Introduction to Ethical Hacking

Module 01

Module Objectives

- Data Breach Investigations Report
- Essential Terminology
- Elements of Information Security
- Top Information Security Attack Vectors
- Information Security Threats
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who Is a Hacker?

- Hacking Phases
- Types of Attacks on a System
- Why Ethical Hacking Is Necessary
- Skills of an Ethical Hacker
- Incident Management Process
- Types of Security Policies
- Vulnerability Research
- What Is Penetration Testing?

This module covers:

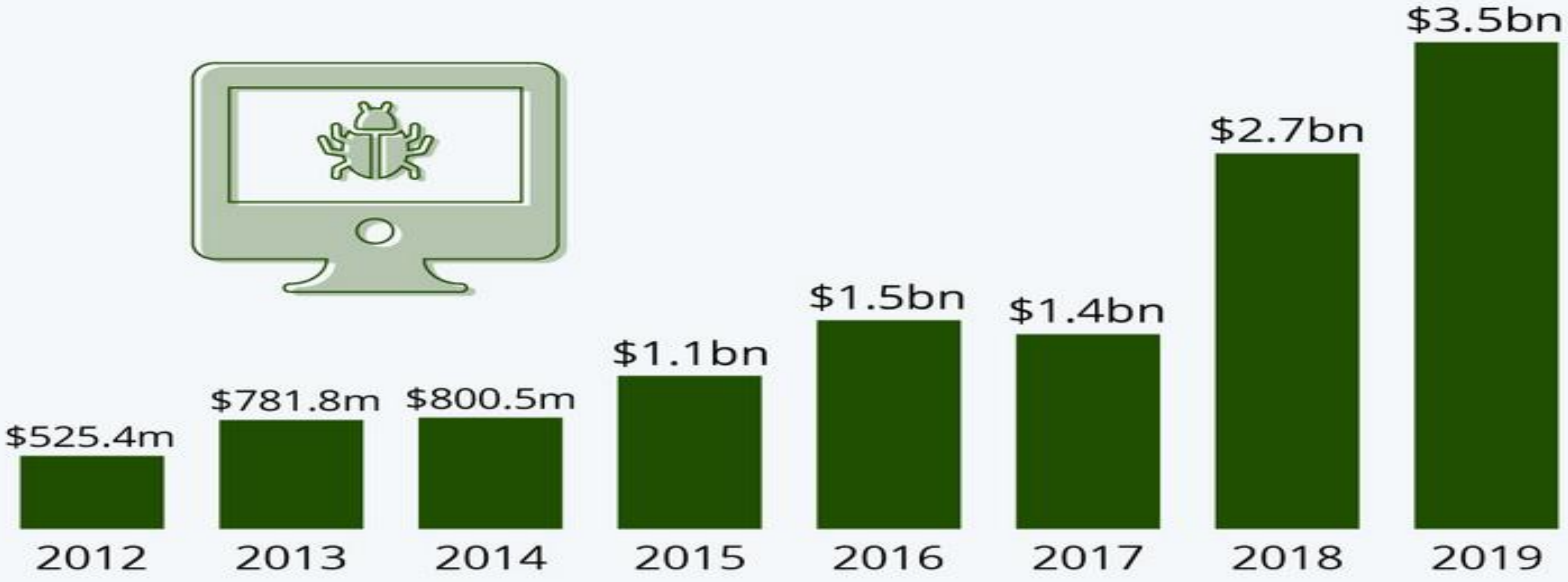
- Data Breach Investigations Report
- Essential Terminology
- Elements of Information Security
- Top Information Security Attack Vectors
- Information Security Threats
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who Is a Hacker?
- Hacking Phases
- Types of Attacks on a System
- Why Ethical Hacking Is Necessary
- Skills of an Ethical Hacker
- Incident Management Process
- Types of Security Policies
- Vulnerability Research
- What Is Penetration Testing?

Module Flow

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts
- Hacking Phases
- Types of Attacks
- Information Security Controls

Internet Crime Current Report: IC3

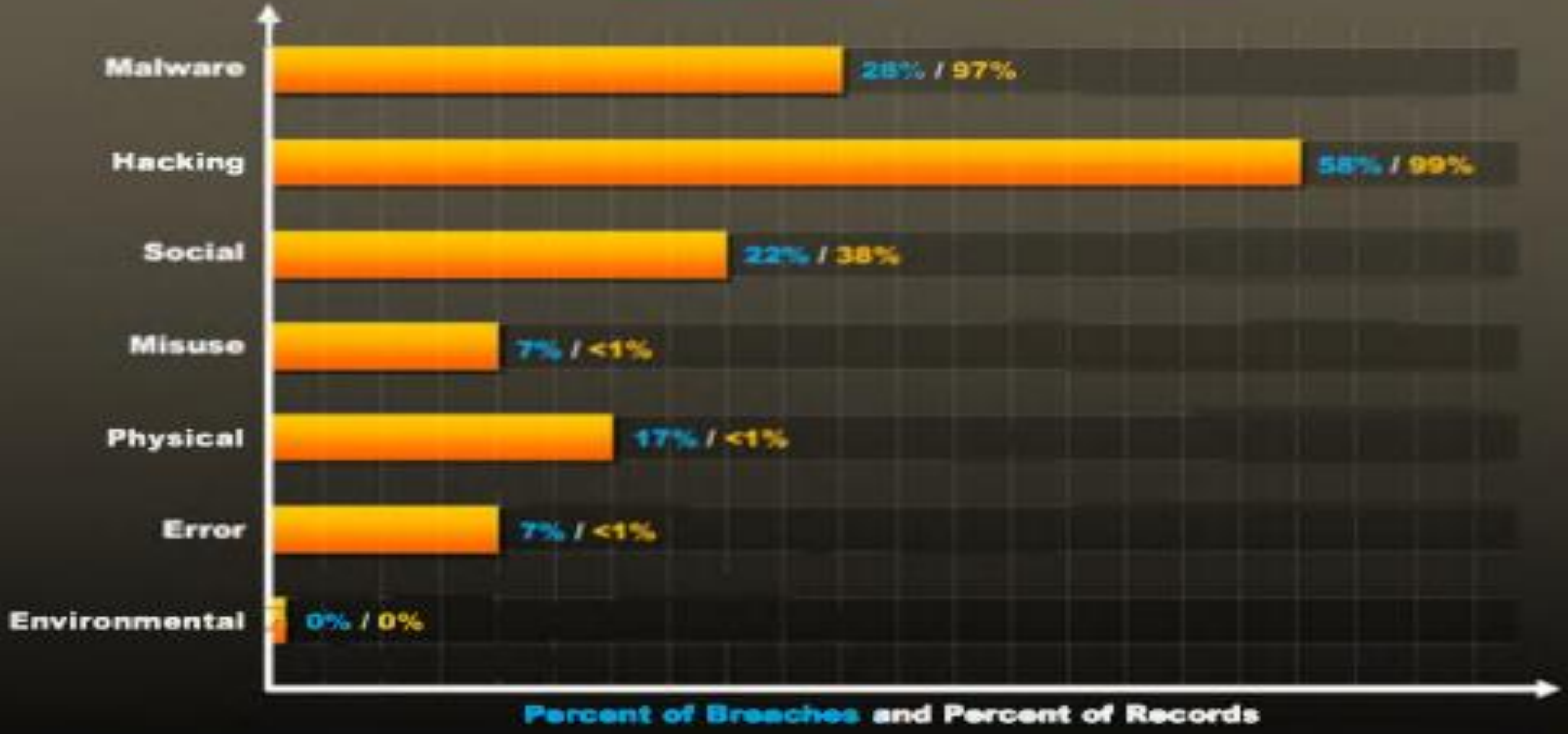
Internet Crime Complaint Center (IC3)



Source: FBI's Internet Crime Complaint Center

Data Breach Investigations Report

Types of hacking by percent of breaches and percent of records



http://www.verizonbusiness.com

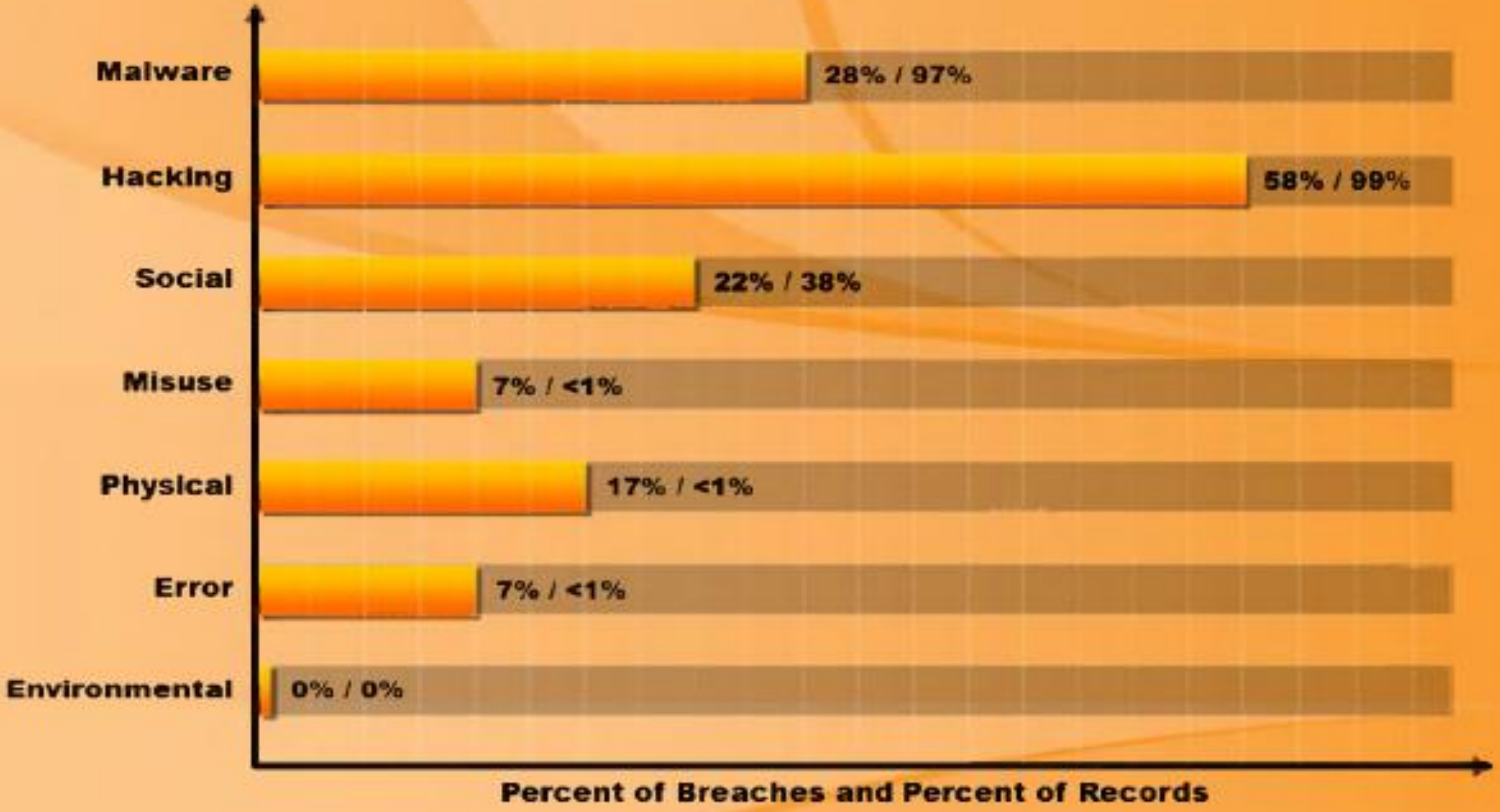


FIGURE 1.1: Data Breach Investigation Report

Essential Terminology

Hack Value

It is the notion among hackers that something is worth doing or is interesting

Target of Evaluation

An IT system, product, or component that is identified/subjected to a required security evaluation

Exploit

A defined way to breach the security of an IT system through vulnerability

Zero-Day Attack

An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability

Vulnerability

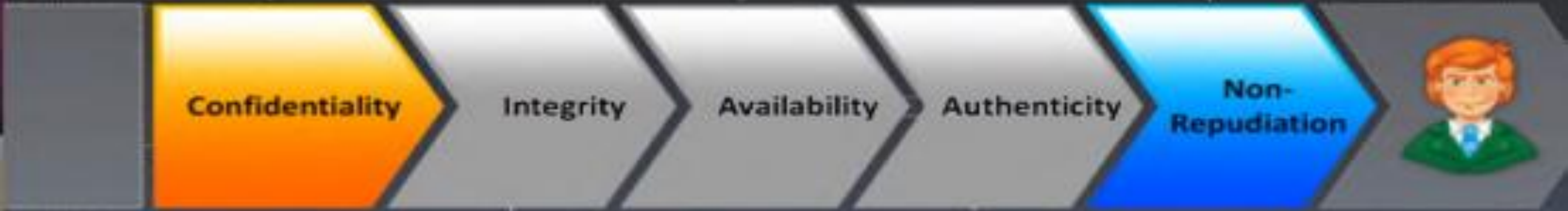
Existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system

Daisy Chaining

Hackers who get away with database theft usually complete their task, then backtrack to cover their tracks by destroying logs, etc.

Elements of Information Security

A state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable



Assurance that the information is accessible only to those authorized to have access

The trustworthiness of data or resources in terms of preventing improper and unauthorized changes

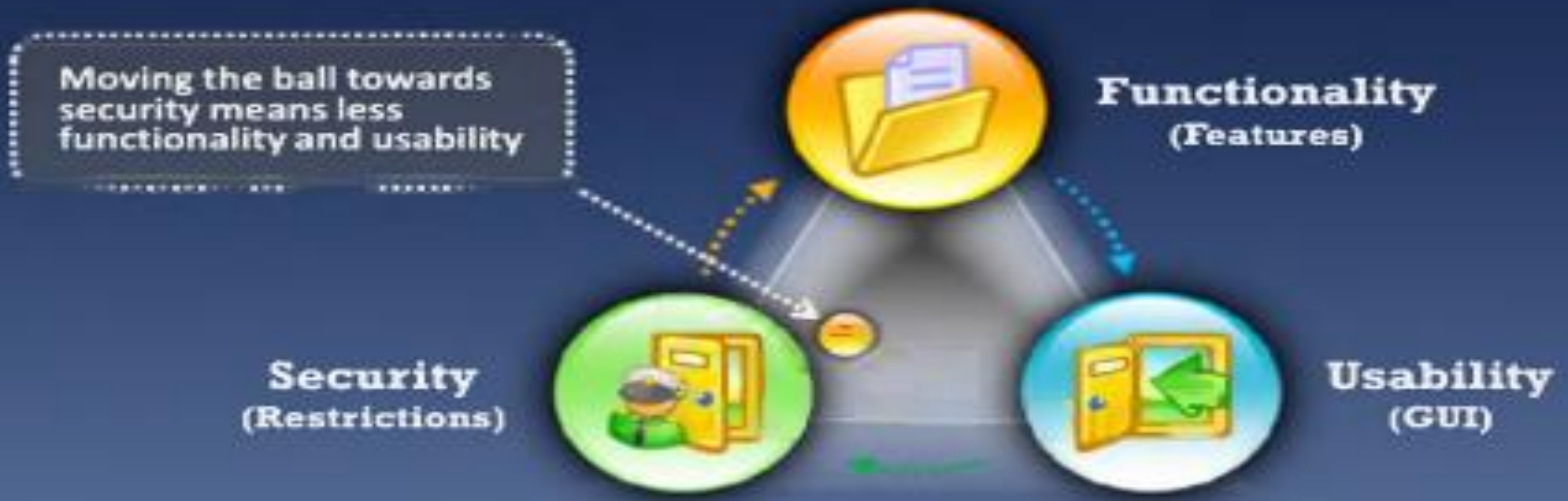
Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users

Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine

Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

The Security, Functionality, and Usability Triangle

Level of security in any system can be defined by the strength of three components:



Moving the ball towards security means less functionality and usability

Functionality
(Features)

Security
(Restrictions)

Usability
(GUI)

Module **Flow**

Information Security Overview

Information Security Threats and Attack Vectors

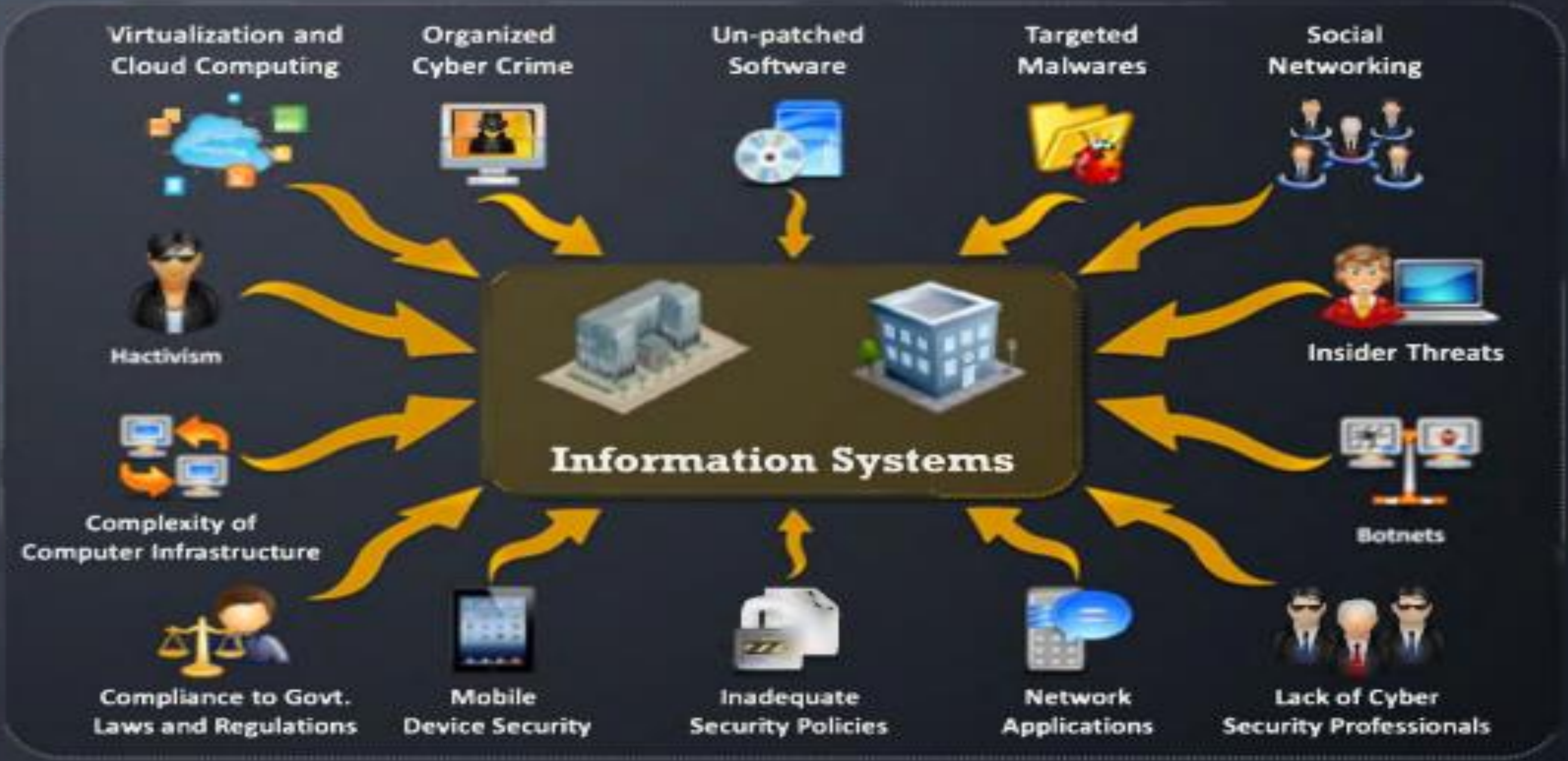
Hacking Concepts

Hacking Phases

Types of Attacks

Information Security Controls

Top Information Security Attack Vectors



Virtualization and Cloud Computing
Organized Cyber Crime
Un-patched Software
Targeted Malwares
Social Networking
Hactivism
Insider Threats
Information Systems
Complexity of Computer Infrastructure
Botnets
Compliance to Govt. Laws and Regulations
Mobile Device Security
Inadequate Security Policies
Network Applications
Lack of Cyber Security Professionals

Motives, Goals, and Objectives of Information Security Attacks

Attacks

Attacks = Motive (Goal) + Method + Vulnerability

Goals

Attackers have motives or goals such as **disrupting business continuity**, information theft, data manipulations, 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

Information Security Threats

Natural Threats

- Natural disasters
- Floods
- Earthquakes
- Hurricanes

Physical Security Threats

- Loss or damage of system resources
- Physical intrusion
- Sabotage , espionage and errors

Human Threats

- Hackers
- Insiders
- Social engineering
- Lack of knowledge and awareness

Information Security Threats

(Cont'd)

Network Threats

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

Host Threats

- Malware attacks
- Target Footprinting
- Password attacks
- Denial of service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Back door Attacks
- Physical security threats

Application Threats

- 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

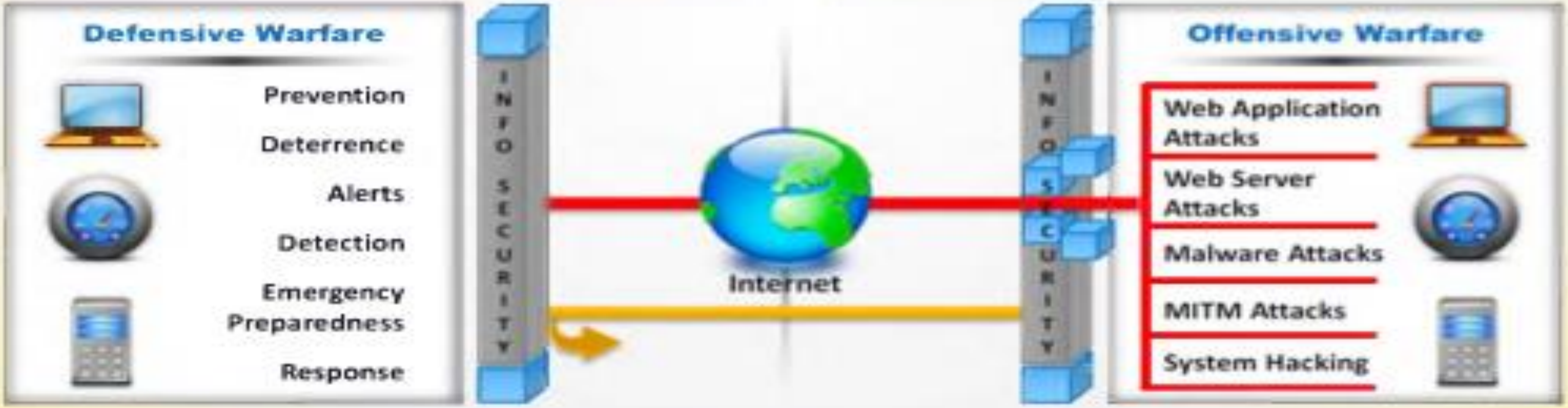
The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to take competitive advantages over an opponent

Defensive Information Warfare

It refers to all strategies and actions to **defend against attacks on ICT assets**

Offensive Information Warfare

It refers to information warfare that involves **attacks against ICT assets** of an opponent



Defensive Warfare

- Prevention
- Deterrence
- Alerts
- Detection
- Emergency Preparedness
- Response

Offensive Warfare

- Web Application Attacks
- Web Server Attacks
- Malware Attacks
- MITM Attacks
- System Hacking

IPv6 Security Threats

Auto Configuration Threats

IPv6 enables auto-configuration of IP networks, which may leave user vulnerable to attacks if the network is not configured properly and securely from the very beginning

Unavailability Reputation-based Protection

Current security solutions use reputation of IP addresses to filter out known sources of malware; vendors will take time to develop reputation-based protection for IPv6

Incompatibility of Logging Systems

IPv6 uses 128-bit addresses, which are stored as a 39-digit string whereas IPv4 addresses stored in a 15-character field; logging solutions designed for IPv4 may not work on IPv6 based networks

Rate Limiting Problem

Administrators use rate limiting strategy to slow down the automated attack tool; however, it is impractical to rate limit at the 128-bit address level

IPv6 Security Threats

(Cont'd)

Default IPv6 Activation

IPv6 may be activated without administrator's knowledge, which will leave IPv4-based security controls ineffective

Complexity of Network Management Tasks

Administrators may adopt easy-to-remember addresses (::10,::20,::F00D, ::C5C0 or simply IPv4 last octet for dual stack) leading to potential vulnerability

Overloading of Perimeter Security Controls

IPv6 has a 40-byte fixed header with an add-on "extension header" that may be chained, which require a complex processing by various security controls systems such as routers, security gateways, firewalls and IDSes

Complexity in Vulnerability Assessment

IPv6's 128-bit address space makes active scanning of infrastructure for unauthorized or vulnerable systems more complex

IPv6 Security Threats (Cont'd)

IPv4 to IPv6 Translation Issues

Translating IPv4 traffic to IPv6 may result in a poor implementation and may provide a potential attack vector

Security Information and Event Management (SIEM) Problems

Every IPv6 host can have multiple IPv6 addresses simultaneously, which leads to complexity of log or event correlation

Denial-of-Service (DOS)

Overloading of network security and control devices can significantly reduce the availability threshold of network resources leading to DoS attacks

Trespassing

IPv6's advanced network discovery features can be exploited by attackers traversing through your network and accessing the restricted resources

Module Flow

Information Security Overview

Information Security Threats and Attack Vectors

Hacking Concepts

Hacking Phases

Types of Attacks

Information Security Controls

Hacking vs. Ethical Hacking

- 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

Effects of Hacking on **Business**

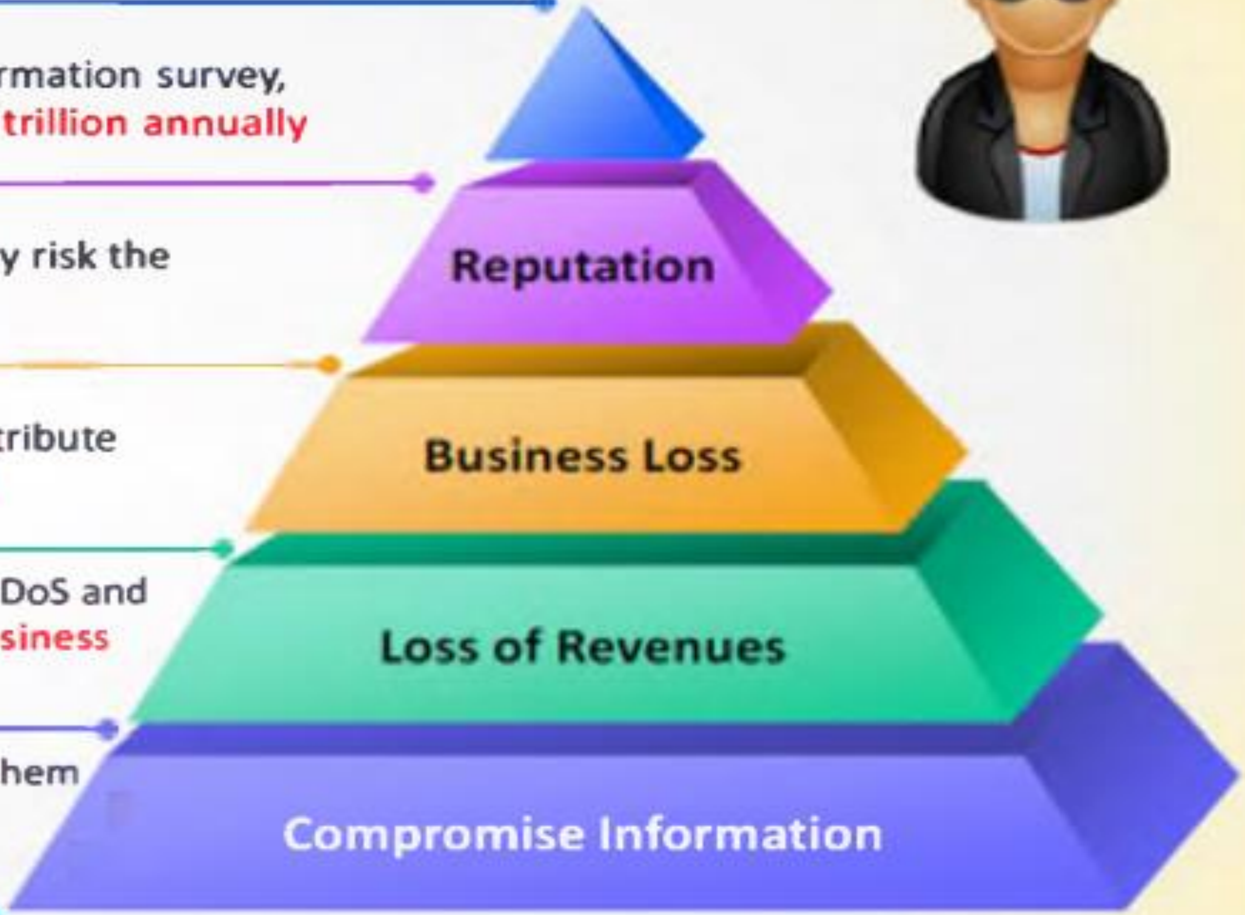
According to the Symantec 2012 State of information survey, information costs businesses worldwide **$1.1 trillion annually**

Theft of **customers' personal information** may risk the business's reputation and invite lawsuits

Hacking can be used to steal, pilfer, and redistribute intellectual property leading to **business loss**

Botnets can be used to launch various types of DoS and other web-based attacks, which may lead to **business down-time** and significant **loss of revenues**

Attackers may **steal corporate secrets** and sell them to competitors, compromise critical financial information, and leak information to rivals



Who Is a Hacker?

Excellent Computer Skills

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

Hobby

For some hackers, hacking is a hobby to see how many computers or networks they can compromise

Do Illegal Things

Their intention can either be to gain knowledge or to poke around to do illegal things

Malicious Intent

Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hacker Classes

Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

Gray Hats

Individuals who work both offensively and defensively at various times

Suicide Hackers

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

Spy Hackers

Individuals employed by the organization to penetrate and gain trade secrets of the competitor

Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

Hacktivism

- Hacktivism is an act of promoting a political agenda by hacking, especially by defacing or disabling websites
- It thrives in the environment where information is easily accessible
- Aims at sending a message through their hacking activities and gaining visibility for their cause
- Common targets include government agencies, multinational corporations, or any other entity perceived as bad or wrong by these groups or individuals
- It remains a fact, however, that gaining unauthorized access is a crime, no matter what the intention is
- Hacktivism is motivated by revenge, political or social reasons, ideology, vandalism, protest, and a desire to humiliate victims

Module Flow

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts
- **Hacking Phases**
- Types of Attacks
- Information Security Controls

Hacking Phases

Reconn-aissance
Scanning
Gaining Access
Mainta-ining Access
Clearing Tracks

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

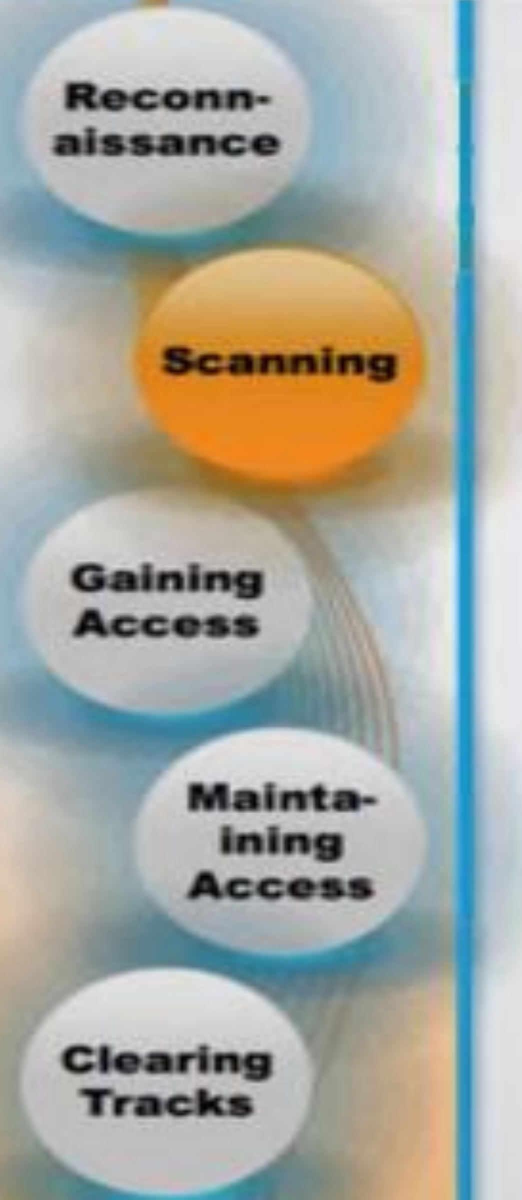
Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department

Hacking Phases
(Cont'd)


Reconn- aissance

Scanning

Gaining Access

Mainta- ining Access

Clearing Tracks

Pre-Attack Phase

Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance

Port Scanner

Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc.

Extract Information

Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack

Hacking Phases
(Cont'd)

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

I Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network

II The attacker can gain access at the operating system level, application level, or network level

III The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

IV Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.

Hacking Phases

(Cont'd)

Reconn-aissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system

Attackers use the compromised system to launch further attacks

Hacking Phases

(Cont'd)

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- **Clearing Tracks**

Hiding

Covering tracks refers to the activities carried out by an attacker to **hide malicious acts**

Intentions

The attacker's intentions include: Continuing access to the victim's system, **remaining unnoticed and uncaught**, deleting evidence that might lead to his prosecution

Overwriting

The attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover tracks to hide their identity

Module **Flow**

Information Security Overview

Information Security Threats and Attack Vectors

Hacking Concepts

Hacking Phases

Types of Attacks

Information Security Controls

Types of Attacks on a System

- Attackers exploit vulnerabilities in an information system to gain unauthorized access to the system resources
- The unauthorized access may result in loss, damage or theft of sensitive information

Types of Attacks

I Operating System Attacks

II Misconfiguration Attacks

III Application Level Attacks

IV Shrink Wrap Code Attacks

Operating System Attacks

- Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to gain access to a network system

Gaining Access

- Buffer overflow vulnerabilities
- Bugs in operating system
- Unpatched operating system

OS Vulnerabilities

- Exploiting specific protocol implementations
- Attacking built-in authentication systems
- Breaking file-system security
- Cracking passwords and encryption mechanisms

Operating System Attacks

Misconfiguration Attacks

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 Attacks

Attackers exploit the vulnerabilities in applications running on organizations' information system to **gain unauthorized access** and **steal or manipulate data**

Poor or nonexistent error checking in applications leads to:

- **Buffer overflow attacks**
- **Sensitive information disclosure**
- **Cross-site scripting**
- **Session hijacking and man-in-the-middle attacks**
- **Denial-of-service attacks**
- **SQL injection attacks**

Other application-level attacks include:

- **Phishing**
- **Session hijacking**
- **Man-in-the-middle attack**
- **Parameter/form tampering**
- **Directory traversal attacks**

Examples of Application-Level Attacks

Session Hijacking

Vulnerable Code

```
<configuration>
 <system.web>
   <authentication mode="Forms">
   <forms cookieless="UseUri">
 </system.web>
</configuration>
```

Attacker may exploit session information in the vulnerable code to perform session hijacking

Secure Code

```
<configuration>
 <system.web>
   <authentication mode="Forms">
   <forms cookieless="UseCookies">
 </system.web>
</configuration>
```

The code can be secured by using `UseCookies` instead of `UseUri`

Denial-of-Service

Vulnerable Code

```
Statement stmnt = conn.createStatement ();
ResultSet rsltset = stmnt.executeQuery ();
stmnt.close ();
```

The code below is vulnerable to denial-of-service attack, as it fails to release connection resource

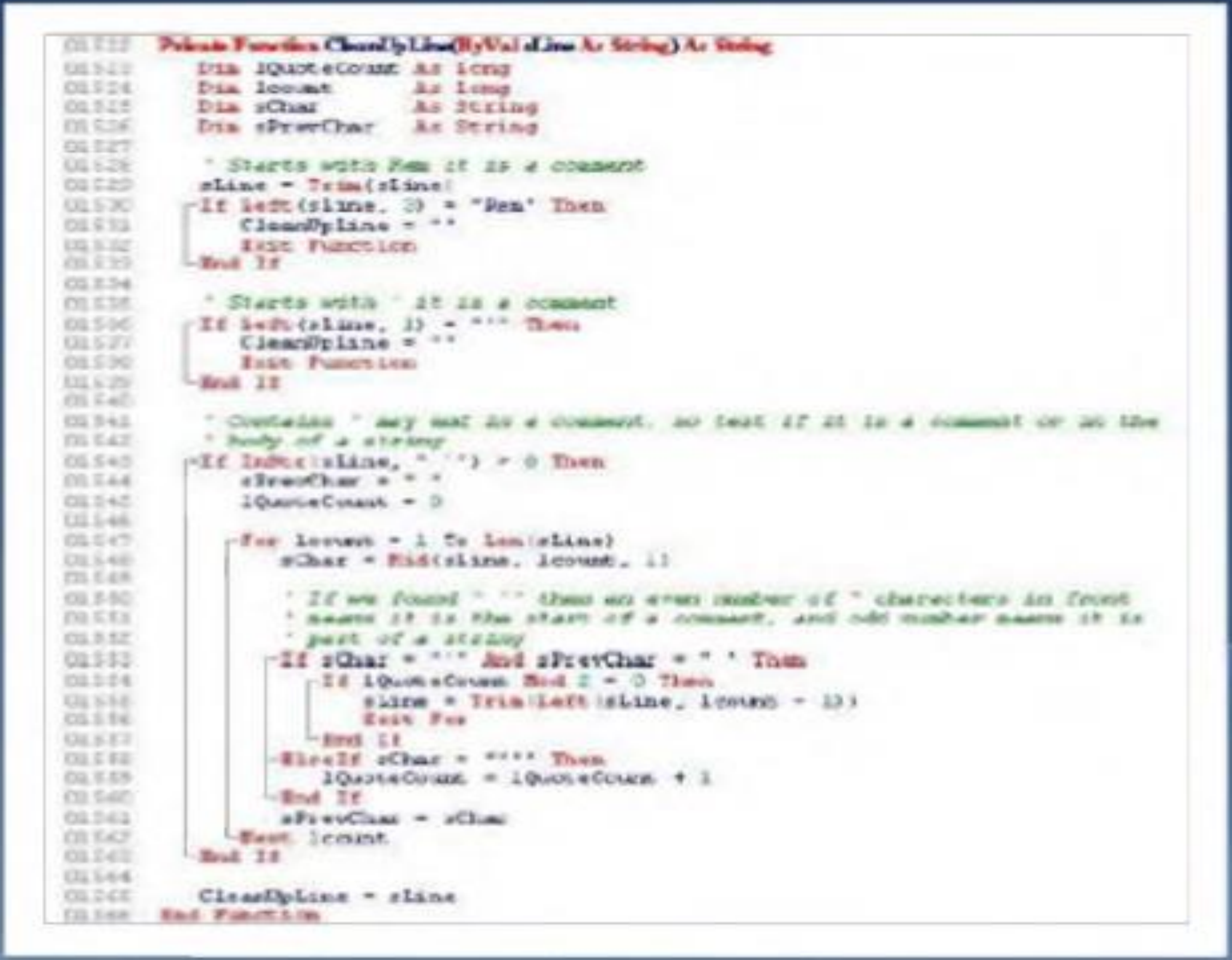
Secure Code

```
Statement stmnt;
try {stmnt = conn.createStatement ();
stmnt.executeQuery (); }
finally {
If (stmnt! = null) {
try { stmnt.close ();
} catch (SQLException sqlexp) { }
} catch (SQLException sqlexp) { }
```

The code can be secured by releasing the resources in a finally block

Shrink Wrap Code Attacks

- 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



```
Private Function CleanUpLine(ByVal sLine As String) As String
    Dim lQuoteCount As Long
    Dim lcount      As Long
    Dim sChar       As String
    Dim sPrevChar   As String

    ' Starts with Rem it is a comment
    sLine = Trim(sLine)
    If Left(sLine, 3) = "Rem" Then
        CleanUpline = ""
        Exit Function
    End If

    ' Starts with ' it is a comment
    If Left(sLine, 1) = "'" Then
        CleanUpline = ""
        Exit Function
    End If

    ' Contains ' may not be a comment, so test if it is a comment or in the
    ' body of a string
    If InStr(sLine, "'") > 0 Then
        sPrevChar = " "
        lQuoteCount = 0

        For lcount = 1 To Len(sLine)
            sChar = Mid(sLine, lcount, 1)

            ' If we found ' '' then an even number of " characters in front
            ' means it is the start of a comment, and odd number means it is
            ' part of a string
            If sChar = "'" And sPrevChar = " " Then
                If lQuoteCount Mod 2 = 0 Then
                    sLine = Trim(Left(sLine, lcount - 1))
                    Exit For
                End If
            ElseIf sChar = """" Then
                lQuoteCount = lQuoteCount + 1
            End If
            sPrevChar = sChar
        Next lcount
    End If

    CleanUpLine = sLine
End Function
```

Module Flow

Information Security Overview

Information Security Threats and Attack Vectors

Hacking Concepts

Hacking Phases

Types of Attacks

Information Security Controls

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary because it allows the countering of attacks from malicious hackers by anticipating methods they can use to break into a system

Reasons why Organizations Recruit Ethical Hackers

- To prevent hackers from gaining access to information breaches
- To fight against terrorism and national security breaches
- To build a system that avoids hackers from penetrating
- To test if organization's security settings are in fact secure

Ethical Hackers Try to Answer the Following Questions

- What can the intruder see on the target system? (Reconnaissance and Scanning phases)
- What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
- Does anyone at the target notice the intruders' attempts or successes? (Reconnaissance and Covering Tracks phases)
- If all the components of information system are adequately protected, updated, and patched
- How much effort, time, and money is required to obtain adequate protection?
- Does the information security measures are in compliance to industry and legal standards?

Scope and Limitations of Ethical Hacking

Scope

- Ethical hacking is a crucial component of risk assessment, auditing, counterfraud, best practices, and good governance
- It is used to identify risks and highlight the remedial actions, and also reduces information and communications technology (ICT) costs by resolving those vulnerabilities

Limitations

- However, unless the businesses first know what it is at that they are looking for and why they are hiring an outside vendor to hack systems in the first place, chances are there would not be much to gain from the experience
- An ethical hacker thus can only help the organization to better understand their security system, but it is up to the organization to place the right guards on the network

Skills of an Ethical Hacker

Platform Knowledge

Has in-depth knowledge of major operating environments, such as Windows, Unix, and Linux

Network Knowledge

Has in-depth knowledge of networking concepts, technologies and related hardware and software

Computer Expert

Should be a computer expert adept at technical domains

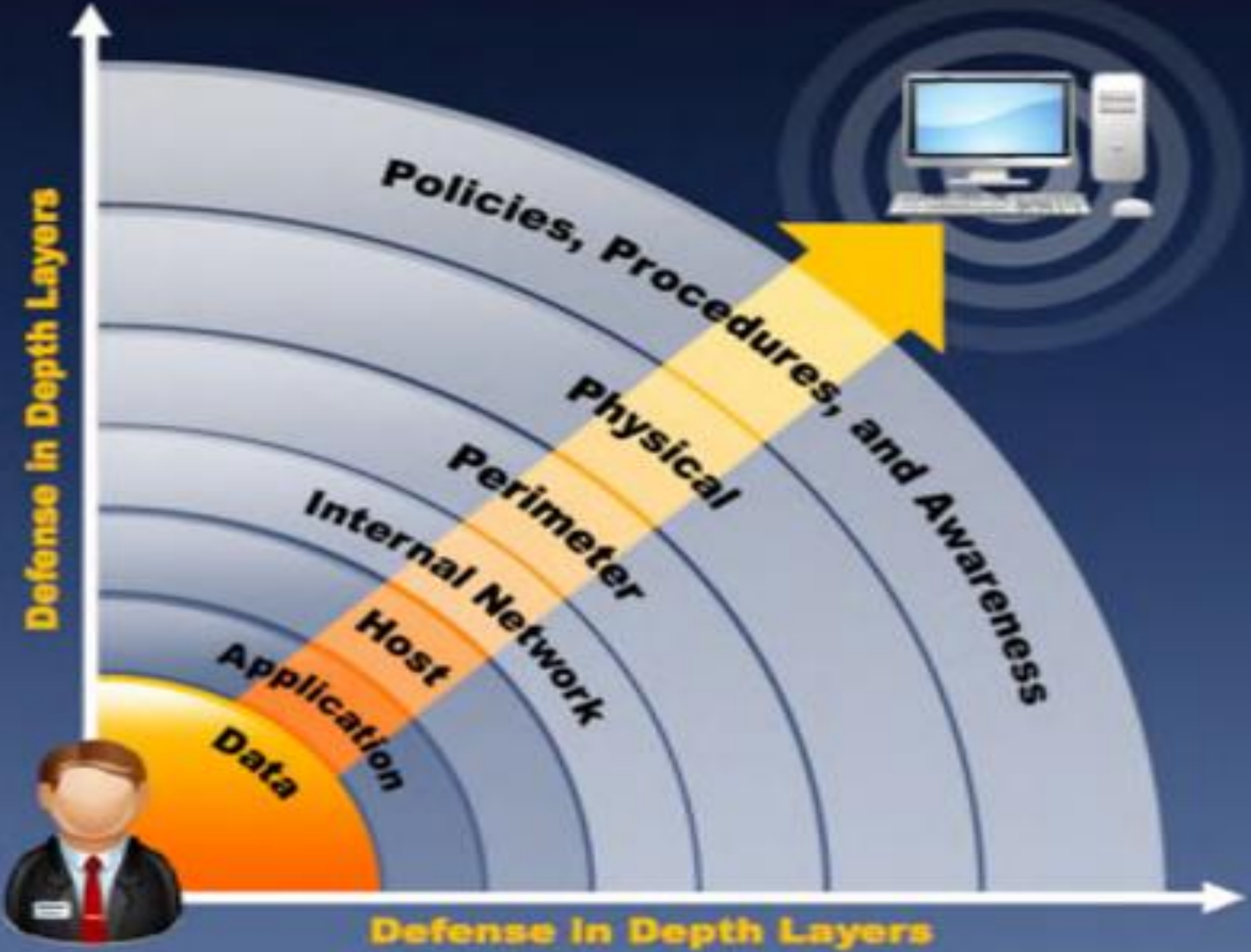
Security Knowledge

Has knowledge of security areas and related issues

Technical Knowledge

Has “high technical” knowledge to launch the sophisticated attacks

Defense in Depth



- 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 Management Process

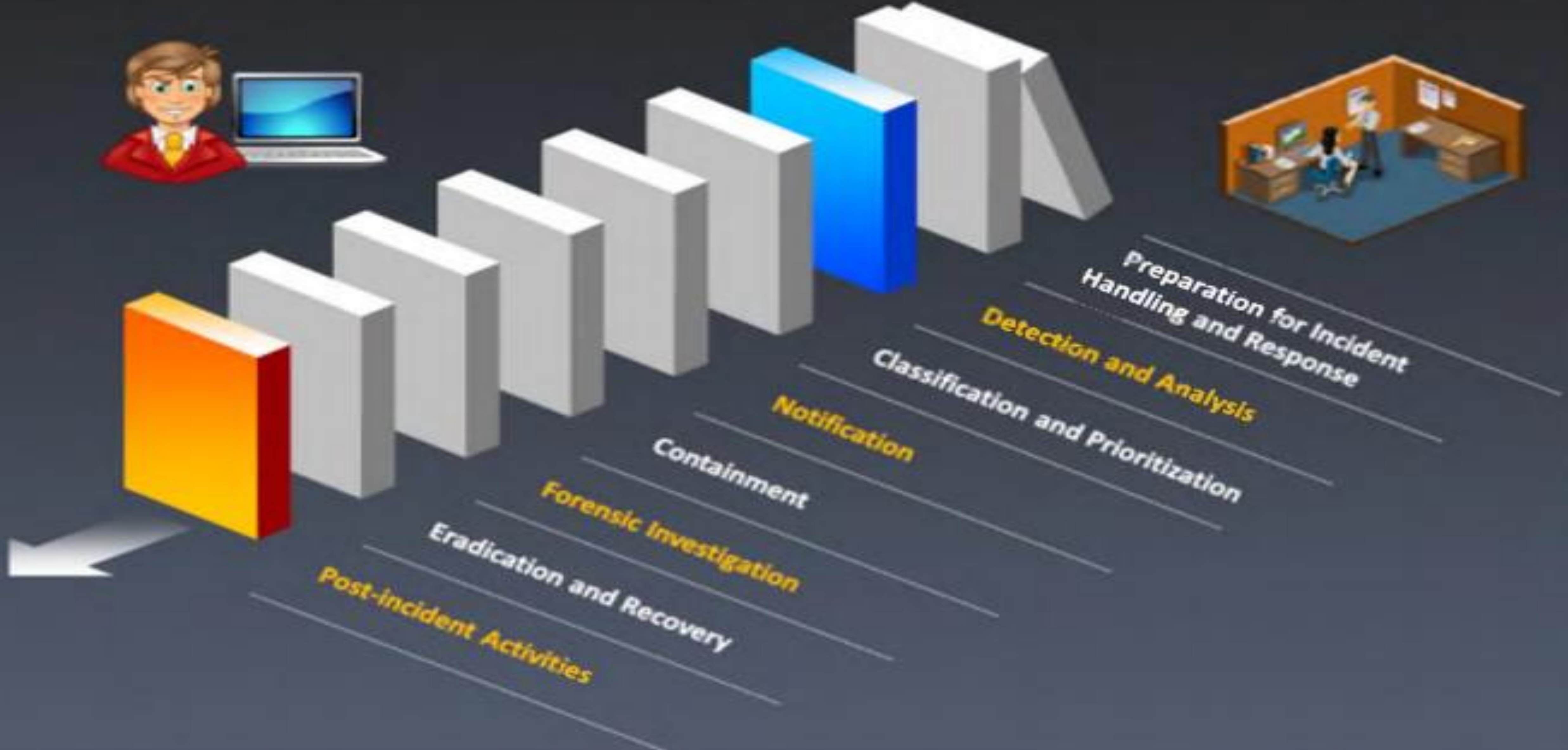
Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore normal service operations as quickly as possible and prevent future reoccurrence of the incident

Purpose of incident management process

1. Improves service quality
2. Pro-active problem resolution
3. Reduces impact of incidents on business/organization
4. Meets service availability requirements
5. Increases staff efficiency and productivity
6. Improves user/customer satisfaction
7. Assists in handling future incidents

Incident Management Process

(Cont'd)



Preparation for Incident Handling and Response

Detection and Analysis

Classification and Prioritization

Notification

Containment

Forensic Investigation

Eradication and Recovery

Post-incident Activities

Information Security Policies

- 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

Classification of Security Policies

User Policy

- Defines what kind of user is using the network
  - Defines the limitations that are applied on users to secure the network
    - Ex: Password management policy

IT Policy

- Designed for IT department to keep the network secure and stable
- Ex: Backup policies, server configuration, patch update, and modification policies, firewall policies

General Policies

- Defines the responsibility for general business purposes
- Ex: High level program policy, business continuity plans, crisis management, disaster recovery

Partner Policy

Policy that is defined among a group of partners

Issue Specific Policies

- Recognize specific areas of concern and describe the organization's status for top level management
- Ex: Physical security policy, personnel security policy, communications security

Structure and Contents of Security Policies

Security Policy Structure

- Detailed description of the policy issues
- Description about the status of the policy
- Applicability of the policy to the environment
- Functionalities of those affected by the policy
- Compatibility level of the policy is necessary
- End-consequences of non-compliance

Contents of Security Policies

- High-level security requirements: Requirement of a system to implement security policies
- Policy description: Focuses on security disciplines, safeguards, procedures, continuity of operations, and documentation
- Security concept of operation: Defines the roles, responsibilities, and functions of a security policy
- Allocation of security enforcement to architecture elements: Provides a computer system architecture allocation to each system of the program

Types of Security Policies

Promiscuous Policy

- No restrictions on Internet or remote access

Permissive Policy

- Policy begins wide open and only known dangerous services/attacks blocked, which makes it difficult to keep up with current exploits

Prudent Policy

- It provides maximum security while allowing known but necessary dangers
- It blocks all services and only safe/ necessary services are enabled individually; everything is logged

Paranoid Policy

- It forbids everything, no Internet connection, or severely limited Internet usage

Steps to Create and Implement Security Policies

1 Perform risk assessment to identify risks to the organization's assets

2 Learn from standard guidelines and other organizations

3 Include senior management and all other staff in policy development

4 Set clear penalties and enforce them and also review and update of the security policy

5 Make final version available to all of the staff in the organization

6 Ensure every member of your staff read, sign, and understand the policy

7 Install the tools you need to enforce policies

8 Train your employees and educate them about the policy

Examples of Security Policies

Acceptable-Use Policy	It defines the acceptable use of system resources
User-Account Policy	It defines the account creation process and authority, rights and responsibilities of user accounts
Remote-Access Policy	It defines who can have remote access, and defines access medium and remote access security controls
Information-Protection Policy	It defines the sensitivity levels of information, who may have access, how is it stored and transmitted, and how should it be deleted from storage media
Firewall-Management Policy	It defines access, management, and monitoring of firewalls in the organization
Special-Access Policy	This policy defines the terms and conditions of granting special access to system resources
Network-Connection Policy	It defines who can install new resources on the network, approve the installation of new devices, document network changes, etc.
Email Security Policy	It is created to govern the proper usage of corporate email
Passwords Policy	It provides guidelines for using strong password protection on organization's resources

Vulnerability Research

- The process of **discovering vulnerabilities and design flaws** that will open an operating system and its applications to attack or misuse
- Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)

An administrator needs vulnerability research:

1. To gather information about security trends, threats, and attacks
2. To find weaknesses and alert the network administrator before a network attack
3. To get information that helps to prevent the security problems
4. To know how to recover from a network attack

Vulnerability Research Websites

CodeRed Center
http://www.eccouncil.org

TechNet
http://blogs.technet.com

Security Magazine
http://www.securitymagazine.com

SecurityFocus
http://www.securityfocus.com

Help Net Security
http://www.net-security.org

HackerStorm
http://www.hackerstorm.co.uk

SC Magazine
http://www.scmagazine.com

Computerworld
http://www.computerworld.com

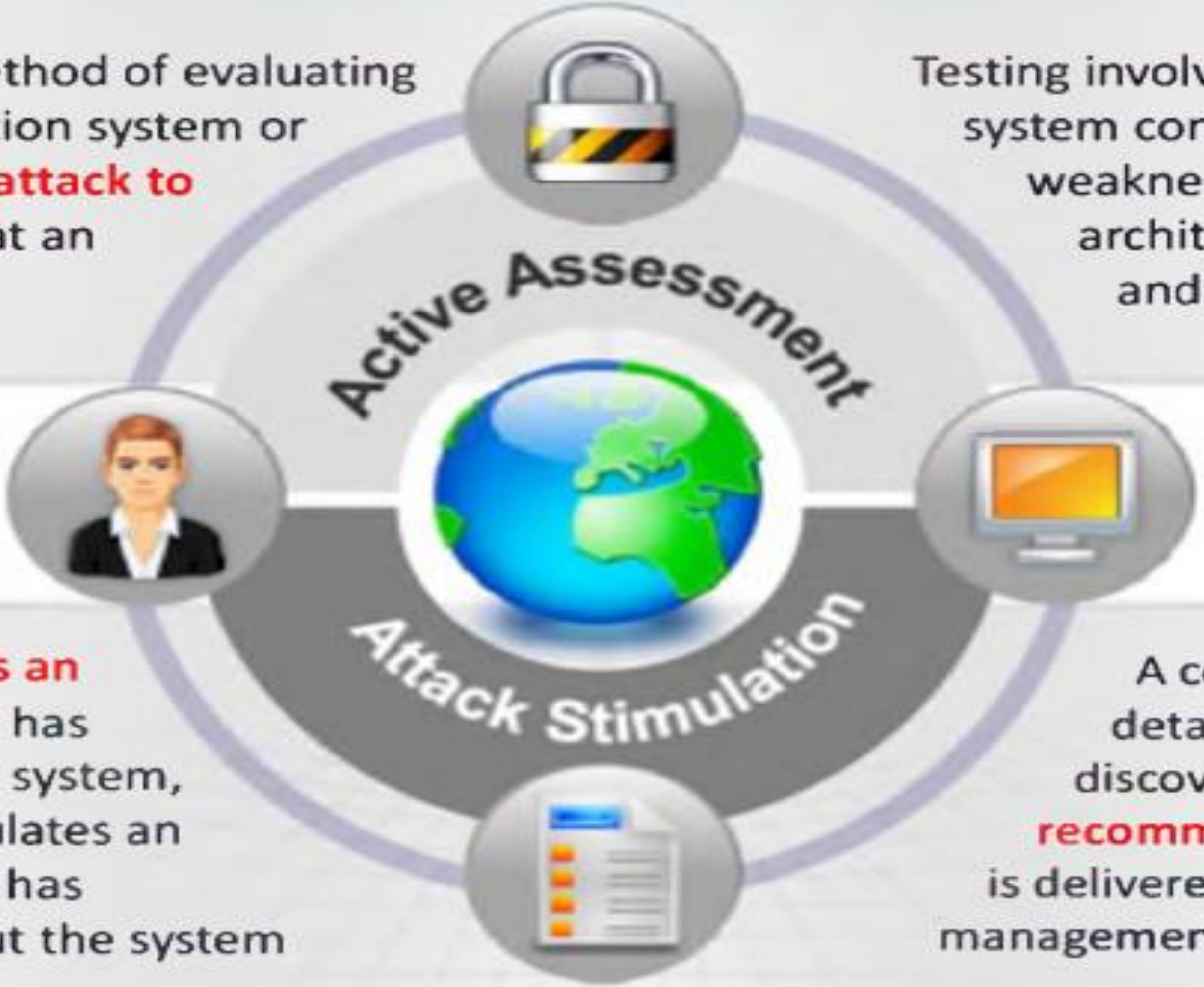
HackerJournals
http://www.hackerjournals.com

WindowsSecurity Blogs
http://blogs.windowsecurity.com

What Is Penetration Testing?

Penetration testing is a method of evaluating the security of an information system or network by **simulating an attack to find out vulnerabilities** that an attacker could exploit

Testing involves **active analysis** of system configurations, design weaknesses, network architecture, technical flaws, and vulnerabilities



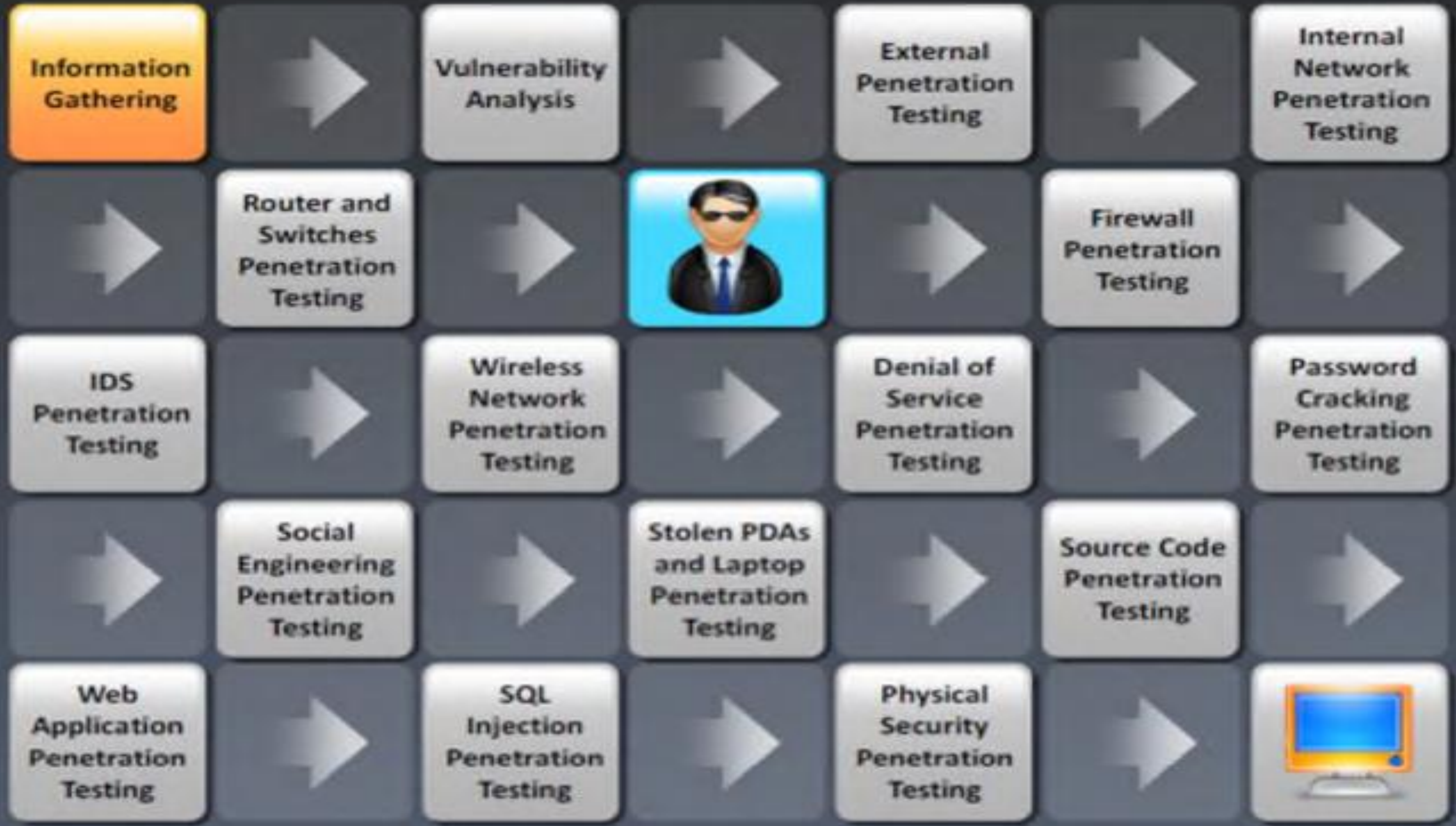
Black box testing **simulates an attack** from someone who has **no prior knowledge** of the system, and white box testing simulates an attack from someone who has **complete knowledge** about the system

A comprehensive report with details of vulnerabilities discovered and suite of **recommended countermeasures** is delivered to the executive, management, and technical audiences

Why Penetration Testing

- Identify the threats facing an organization's information assets
- Reduce an organization's expenditure on IT security and enhance Return On Security Investment (ROSI) by identifying and remediating vulnerabilities or weaknesses
- Provide assurance with comprehensive assessment of organization's security including policy, procedure, design, and Implementation
- Gain and maintain certification to an industry regulation (BS7799, HIPAA etc.)
- Adopt best practices in compliance to legal and industry regulations
- For testing and validating the efficiency of security protections and controls
- For changing or upgrading existing infrastructure of software, hardware, or network design
- Focus on high-severity vulnerabilities and emphasize application-level security issues to development teams and management
- Provide a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- Evaluate the efficiency of network security devices such as firewalls, routers, and web servers

Penetration Testing Methodology



Information Gathering

Vulnerability Analysis

External Penetration Testing

Internal Network Penetration Testing

Router and Switches Penetration Testing

Firewall Penetration Testing

IDS Penetration Testing

Wireless Network Penetration Testing

Denial of Service Penetration Testing

Password Cracking Penetration Testing

Social Engineering Penetration Testing

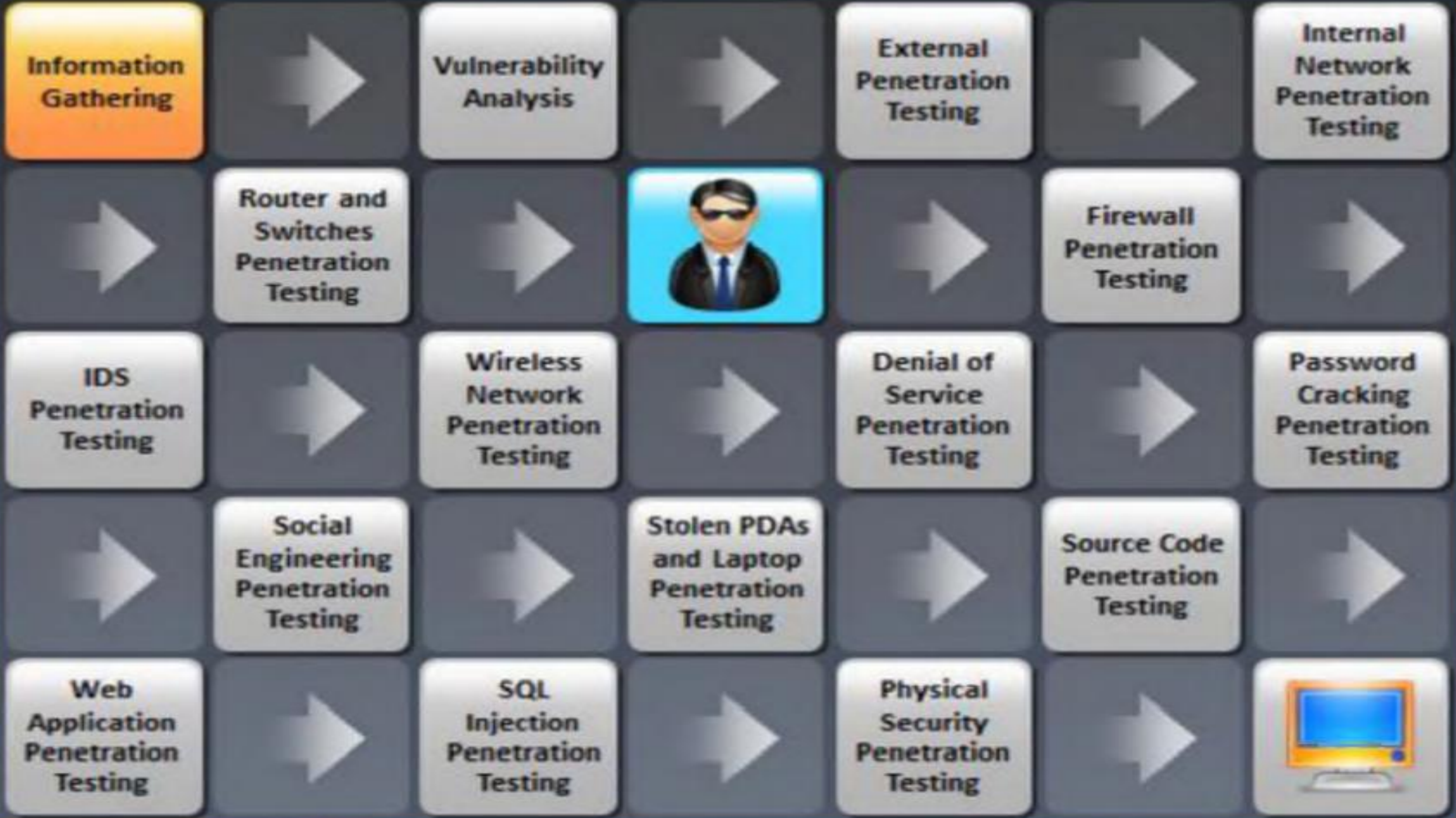
Stolen PDAs and Laptop Penetration Testing

Source Code Penetration Testing

Web Application Penetration Testing

SQL Injection Penetration Testing

Physical Security Penetration Testing



Information Gathering

Vulnerability Analysis

External Penetration Testing

Internal Network Penetration Testing

Router and Switches Penetration Testing

Firewall Penetration Testing

IDS Penetration Testing

Wireless Network Penetration Testing

Denial of Service Penetration Testing

Password Cracking Penetration Testing

Social Engineering Penetration Testing

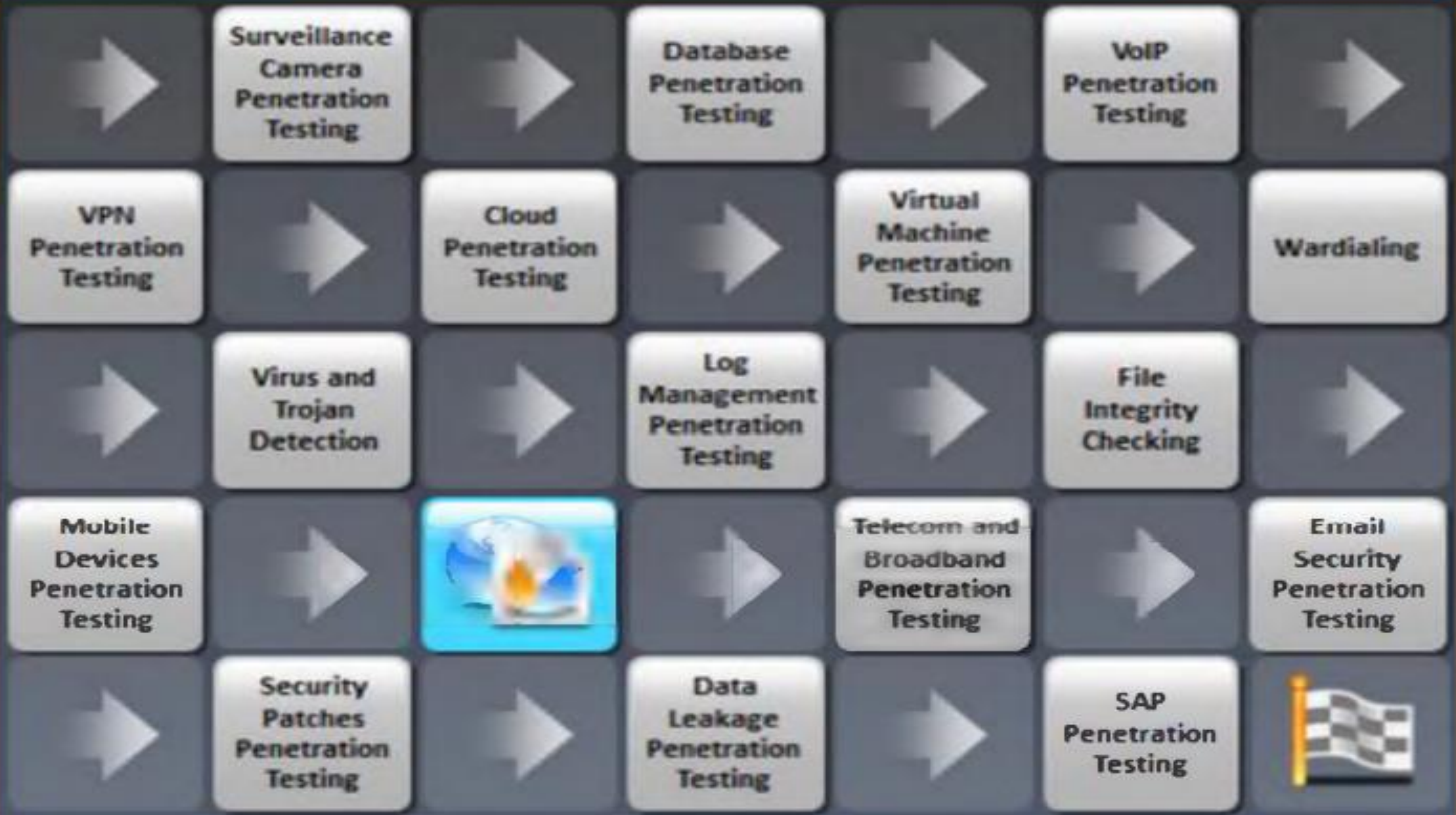
Stolen PDAs and Laptop Penetration Testing

Source Code Penetration Testing

Web Application Penetration Testing

SQL Injection Penetration Testing

Physical Security Penetration Testing



Surveillance Camera Penetration Testing

Database Penetration Testing

VoIP Penetration Testing

VPN Penetration Testing

Cloud Penetration Testing

Virtual Machine Penetration Testing

Wardialing

Virus and Trojan Detection

Log Management Penetration Testing

File Integrity Checking

Mobile Devices Penetration Testing

Telecom and Broadband Penetration Testing

Email Security Penetration Testing

Security Patches Penetration Testing

Data Leakage Penetration Testing

SAP Penetration Testing

Module Summary

- Complexity of security requirements is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- Hacker or cracker is one who accesses a computer system by evading its security system
- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security
- Ethical hackers help organization to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities
- Ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and technical knowledge skills
- Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance