▪ Act of protecting the systems that hold and process our critical data

o Basics and Fundamentals

● CIA Triad

o Confidentiality

▪ Information has not been disclosed to unauthorized people

o Integrity

▪ Information has not been modified or altered without proper

authorization

o Availability

▪ Information is able to be stored, accessed, or protected at all times



● AAA of Security



o Authentication

▪ When a person’s identity is established with proof and confirmed by a

system

● Something you know

● Something you are

● Something you have

● Something you do

● Somewhere you are

o Authorization

▪ Occurs when a user is given access to a certain piece of data or certain

areas of a building

o Accounting

▪ Tracking of data, computer usage, and network resources

▪ Non-repudiation occurs when you have proof that someone has taken an

Action

● Security Threats

o Malware

▪ Short-hand term for malicious software

o Unauthorized Access

▪ Occurs when access to computer resources and data occurs without the

consent of the owner

o System Failure

▪ Occurs when a computer crashes or an individual application fails

o Social Engineering

▪ Act of manipulating users into revealing confidential information or

performing other detrimental actions

● Mitigating Threats

o Physical Controls

▪ Alarm systems, locks, surveillance cameras, identification cards, and

security guards

o Technical Controls

▪ Smart cards, encryption, access control lists (ACLs), intrusion detection

systems, and network authentication

o Administrative Controls

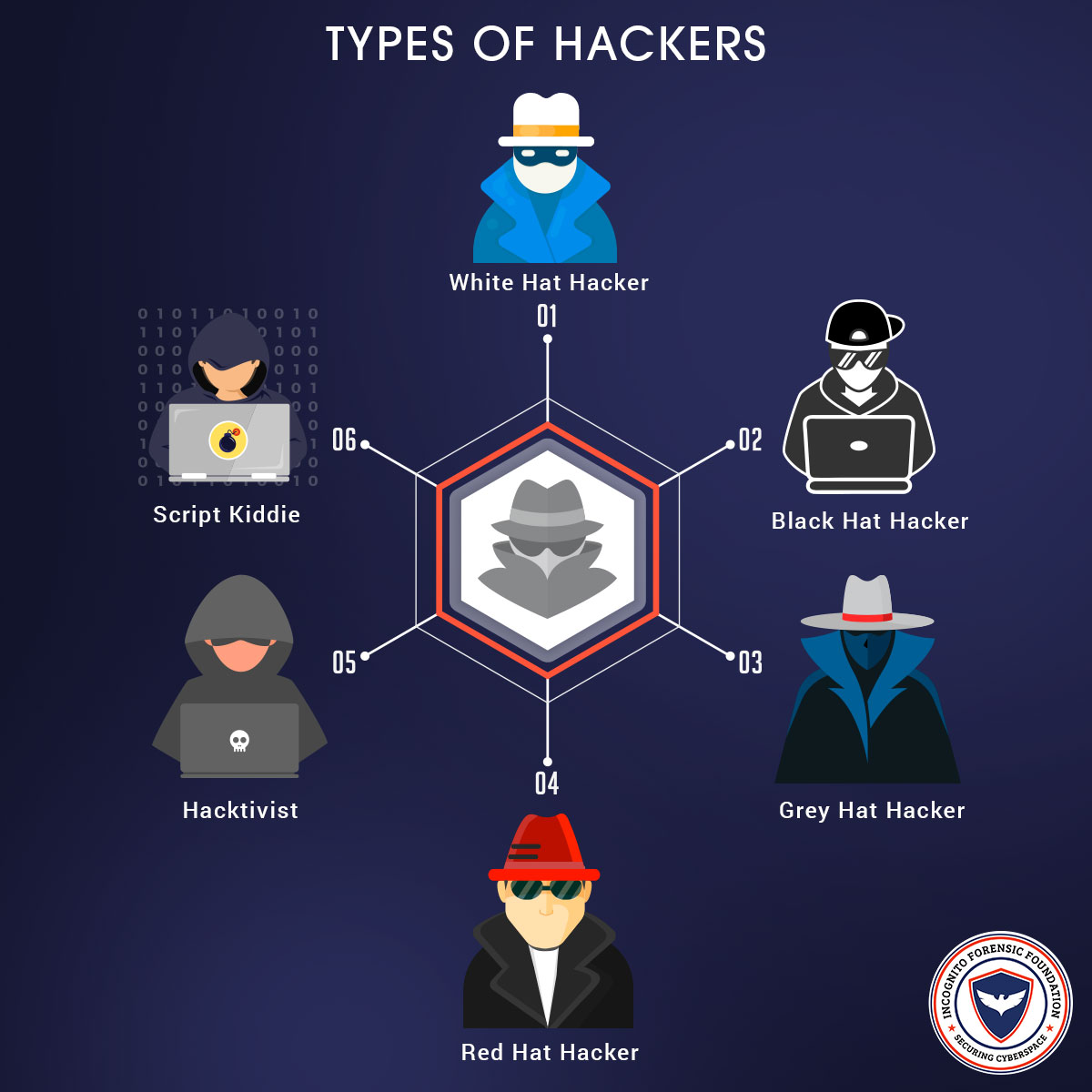
▪ Policies, procedures, security awareness training, contingency planning,

and disaster recovery plans

▪ User training is the most cost-effective security control to use

● Hackers

o Five Types of Hackers



▪ White Hats

● Non-malicious hackers who attempt to break into a company’s

systems at their request

▪ Black Hats

● Malicious hackers who break into computer systems and

networks without authorization or permission

▪ Gray Hats

● Hackers without any affiliation to a company who attempt to

break into a company’s network but risk the law by doing so

▪ Blue Hats

● Hackers who attempt to hack into a network with permission of

the company but are not employed by the company

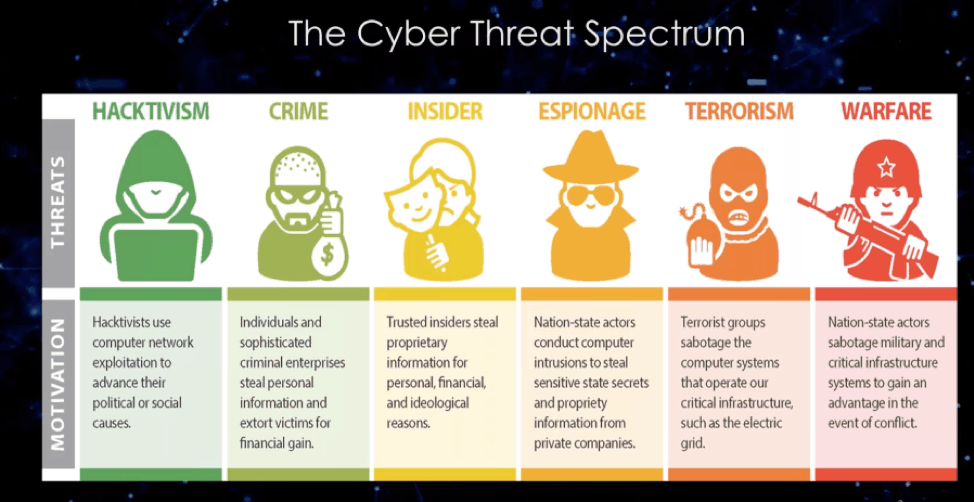
▪ Elite

● Hackers who find and exploit vulnerabilities before anyone else

Does

● 1 in 10,000 are elite

● Threat Actors



o Script Kiddies

▪ Hackers with little to no skill who only use the tools and exploits written

by others

o Hacktivists

▪ Hackers who are driven by a cause like social change, political agendas, or

terrorism

o Organized Crime

▪ Hackers who are part of a crime group that is well-funded and highly

sophisticated

o Advanced Persistent Threats

▪ Highly trained and funded groups of hackers (often by nation states) with

covert and open-source intelligence at their disposal

**Malware**

o Virus

▪ Code that infects a computer when a file is opened or executed

o Worm

▪ Acts like a virus but can self-replicate

o Trojan

▪ Appears to do a desired function but also does something malicious

o Ransomware

▪ Takes control of your computer or data unless you pay

o Spyware

▪ Software that collects your information without your consent

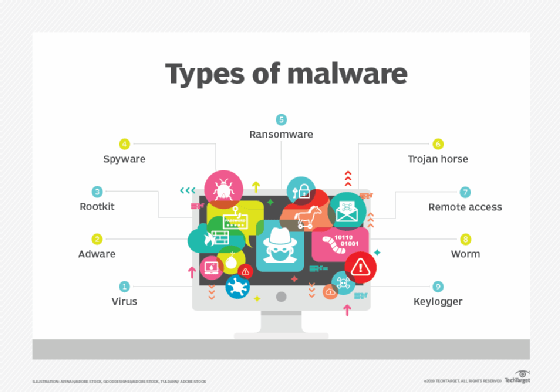
o Rootkit

▪ Gains administrative control of your system by targeting boot loader or

kernel

o Spam

▪ Abuse of electronic messaging systems



• Disk Encryption

o Encryption scrambles data into unreadable information

o Self-Encrypting Drive (SED)

▪ Storage device that performs whole disk encryption by using embedded

hardware

o Encryption software is most commonly used

▪ FileVault

▪ BitLocker

o Trusted Platform Module (TPM)

▪ Chip residing on the motherboard that contains an encryption key

▪ If your motherboard doesn’t have TPM, you can use an external

USB drive as a key

o Advanced Encryption Standard

▪ Symmetric key encryption that supports 128-bit and 256-bit keys

o Encryption adds security but has lower performance

o Hardware Security Module (HSM)

▪ Physical devices that act as a secure cryptoprocessor during the

encryption process

**Mobile Device Security**



• Securing Wireless Devices

o WiFi Protected Access 2 (WPA2) is the highest level of wireless security

o AES

▪ Advanced Encryption Standard

o Bluetooth pairing creates a shared link key to encrypt the connection

o Wired devices are almost always more secure than wireless ones

• Mobile Malware

o Ensure your mobile device is patched and updated

o Only install apps from the official App Store or Play Store

o Do not jailbreak/root device

o Don’t use custom firmware or a custom ROM

o Only load official store apps

o Always update your phone’s operating system

• SIM Cloning & ID Theft

o Subscriber Identity Module (SIM)

▪ Integrated circuit that securely stores the international mobile subscriber

identity (IMSI) number and its related key

o SIM Cloning

▪ Allows two phones to utilize the same service and allows an attacker to

gain access to the phone’s data

▪ SIM v1 cards were easy to clone but newer SIM v2 cards are much harder

▪ Be careful with where you post phone numbers

• Bluetooth Attacks

o Bluejacking

▪ Sending of unsolicited messages to Bluetooth-enabled devices

o Bluesnarfing

▪ Unauthorized access of information from a wireless device over a

Bluetooth connection

o Bluejacking sends information to a device

o Bluesnarfing takes information from a device

• Mobile Device Theft

o Always ensure your device is backed up

o Don’t try to recover your device alone if it is stolen

o Remote Lock

▪ Requires a PIN or password before someone can use the device

o Remote Wipe

▪ Remotely erases the contents of the device to ensure the information is

not recovered by the thief

• Security of Apps

o Only install apps from the official mobile stores

o TLS

▪ Transport Layer Security

o Mobile Device Management

▪ Centralized software solution that allows system administrators to create

and enforce policies across its mobile devices

o Turn location services off to ensure privacy

o Geotagging

▪ Embedding of the geolocation coordinates into a piece of data (i.e., a

photo)

o Geotagging should be considered when developing your organization’s

security policies

• Bring Your Own Device

o BYOD introduces a lot of security issues to consider

o Storage Segmentation

▪ Creating a clear separation between personal and company data on a

single device

o Mobile Device Management

▪ Centralized software solution for remote administration and

configuration of mobile devices

o CYOD

▪ Choose Your Own Device

o MDM can prevent certain applications from being installed on the device

o Ensure your organization has a good security policy for mobile devices

• Hardening Mobile Devices

1. Update your device to the latest version of the software

2. Install AntiVirus

3. Train users on proper security and use of the device

4. Only install apps from the official mobile stores

5. Do not root or jailbreak your devices

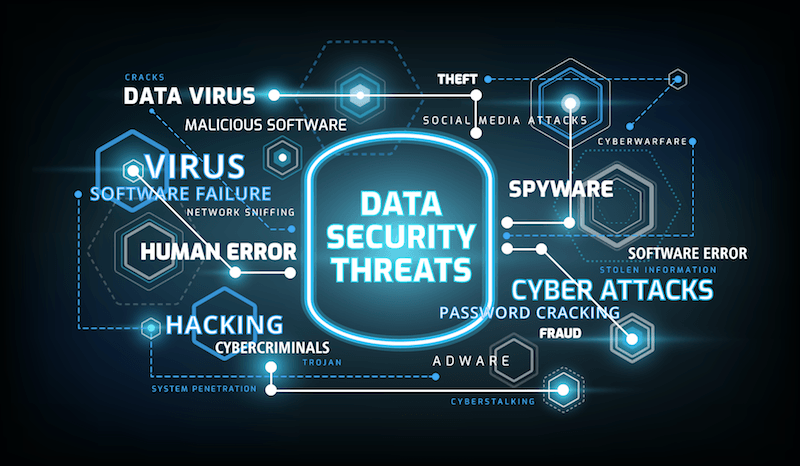
6. Only use v2 SIM cards with your devices

7. Turn off all unnecessary features

8. Turn on encryption for voice and data

9. Use strong passwords or biometrics

10. Don’t allow BYOD



• Application Security

• Web Browser Security

o Ensure your web browser is up-to-date with patches…

▪ …but don’t adopt the newest browser immediately

o Which web browser should I use?

o General Security for Web Browsers

▪ 1. Implement Policies

• Create and implement web browsing policies as an administrative

control or technical control

▪ 2. Train Your Users

• User training will prevent many issues inside your organization

▪ 3. Use Proxy & Content Filter

• Proxies cache the website to reduce requests and bandwidth

usage

• Content filters can be used to blacklist specific websites or entire

categories of sites

▪ 4. Prevent Malicious Code

• Configure your browsers to prevent ActiveX controls, Java applets,

JavaScript, Flash, and other active content

• Web Browser Concern

o Cookies

▪ Text files placed on a client’s computer to store information about the

user’s browsing habits, credentials, and

Other dataZ

o Locally Shared Object (LSO)

▪ Also known as Flash cookies, they are stored in your Windows user

profile under the Flash folder inside of your AppData folder

o Add-on

▪ Smaller browser extensions and plugins that provide additional

functionality to the browser

o Advanced Security Options

▪ Browser configuration and settings for numerous options such as SSL/TLS

settings, local storage/cache size, browsing history, and much more

• Securing Applications

o Use passwords to protect the contents of your documents



**• Perimeter Security**

o Perimeter Security

▪ Security devices focused on the boundary between the LAN and the WAN

in your organization’s network

▪ Perimeter security relies on several different devices

**• Firewalls**

o Firewalls screen traffic between two portions of a network

▪ Software

▪ Hardware

▪ Embedded

o Packet Filtering

▪ Inspects each packet passing through the firewall and accepts or rejects it

based on the rules

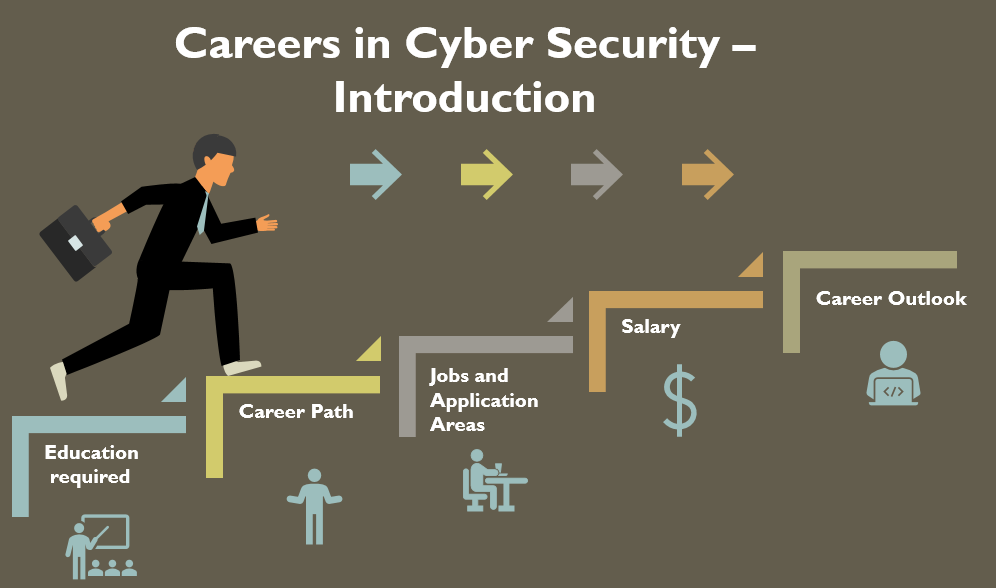
▪ Stateless Packet Filtering

▪ Stateful packet filtering tracks the requests leaving the network

o NAT Filtering

▪ Filters traffic based upon the ports being utilized and type of connection

(TCP or UDP)



o Application-layer gateway conducts an in-depth inspection based upon the

application being used

o Circuit-Level gateway

▪ Operates at the session layer and only inspects the traffic during the

establishment of the initial session over TCP or UDP

o MAC Filtering

o Explicit Allow

▪ Traffic is allowed to enter or leave the network because there is an ACL

rule that specifically allows it

▪ Example: allow TCP 10.0.0.2 any port 80

o Explicit Deny

▪ Traffic is denied the ability to enter or leave the network because there is

an ACL rule that specifically denies it

▪ Example: deny TCP any any port 23

o Implicit Deny

▪ Traffic is denied the ability to enter or leave the network because there is

no specific rule that allows it

▪ Example: deny TCP any any port any

o Most operate at Layer 3 (blocking IP addresses) and Layer 4 (blocking ports)

o Web Application Firewall

▪ Firewall installed to protect your server by inspecting traffic being sent to

a web application

▪ A WAF can prevent a XSS or SQL injection

• Proxy Server

o Proxy Server

▪ A device that acts as a middle man between a device and a remote server

▪ IP Proxy

• IP Proxy is used to secure a network by keeping its machines

anonymous during web browsing

▪ Caching Proxy

• Attempts to serve client requests by delivering content from itself

without actually contacting the remote server

• Disable Proxy Auto-Configuration (PAC) files for security

▪ Internet Content Filter

• Used in organizations to prevent users from accessing prohibited

websites and other content

▪ Web Security Gateway

• A go-between device that scans for viruses, filters unwanted

content, and performs data loss prevention functions

• Honeypots and Honeynets

o Honeypots and honeynets are used to attract and trap potential attackers

o Honeypot

▪ A single computer (or file, group of files, or IP range) that might be

attractive to an attacker

o Honeynet

▪ A group of computers, servers, or networks used to attract an attacker

o Honeypots are normally used in security research

• Data Loss Prevention

o Data Loss Prevention

▪ Systems designed to protect data by conducting content inspection of

data being sent out of the network

▪ Also called Information Leak Protection (ILP) or Extrusion Prevention

Systems (EPS)

▪ DLP is used to ensure your private data remains secure



**REASON FOR CHOOSING COMPTIA Security+**

**All of the above was part of my training during my summer break I specially choose the Security+ by Comptia for reasons stated below :**

* **I was interested in cyber security since my first semester.**
* **Security a thing you need to know no matter in which device you use.**
* **One need to learn how to keep themselves safe over internet.**
* **It had video lectures of all the topics from which one can easily learn. I prefer learning from video rather than books and notes. I know books and notes and thesis have their own significance but still video lecture or face to face lectures make it easy to understand faster as we are involved Practically.**
* **It had 200+ MCQs problems with video explaind solutions.**
* **It had track based learning and weekly assesment to test my skills.**
* **It was a great opportunity for me to invest my time in learning instead of wasting it here and there during my summer break in this Covid-19 panademic.**
* **It contained a lot of knowledge for such a resonable price.**
* **This was for 1 year which I can use to learn even after my training whenever I want to revise.**
* **Along with all these reasons one of the reason was the Comptia platform which is offering the course because Comptia is one of the best platform for Computer Science Students.**

**PROJECTS**

* **Port Scanner**
* **Random Password Generator**
* **Script To Decode Base64 incoded Text**

1. Port Scanner is a tool written in python programming language which takes ip address as an input and scans for its open ports.
2. Random password generator is also coded in python Programming language which generates passwords randomly as per user needs, a combination of numbers, letters, and special characters
3. A script that has been written in bash in unix to decode base64 incoded texts.

**BIBLIOGRAPHY**

* Comptia Security+ notes
* Comptia security + website
* Comptia security + Course