ch4p73r 1

1n7r0duc710n 70 h4ck1n6 4nd pr3v3n710n

m0hd 24k1

Topic

- Describe the role of an ethical hacker
- List the type of hackers
- The Attacker processes
- Types of attack
- Describe what you can do legally as an ethical hacker
- Describe what you cannot do as an ethical hacker

HACKER

What my friends think I do

What my Mom thinks I do

What society thinks I do

What the government thinks I do

What I think I do

What I actually do

2019 Data Breach Investigation report

Summary of findings

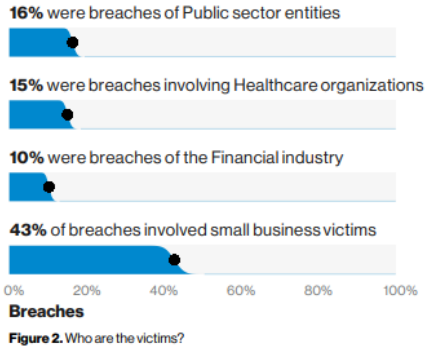


Figure 2. Who are the victims?

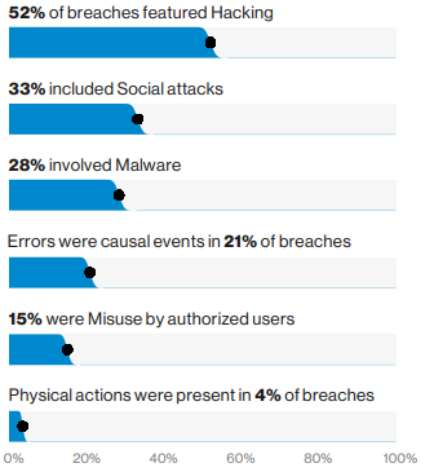


Figure 3. What tactics are utilized?

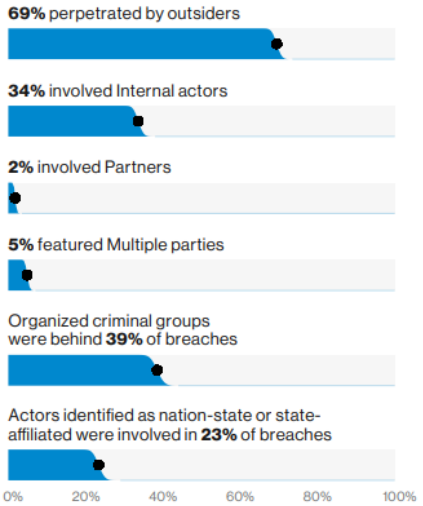


Figure 4. Who's behind the breaches?

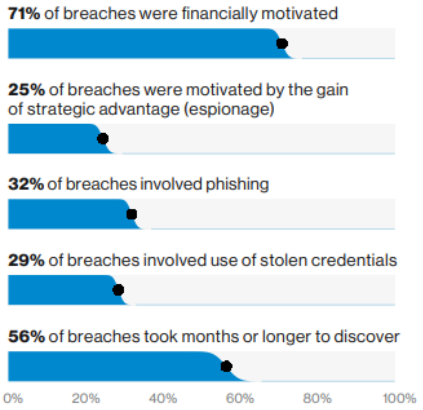


Figure 5. What are other commonalities?

2018 major cybercrime attack

- 500 Million Guest Records Stolen from Marriott
  - Starwood Hotels confirmed its hotel guest database of about 500 million customers had been stolen in a data breach.
- FIFA Hacked
  - FIFA's computer systems were hacked earlier this year for the second time, and officials from European soccer's governing body fear they also might have suffered a data breach.
- Google+ Shuts Down After Vulnerability Exposes 50,000
  - Google is going to shut down its social media network Google+ after the company suffered a massive data breach that exposed the private data of hundreds of thousands of Google Plus users to third-party developers.
  - According to the tech giant, a security vulnerability in one of Google+'s People APIs allowed third-party developers to access data of more than 500,000 users, including their usernames, email addresses, occupation, date of birth, profile photos and gender-related information.
- Nearly 50 Million Facebook Users Compromised in Breach
  - Nearly 50 million Facebook accounts were compromised by an attack that gave hackers the ability to take over users' accounts.
  - The breach was discovered by Facebook engineers Sept. 25, the company said, and patched two days later. Users whose accounts were affected were notified by Facebook. Those users were logged out of their accounts and required to log back in.
- Private information of over a million students and alumni of Universiti Teknologi MARA (UiTM) enrolled between 2000 and 2018 has been leaked in a massive data breach.
  - The leaked data includes personal details like students' names, MyKad numbers, house and email addresses, campus codes, campus names, programme codes, course levels, student IDs and mobile numbers.

https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=0d39dd96-835b-44c7-b710-139e560f6ae0

UiTM students' data allegedly stolen

NATION

Saturday, 26 Jan 2019

By Angelin Yeoh, Qishin Tariq and Sandhya Menon

PETALING JAYA: Private information of over a million students and alumni of Universiti Teknologi MARA (UiTM) enrolled between 2000 and 2018 has been leaked in a massive data breach.

The leaked data includes personal details like students' names, MyKad numbers, house and email addresses, campus codes, campus names, programme codes, course levels, student IDs and mobile numbers.

Tech portal Lowyat.net reported that records of 1,164,540 students had been compromised, affecting records from UiTM campuses around the country, including the main one in Shah Alam.

It also affects students enrolled in UiTM accredited courses at external colleges like Kolej Yayasan Terengganu, Institut Teknologi Perak and Institut Yayasan Bumiputera

been disabled, it is still in the possession of the unauthorised person, and could still be publicly disclosed in the future."

Singapore, July 2018: the city-state suffers its largest data breach

Last summer Singapore was subject to the largest data breach in its history with 1.5 million patients to SingHealth's specialist outpatient clinics affected by it, including Prime Minister Lee Hsien Loong and several ministers.

Personal information stolen included names, National Registration Identity Card numbers, addresses, gender and dates of birth. 160,000 patients had details related to outpatient dispensed medicines as well.

A committee of inquiry (COI) was set in October to investigate into the events and contributing factors leading to the cyber attack.

During the COI, which finished on 30 November, it was established that intrusions into SingHealth's electronic medical records (EMR) system - a critical information infrastructure in Singapore - began undetected on June 27 but were discovered on July 4 and terminated by a database administrator at Integrated Health Information Systems (IHiS), the agency which runs the IT systems of all public

Hacking

The British Airways hack is impressively bad

BA is the latest company to be hit by hackers. We chart the biggest data breaches of 2018

By MATT BURGESS

Friday 7 September 2018

- 1. MyDoom's Mass Infection: Estimated damage: $38 billion

McAfee said this 2004 worm tops its list for monetary damage. Designed to infect computers and send spam e-mail, the worm slowed global Internet access by 10 percent and reduced access to some websites by 50 percent. McAfee said it led to billions of dollars in lost productivity and online sales.

- 2. "I Love You" Worm: Estimated damage: $15 Billion

Named for the subject line of the e-mail that delivered it, this worm hit millions of users in 2000. When users opened the attached "love letter," they actually downloaded a virus that ended up costing companies and government agencies $15 billion in cleanup.

- 3. Conficker: Estimated damage: $9.1 Billion

This worm originated in 2007 and has infected millions of computers since, installing keystroke-logging and PC-controlling software that gave cybercrooks a way to steal users' personal information and access their machines.

- 4. Stuxnet Worm: Damage unknown

This recent worm was designed to hijack and potentially cripple real-world targets such as nuclear power plants, factories and oil rigs. Stuxnet has reportedly damaged nuclear facilities in Iran and government facilities in the U.S., India and Indonesia, McAfee said, but its creators are still unknown.

- 5. Zeus Botnet: Damage unknown

Named for the all-powerful Greek god, this circa 2007 worm is known for stealing personal information by capturing data entered on Internet banking sites. More recently, the worm has shown its ability even to infect mobile devices.

Five Most Famous (or Infamous) Pretexters

1. Kevin Mitnick

WANTED
BY U.S. MARSHALS

THE SNOWDEN FILES

The Inside Story of the World's Most Wanted Man

LUKE HARDING

Award-winning Correspondent for *The Guardian*

2000 MafiaBoy

Michael "Mafiaboy" Calce

Once upon a time, "distributed denial of service attacks" were just a way for quarreling hackers to knock each other out of IRC. Then one day in February 2000, a 15-year-old Canadian named Michael "MafiaBoy" Calce experimentally programmed his botnet to hose down the highest traffic websites he could find. CNN, Yahoo, Amazon, eBay, Dell and eTrade all buckled under the deluge, leading to national headlines and an emergency meeting of security experts at the White House.

Compared to modern DDoS attacks, MafiaBoy's was trivial. But his was the cyberstrike that put the internet's security issues on a national stage, and inaugurated an era where any pissed off script kiddy could take down part of the web at will.

2005 –
2008

Albert Gonzalez

He called it “Operation Get Rich or Die Tryin’.” For nearly four years ending in 2008, 28-year-old Albert “Segvec” Gonzalez and his accomplices in America and Russia staged the biggest data thefts in history, stealing credit and debit card magstripe data for sale on the black market. Using Wi-Fi hacking and SQL injection, the gang popped companies like 7-Eleven, Dave & Buster’s, Office Max, TJX, and the credit card processor Heartland Payment Systems, which alone gave up 130 million cards.

Albert "Segvec" Gonzalez

The intrusions didn’t just make Gonzalez a millionaire — he buried $1.1 million in his parents’ backyard — they exposed slipshod security in America’s card-processing infrastructure, and positioned the former Secret Service informant to break a new record: longest U.S. prison term for hacking. His plea agreements envision a 17- to 25-year sentence. It could be worse. One of Gonzalez’s overseas

2006 Max Vision

In 2006, a former computer security researcher turned professional black hat weighed and measured the computer underground, and found it wanting. So in a two-night hackfest from his San Francisco safe house, Max Vision (aka Iceman) trained his guns on the online carder forums where hackers and fraudsters buy and sell stolen data, fake IDs and specialized underground services.

Max "Iceman" Vision

When he was done hacking in and wiping out their databases, he absorbed their content and membership into his own site, CardersMarket, turning it into the largest English-speaking criminal marketplace on the web — 6,000 members strong. The hostile takeover got the attention of the feds who'd thoroughly infiltrated some of the sites he hacked, and a year later FBI and Secret Service tracked Iceman to his hideout. He's now awaiting sentencing for stealing 2 million credit cards that rang up $86 million in fraudulent charges.

2004 Foonet

Saad Echouafni

Years before there was a Russian Business Network, a small ISP hosted in a suburban basement in Ohio gained the dubious reputation as the first black-hat hosting company. It was a safe spot for hackers and packet monkeys to attack an unsuspecting internet. Foonet's hosted clients included Carder Planet — the dedicated "carder forum" for credit card hackers — and its IRC servers were where legendary German hacker Axel "Ago" Gembe controlled his Agobot network of compromised Windows boxes.

After two FBI raids, in 2004, Foonet's founder and some of the staff were indicted for a DDoS-for-hire scheme that collaterally slammed Amazon.com and the Department of Homeland Security. Foonet's owner, Saad Echouafni, skipped out on $750,000 to flee the country, and remains on the FBI's wanted list today.

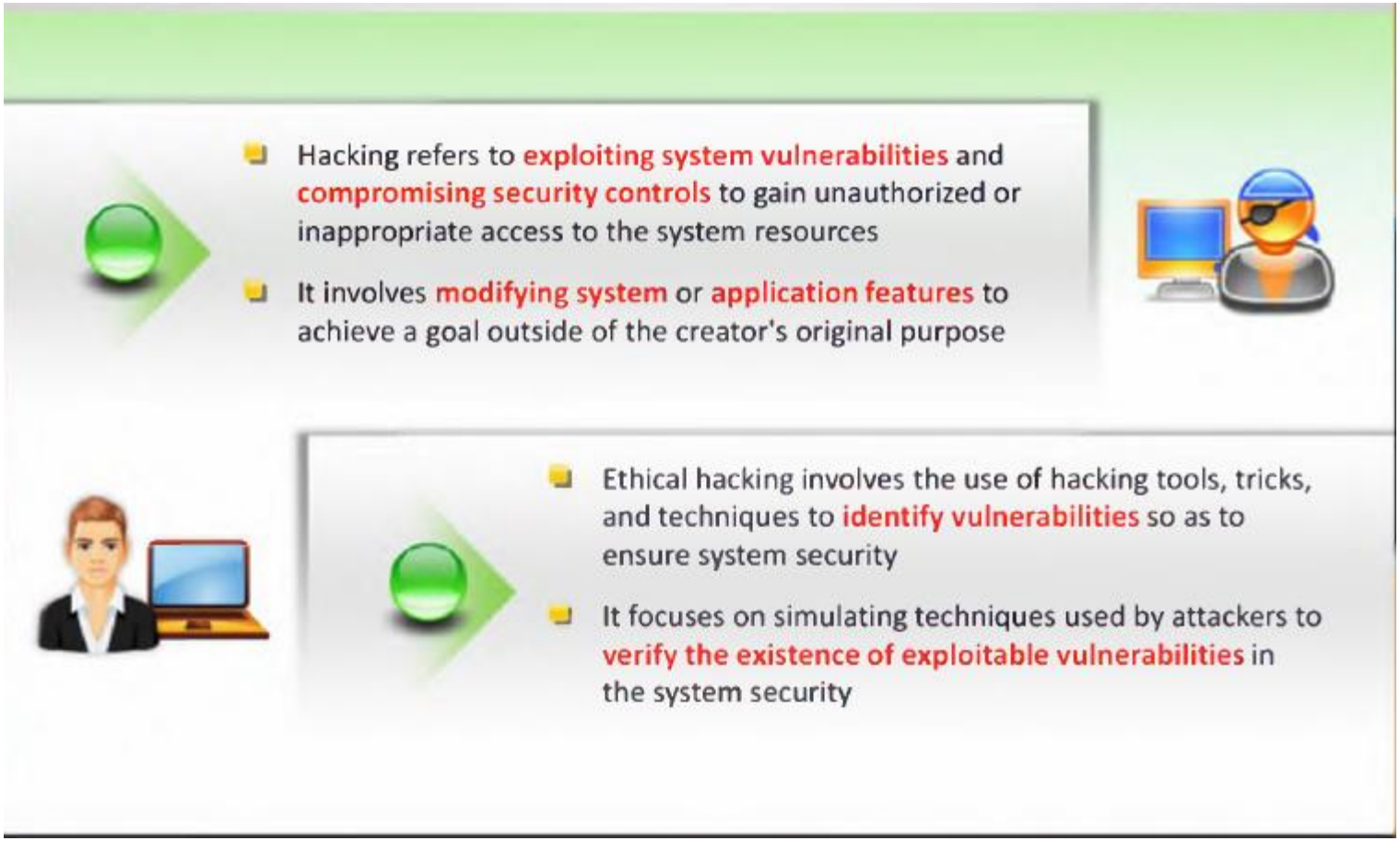
What Is Hacker ?

- *Hacker* is one of the most misunderstood and overused terms in the security industry.
- It has almost become the technological equivalent of a boogeyman, which so many either fear or end up ignoring.
- What is a hacker and where do we, as ethical hackers, fit in? Well, to answer that question let’s take a look at the history of hacking along with some notable events.

Introduction to Ethical Hacking

- Ethical hackers
  - Employed by companies to perform penetration tests
- Penetration test
  - Legal attempt to break into a company's network to find its weakest link
  - Tester only reports findings, does not solve problems
- Security test
  - More than an attempt to break in; also includes analyzing company's security policy and procedures
  - Tester offers solutions to secure or protect the network

H Vs EH


Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources
It involves modifying system or application features to achieve a goal outside of the creator's original purpose
Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security
It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the system security

Hackers Category

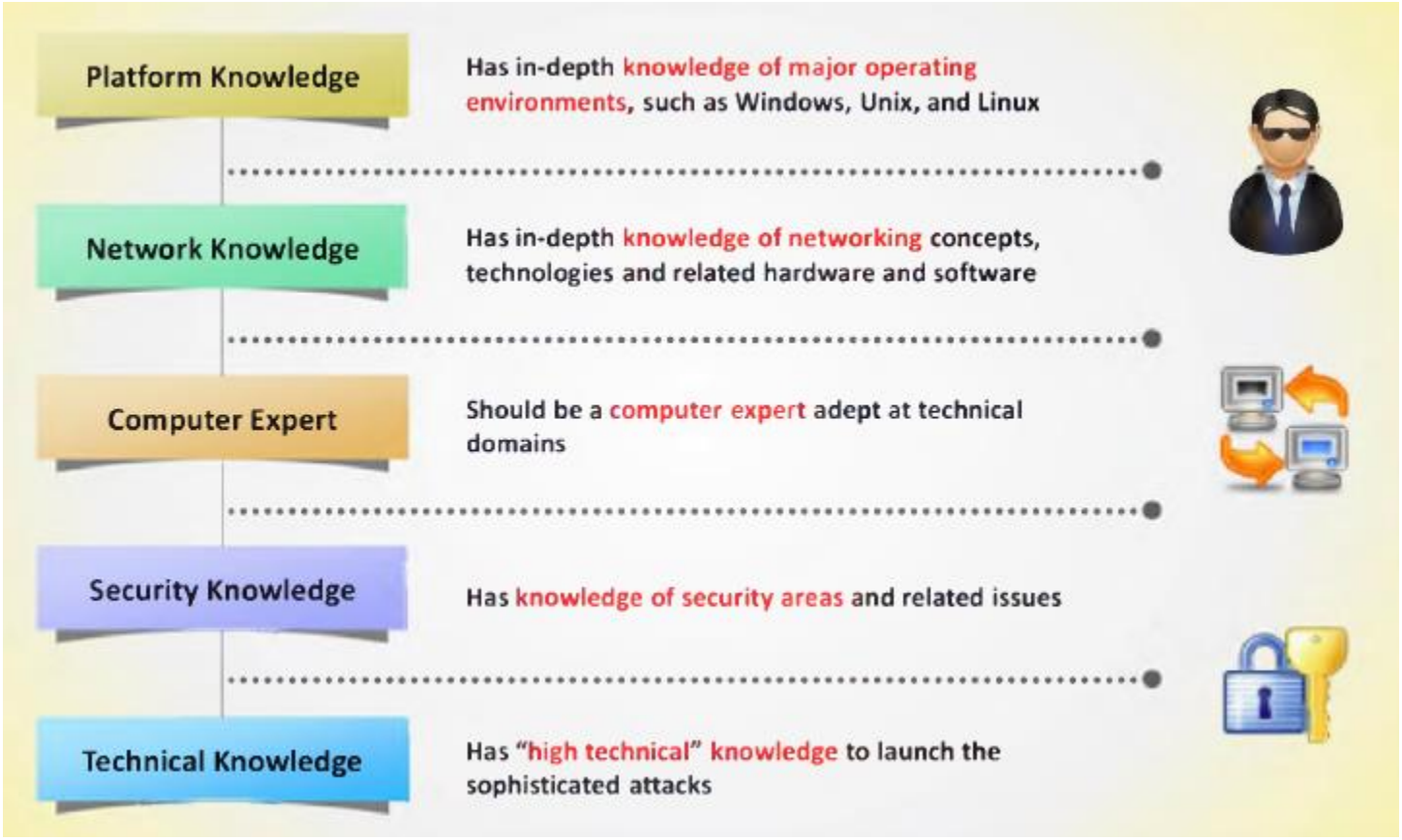
- Hackers
  - Access computer system or network without authorization
  - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
  - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities but with owner's permission

- Script kiddies or packet monkeys
  - Young inexperienced hackers
  - Copy codes and techniques from knowledgeable hackers
- Experienced penetration testers write programs or scripts using these languages
  - Practical Extraction and Report Language (Perl), C, C++, Python, JavaScript, Visual Basic, SQL, and many others
- Script
  - Set of instructions that runs in sequence

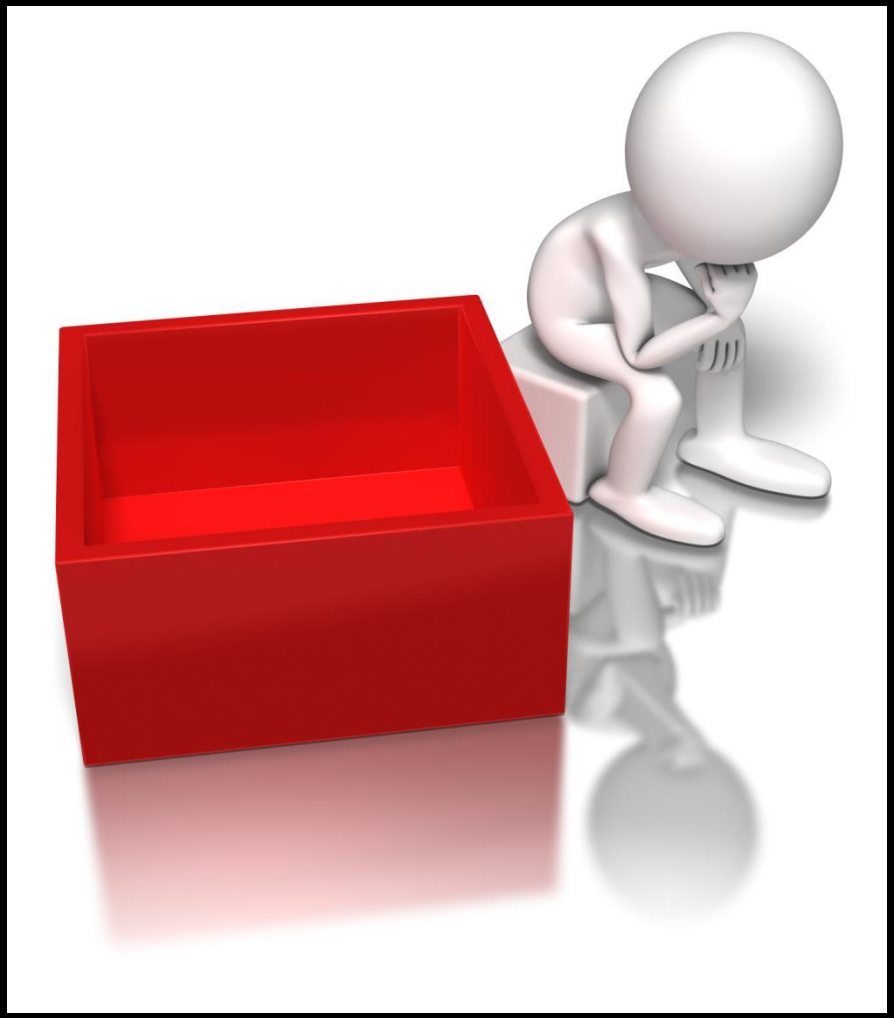
Terminology

- Hack Value
  - It is the notion among hackers that something is worth doing or is interesting
- Exploit
  - A defined way to breach the security of an IT system through vulnerability
- Vulnerability
  - Existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system
- Target of Evaluation
  - An IT system, product, or component that is identified/subjected to a required security evaluation
- Zero-Day Attack
  - An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability
- Daisy Chaining
  - Hackers who get away with database theft usually complete their task, then backtrack to cover their tracks by destroying logs, etc.

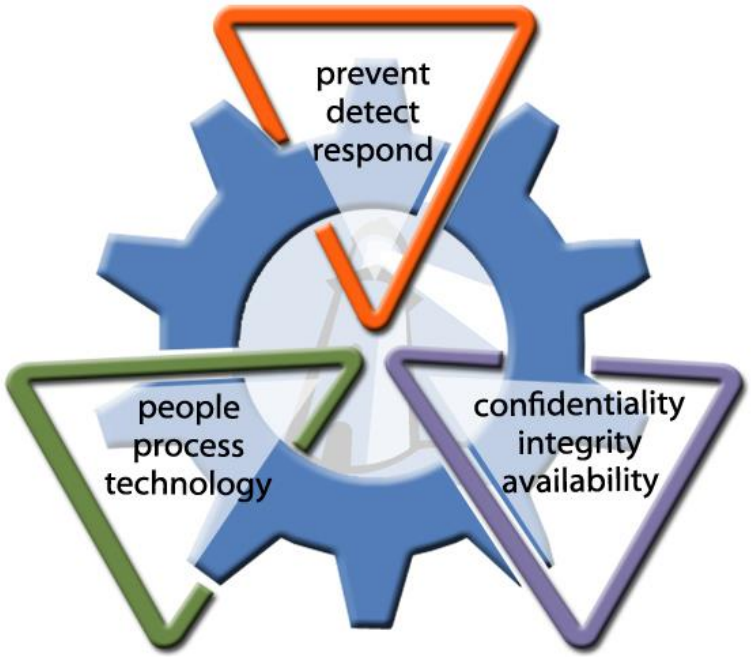
Skill Required For Ethical hacking



How the hacker think ?

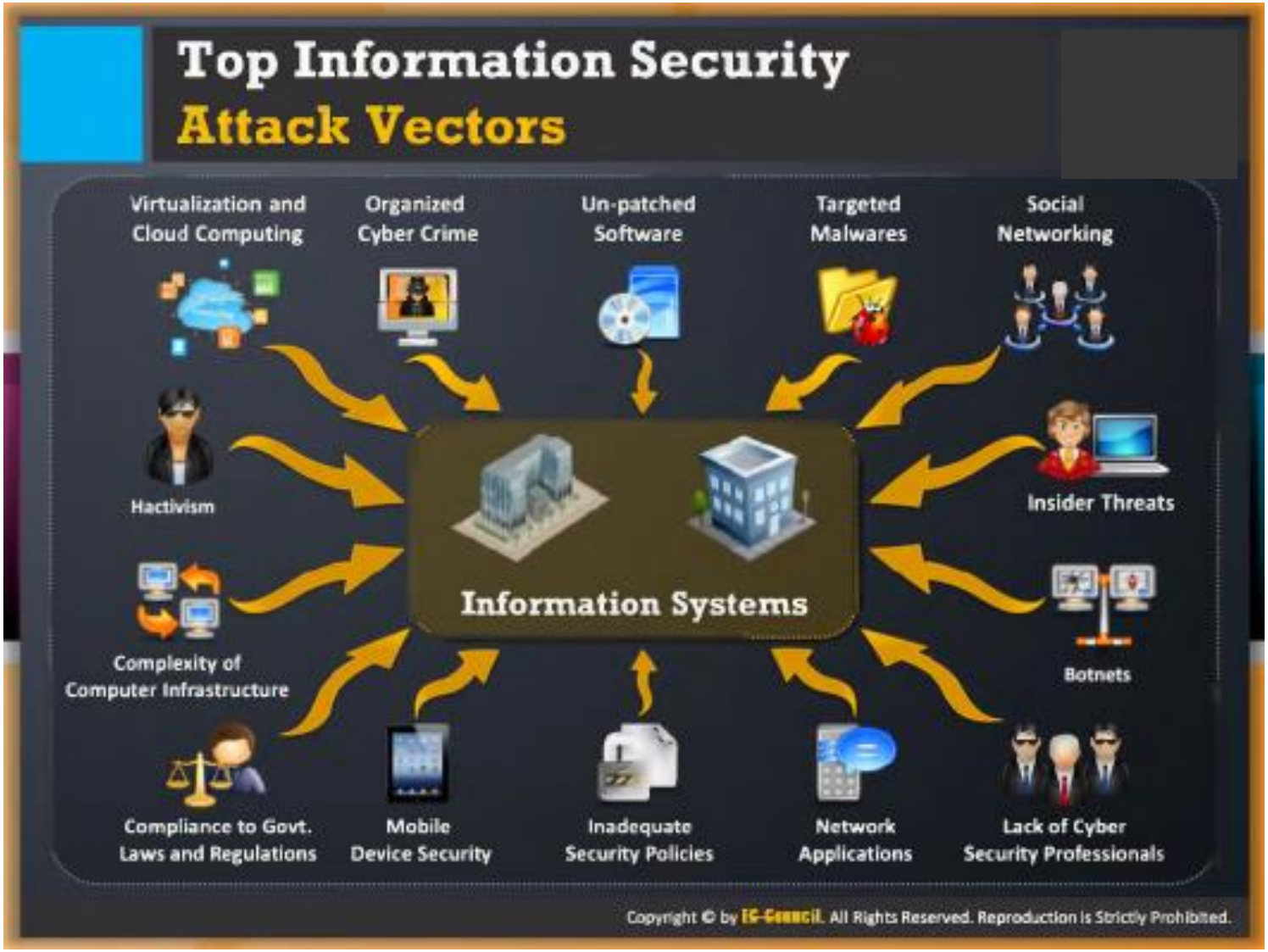


Info. Sec. Element



Cyber Security Triads

Top Information Security Attack Vector



Motives , Goals , and Objectives

Goals

- Attackers have motives or goals such as disrupting business continuity , information theft, data manipu lations , or taking revenge

Motives

- A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system

Objectives

- Attackers try various tools , attack methods , and techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

Attacks = Motive (Goal) + Method + Vulnerability

Information Security Threats

- Natural Threats
  - Natural threat sinclude natural disasters such as earth quakes, hurricanes , floods , or any nature – created disaster that can not be stop.
  - Information damage or lost due to natural threats can not be prevented as no one knows in advance that the setypes of threats will occur.
  - However, you can implement a few safeguards against natural disasters by adopting disaster recovery plans and contingency plans.
- Physical Security Threats
  - Physical threats may include loss or damage of system resources through fire, water, theft and physical impact.
  - Physical impact on resources can be due to a collision or other damage, either intentionally or unintentionally.
  - Some times, power may also damage hardware used to store information.

- Human Threats
  - Human threats include threats of attacks performed by both insiders and outsiders.
  - Insider attacks refer to attacks performed by disgruntled or malicious employees.
  - Outsider attacks refer to attacks performed by malicious people not within the organization.
  - Insider attacker scan be the biggest threat to information system as they may know the security posture of the information system, while outsider attackers apply many tricks such as social engineering to learn the security posture of the information system .

- Network Threats
  - A network is defined as the collection of computers and other hardware connected by communication channels to share resources and information.
  - As the information travels from one computer to the other through the communication channel, a malicious person may break into the communication channel and steal the information traveling over the network .
  - The attacker can impose various threats on a target network :

- Information gathering
- Sniffing and eavesdropping
- Spoofing
- Session hijacking and man-in-the-middle attacks
- SQL injection
- ARP Poisoning
- Password-based attacks
- Denial of service attack
- Compromised-key attack

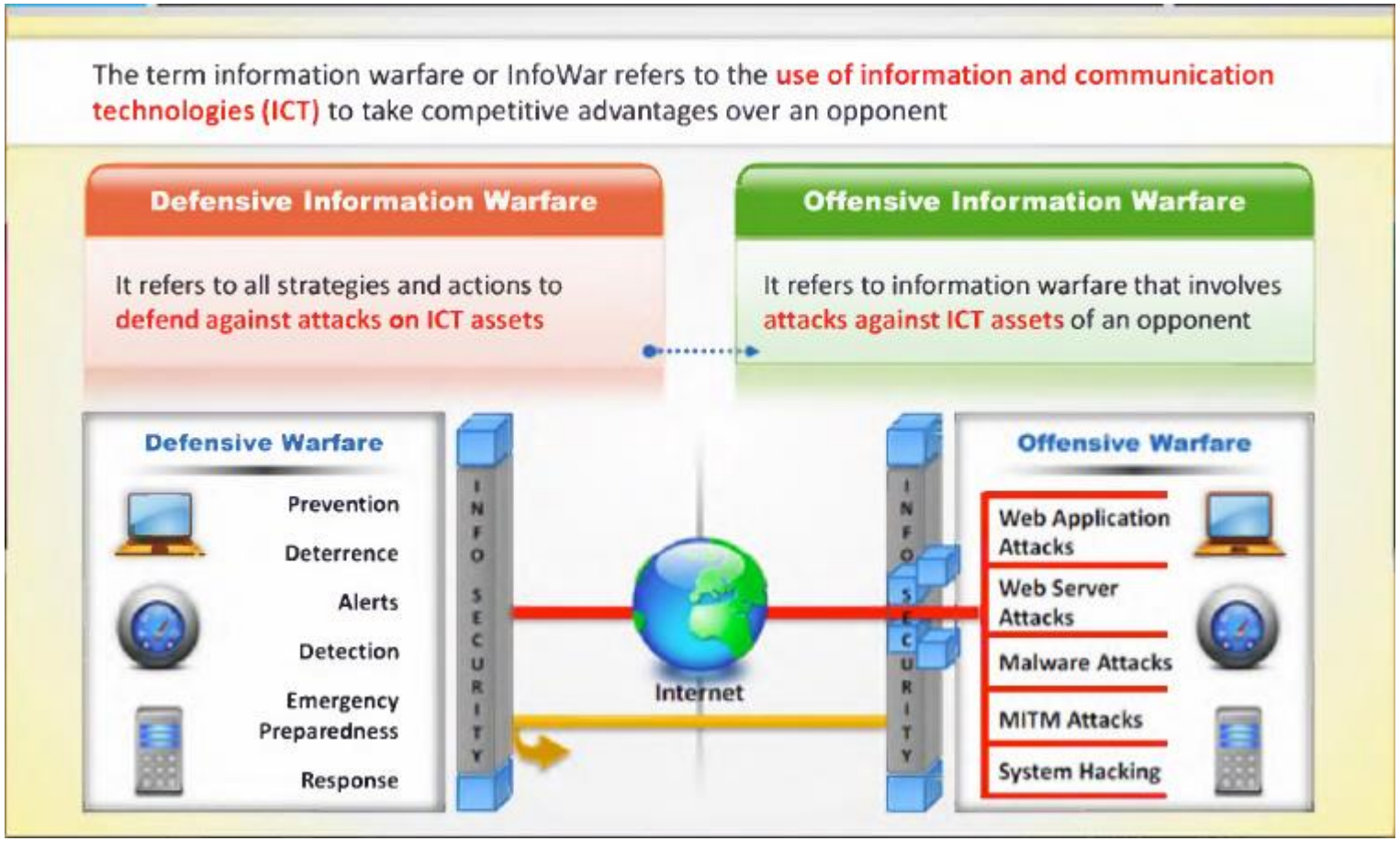
- Host Threats
- Host threats are directed at a particular system on which valuable in formation resides
- Attackers try to breach the security of the information system resource. The following are possible threats to the host :

- Malware attacks
- Target Foot printing
- Password attacks
- Denial of service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Backdoor Attacks
- Physical security threats

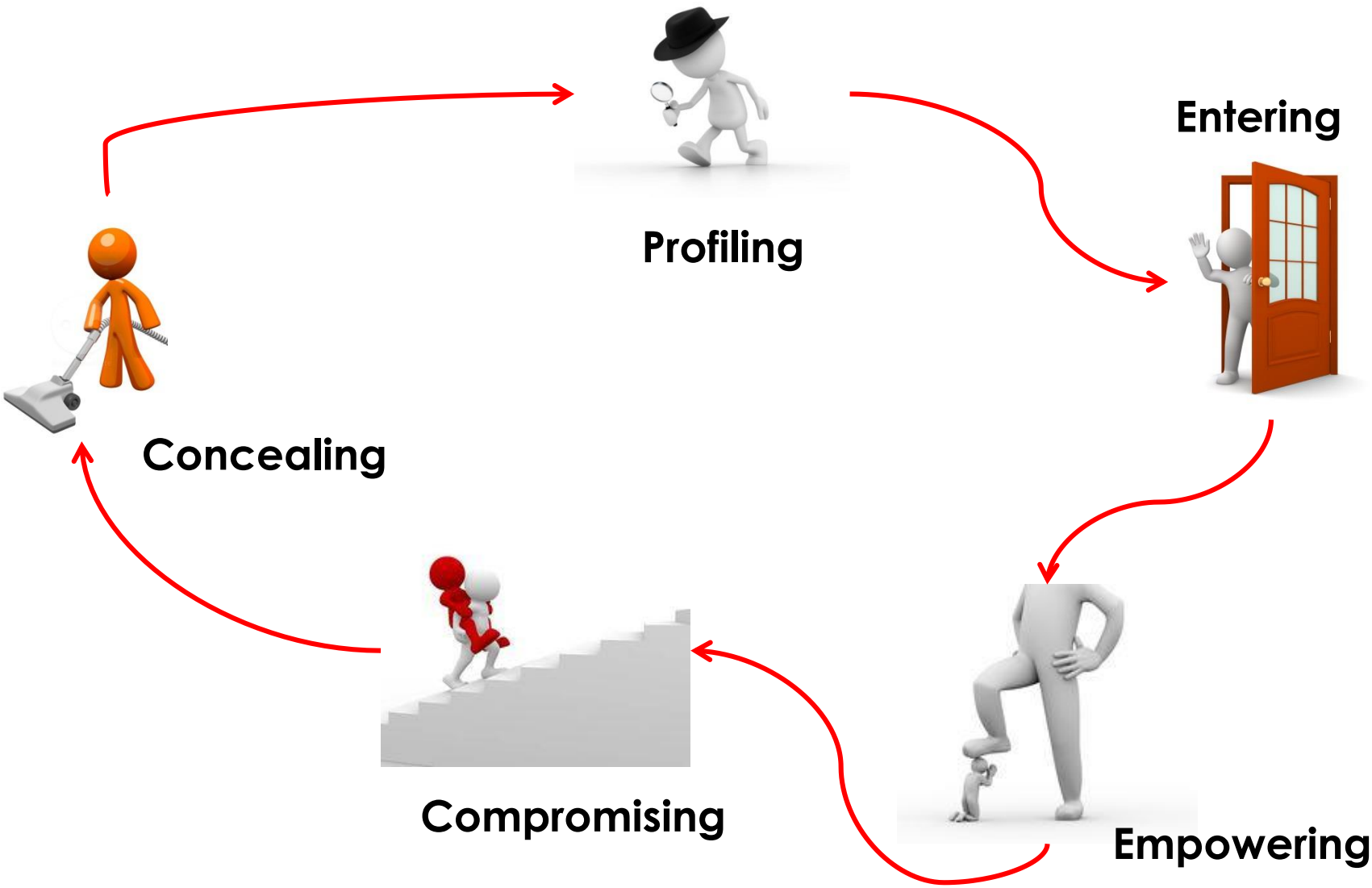
- Application Threats
- If the proper security measures are not considered dur ing development of the particular application, the application might be vulnerable to different types of application attacks .
- Attackers take advantage of vulnerabilities present in the application to steal or damage the information.
- The following are possible threats to the application :

- Data/Input validation
- Authentication and Authorization attacks
- Configuration management
- Information disclosure
- Session management issues
- Buffer overflow issues
- Cryptography attacks
- Parameter manipulation
- Improper error handling and exception management
- Auditing and logging issues

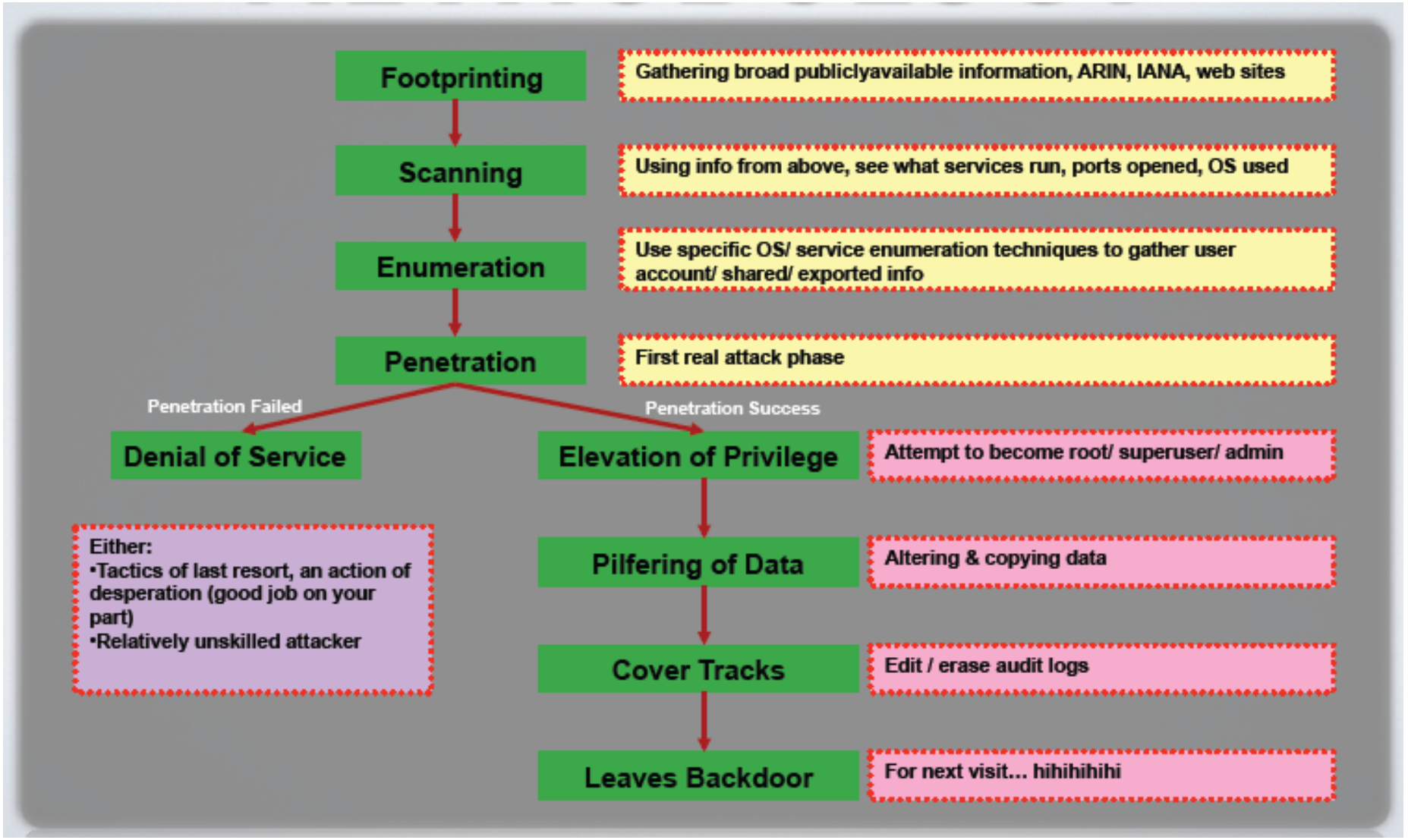
Information Warfare



Hacking Life Cycle



Attack Phase



TIME
& DETERMINATION are the KEY!

If the attacker want to break into the system, they will always able to.

Types of attack

- There are several ways an attacker can gain access to a system .
- The attacker must be able to exploit a weakness or vulnerability in a system :

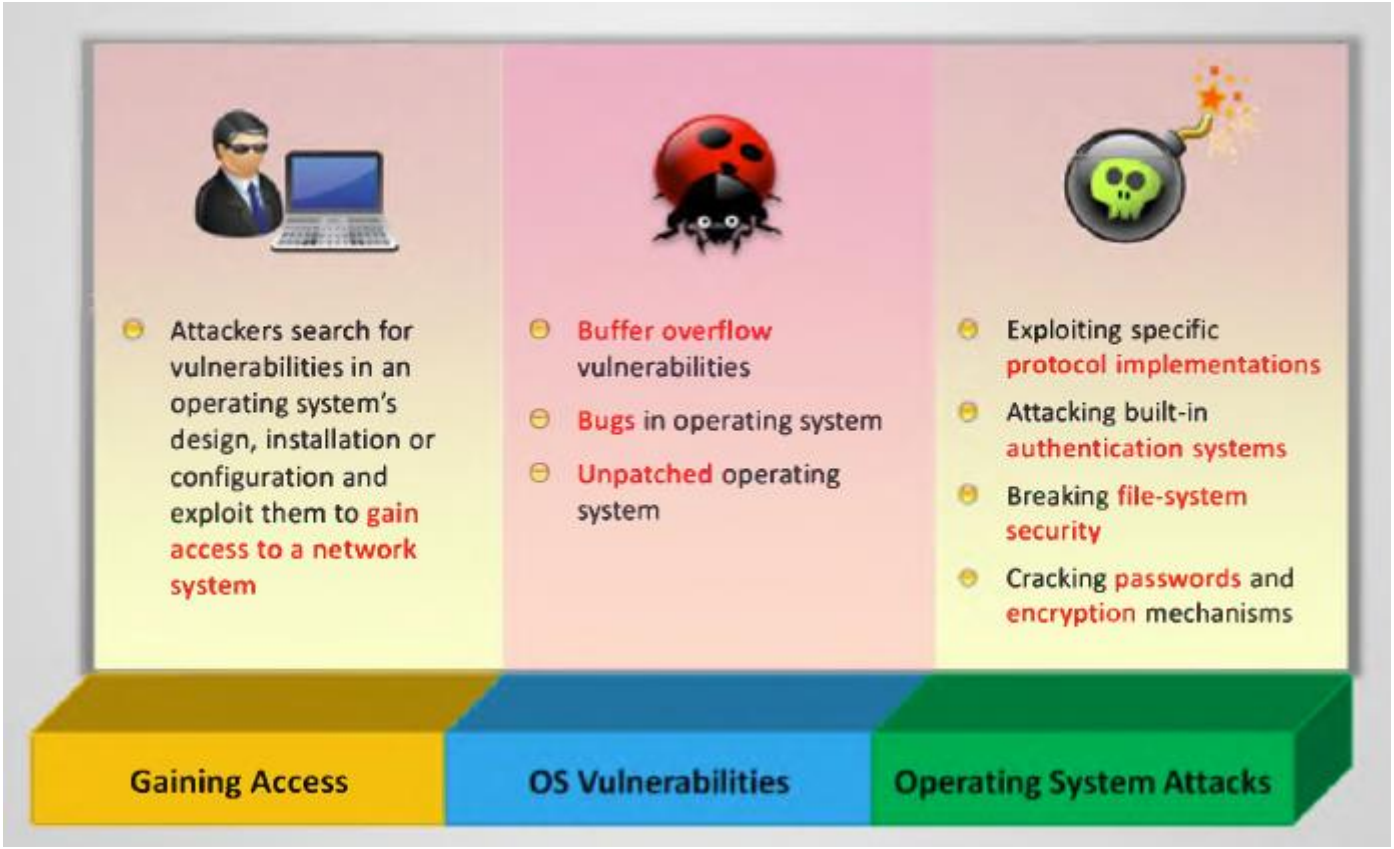
  - **Operating system attacks :**
    - Attackers search for OS vulnerabilities and exploit them to gain access to a network system .

  - **Application-level attacks:**
    - Software applications come with myriad functionalities and features . There is a dearth of tim to perform complete testing before releasing products. Those applications have various vulnerabilities and become a source of attack .

  - **Misconfiguration attacks:**
    - Most administrators don't havem the necessary skills to maintain or fix issues, which may lead to configuration errors. Such configuration errors may become the sources for an attacker to enter into the target's network or system.

  - **Shrink wrap code attacks:**
    - Operating system applications come with numerous sample scripts to make the job of administrator easy, but the same scripts have various vulnerabilities, which can lead to shrink wrap code attacks .

OS Attack


Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to gain access to a network system
Buffer overflow vulnerabilities
Bugs in operating system
Unpatched operating system
Exploiting specific protocol implementations
Attacking built-in authentication systems
Breaking file-system security
Cracking passwords and encryption mechanisms
Gaining Access
OS Vulnerabilities
Operating System Attacks

Miss configuration

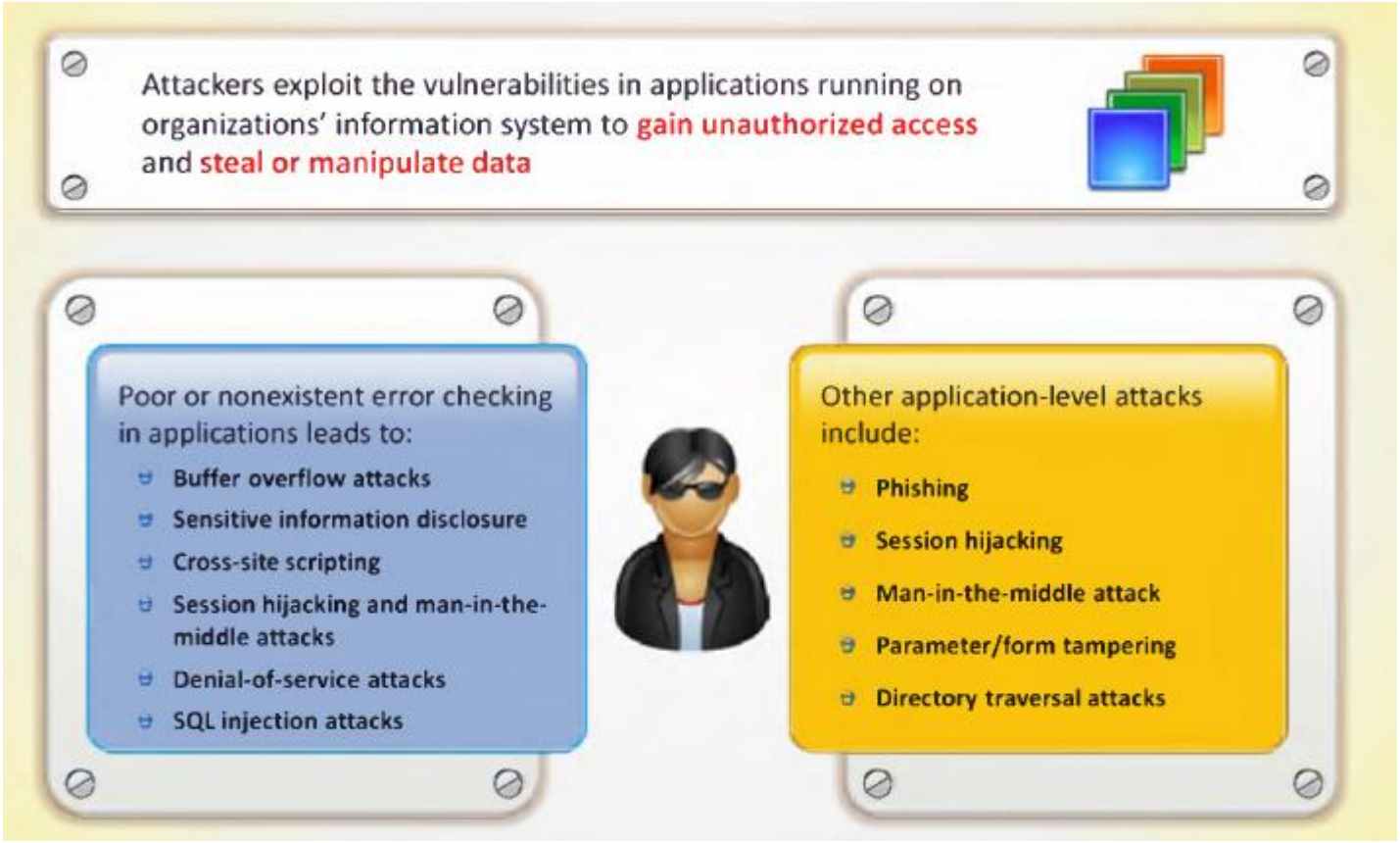
If a system is misconfigured, such as a change is made in the file permission, it can no longer be considered secure

Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in illegal access or possible owning of the system

The administrators are expected to change the configuration of the devices before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system

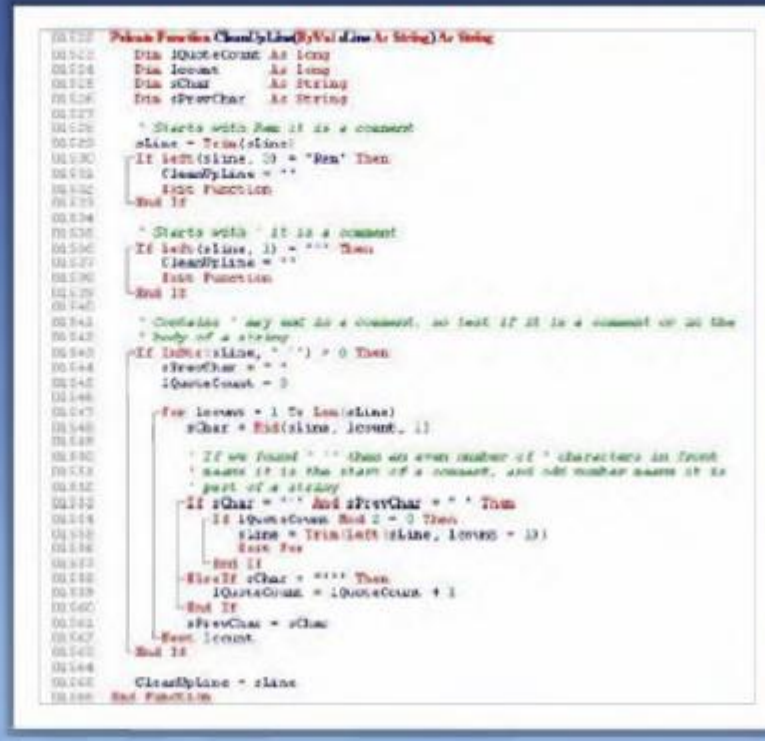
In order to optimize the configuration of the machine, remove any redundant services or software

Application Level Attack

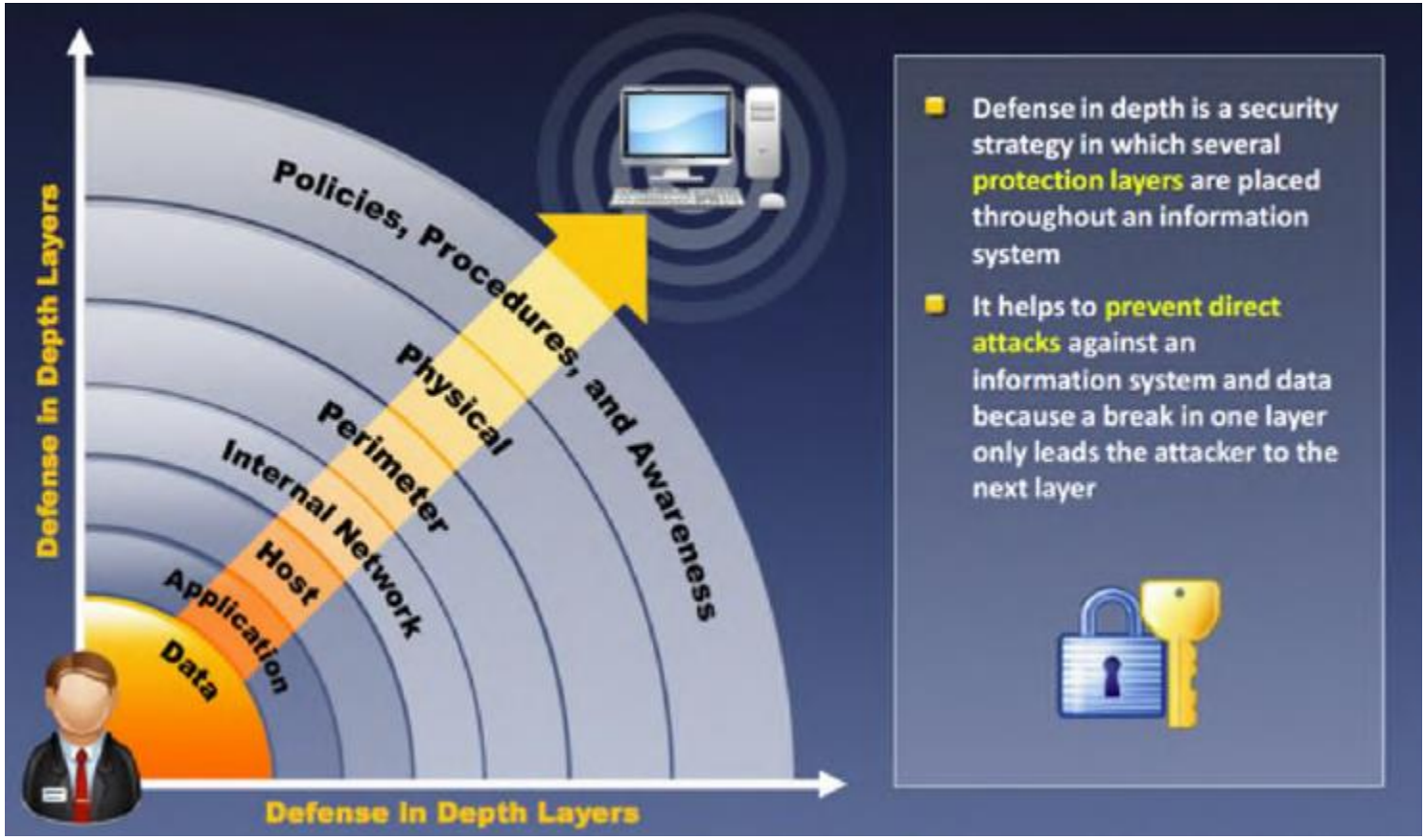


Shrink Wrap Code

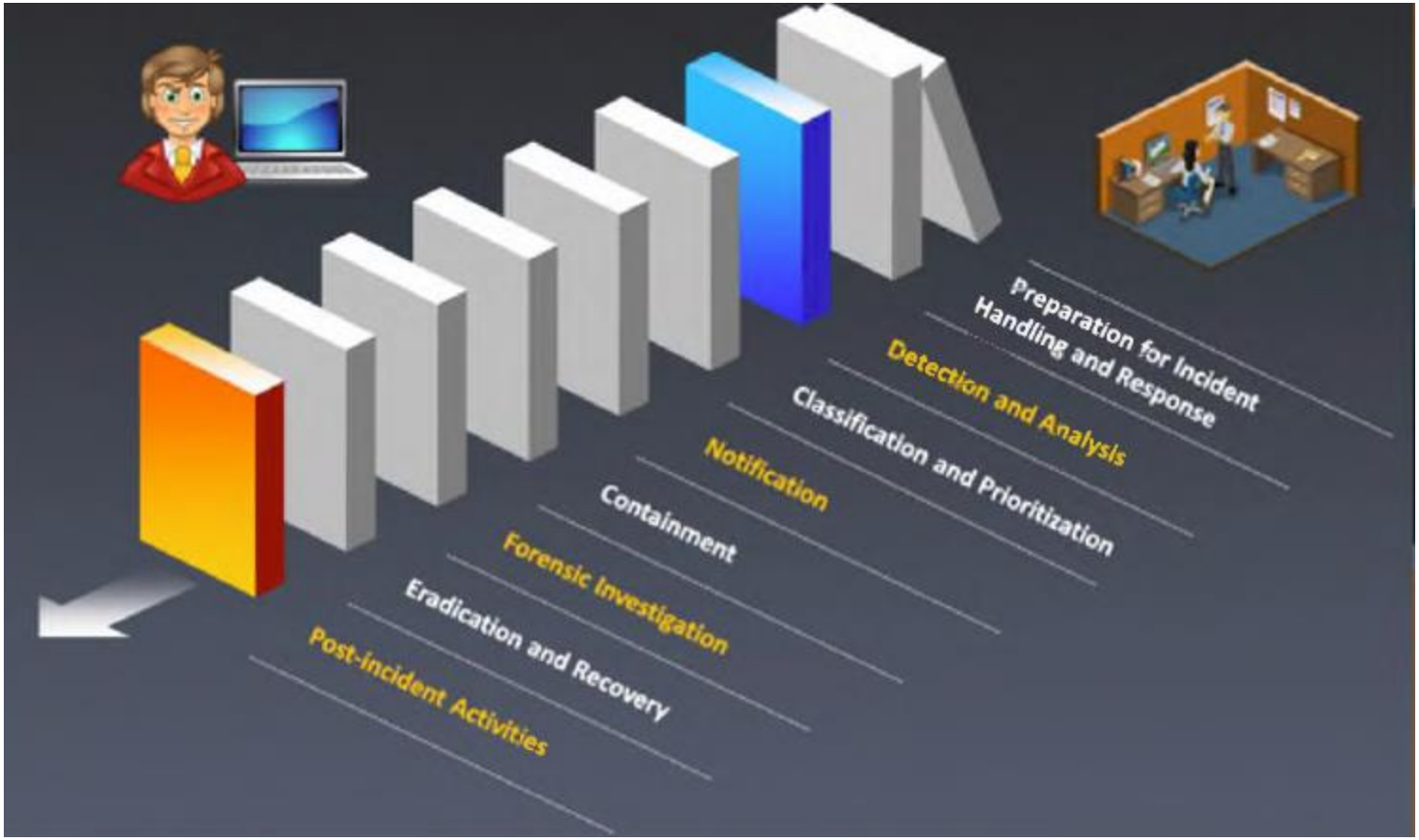
- Why reinvent the wheel when you can buy off-the-shelf **libraries** and code?
- When you install an **OS** or **application**, it comes with supporting sample scripts to perform various administration tasks
- Application developers also use **off-the-shelf libraries** and code to reduce development time and cost
- The problem is **not fine tuning** or customizing these scripts
- **Shrink wrap code** or **default code** attack refers to attacks that exploit default configuration and settings of the off-the-shelf libraries and code



Mitigation


Defense in Depth Layers
Policies, Procedures, and Awareness
Physical
Perimeter
Internal Network
Host
Application
Data
Defense in Depth Layers
Defense in depth is a security strategy in which several protection layers are placed throughout an information system
It helps to prevent direct attacks against an information system and data because a break in one layer only leads the attacker to the next layer

Incident Mgmt and Response


Preparation for Incident Handling and Response
Detection and Analysis
Classification and Prioritization
Notification
Containment
Forensic Investigation
Eradication and Recovery
Post-incident Activities

Security Policy

- Security policies are the foundation of the **security infrastructure**
- A security policy is a document or set of documents that **describes the security controls** that will be implemented in the company at a high level

Goals of Security Policies

1. Maintain an outline for the management and administration of network security
2. Protection of organization's computing resources
3. Elimination of legal liability from employees or third parties
4. Ensure customers' integrity and prevent waste of company computing resources
5. Prevent unauthorized modifications of the data
6. Reduce risks caused by illegal use of the system resource, loss of sensitive, confidential data, and potential property
7. Differentiate the user's access rights
8. Protect confidential, proprietary information from theft, misuse, unauthorized disclosure

What You Can Do Legally

- Laws involving technology change as rapidly as technology itself
- Find what is legal for you locally
  - Laws change from place to place
- Be aware of what is allowed and what is not allowed

Laws of the Land

- Tools on your computer might be illegal to possess
- Contact local law enforcement agencies before installing hacking tools
- Written words are open to interpretation
- Governments are getting more serious about punishment for cybercrimes

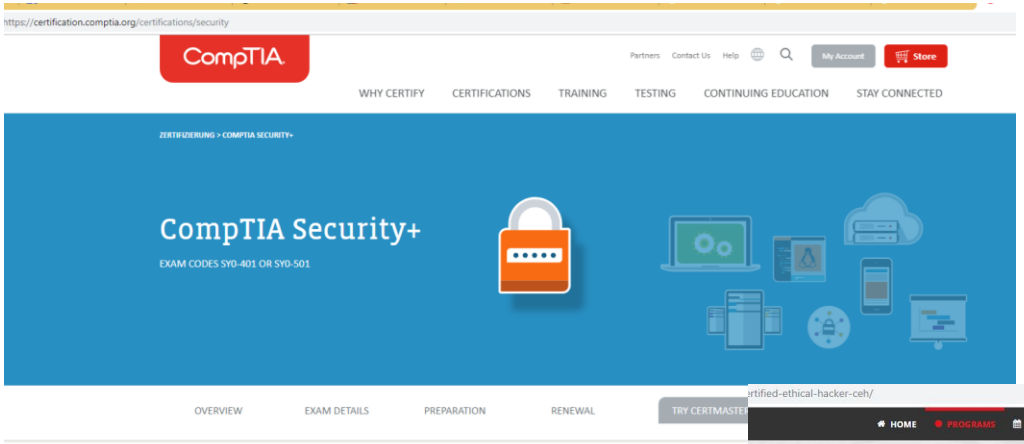
Is Port Scanning Legal?

- Some states deem it legal
- Not always the case
- US Federal Government does not see it as a violation
  - Allows each state to address it separately
- Read your ISP's "Acceptable Use Policy"
  - IRC "bots" may be forbidden
    - Program that sends automatic responses to users
    - Gives the appearance of a person being present

What You Cannot Do Legally

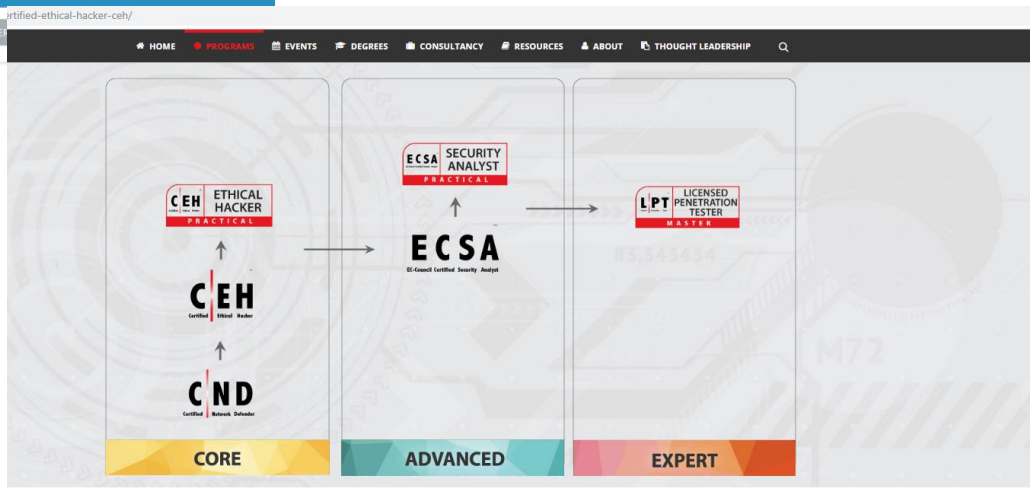
- Accessing a computer without permission is illegal
- Other illegal actions
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs

Security Professional Certification



CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career.

Why is it different?



Certified Ethical Hacker Certification

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Security Professional Certification

ty.com/information-security-certifications/oscp-offensive-security-certified-professional/

OFFENSIVE® security

Courses Certifications Online Labs Penetration Testing Projects Blog About ENROLL NOW

Offensive Security Certified Professional (OSCP) Overview

OFFENSIVE® security OSCP MOST POPULAR

GET CERTIFIED

Limited seats available for each course session

- OSCP is the most well-recognized and respected certifica… info security professionals
- To become certified, you must complete Offensive Secur… Penetration Testing with Kali Linux (PwK) course and pas… hour hands-on exam
- An OSCP has mastered a comprehensive and practical understanding of the penetration testing process
- For hands-on experience, each student receives access t… penetration testing lab where techniques learned within… course can be practiced

Real World Exams

The *OSCP examination* consists of a virtual network containing targets of varying configurations and operating systems. At the start of the exam, the student receives the exam and connectivity instructions for an isolated exam network that they have no prior knowledge or exposure to.

The successful examinee will demonstrate their ability to research the network (information gathering), identify any vulnerabilities and successfully execute attacks. This often includes modifying exploit code with the goal to compromise the systems and gain administrative access.

…ications/CISSP#

REGISTER FOR EXAM SIGN IN

(ISC)² ABOUT CERTIFICATIONS EDUCATION & TRAINING MEMBERS NEWS & EVENTS ADVOCACY COMMUNITY

CISSP®

Become a CISSP – Certified Information Systems Security Professional

Accelerate your cybersecurity career with the CISSP certification.

Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program. With a CISSP, you validate your expertise and become an (ISC)² member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

Prove your skills, advance your career, and gain the support of a community of cybersecurity leaders here to support you throughout your career.

Free CISSP Ultimate Guide

Get everything you need to know about preparing for the CISSP exam, including:

- Why you should get certified
- CISSP *Fast Facts*
- What to expect on the exam
- How to prepare for the exam
- Value of (ISC)² certification

DOWNLOAD

Security Professional Certification

Ethical Hacking in a Nutshell

- What it takes to be a security tester
  - Knowledge of network and computer technology
  - Ability to communicate with management and IT personnel
  - Understanding of the laws
  - Ability to use necessary tools