BUBT
BANGLADESH UNIVERSITY OF BUSINESS AND TECHNOLOGY
Committed to Academic Excellence

Introduction to Ethical Hacking

Dr. Abdullah-Al-Musa

(B.Sc(Hons) In Computing, M.Engg In Information System Security , PhD)

Lecturer

Department of Computer Science & Engineering

Bangladesh University of Business and Technology (BUBT)

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

BUBT | BANGLADESH UNIVERSITY OF BUSINESS AND TECHNOLOGY

Committed to Academic Excellence

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users or interrupting normal business processes. Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.(Mary Ellen O'Connell., 2020)

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

The term applies in a variety of contexts

The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security **is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware (Heberlein et al., 2014).**

The term applies in a variety of contexts

Application security **focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.**

Information security **protects the integrity and privacy of data, both in storage and in transit.**

The term applies in a variety of contexts

Operational security **includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.**

The term applies in a variety of contexts

Disaster recovery **and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.**

The term applies in a variety of contexts

End-user education **addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization. (Jamie Collier.,2018)**

Motivations of Attacks

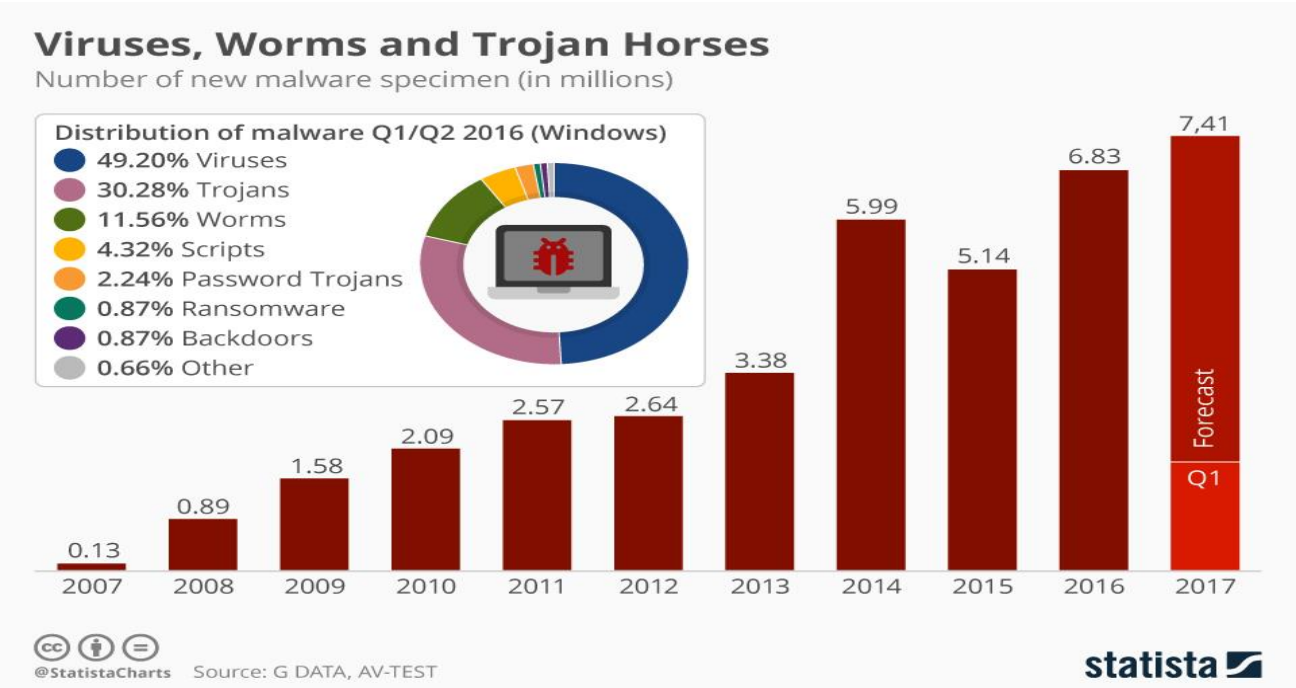
Attacks = Motive (Goal) + Method + Vulnerability

- 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

Distributed Attacks



Cyber Security Incident Management

Security incident management is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. It seeks to give a robust and comprehensive view of any security issues within an IT infrastructure. A security incident can be anything from an active threat to an attempted intrusion to a successful compromise or data breach. Policy violations and unauthorized access to data such as health, financial, social security numbers, and personally identifiable records are all examples of security incidents (Rasmussen et al.,2012)

Cyber Security Incident Management

As cyber security threats continue to grow in volume and sophistication, organizations are adopting practices that allow them to rapidly identify, respond to, and mitigate these types of incidents while becoming more resilient and protecting against future incidents.

Cyber Security Incident Management

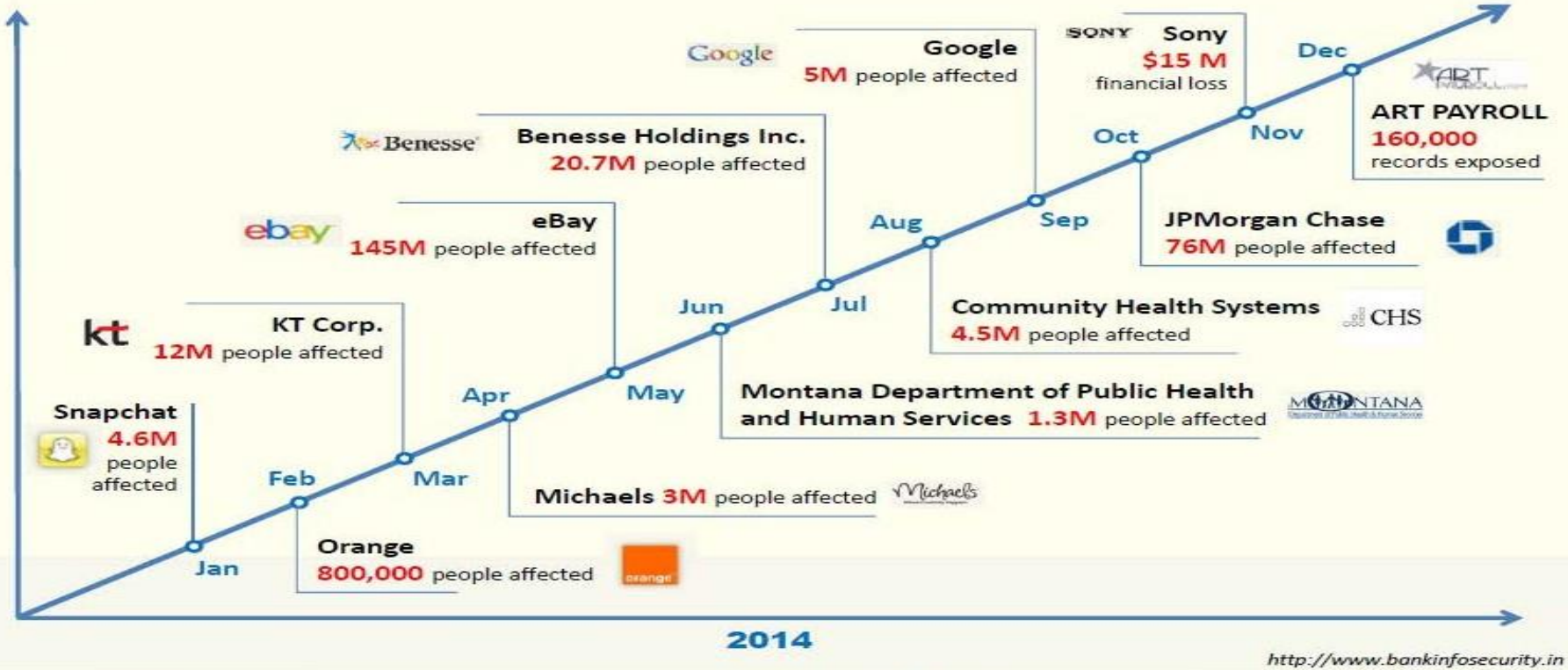
Security incident management utilizes a combination of appliances, software systems, and human-driven investigation and analysis. The security incident management process typically starts with an alert that an incident has occurred and engagement of the incident response team. From there, incident responders will investigate and analyze the incident to determine its scope, assess damages, and develop a plan for mitigation.(Abdullah et al., 2019). This means that a multi-faceted strategy for security incident management must be implemented to ensure the IT environment is truly secure. The ISO/IEC Standard 27035 outlines a five-step process for security incident management, including:

Cyber Security Incident Management

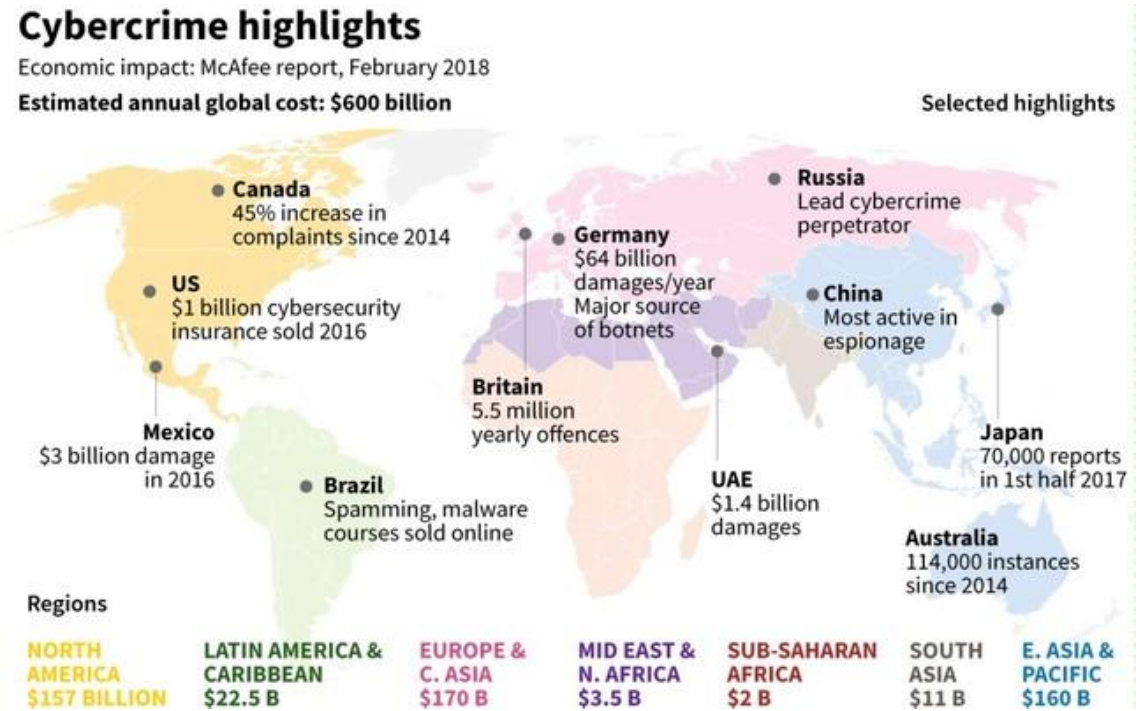
1. Prepare for handling incidents.
2. Identify potential security incidents through monitoring and report all incidents.
3. Assess identified incidents to determine the appropriate next steps for mitigating the risk.
4. Respond to the incident by containing, investigating, and resolving it.
5. Learn and document key take always from every incident.

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
Orange
800,000 people affected
Mar
Michaels 3M people affected
Apr
eBay
145M people affected
May
Benesse Holdings Inc.
20.7M people affected
Jun
Google
5M people affected
Jul
Montana Department of Public Health and Human Services 1.3M people affected
Aug
Community Health Systems
4.5M people affected
Sep
Sony
$15 M
financial loss
Oct
JPMorgan Chase
76M people affected
Nov
ART PAYROLL
160,000
records exposed
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

How Security Incident Management Works

While incident response measures can vary depending on the organization and related business functions, there are general steps that are often taken to manage threats. The first step may start with a full investigation of an anomalous system or irregularity within system, data, or user behavior.

For example, a security incident management team may identify a server that is operating more slowly than normal. From there the team will assess the issue to determine whether the behavior is the result of a security incident. If that proves to be the case, then the incident will be analyzed further

How Security Incident Management Works

information is collected and documented to figure out the scope of the incident and steps required for resolution, and a detailed report is written of the security incident.

If needed, law enforcement may be involved. If the incident involves exposure or theft of sensitive customer records, then a public announcement may be made with the involvement of executive management and a public relations team.(Martin Gilje et al.,2018)(Maria et al.,2016).

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

The Early Days of Hacking

Hacker is one of the most misunderstood and overused terms in the security industry. Everyone from the nightly news to authors to Hollywood and the rest of the media uses the term frequently. The idea of hacking and hackers goes way back to the first technology enthusiasts who wanted to learn about new technology and were curious about how it worked.

The Early Days of Hacking

They were the same types of people who today are interested not only in acquiring all sorts of technology but also in learning how to customize and tweak it to do new things that the original designers never intended.
in the early days (pre-1970), these hackers may have been found taking apart and learning about the inner workings of radios and early computers.

The Early Days of Hacking

They were the same types of people who today are interested not only in acquiring all sorts of technology but also in learning how to customize and tweak it to do new things that the original designers never intended.
In the early days (pre-1970), these hackers may have been found taking apart and learning about the inner workings of radios and early computers.

The Early Days of Hacking

As technology progressed, these individuals moved to more complex and advanced systems available at the time. Fast-forward to the 1970s, and the mainframes that were present on college campuses and corporate environments were the target of interest by new generations of hackers.

The Early Days of Hacking

Later, in the 1980s, the PC was the newest piece of technology, with hackers moving to this environment. In fact, the 1980s saw hackers starting to engage in more mischievous and later malicious activities; adding to the situation was that fact that their attacks could now be used against many more systems because more people had access to PCs.

The Early Days of Hacking

In the 1990s, the Internet was made accessible to the public, and systems became interconnected; as a result, curiosity and mischief could easily spread beyond a small collection of systems and go worldwide. Since 2000, smartphones, tablets, Bluetooth, and other technologies have been added to the devices and technologies that hackers target. As you can see, as technology evolves, so do hackers' attacks in response to what's available at the time.

The Early Days of Hacking

When the Internet became available to the public at large, hacking and hackers weren't too far behind. When the first generations of browsers became available in the early 1990s, attacks grew in the form of website defacements and other types of mischief. The first forays of hacking in cyberspace resulted in some humorous or interesting pranks, but later more aggressive attacks started to emerge.

The Early Days of Hacking

Incidents such as the hacking of movie and government websites were some of the first examples. Until the early 2020s, website defacing was so common that many incidents were no longer reported.

Current Developments

In the early 2020s, more malicious activity started to appear in the form of more advanced attacks. In the first few years of the new millennium, the aggressiveness of attacks increased, with many attacks criminally motivated. Malicious attacks that have occurred include the following (although there are many more):

Current Developments

Denial-of-service attacks
Manipulation of stock prices
Identity theft
Vandalism
Credit card theft
Piracy
Theft of service

Hacking: Fun or Criminal Activity?

In 1988, Cornell University student Robert T. Morris, Jr., created what is considered to be the first Internet worm. Due to an oversight in the design of the worm, it replicated extremely quickly, indiscriminately resulting in widespread slowdowns affecting the whole Internet.

Hacking: Fun or Criminal Activity?

In 1999, David L. Smith created the Melissa virus, which was designed to email itself to entries in a user's address book and later delete files on the infected system.

In 2016, Gary McKinnon connected to deleted critical files on U.S. military networks, including information on weapons and other systems. He performed this action after compromising roughly 2000 computer systems inside the U.S. military's network.

Hacking: Fun or Criminal Activity?

In 1999, David L. Smith created the Melissa virus, which was designed to email itself to entries in a user's address book and later delete files on the infected system.

In 2016, Gary McKinnon connected to deleted critical files on U.S. military networks, including information on weapons and other systems. He performed this action after compromising roughly 2000 computer systems inside the U.S. military's network.

Hacking: Fun or Criminal Activity?

In any case, hacking is indeed a crime, and **be prosecuted under laws** anyone engaging in such activities can that vary from location to location. The volume, frequency, and seriousness of attacks have only increased and will continue to do so as technology evolves.

some generic examples of cybercrime

Stealing passwords and usernames, or using vulnerabilities in a system to gain access, falls under the category of theft of access and the stealing of services and resources that the party would not otherwise be given access to. In some cases stealing credentials but not using them is enough to constitute a cybercrime. In a few states even sharing usernames and passwords with a friend or family member is a crime.

some generic examples of cybercrime

Network intrusions are a form of digital trespassing where a party goes someplace that they would not otherwise have access to. Access to any system or group of systems to which a party would not normally be given access is considered a violation of the network and therefore a cybercrime.

some generic examples of cybercrime

Network intrusions are a form of digital trespassing where a party goes someplace that they would not otherwise have access to. Access to any system or group of systems to which a party would not normally be given access is considered a violation of the network and therefore a cybercrime.

some generic examples of cybercrime

Social engineering is both the simplest and the most complex form of hacking or exploiting a system by going after its weakest point, the human element. On the one hand, this is easy to attempt because the human being is many times the most accessible component of a system and the simplest to interact with.

some generic examples of cybercrime

Fraud is the deception of another party or parties to elicit information or access typically for financial gain or to cause damage.

some generic examples of cybercrime

Software piracy is the possession, duplication, or distribution of software in violation of a license agreement or the act of removing copy protection or other license- enforcing mechanisms.

some generic examples of cybercrime

Malicious code refers to items such as viruses, worms, spyware, adware, rootkits, and other types of malware. This crime covers any type of software deliberately written to wreak havoc and destruction or disruption.

some generic examples of cybercrime

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are ways to overload a system's resources so it cannot provide the required services to legitimate users.

Ransomware is a relatively newer class of malware that is designed to hunt down and encrypt files on a target system. Once such files are found, the code will encrypt the data and then tell the victim that they must pay a certain amount to get their data back.

concepts in mind when performing the tasks and responsibilities of a pentester:

Confidentiality The core principle that refers to the safeguarding of information and keeping it away from those not authorized to possess it. Examples of controls that preserve confidentiality are permissions and encryption.

concepts in mind when performing the tasks and responsibilities of a pentester:

Integrity Deals with keeping information in a format that is true and correct to its original purposes, meaning that the data that the receiver accesses is the data the creator intended them to have.

concepts in mind when performing the tasks and responsibilities of a pentester:

Availability The final and possibly one of the most important items that you can perform, availability deals with keeping information and resources available to those who need to use it. Information or resources, no matter how safe and sound, are useful only if they are available when called upon.

Practices for Security Incident Management

Organizations of all sizes and types need to plan for the security incident management process. Implement these best practices to develop a comprehensive security incident management plan:

- Develop a security incident management plan and supporting policies that include guidance on how incidents are detected, reported, assessed, and responded to. Have a checklist ready for a set of actions based on the threat. Continuously update security incident management procedures as necessary, particularly with lessons learned from prior incidents.

Practices for Security Incident Management

- Establish an incident response team (sometimes called a CSIRT) including clearly defined roles and responsibilities. Incident response team should include functional roles within the IT/security department as well as representation for other departments such as legal, communications, finance, and business management or operations.
- Develop a comprehensive training program for every activity necessary within the set of security incident management procedures. Practice security incident management plan with test scenarios on a consistent basis and make refinements as need be.

Practices for Security Incident Management

- After any security incident, perform a post-incident analysis to learn from your successes and failures and make adjustments to security program and incident management process where needed.

(Inger Anne et al.,2014).

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

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

Ethical hacking is necessary as it **allows to counter attacks from malicious hackers** by anticipating methods used by them to break into a system

Reasons why Organizations Recruit Ethical Hackers

To **prevent hackers** from gaining access to organization's information systems

To **uncover vulnerabilities** in systems and explore their potential as a risk

To analyze and **strengthen an organization's security posture** including policies, network protection infrastructure, and end-user practices

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**

Penetration testing of Cyber Security

A penetration test, colloquially known as a pen test, pen test or ethical hacking, is an authorized simulated cyber attack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment. The test is performed to identify weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

The process typically identifies the target systems and a particular goal, then reviews available information and undertakes various means to attain that goal. A penetration test target may be a white box (about which background and system information are provided in advance to the tester) or a black box (about which only basic information—if any—other than the company name is provided). A gray box penetration test is a combination of the two (where limited knowledge of the target is shared with the auditor).A penetration test can help identify a system's vulnerabilities to attack (and estimate how vulnerable it is).

Penetration testing of Cyber Security

Penetration tests are a component of a full security audit. For example, the Payment Card Industry Data Security Standard requires penetration testing on a regular schedule, and after system changes. Several standard frameworks and methodologies exist for conducting penetration tests. (Nektaria et al., 2020).

Penetration testing of Cyber Security

Flaw hypothesis methodology is a systems analysis and penetration prediction technique where a list of hypothesized flaws in a software system are compiled through analysis of the specifications and documentation for the system.

The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually exists, and on the ease of exploiting it to the extent of control or compromise. The prioritized list is used to direct the actual testing of the system.

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 is an **examination of the ability of a system or application**, including current security procedures and controls, to withstand assault

It recognizes, measures, and classifies security vulnerabilities in a **computer system**, **network**, and **communication channels**

A vulnerability assessment may be used to:

Identify weaknesses that could be exploited

Predict the effectiveness of additional security measures in protecting information resources from attack

Vulnerability Assessment Types

Network Vulnerability Assessment Method

Phase I – Acquisition

- Collect documents required to:
  - Review laws and procedures related to network vulnerability assessment
  - Identify and review document related to network security
  - Review the list of previously discovered vulnerabilities

Phase II - Identification

- Conduct interviews with customers and employees involved in system architecture design, and administration
- Gather technical information about all network components
- Identify different industry standards which network security system complies to

Phase III - Analyzing

- Review interviews
- Analyze the results of previous vulnerability assessment
- Analyze security vulnerabilities and identify risks
- Perform threat and risk analysis
- Analyze the effectiveness of existing security controls
- Analyze the effectiveness of existing security policies

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

- **CodeRed Center**
  http://www.eccouncil.org
- **Microsoft Vulnerability Research (MSVR)**
  http://technet.microsoft.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**
  http://www.windowsecurity.com

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

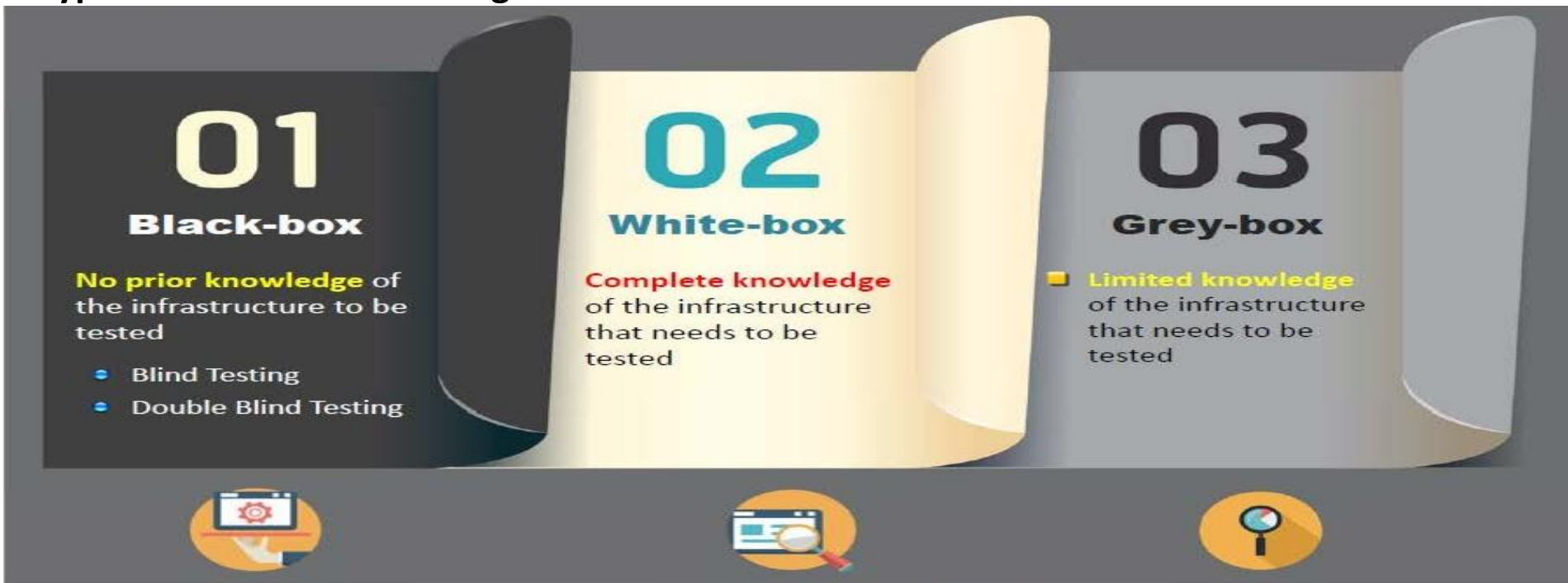
03 A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited

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

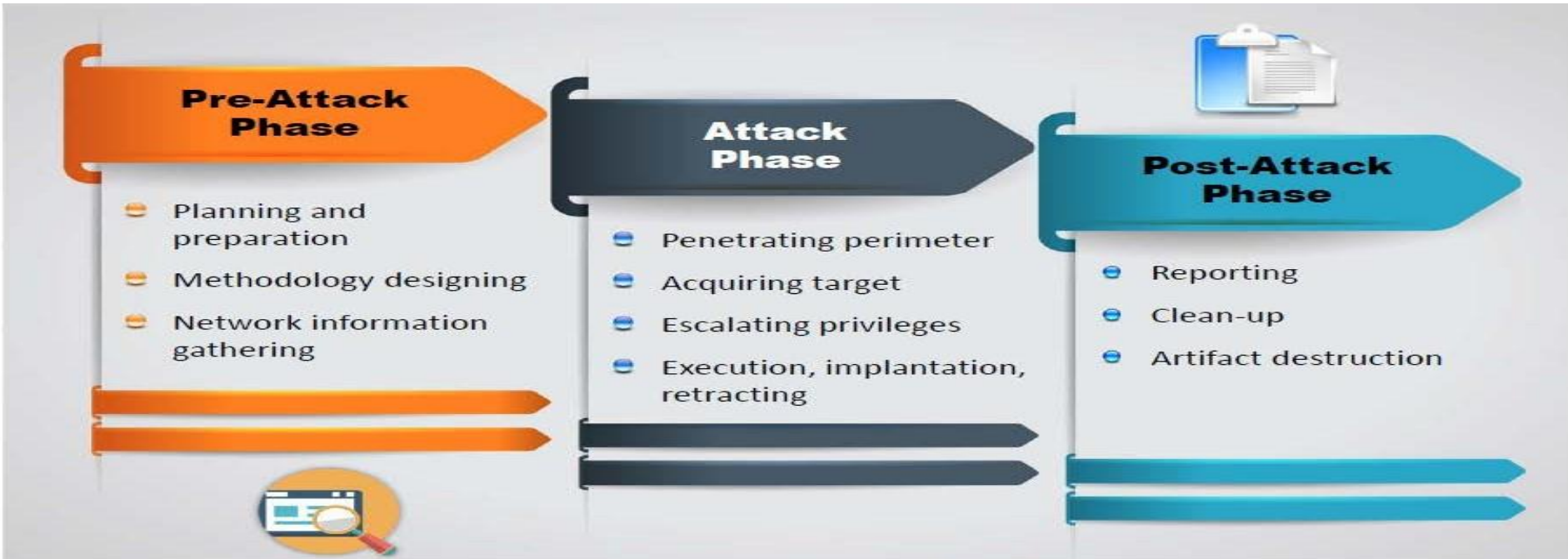
Why Penetration Testing

- 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



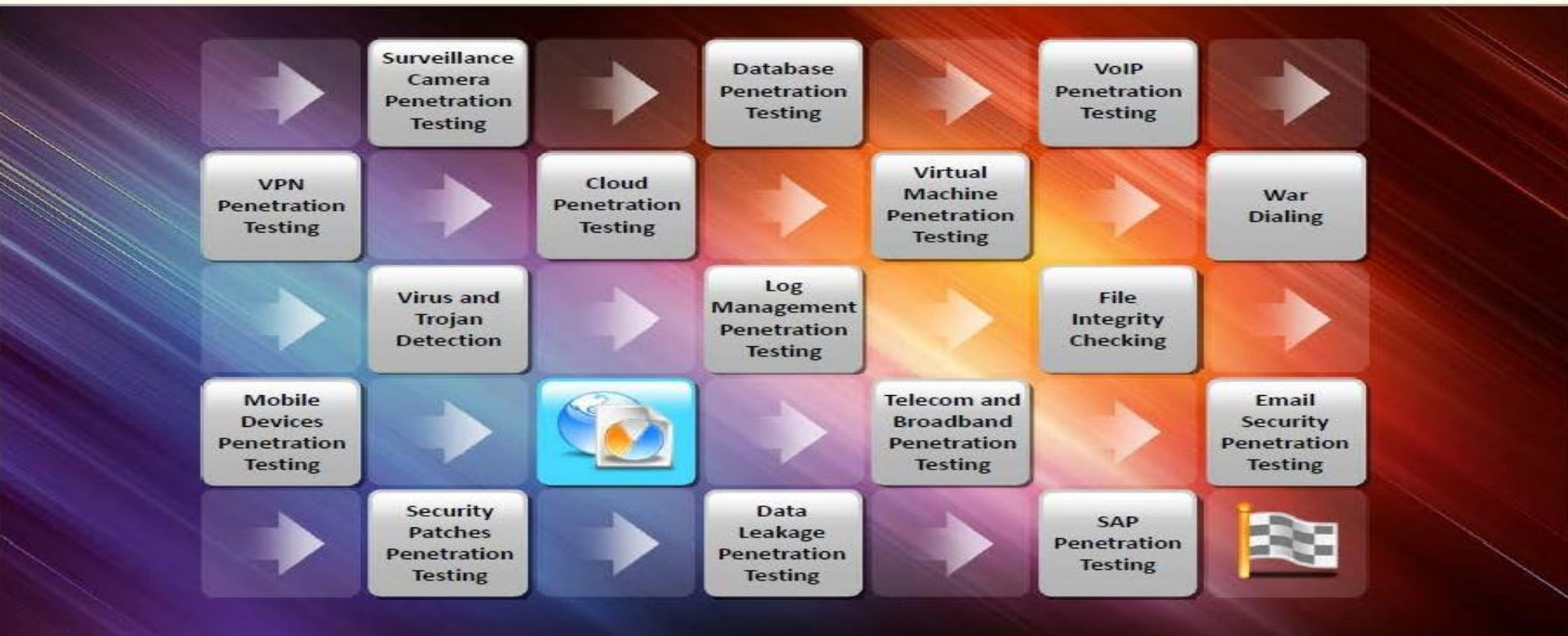
Phase of Penetration Testing



Penetration Testing

BUBT | BANGLADESH UNIVERSITY OF BUSINESS AND TECHNOLOGY

Committed to Academic Excellence



Next Class

- Webserver and Web Application Penetration Testing
- Vulnerabilities Testing
- Web Application Hacking
- How to Secure Website, Web Application, Web Server

Digital Evidence-Collection Techniques

Proper collection of evidence is essential and is something that is best left to professionals. In addition, when a digital crime has been suspected it becomes mandatory to have trained cyber security and digital forensic professionals involved in the process.

Digital Evidence-Collection Techniques

The process here is really one of digital forensics—the methodical and defensible process of collecting information from a digital crime scene. This process is best left to those professionals trained to do so because novices can inadvertently damage evidence in such a way that makes the investigation impossible or indefensible in court. Trained personnel will know how to avoid these mistakes and properly collect everything relevant.

Digital Evidence Types

Evidence is the key to proving a case, and not all evidence is created equal and should not be treated as such. Collecting the wrong digital evidence or treating evidence incorrectly can have an untold impact on any company's case, which should not be underestimated.

Digital Evidence Types

Evidence is the key to proving a case, and not all evidence is created equal and should not be treated as such. Collecting the wrong digital evidence or treating evidence incorrectly can have an untold impact on any company's case, which should not be underestimated.

Some of the different types of digital evidence that can be collected :

Best : The best digital evidence is category evidence that is admissible by requirement in any court of law. The existence of best evidence eliminates your ability to use any copies of the same evidence in court.

Some of the different types of digital evidence that can be collected :

Secondary : Secondary digital evidence is a copy of the original evidence. This could be items such as backups and drive images. This type of evidence may not always be admissible in a court of law and is not admissible if best evidence of the item exists.

Some of the different types of digital evidence that can be collected :

Direct : Direct digital evidence is received as the result of testimony or interview of an individual. This individual could have obtained their evidence as a result of observation. Evidence in this category can be used to prove a case based on its existence..

Some of the different types of digital evidence that can be collected :

Conclusive : Conclusive digital evidence includes that which is above dispute. Conclusive digital evidence is considered so strong that it directly overrides all other evidence types by its existence.

Some of the different types of digital evidence that can be collected :

Opinion : Opinion digital evidence is derived from an individual's feelings. Opinion evidence is divided into the following types: Expert-Any evidence that is based on known facts, experience, and an expert's knowledge. Non-expert-Any evidence that is derived from fact alone and comes from a non-expert in the field.

Some of the different types of digital evidence that can be collected :

Corroborative : Corroborative digital evidence is obtained from multiple sources and is supportive in nature. This type of evidence cannot stand on its own and is used to bolster the strength of other evidence.

Some of the different types of digital evidence that can be collected :

Circumstantial : Circumstantial digital evidence can be obtained from multiple sources, but unlike corroborative evidence it is only able to indirectly infer a crime.

Chain of Custody

When collecting evidence the chain of custody must be maintained at all times. The chain of custody documents the whereabouts of the evidence from the point of collection to the time it is presented in court and then when it is returned to its owner or destroyed. The chain is essential because any break in the chain or question about the status of evidence at any point can result in a case being thrown out.

Chain of Custody

A chain of custody needs to include every detail about the digital evidence, from how it was collected up to how it was processed.

A chain of custody can be thought of as enforcing or maintaining six key points. These points will ensure that you focus on how information is handled at every step:

Six key points

What evidence has been collected?
How was the evidence obtained?
When was the evidence collected?
Who has handled the evidence?
What reason did each person have for handling the evidence?
Where has the evidence traveled and where was this evidence ultimately stored?

Also remember if you are involved to keep the chain of custody information up to date at all times. Every time any evidence is handled by an investigator, you must update the record to reflect this. You may be asked at some point to sign off on where evidence was or that it was collected from you; this would be an example of where you would fit in regard to the chain of custody.

This information should explain every detail such as what the evidence actually consists of, where it originated, and where it was delivered to. It is important that no gaps exist at any point.

For added legal protection, digital evidence can be validated through the use of hashing to prove that it has not been altered. Ideally the digital evidence you collected at the crime scene is the same evidence you present in court.

Remember, a verifiable or non-verifiable chain of custody can win or lose a case.

Rules of Evidence

All digital evidence, no matter the type, may not be admissible in court. Evidence cannot be presented in court unless certain rules are followed, and you should review those rules ahead of time. The five rules of evidence presented here are general guidelines and are not consistent across jurisdictions:

Rules of Evidence

Reliable—The digital evidence presented is consistent and leads to a common conclusion.

Preserved—Chain of custody comes into play and the records help identify and prove the preservation of the evidence in question.

Rules of Evidence

Relevant—The digital evidence directly relates to the case being tried.
Properly identified—Records can provide proper proof of preservation and identification of the evidence.
Legally permissible—The evidence is deemed by the judge to fit the rules of evidence for the court and case at hand.

Recovering from a Cyber crime Incident

When a cyber crime incident happens, and it will happen, the company should have a plan to restore business operations as quickly and effectively as possible. This may require and possibly your team to correctly assess the damage, complete the investigation, and then initiate the recovery process.

Recovering from a Cyber crime Incident

From the time of the initial cyber crime incident onward, the organization presumably has been operating at some reduced capacity, and so you need to recover the systems and environment as quickly as possible to restore normal business operations. Other key requirements are the need to generate a report on what happened and the ability to communicate with appropriate team members..

Ethics and the Law

As an ethical hacker, you need to be aware of the law and how it affects what you do. Ignorance or lack of understanding of the law not only is a bad idea but can quickly put you out of business. In fact, under some situations the cybercrime may be serious enough to get you prosecuted in several jurisdictions in different states, counties, or even countries due to the highly distributed nature of the Internet.

Remember the following points when developing a contract and establishing guidelines:

Trust : The client is placing trust in you to use proper discretion when performing a penetration test. If you break this trust, it can lead to the questioning of other details such as the results of the test.

Remember the points when developing a contract and establishing guidelines:

Trust : The client is placing trust in you to use proper discretion when performing a penetration test. If you break this trust, it can lead to the questioning of other details such as the results of the test.

Thank you

Q & A