Ethical Hacking and Cyber Security

TechHacker Online Course

Ansh Bhawnani

Module 1
Introduction

Ansh Bhawnani

Introduction to Ethical Hacking

1. Information Security

What is Information?

- Meaningful form of data

- Can be called as processed data

- Data has no context, info does

- **Computer** is data

- **This is my computer** is information

What is Information?

DATA   INFORMATION

What is Information Security?

- What will I do with your birthday?
- I can definitely do with your phone number

- Protecting information from unauthorized access
- Employing tools and policies
- IT IS THE BASIC NEED OF EVERYONE

What is Information Security?

- Wonder how people have realized the sensitivity of information!
- *Enigma Machine* which was used by Germans to encrypt warfare data.
- What if someone is constantly watching you??

- Security is the quality of information
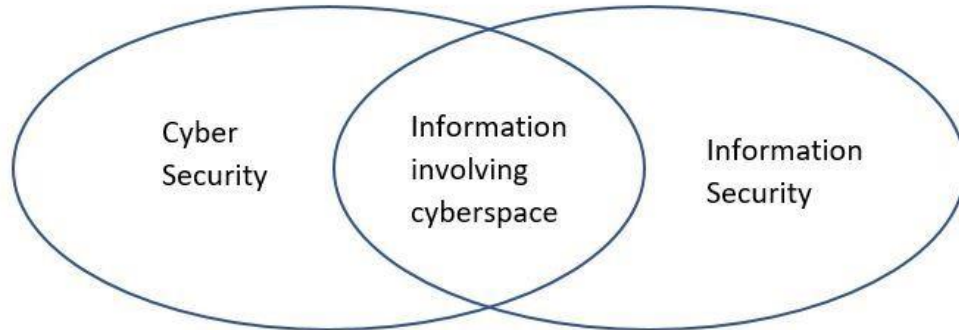- Security is freedom
- Security is an asset

- Information is everywhere
- This is the information age
- Information in digital systems makes *cyber security*

What is Information Security Threats?

- Threat is a constant danger to an asset
- It can be a person, object or an event

- Threats can be categorized and ranked

Types of Threats

- *Inadvertent threats* (human failure)

- *Physical disasters* (natural disasters)

- *Technical failures* (hardware or software)

- *Deliberate acts* (hacking, espionage)

Information Security does not deal with?

- Cyber warfare
- Information warfare
- Negative impacts of people on Internet (sexual abuse, cyber stalking, etc.)
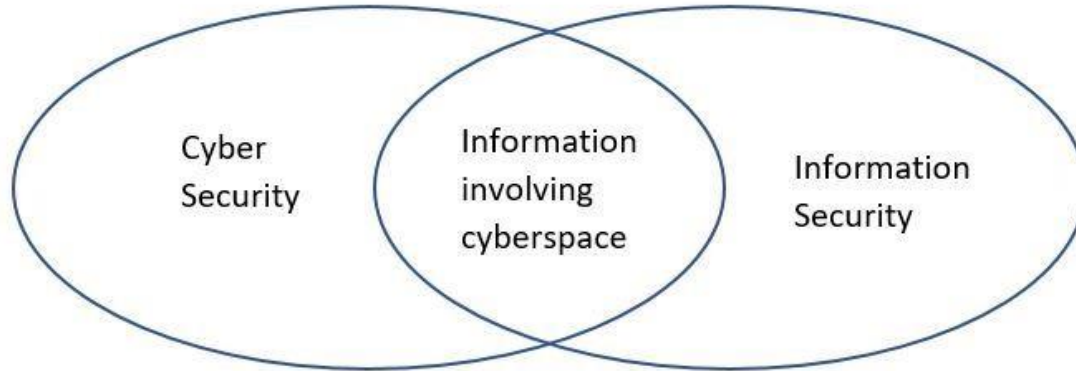- IoT security

Then who deals with them?

2. Cyber Security

What is Cyber Security?

- Protection of cyber space against cyber threats and cyberspace vulnerabilities
- Any threats to information via the cyber space

- Deals with deliberate acts
- Doesn't deal with physical and personal security
- Threats via cyberspace, not threats for Cyberspace

What is Cyber Security?

Cyber Security · Information involving cyberspace · Information Security

3. Objectives of Cyber Security

Objectives of Cyber Security

- **Confidentiality**: No telling to unauthorized parties

- **Integrity:** Completeness and accuracy of data

- **Availability:** When needed, data is available

Objectives of Cyber Security

■ **Non-repudiation**: I should accept I sent you the message and you should accept you received it

■ **Authenticity:** You should actually be who you tell you are

3. The CIA Triad

Confidentiality

- Roughly but wider than privacy
- Sensitive data should not reach wrong people
- Sensitive data should reach right people

Measures:
- Data encryption
- Authentication (maybe multi-factor)
- More sensitive, more physical

Integrity

- Data should be consistent, trustworthy and accurate
- Data must not change in transit
- Most complex to implement

Measures:
- Backups
- Cryptographic measures (checksums)
- Access control

Availability

- Data should be available as and when needed
- Updated software and hardware
- Adequate system capacity and bandwidth

Measures:
- Firewalls rules
- Patch management and disaster recovery
- Load balancers

4. What is Hacking?

What is Hacking?

- Hacking is a very wide term

- Introduced in the 1960s, the term "Hacker", at MIT

- That time was of more hardcore programming

- Those were the most intelligent and advanced hackers

- All started by the end of 1960s, when *ARPANET* was founded by the US military.

What is Hacking?

- There is no standard definition of hacking

- Media continues to add false information about hacking

- There are good hackers, and there are bad

- Bad ones need to be discussed, but not learnt
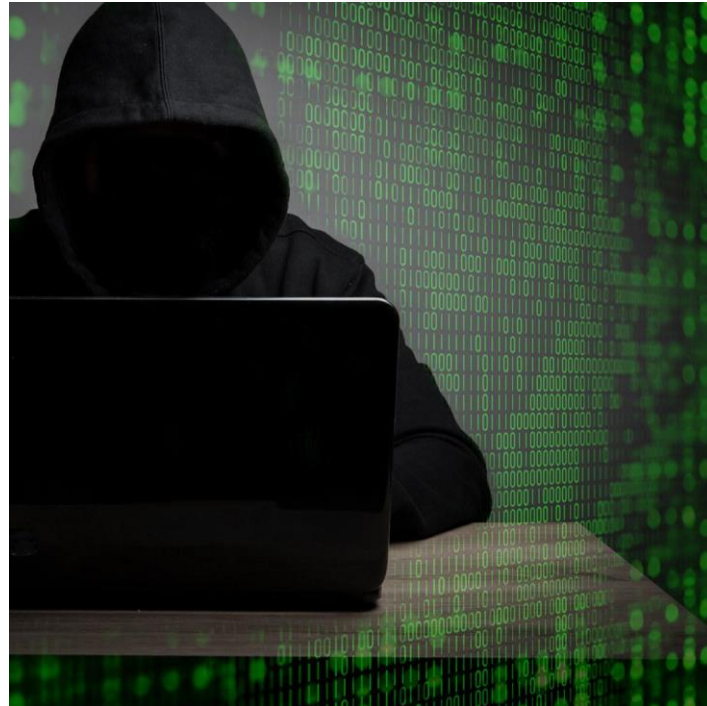
- Good ones are to be focused, the *Ethical Hackers*

WHO IS A HACKER?

- Steal facebook password?

- Hack a wifi?

- A CS Student?

- Get me unlimited coins in the game?

- HACKS NASA WITH HTML?

A Terrorist?

"*Hacking has evolved from teenage mischief into a billion-dollar growth business.*"

WHO IS A HACKER?

- Using his/her skills and knowledge to gain unauthorized access to a software, computer, or a network

- Uses his/her own tools and techniques

- Is NOT always bad

- Can go to prison, or earn millions

- One of the most risky professions of them all

"*The quieter you become, the more you are able to hear.*

TYPES OF HACKERS

1

WHITE HAT HACKERS

Security Professionals, hack with permissions

White Hat Hacker

- The ethical hackers, also break into systems

- Not to exploit them, but to help management fix them

- The same thrill, same swag, but bonus money and respect

- Even work with Government, cyber cells and police

2

BLACK HAT HACKERS

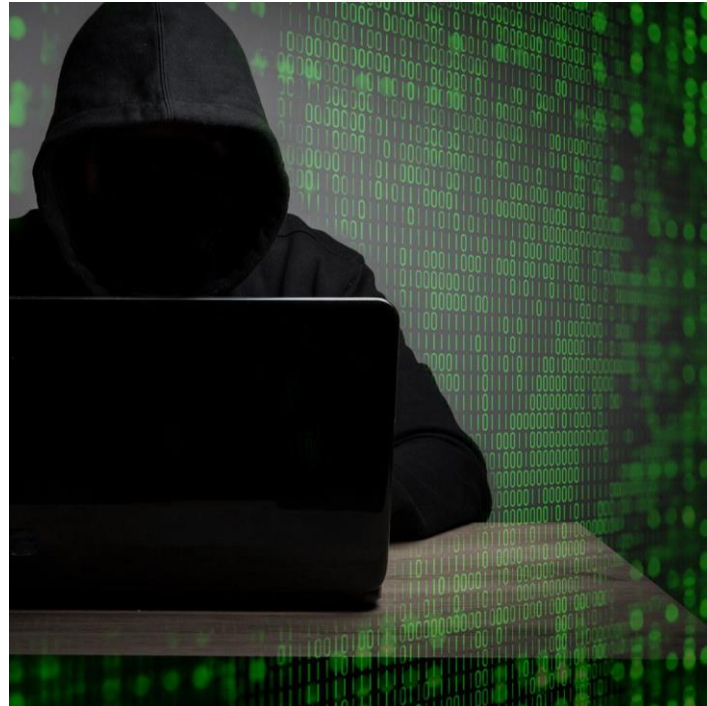Criminals, highly destructive, penetrate to destroy and cause damage

Black Hat Hacker

- That typical hacker you might have heard of

- Use undisclosed vulnerabilities, tools and exploits

- Just randomly hack systems to create havoc

- Or to take revenge or fulfil personal desires

- Most common desires: Financial gain, spying, revenge

Black Hat Hacker

3

GREY HAT HACKERS

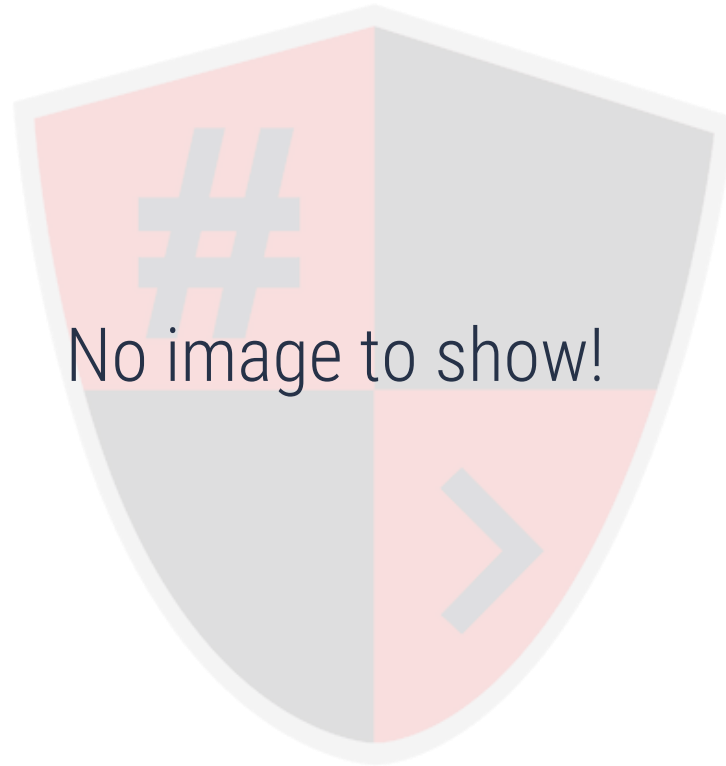Don't have permissions, but no malicious intent

Grey Hat Hacker

- Not completely white, not completely black

- Hack without permissions and authorization, sometimes report

- Demand compensation/money for fix

- Whether to say illegal, totally depends on the victim party

- Don't actually have any professional gain

No image to show!

5. What is Ethical Hacking?

Ethical Hacking

- Performed by a company or individual to help identify potential threats on a computer or network

- Search for any weak points that could be exploited by malicious hackers

- This information is then used by the organization to improve the system security

- Very underrated and criticized, especially in India

Ethical Hacking

It is way more wider than we think!

HACKING IS HACKING, NO MATTER HOW YOU LOOK AT IT!!

IF YOU HACK, YOU ARE A COMPUTER CRIMINAL OR CYBER CRIMINAL!!

But actually, the cyber space is more safer as we see it because of ethical hackers

WHO IS AN ETHICAL HACKER?

WHO IS A ETHICAL HACKER?

- Security Professional
- Tests the security and identifies loopholes
- Creates reports and analysis
- Authorized with proper permissions
- Earns money and respect

6. Information Warfare

Information Warfare

"Tactical and strategic use of information, to gain an advantage."

In the earlier days, information was more physical

Groups of people involved, especially Government, to tackle enemies

Countries spent millions in secret intelligence and spies

Military used weapons and army power to send policy implementations

Information Warfare

◼ Today, this warfare involves most of the digital media.

◼ It has become cyber warfare

◼ Government spends millions for IT infrastructure to attack, defend from attacks

◼ Now it mostly revolves around terrorism

Common practices of cyber warfare:
◼ Using viruses and malwares
◼ Exploiting electronic communication systems and networks
◼ Stealing info via unauthorized access

Information Warfare

Current Providers

TOP SECRET//SI//ORCON//NOFORN
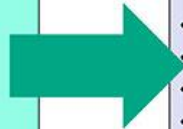
(TS//SI//NF) PRISM Collection Details

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

7. Need for Ethical Hackers

Need for Ethical Hackers

There is a hack attack every 39 seconds

The average cost of a data breach in 2020 will exceed $150 million

Companies have spend $2 trillion total in 2019

$6 trillion is expected to be spent globally on cybersecurity by 2021

Cybersecurity jobs worldwide will reach 3.5 million by 2021

"Cybercrime is the greatest threat to every company in the world."

Need for Ethical Hackers

- Who will prevent wastage of this money?

- Who will help developers fix their bugs in production?

- Who will stop those black hats and their malicious activities to damage our cyberspace?

- Who will ensure security to the companies?

- Who will ensure national security?

- Who will help to keep the cyber space safe and clean?

Careers in Ethical Hacking

CAREERS IN HACKING?

1,000,000

Ethical Hackers would be needed by 2020 in India

5,80,000

Average Salary

2,50,000

For a beginner/Fresher

20,00,000+

For a professional

150,000$

Average Salary

80,000$

For a beginner/Fresher

250,000$

For a professional

PROFESSIONAL CERTIFICATIONS

TO BECOME AN ETHICAL HACKER?

Security

- ➤ Certified Ethical Hacker (CEH)

- ➤ Offensive Security Certified Professional (OSCP)

- ➤ CompTIA Security+, Pentest+

- ➤ GIAC Penetration Tester(GPEN)

- ➤ Certified Information Systems Security Professional (CISSP)
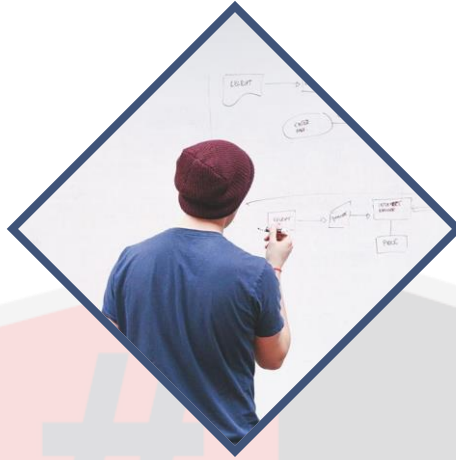
TO BECOME AN ETHICAL HACKER?

Networking

➤ Cisco Certified Network Associate (CCNA)

➤ CompTIA Network+

➤ Cisco Certified Network Professional (CCNP)

➤ Cisco Certified Internetwork Expert (CCIE)

➤ AWS Certified Solutions Architect

"If you are online, you are vulnerable."

IS HACKING ILLEGAL?

- Not always

- Ethical Hacking is completely LEGAL

- There is a huge need for ethical hackers

- Hack systems, earn money

> **"** *To become a hacker, you need to think like one.*

Course Overview

What will you learn?

- **Module 2: Basics and Environment setup**
- **Module 3: Linux Basics**
- **Module 4: Networking Basics**
- **Module 5: Footprinting/Reconnaissance**
- **Module 6: Scanning**
- **Module 7: Enumeration**
- **Module 8: System Hacking**

What will you learn?

- Module 9: Malwares
- Module 10: Sniffing
- Module 11: Social Engineering
- Module 12: Denial of Service
- Module 13: Session Hijacking
- Module 14: Hacking Web Servers
- Module 15: Hacking Web Applications

What will you learn?

- **Module 16: Evading IDS, Firewalls**
- **Module 17: Wireless Hacking**
- **Module 18: Hacking Mobile Platforms**
- **Module 19: Cryptography**
- **Module 20: Cloud Computing**
- **Module 21: Forensics**
- **Module 22: Bug Hunting and Pentesting**

What will you get?

- Detailed explanation videos
- Practical labs at every module
- Study materials
- Reference materials
- Books to read
- Contact support
- Access anywhere
- Certificate of completion

Prerequisites

- Basic Computer and IT Skills

- Basic knowledge of Operating Systems

- Basic networking knowledge
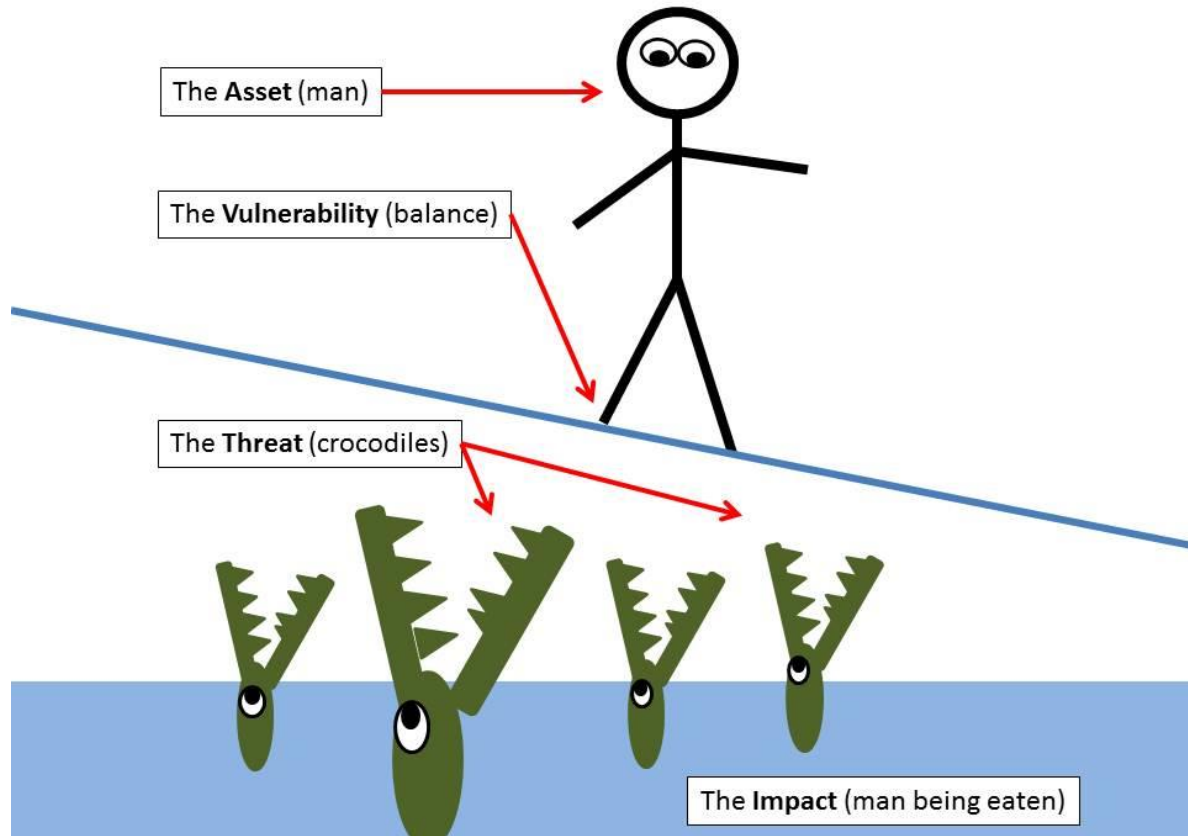
- A computer, with min 4 GB RAM

- PATIENCE!!

General Terminologies

- **Vulnerability**: A weakness that can be exploited

- **Threat**: One who exploits a vulnerability

- **Risk**: Damage caused by exploiting the vulnerability

- **Asset**: Which needs to be accessed after exploitation

- **Bug**: Error, fault or flaw in a computer program that may cause unexpected behavior

The **Asset** (man)

The **Vulnerability** (balance)

The **Threat** (crocodiles)

The **Impact** (man being eaten)

Hacker: Gains access with or without malicious intent

Cracker: Gains access to damage assets and cause harm, always malicious

- **Infosec:** Information Security/Cyber Security/Data Security

- **Penetration Testing:** Testing and reporting the security loopholes

- **Vulnerability Assessment:** Testing and reporting the security loopholes, and tells how to fix them

- **Cyber Espionage:** Spying on someone to gain illicit access to confidential information (large institutions)
- **Exploits:** Designed to cause unexpected behaviors that an attacker can take advantage of to perform harmful actions
- **Script Kiddie:** Newbies/noobs so called hackers without any skills
- **Zero-day:** Vulnerability not known to professionals only to be exploited by hackers

TO BECOME AN ETHICAL HACKER?

Learn

Code

Apply

TO BECOME AN ETHICAL HACKER?

- Programming is important!

- Have a Hacker's mindset

- Be verbose, but don't talk much

- Logical thinking

- Don't learn it all, but know it all

- **Computer Basics**: Hardware, Software, processing methodology

- **Web and Internet**: HTTP, DNS, Web Servers, FTP, SMTP

- **Networking:** TCP/IP, ARP, Devices, types, Routing and Switching

- **Operating Systems**: Linux (Kali, Parrot, Red Hat), Windows, Android, iOS, MAC

TO BECOME AN ETHICAL HACKER?

Programming:

➤ Reverse Engineering- Assembly, C, C++

➤ Script Writing- Python, Ruby, Perl

➤ Web App Testing- JavaScript, PHP, SQL, JSP, Python

➤ Shell Scripting- Bash

TO BECOME AN ETHICAL HACKER?

- OWASP Top 10
- GitHub
- Bug Bounty Programs
- Hacking Forums
- Stack
- Soft Skills
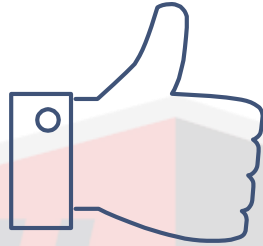- **PRACTICE, PRACTICE AND PRACTICE**

HACKING

Is an art, practised through a creative mind.

THANKS!

Any questions?