Introduction to Ethical Hacking

Prof. Dr. M. Ameer Ali

Professor & Chairman

Department of Computer Science & Engineering

Bangladesh University of Business and Technology (BUBT)

European Union

- Overview of Current Security Trends
- Understanding the Elements of Information Security
- Understanding Information Security Threats and Attack Vectors
- Overview of Hacking Concepts, Types, and Phases
- Understanding Ethical Hacking Concepts and Scope

- Overview of Information Security Management and Defense-in-Depth
- Overview of Policies, Procedures, and Awareness
- Overview of Physical Security and Controls
- Understanding Incident Management Process
- Overview of Vulnerability Assessment and Penetration Testing
- Overview of Information Security Acts and Laws

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. Information Security Laws and Standards

Course Outcome

- Web and Network Penetration Testing
- Network scanning
- Ethical hacking including website and databases
- SQL injection
- Designing secure web application

Career

- Security Officer
- Security Professional

Cyber Crime

- Offences against computer data and systems
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

Types of Cyber Crime

- Hacking
- Denial of service attack
- Virus Dissemination
- Computer Vandalism
- Cyber Terrorism
- Software Piracy

Motivations of Hacking

Attacks = Motive (Goal) + Method + Vulnerability

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

Motives Behind Information Security Attacks

- Disrupting business continuity
- Information theft
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge

European Union

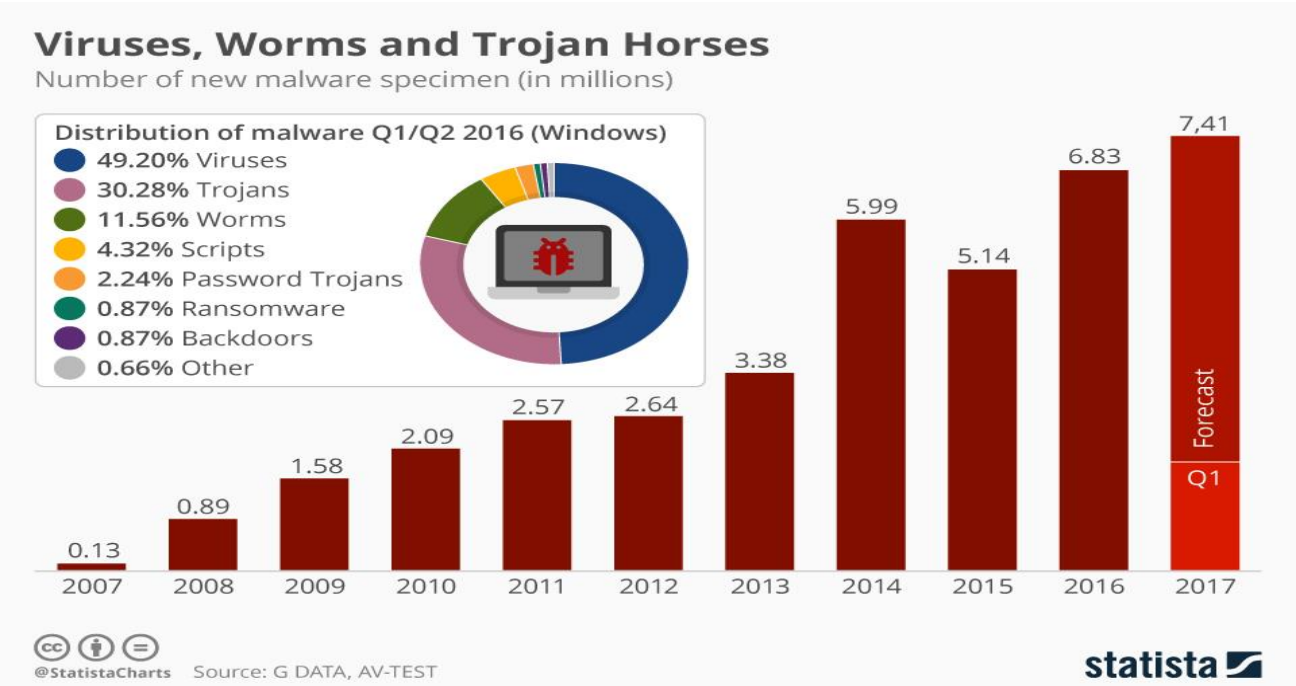
Asi@Connect

TEIN CC COOPERATION CENTER

BdREN

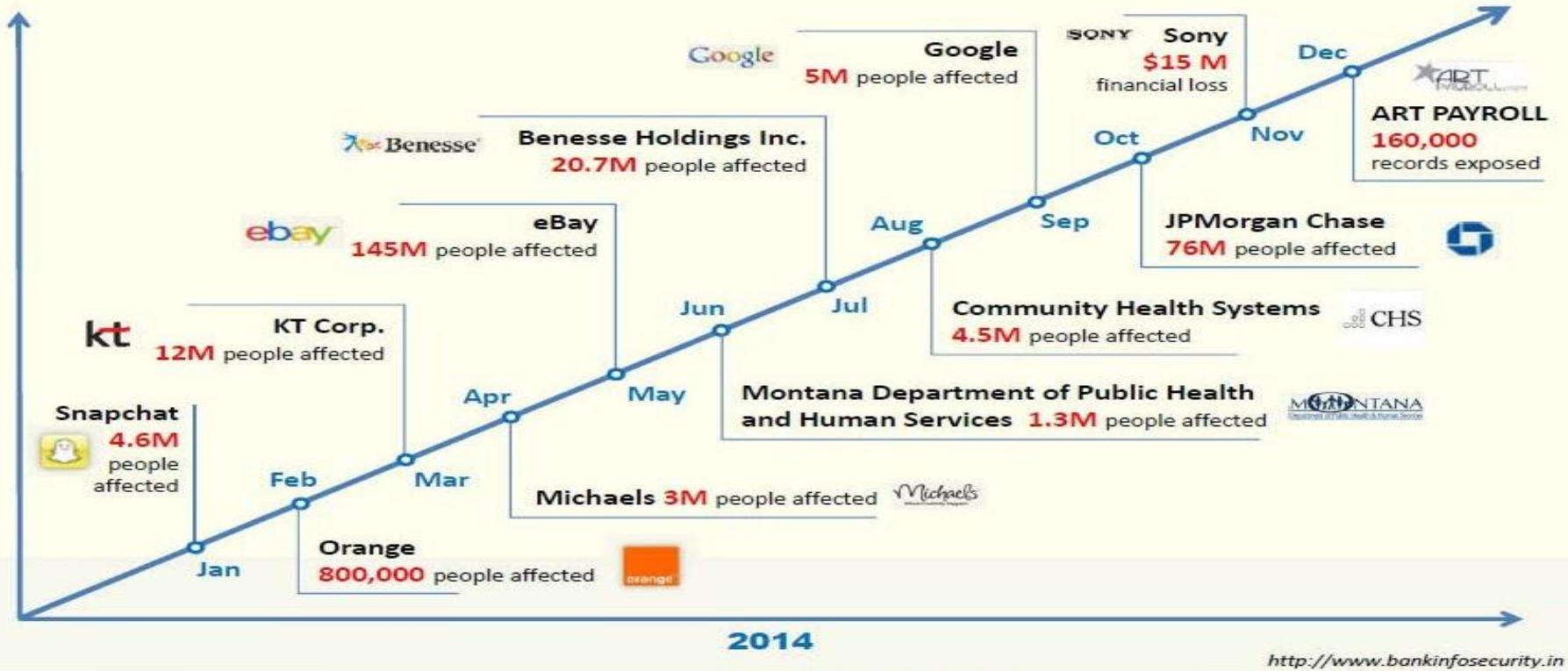
NORDUnet Nordic Gateway for Research & Education

Distributed Attacks

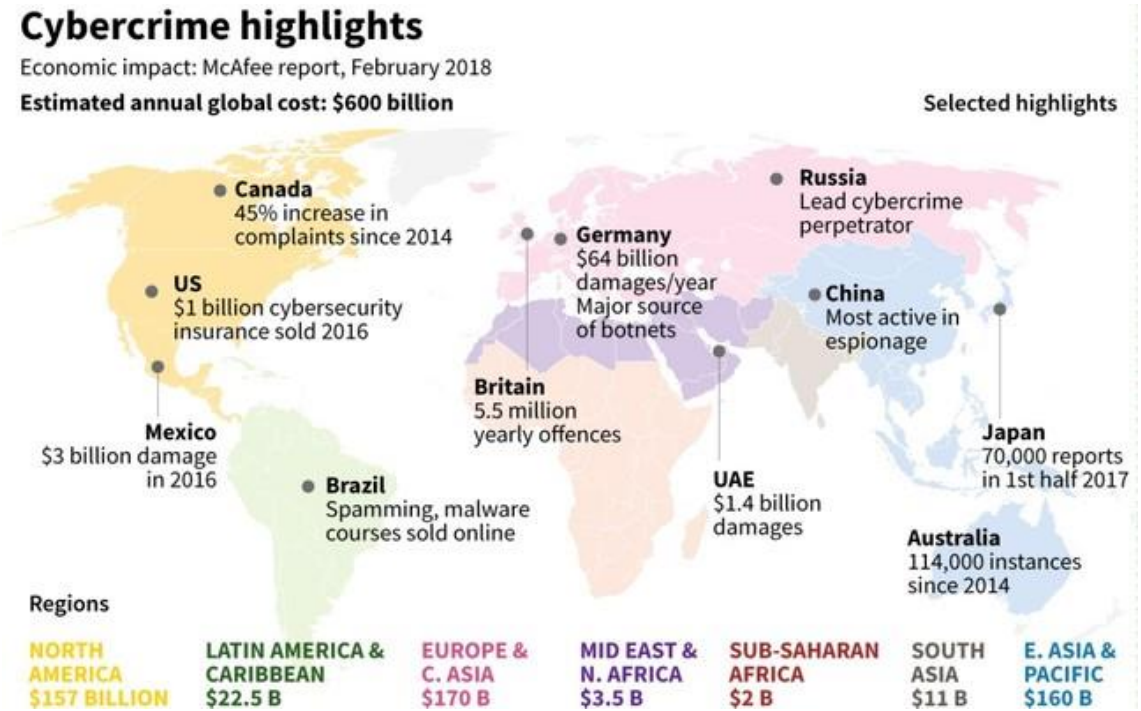


Incidents


56 million debit and credit card numbers were stolen
THE HOME DEPOT
Incident occurred due to custom-built malware
http://krebsonsecurity.com


Snapchat
4.6M people affected
Jan
KT Corp.
12M people affected
Feb
eBay
145M people affected
Mar
Benesse Holdings Inc.
20.7M people affected
Apr
Google
5M people affected
May
Orange
800,000 people affected
Michaels 3M people affected
Jun
Montana Department of Public Health and Human Services 1.3M people affected
Jul
Community Health Systems
4.5M people affected
Aug
JPMorgan Chase
76M people affected
Sep
Sony
$15 M financial loss
Oct
ART PAYROLL
160,000 records exposed
Nov
Dec
2014
http://www.bankinfosecurity.in

Cyber Crime Global Cost



Cyber Law

- Very Strict Law
- Borderless
- Can arrest without warrant
- No witness is required

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of " fair use" Online Copyright Infringement Liability Limitation Act	http://www.copyright.gov
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Freedom of Information Act (FOIA)	http://www.foia.gov
	Computer Fraud and Abuse Act	http://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	http://www.ftc.gov

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	http://www.comlaw.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	http://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	http://home.heinonline.org
	Industrial Design Protection Act	http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	http://www.wipo.int
	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

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

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

Types of Hacker

Ethical Hacking

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

Ethical hackers performs security assessment of their organization **with the permission of concerned authorities**

Ethical Hacking

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**?

Are the **information security measures** in compliance to industry and legal standards?

Skills of Hacker

1 Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has "**high technical**" **knowledge** to launch the sophisticated attacks

2 Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- **Ability to learn** and adapt new technologies quickly
- **Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**

Hacking Terminology

Hack Value

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

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 event compromising the security of the system

Daisy Chaining

It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information

Exploit

A breach of IT system security through vulnerabilities

Doxing

Publishing personally identifiable information about an individual collected from publicly available databases and social media

Payload

Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer

Bot

A "bot" is a software application that can be controlled remotely to execute or automate predefined tasks

- 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

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

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

Port Scanner

Extract Information

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

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

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

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

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

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

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

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

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

04 Attackers use the compromised system to **launch further attacks**

01

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

02

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

03

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

Attackers always cover tracks to hide their identity

- 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 recurrence of the incident

1. Preparation for Incident Handling and Response
2. Detection and Analysis
3. Classification and Prioritization
4. Notification
5. Containment
6. Forensic Investigation
7. Eradication and Recovery
8. Post-incident Activities

Responsibility of Incident Management Team

Managing security issues by taking a **proactive approach** towards the customers' security vulnerabilities and **by responding effectively** to potential information security incidents

Providing a **single point of contact** for reporting security incidents and issues

Developing or **reviewing** the processes and procedures that must be followed in response to an incident

Reviewing **changes in legal and regulatory requirements** to ensure that all processes and procedures are valid

Managing the response to an incident and ensuring that **all procedures are followed** correctly in order **to minimize** and **control the damage**

Reviewing existing controls and recommending steps and technologies to **prevent future security incidents**

Identifying and **analyzing** what has happened during an incident, including the impact and threat

Establishing **relationship with local law enforcement agency**, **government agencies**, key partners, and suppliers

Vulnerability Assessment

Vulnerability Assessment Types

Network Vulnerability Assessment Method

Network Vulnerability Assessment Method

Phase IV - Evaluation

- Determine the probability of exploitation of **identified vulnerabilities**
- Identify the gaps between **existing and required security measures**
- **Determine the controls** required to mitigate the identified vulnerabilities
- **Identify upgrades** required to the network vulnerability assessment process

Phase V - Generating Reports

- The result of analysis must be presented in a **draft report** to be evaluated for further variations
- **Report should contain:**
  - Task rendered by each team member
  - Methods used and findings
  - General and specific recommendations
  - Terms used and their definitions
  - Information collected from all the phases
- All documents must be **stored in a central database** for generating the final report

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:

To gather information about **security trends**, **threats**, and **attacks**

To find **weaknesses**, and alert the network administrator before a **network attack**

To know **how to recover** from a network attack

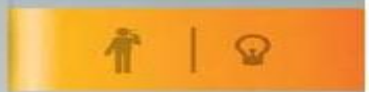
To **get information** that helps to prevent the security problems

Vulnerability Research Websites

Penetration Testing

01

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

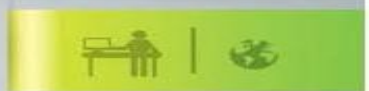


02

Security measures are actively analyzed for design weaknesses, technical flaws and vulnerabilities

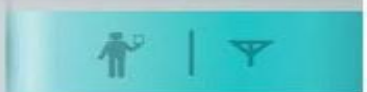
03

A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited



04

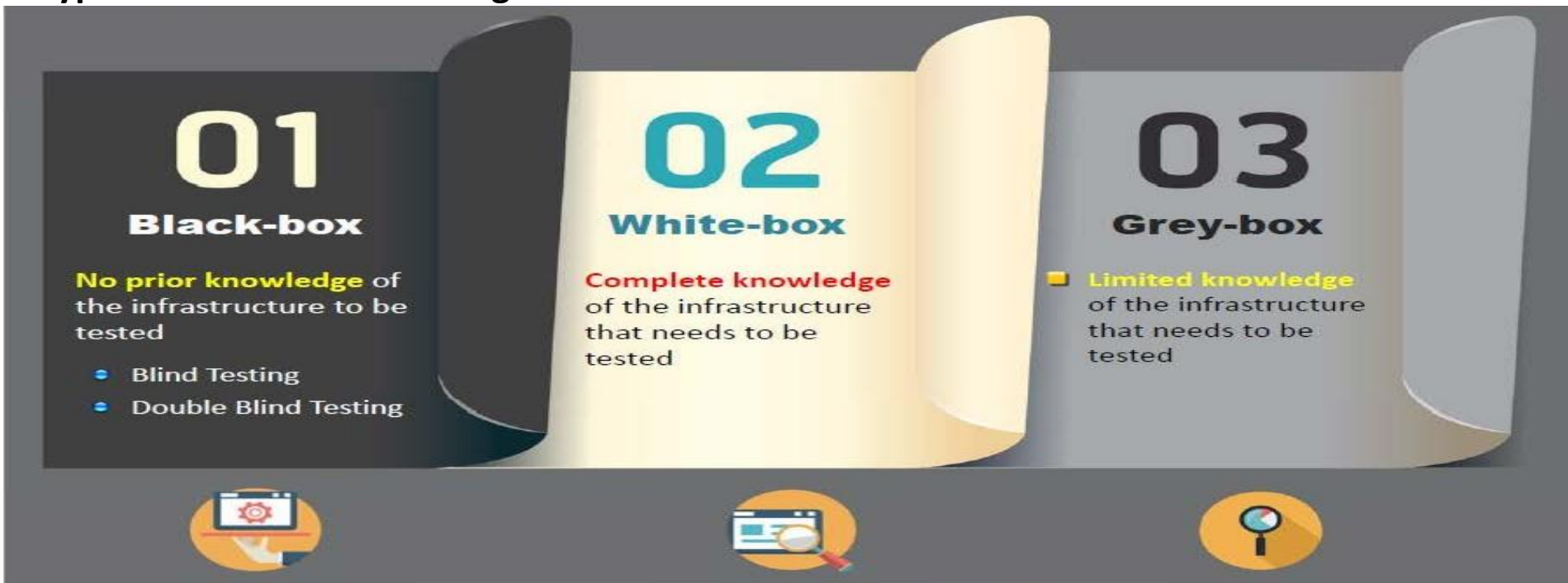
The results are delivered comprehensively in a **report**, to executive management and technical audiences



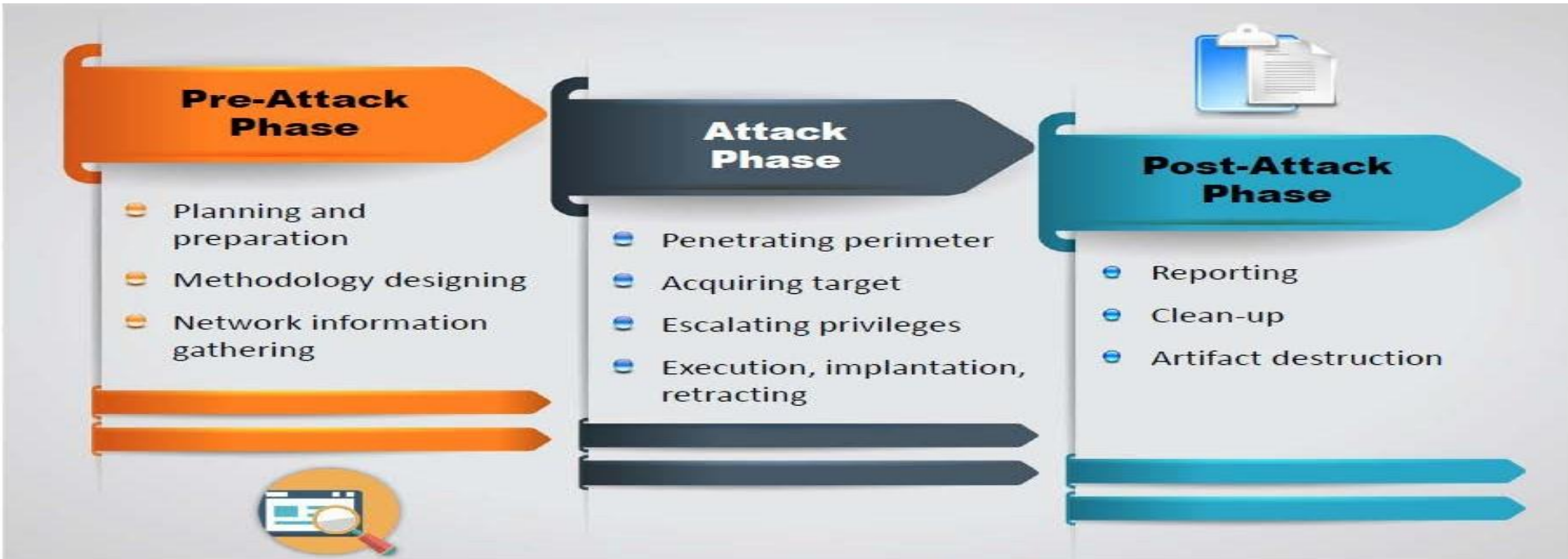
Why Penetration Testing

- 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 efficacy 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 efficacy of **network security devices** such as firewalls, routers, and web servers

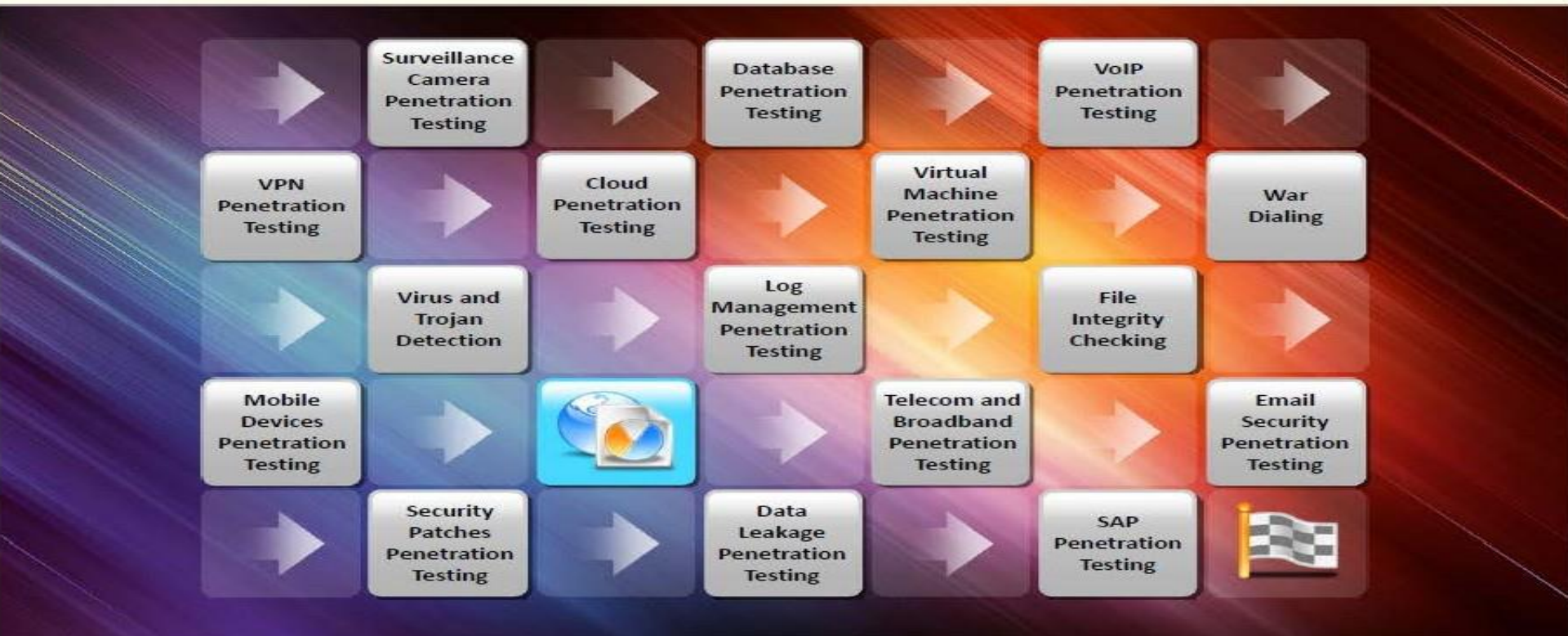
Types of Penetration Testing



Phase of Penetration Testing



Penetration Testing


Surveillance Camera Penetration Testing
Database Penetration Testing
VoIP Penetration Testing
VPN Penetration Testing
Cloud Penetration Testing
Virtual Machine Penetration Testing
War Dialing
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