TCS332 Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Head of Cyber security and IoT research group

(Research h-index: 44, i10-index:74)

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Unit 1. Introduction to information security

Topics to be discussed:

- **1. Steps to fix a cyber crime**
- **2. Penetration Testing and its Phases**
- **3. Type of Hackers**

Steps to fix a cyber crime (threat/risk)

- Identify cyber threats,
- Analyze, evaluation and treatment of cyber threats

Steps to fix a cyber crime

- Organization realistically does the assessment of the vulnerabilities of its digital system components not just for **technology flaws** (i.e., in design, encryption, event logging or software malfunction) **but for human factors**.

Steps to fix a cyber crime

- Trusted insiders present the highest risk (motivated either by malice or more commonly by accident) as well as third-party contractors, vendors, or temporary workers (i.e., privileged users).
- The organization should follow **structured approach** for assessment and management of cyber risk.

Steps to fix a cyber crime

This involves a six-part approach:

(1) Generating an integrated view of information risk:

- It provides a guidance for generating an integrated view of information risk.
- Ranging from an organization's business processes through to its technology **(process means ongoing activities in an organization).**

Steps to fix a cyber crime

This involves a six-part approach:

(2) Assessment of worst case:

- It provides guidance for realistically assessing worst-case scenarios- the **potential business impact** if information assets (i.e., data server) become compromised. **(For example, financial lose associated with that.**

Steps to fix a cyber crime

(3) Mapping of different types of threats, both malicious and accidental:

- It involves mapping of different types of threats, both **malicious (by the attacker) and accidental (by insiders),** that could potentially affect the business.

Steps to fix a cyber crime

(4) Assessment of vulnerabilities to different threat events and the strength of deployed controls:

- It involves assessing your vulnerabilities to different threat events (i.e., different threat environment) and the strength of the deployed controlling mechanisms (i.e., authentication, access control, firewall, IDS etc.).

Steps to fix a cyber crime

(5) Evaluating risk appetite and likelihood of a successful threat:

- It evaluates the organization's risk appetite and likelihood of a successful threat **(computation of probability of its happening).**

Risk appetite- Means how much risk a organization can tolerate (handle).

Steps to fix a cyber crime

(6) Developing practical approaches to address the information risks that have been identified:

- It involves developing practical approaches to addressing the information risks which have been identified. **(Basically which tools and techniques you will use in that situation).**

Steps to fix a cyber crime

• Other factors which should be examined include

-- organization capability (financial, technical, HR),

-- security culture,

-- commitment,

-- people,

-- user privilege patterns,

-- technology,

-- leadership,

-- policy, and environment.

Steps to fix a cyber crime

The focus begins and ends with the organization's data:

-- How it is protected (i.e., tools and techniques),

-- Which data is truly mission critical (i.e., highly confidential data),

-- What behaviors need to be protected against (i.e., vulnerabilities, threats and attacks),

-- Who really needs to access it and when (i.e., users).

Penetration Testing and its Phases

Penetration Testing and its Phases

- A penetration test or pen test, is a simulated cyber attack which is used against a system to check for exploitable vulnerabilities.

Penetration Testing and its Phases

- Pen testing can involve the attempted breaching of any number of application systems, (i.e., application protocol interfaces, web servers, etc.) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Penetration testing stages

The pen testing process can be broken down into five stages.

1. **Planning and reconnaissance**
2. **Scanning**
3. **Gaining Access**
4. **Maintaining access**
5. **Covering tracks**

Penetration testing stages

1. Planning and reconnaissance:

- Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
- Gathering intelligence (i.e., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

Penetration testing stages

2. Scanning:

- The next step is to understand how the target application will respond to various intrusion attempts.

Penetration testing stages

- There are two ways:

2.a) Static analysis:

- Inspecting an application’s code to estimate the way it behaves while running.
- These tools can scan the entirety of the code in a single pass (i.e., PVS-Studio).

Penetration testing stages

2.b) Dynamic analysis:

- Inspecting an application’s code in a running state.
- This is a more practical way of scanning, as it provides a real-time view into an application’s performance (i.e., AddressSanitizer, Burp Suite tool).

Penetration testing stages

3. Gaining Access

- This phase requires taking control of one or more network devices in order to either extract data from the target, or to use that device to then launch attacks on other targets.

Penetration testing stages

3. Gaining Access

- It uses web application attacks, i.e., cross-site scripting, SQL injection and backdoors, to identify vulnerabilities in the target system.
- Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc.

Penetration testing stages

4. Maintaining Access

- The goal of this stage is to see if the vulnerability can be used to achieve a **persistent presence** in the exploited system for the **long time**.
- To get the knowledge about the attacker’s gain in that in-depth access.

Penetration testing stages

4. Maintaining Access

- The idea is to imitate advanced **persistent threats**, which often **remain in a system for months** in order to steal an organization's most sensitive data.
- It requires taking the steps involved in being able to be persistently within the target environment in order to **gather as much data as possible**.

Penetration testing stages

4. Maintaining Access

- It includes things like **back door installation** on target machines so that one can maintain the gained access and connect to the target any time.

Penetration testing stages

5. Covering Tracks

- Take all necessary steps to remove all semblance (evidences) of detection.
- Any changes that were made, authorizations that were escalated etc., all must return to a state of non-recognition by the host network's administrators **(everything should be same like the initial phase of the system).**

Penetration testing stages

Analysis of Pen test (Outcomes):

- The results of the penetration test are then **compiled into a report** detailing:

--Specific vulnerabilities that were exploited.

--Sensitive data that was accessed.

--The amount of time the pen tester was able to remain in the system undetected.

Penetration testing stages

Analysis of Pen test (Outcomes):

- This information is analyzed by security expert to update the security settings and to provide solutions for patching the vulnerabilities.
- This will also protect against future attacks.

Type of Hackers

- White Hat
- Gray Hat
- Black Hat

Hackers

- A hacker is someone who uses certain techniques for breaching the defense and exploiting the weaknesses in a system or in a network.
- "Hacker" doesn't mean "criminal" or "bad guy".
- Tech writers often refer to "black hat", "white hat", and "gray hat" hackers.
- These terms define different groups of hackers based on their behavior.

Black Hats

- Black-hat hackers, or “black hats” are the type of hacker on which media/people have main focus.
- Black-hat hackers violate system’s security for **personal gain** **(such as stealing credit card numbers)** or for pure maliciousness (such as **creating a botnet** and using that botnet to perform DDOS attacks against websites they don’t like.)
- Whatever they do come under criminal activities.

Black Hats

- They perform these illegal activities for their personal gain and to harm others.
- A black-hat hacker who finds a new, “zero-day” vulnerability would sell it to some other criminal organizations or use it to compromise that system.

White Hats

- White-hat hackers are the opposite of the black-hat hackers.
- They’re the “ethical hackers”, experts who use their skills for good, ethical, and legal purposes rather than in bad, unethical, and criminal purposes.
- Many white-hat hackers work to test the security of organization’s computer systems.

White Hats

- The organization authorizes the white-hat hacker to attempt to compromise their systems.
- The white-hat hacker uses their knowledge to compromise the organization’s systems, just like the black hat hackers.

White Hats

- However, instead of using their access to steal the data from the system, white-hat hacker reports back to the organization and informs them of how they gained access, allowing the organization to improve the security of their systems.
- This is also known as **“penetration testing”.**

White Hats

- A white-hat hacker who finds a security vulnerability would disclose it to the developer, allowing them to patch their product and improve its security before it will be compromised.
- Organizations (i.e., Google) also pay **“bounties” (certain amount of money)** for revealing the discovered vulnerabilities in their systems.

Gray Hats

- A gray-hat hacker falls in between black hat and white hat.
- A gray hat doesn’t work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things.
- A black hat hacker would compromise a system without permission, stealing the data inside for their own personal gain or for other kind of destructions.
- A white-hat hacker would ask for permission before testing the system’s security and alert the organization after compromising it.

Gray Hats

- A gray-hat hacker tries to compromise a system without permission and then inform the organization about that vulnerability to allow them to fix the problem.
- Moreover, gray-hat hacker does not use their access for bad purposes.
- But **unauthorized accessing of a system comes under illegal activities.**

Gray Hats

- If a gray-hat hacker discovers a security flaw in a piece of software (i.e., OS) or on a website, they may disclose the flaw publically instead of privately disclosing the flaw to the organization and giving them time to fix it.
- They wouldn’t take advantage of the flaw for their own personal gain unlike the black-hats.

Disadvantage: Public disclosure of a flaw (vulnerability) may help the black-hat hackers and they can try to exploit that vulnerability.

MCQ round

- Q1: Who does the task of ethical hacking.
- (a) Gray hat
- (b) White hat
- (c) Black hat
- (d) None

MCQ round

- Q1: Who does the task of ethical hacking.

Answer: Option (b)

MCQ round

- Q2: Who may be malicious for an organisation.
- (a) Gray hat
- (b) White hat
- (c) Black hat
- (d) Both (a) and (c)

MCQ round

- Q2: Who may be malicious for an organisation.

Answer: Option (d)

MCQ round

- Q3: Which is not a stage of penetration testing.
- (a) Planning and reconnaissance
- (b) Scanning
- (c) Gaining Access
- (d) All are the stages of penetration testing

MCQ round

- Q3: Which is not a stage of penetration testing.
- Answer: Option (d)

MCQ round

- Q4: Read the following statements:
- Statement 1: Static analysis: Inspecting an application’s code to estimate the way it behaves while running.
- Statement 2: Dynamic analysis: Inspecting an application’s code in a running state.
- (a) Statement 1 is correct
- (b) Statement 2 is correct
- (c) Only statement 2 is correct
- (d) Both are correct statements

MCQ round

- Q4: Read the following statements:
- Answer: Option (d) is correct.

MCQ round

- Q5:Steps required for a cyber crime are:
- (a) Generating an integrated view of information risk
- (b) Assessment of worst case
- (c) Mapping of different types of threats
- (d) All steps are required

MCQ round

- Q5:Steps required to a cyber crime are:
- Answer: Option (d) is correct.

References

- Zero Trust Model: Can Trusting No One Be the Answer to Your Cybersecurity Problems (Information available at: https://www.ekransystem.com/en/blog/zero-trust-security-model
- Textbook: Penetration Testing: A Hands-on Introduction to Hacking by Georgia Weidman
- Textbook: Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives by Sunit Belapure and Nina Godbole
- Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, (2e), Thomson Learning, 2007
- psu.edu
- Pen test. Information available at: https://www.imperva.com/learn/application-security/penetration-testing/

❑ Identifying, Analyzing, and Evaluating Cyber risks. Information available at: https://www.securityforum.org/uploads/2017/05/ISF_c07.pdf