Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Introduction: Advanced Cybersecurity, Cyberrisk & Risk Assessment

Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

- *Testing Terminologies*
- *Information Security*
- *Hacking*
- *Understanding Risk*
- *Assessing, Managing and Monitoring Risk*
- *Cyber risk resilience*
- *Penetration Testing*
- *Laws and Standards*

Lab/ Tutorials

- *Download and Setup your Lab.*
- *Coursework Description.*

During this week, we shall discuss about the overview of Information security, the threats and attack vectors.

In continuation, let us try to understand the hacking concepts and the reasons to stay ethical. To add more insight, let us also look at various security laws and standards.

"Risk" is a very important concept when looking to enhance the security. Let us also understand various risk factors and the importance of cyber risk resilience.

Information Security – Elements

- *Information is wealth!!! It is important to secure our information. However, in order to secure our information, we must focus on ensuring security on the infrastructure where the information lies on.*
- *Information Security is to secure both information and its infrastructure avoiding incidents like theft, tampering and disruption of information and services.*
- *In order to secure our information, few elements are considered….*

Confidentiality

Authenticity

Integrity

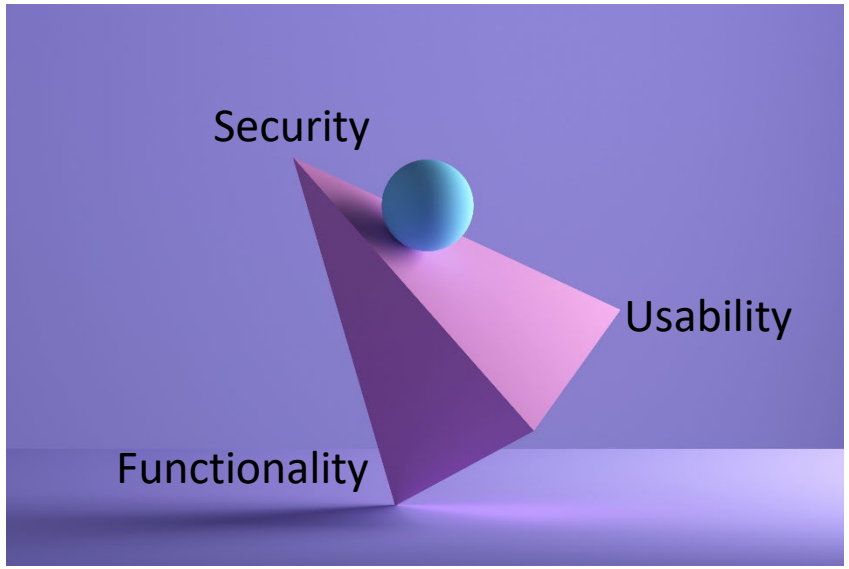
Non-Repudiation

Availability

The information is available and could be accessed only by those who are intended to.

Information Security – Elements

- *What is the real-time problem in achieving those security elements?*



Balancing between these is the challenge here…

Information Security - Attack

- *If you need to enhance security, first understand the attacks.*
- *Attack doesn't happen in a moment.*
- *Always, an **attack needs proper planning**.*

- *Motive behind an Attack*
- *Method to Attack*
- *Weak point (Vulnerability) to Attack*

Can you list out some motives behind an attack?

- *Interrupting Services*
- *Create a loss*
- *Demanding money (Ransomware)*
- *Political cause*
- *Terrorism*

Information Security – Attacks

Operating System Attacks — Focus on OS vulnerabilities. Use those vuln. to exploit and gain access

- Eg: Unpatched OS, Buffer overflow vuln.

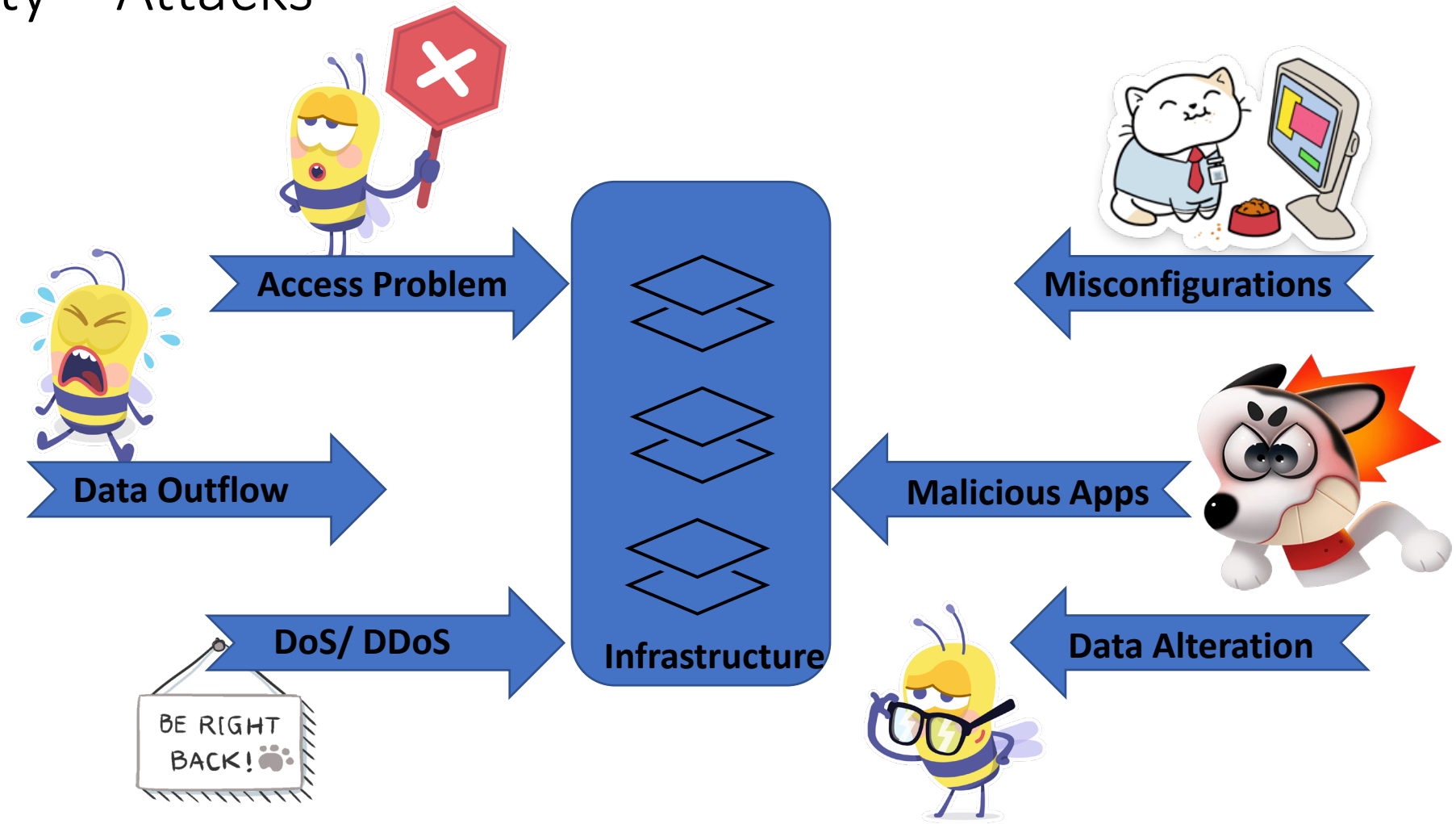
Application Attacks — Focus on Application's running in a network, look for their vuln. Exploit and gain access

- Eg: Session Hijacking, SQL injection, Cross-site scripting

Misconfiguration Attacks — Configurations in any applications/ webservers, networks that could possibly allow unauthorised access

Shrink-wrap code Attacks — Due to default configurations left in production env., leading to exploiting and access gaining

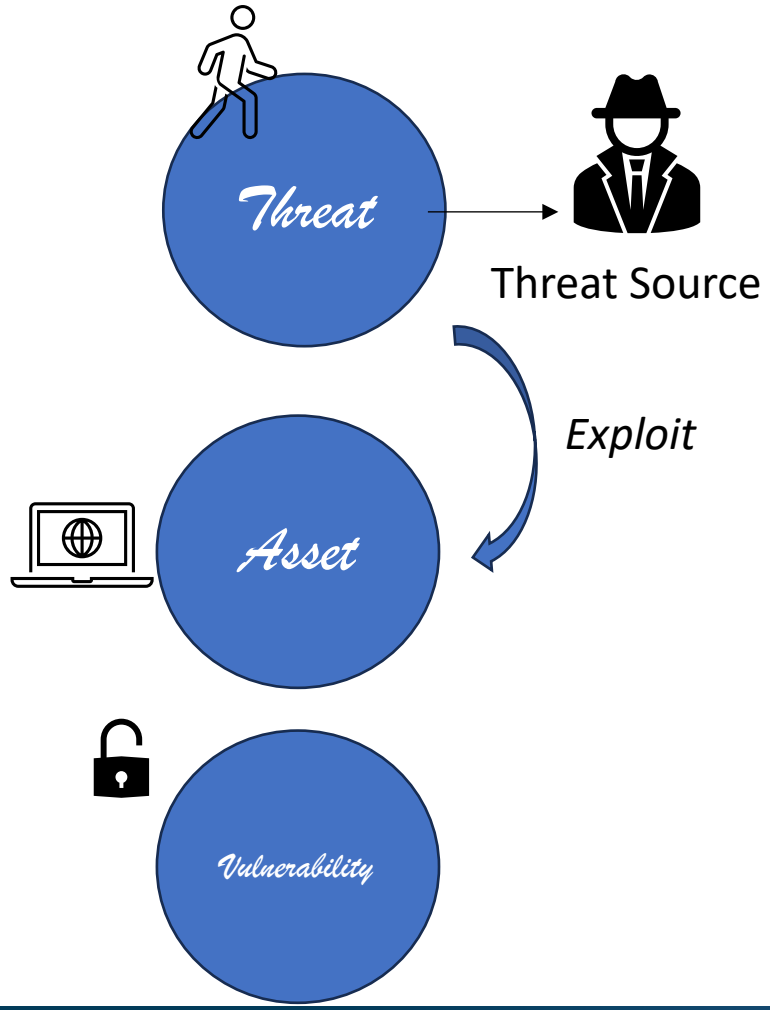
Information Security – Attacks

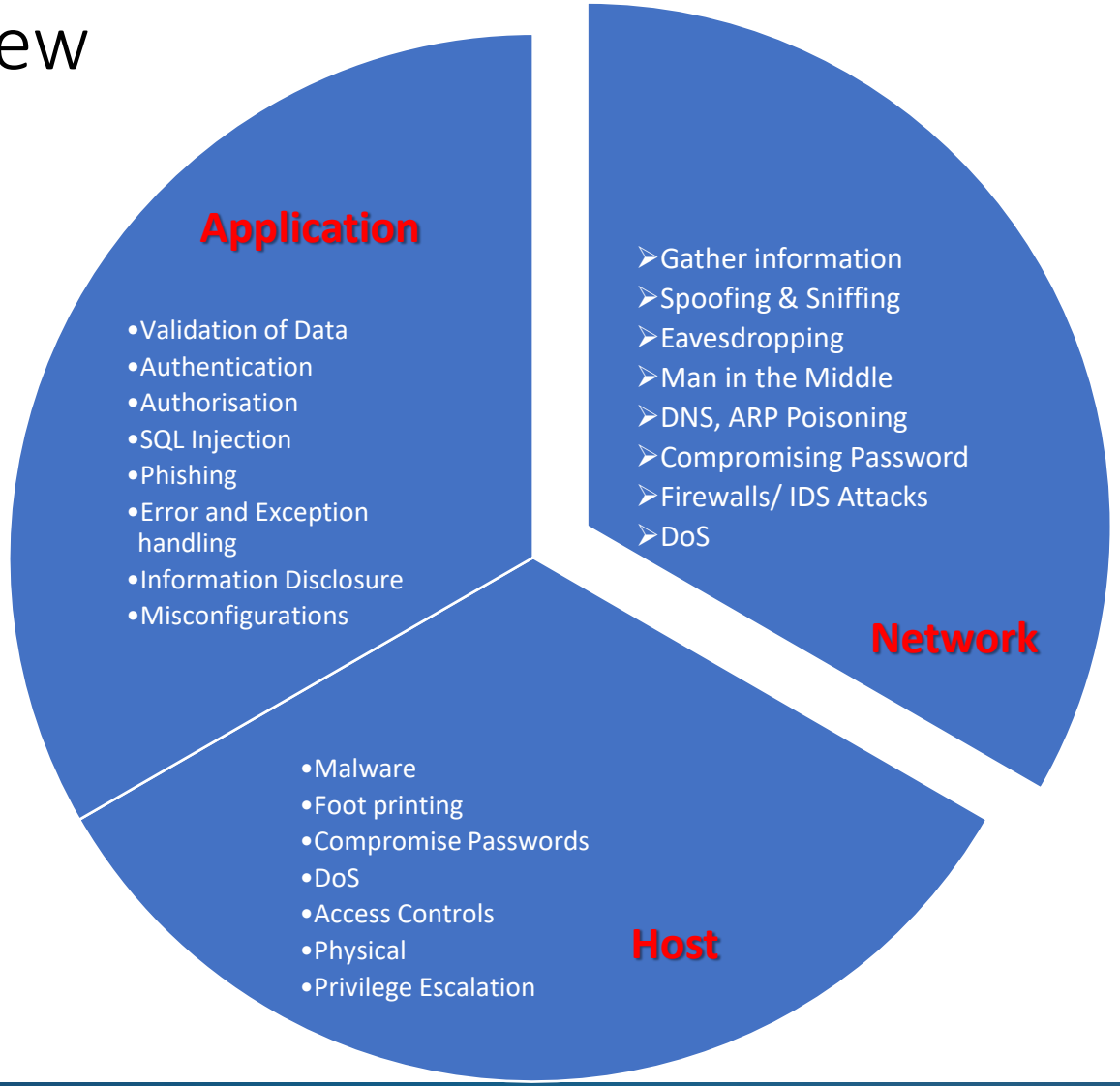


Information Security – Attack Vectors

- *Viruses, Worms – Infect a network very quickly*
- *Phishing – forged emails to get the victim's personal/account information*
- *Insider Attack – Someone inside the organisation*
- *Botnet – Network of compromised systems together to pursue an attack*
- *Advanced Persistent Threats – Getting information without the knowledge of the user*
- *Ransomware – Demands financial transactions*
- *Web Application Threats – Web infrastructure/ information threat*
- *IoT Threats – Compromise networks via IoT devices*
- *Cloud Computing Threats – Compromise cloud space to get secured/ private information*

Information Security – Overview





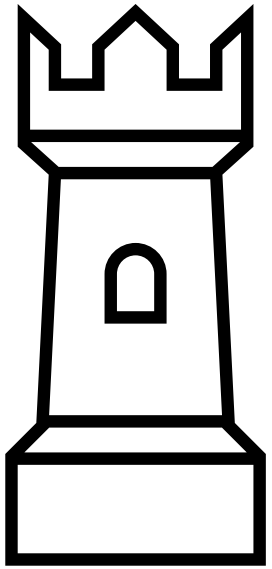
Information Security – Overview

Threat Source	Attack Surface	Motive	Capability	Threat
Script Kiddie	Company Website	To prove skills	Relatively unskilled	DoS attack on the system
Hacker	VPN	Personal gains, Monetary gains	Highly skilled with resources	Data Tampering
Hacktivist	Company Website	Political agenda	Relatively skilled with adequate resources	Defacing the website
Malware		Personal gains, Monetary gains	Highly skilled	

Threat	Vulnerability	Description
DoS attack on the system	Inadequate detection capabilities	Existing system not adequate to detect newer DoS attacks
Data Tampering	Weak Encryption	Encryption adopted is weak and inadequate
Defacing the website	Insecure design	Secure coding practices not followed, website is prone to injection attacks

Information Security – Approach

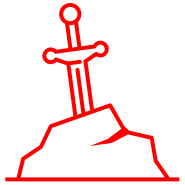
- *Approach to secure your cyber infrastructure is similar to real-time security measures…. Like in a War!!*
- *In a real War – You either Defend or Offend….Same here in securing infrastructure….*
- *Here, you use your technical resources to take advantage…*



I am defending against attacks on my infrastructure!!!

Detection
Prevention
Deterrence
Response
Alerts
Emergency Action Plans

I am attacking against my targets infrastructure!!!



System Hacking
Malware
Man-in-the-Middle Attacks
Web Application Attacks
Web Server Attacks

Hacking

A catchy word in today's world… that would make everyone to look at…

Hacking is

- ***exploiting the vulnerabilities and successfully compromising*** *an infrastructure's control.*
- ***Make changes to a system*** *to initiate actions that are not intended by the owner*

Hacking

A catchy word in today's world… that would make everyone to look at…

- ***exploiting the vulnerabilities and successfully compromising*** *an infrastructure's control.*
- ***Make changes to a system*** *to initiate actions that are not intended by the owner*

The reason for Hacking varies…However, generally the actions may lead to

- ***Stealing information***
- ***Cause intentional damage/ loss***
- ***Redistribution of Intellectual property***
- ***Personal gain***
- ***Recognition***
- ***and more…***

Hackers are

- ***Just like you and me…. a normal person (maybe sitting next to you!!!)***
- ***Ethical/ Unethical/ Neutral***
- ***Script Kiddies/ Suicide Hackers***
- ***Cyber Terrorists/ State Sponsored/ Hacktivist***

- ***Know about Operating Systems (Win. Lin. Uni Mac)***
- ***Know Networks***
- ***Update on technical skills***
- ***Ethics, Standards, Laws & Security Policies***

Purpose of Hackers

- ***Defensive/ Offensive***
- ***Hobby***
- ***Illegal Activities***

Hacking: Phases

- *There are different phases of hacking*

Reconnaissance

- Initial phase – Known target - looking for information.
- At this point, no much information is available.
- Targeting Employees/users, Systems, Applications, hardwares etc

Scanning

- Pre-attack phase – use information gathered.
- Initiate scan over network, ports etc.
- Involves use of ping tools, vulnerability scanners
- Gains machine, port, OS details
- Ready to attack

Gaining Access

- Access to OS, Application, Network
- Escalate privileges
- Actions like password attack, buffer overflow, DoS, session hijacking etc

Maintain Access

- Hold control, Use Backdoors, Rootkits, Trojans
- Upload/ Download, Manipulate information
- Use for further attacks

Clearing Tracks

- Hide the executed actions to avoid getting caught. However, continue access.
- Overwrite server, system logs to avoid being seen.

Hacking Ethically

- *Hacking is same. It depends on the purpose. If the purpose is to identify the vulnerabilities to secure infrastructure, it is Ethical.*
- *As an Ethical Hacker (if you want to be one ☺), you must think like an attacker to mitigate their strategies, overcome attacks and ensure security.*
- *Use techniques of attackers to check your infrastructure on any exploitable vulnerabilities with required permissions.*

- *As an Ethical Hacker, your goal should be to*
  - *identify vulnerabilities,*
  - *strengthen security,*
  - *stop hackers from compromising your infrastructure,*
  - *prevent security breaches,*
  - *protect information,*
  - *create awareness.*

- *Ethical Hacking is a part of organizations*
  - *Risk Assessment & Auditing,*
  - *Security best practices.*
  - *Identifying risks and propose mitigations*

Cyber Risk

NIST (National Institute of Standards and Technology) defines Risk as

"The level of potential impact on an organization operations (including mission, functions, image, or reputation), organization assets, or individuals of a threat or a given likelihood of that threat occurring."

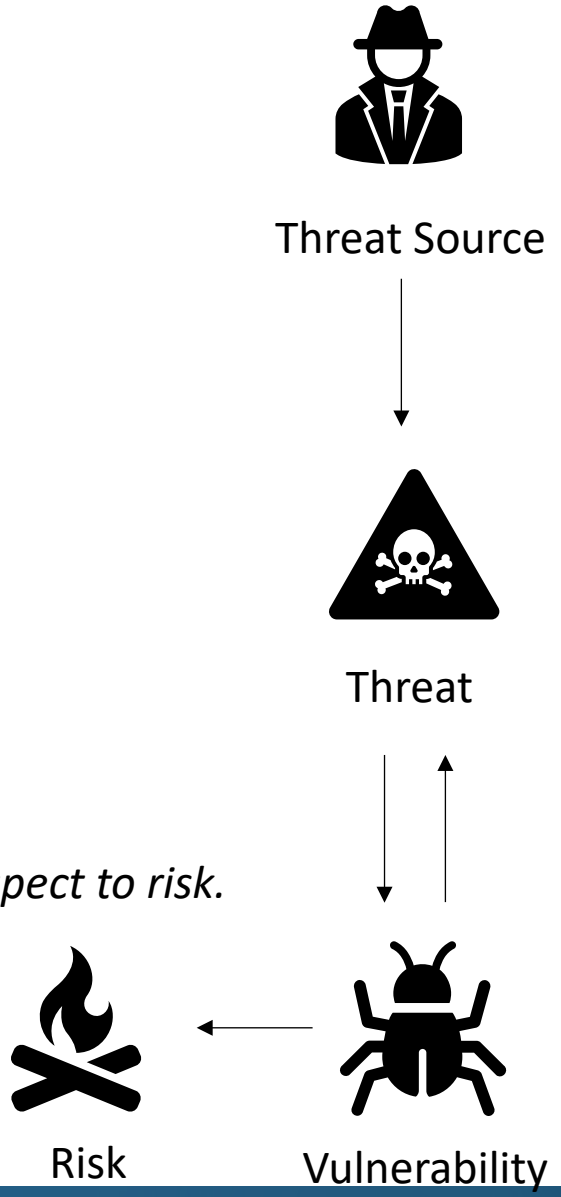
- *In short, risk can be considered as the potential loss of assets in an organization when an adverse event or threat materializes.*

It could be

- Accidental security breaches
- Deliberate security breaches
- Poorly configured IT systems
- *Additionally, breaches (accidental or deliberate) in any organization's supply chain or extended enterprises may introduce newer risks in the organization.*
- **Any risk arising due to a cyber threat is called a cyber risk.**
- Not every risk is a cyber risk. A risk can be considered a cyber risk only if any cyber threat is a contributing factor.

Cyber Risk - Taxonomy

- **Risk** *is the likelihood of an incident and its consequence for an asset.*
- **Incident** *is any event that harms or reduces the value of an asset.*
- **Asset** *is anything that holds value to a party.*
- **Party** *is any organization or system for which a risk assessment is carried out.*
- **Likelihood** *is the chance that something will occur.*
- **Consequence** *is the impact of an incident on an asset in terms of harm or reduced asset value.*
- **Risk level** *is the magnitude of risk as derived from its likelihood and its consequence.*
- **Risk Management:** *The list of coordinated activities to direct & control an organization with respect to risk.*
- **Target (of assessment):** *The parts of the system subjected to Risk Assessment.*



Cyber Risk – Components & Types

Risk consists of 3 components:

- **Consequence**
- **Likelihood**
- **Incident**

The gravity of any risk is measured by its likelihood and consequence.

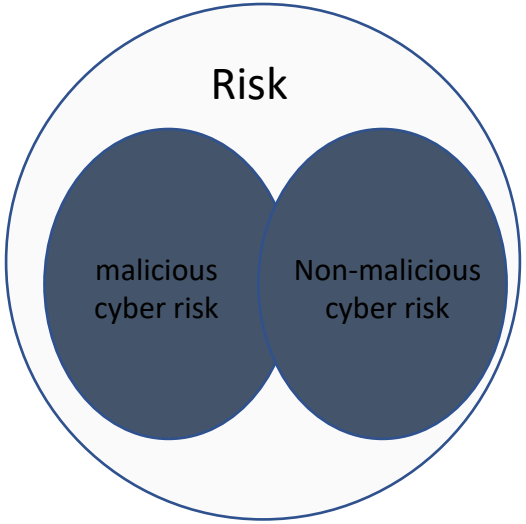
A single incident may give rise to multiple risks.

Types of Cyber Risk:

- **Malicious Cyber Risks**
- **Non-malicious Cyber Risks**

Unauthorized data access by a hacker - Malicious Cyber Risk

Accidental posting of the data by an inadequately trained employee - Non-malicious Cyber Risk



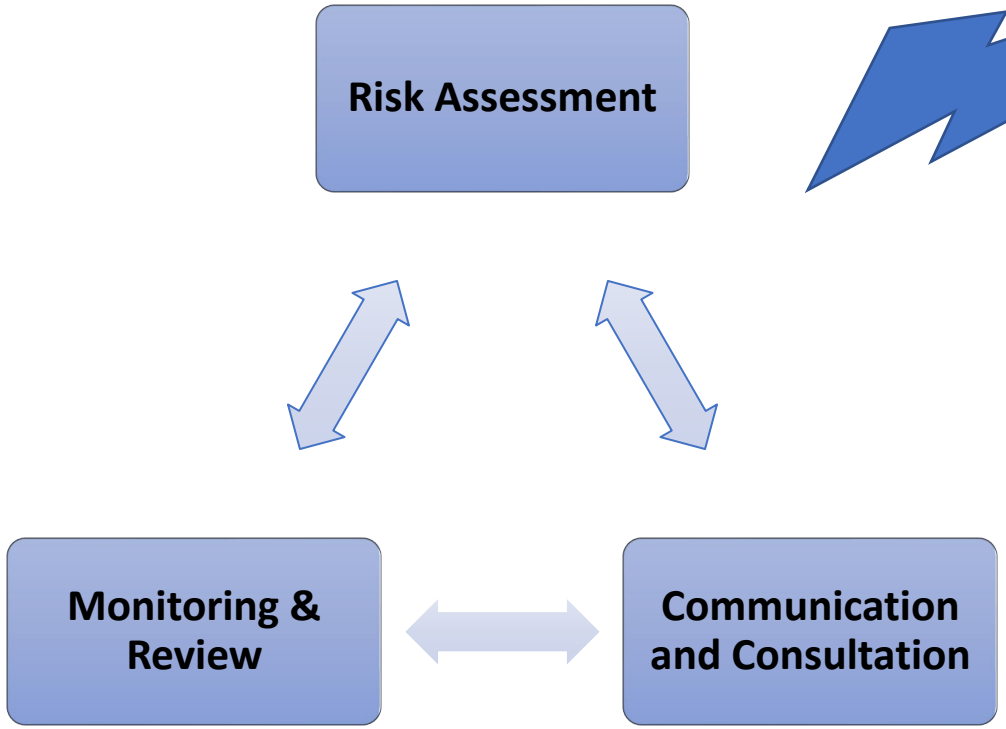
Cyber Risk – Components & Types

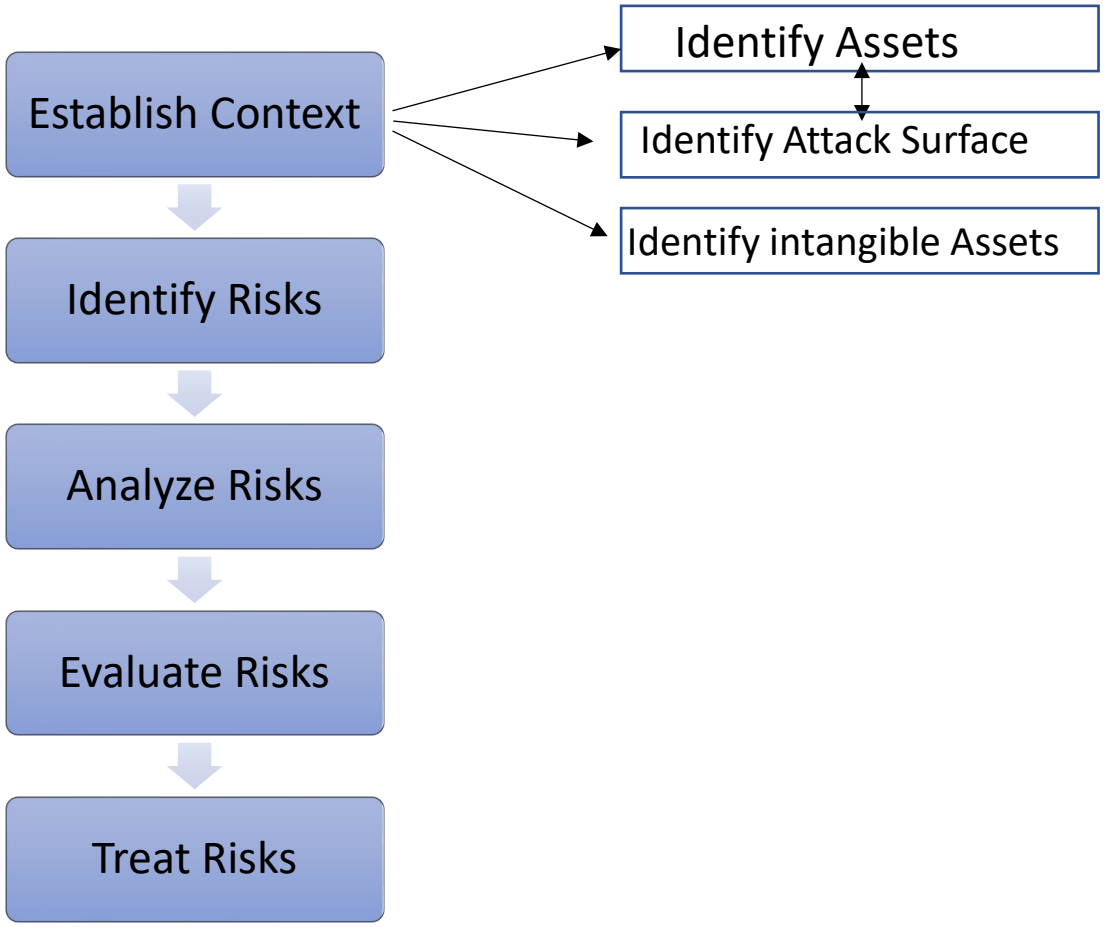
Risks can be categorized as

- **Inherent Risks** *that exist inside a system in the absence of any controls*
  - Varies across industries - risks in healthcare are different from risks in the fintech industry.
  - Mishandling of critical and sensitive data, Inadequate device security, Improper access controls.
- **Residual Risks** *that remain inside the system even after controls have been set up for handling it.*
  - Risk that remains within the set of controls currently in place.
  - Residual risks are subject to compliance. For example, ISO 27001 mandates monitoring residual risks.
  - Cyber attacks, Phishing, Insider threats

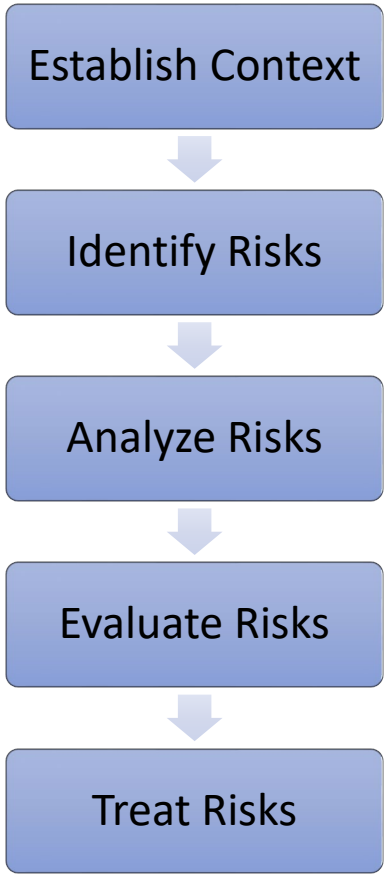
Every organization is exposed to risks. To efficiently manage these risks, a robust risk management process is needed for every organization.

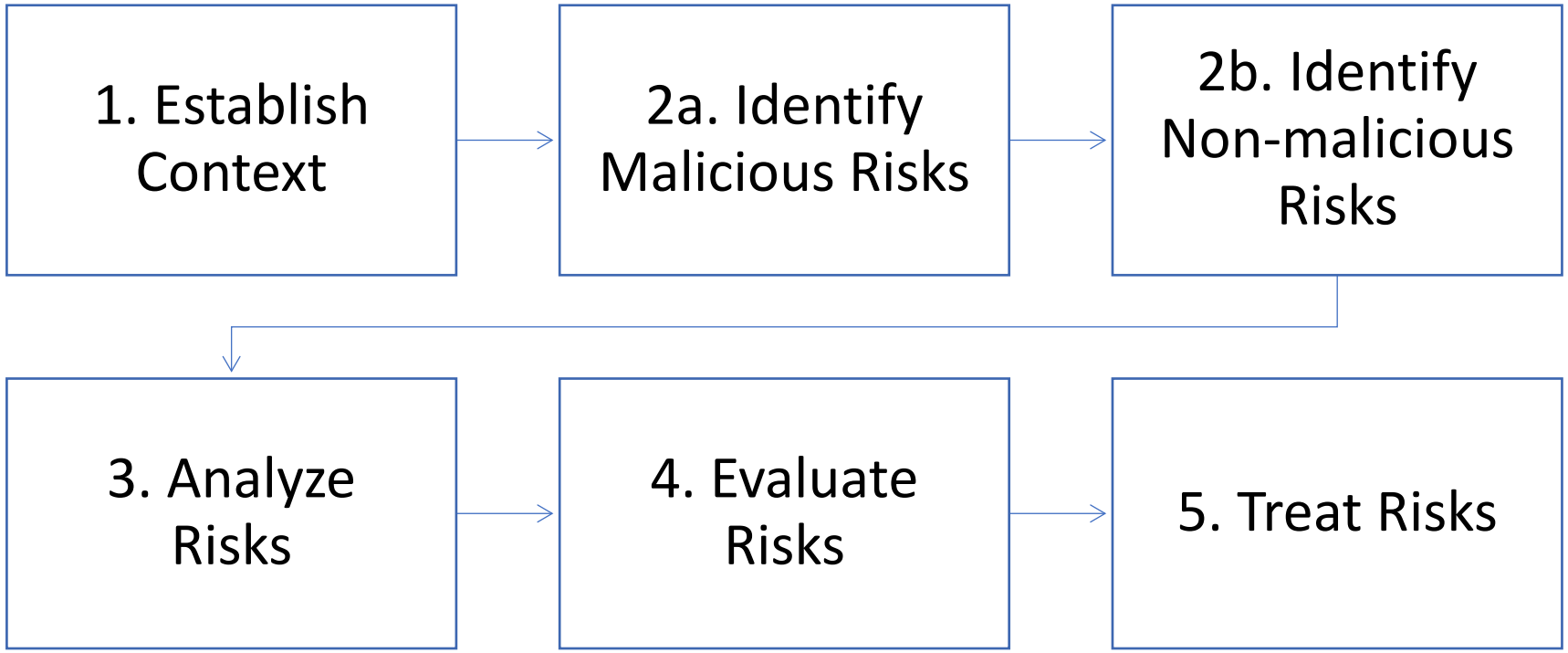
Cyber Risk – Management Process





Cyber Risk – Management Process





Cyber Risk – Monitoring

Monitoring can be through

- ✓ Logs, event logs
- ✓ Look for attacks and frequency of attacks
- ✓ Identify key risk indicators

Key Risk Indicators:

- KRIs can help identifying the overall risk posture of the organization. A number of variables may be considered when conducting a risk assessment and monitoring exercise.

Cyber Risk – Management Framework

Risk Management Frameworks standardize the processes integrating security, supply chain risk management activities into the development lifecycle.

We will look at the NIST Risk Management Framework in detail.

NIST Risk Management Framework:

The NIST Risk Management Framework was developed by the Department of Defense (DoD) and adopted in 2010 to provide the guidelines on how cyber systems should be architected and secured.

This framework includes several sub systems and processes and requires organizations to implement data security and identify cyber risks through threat modeling.

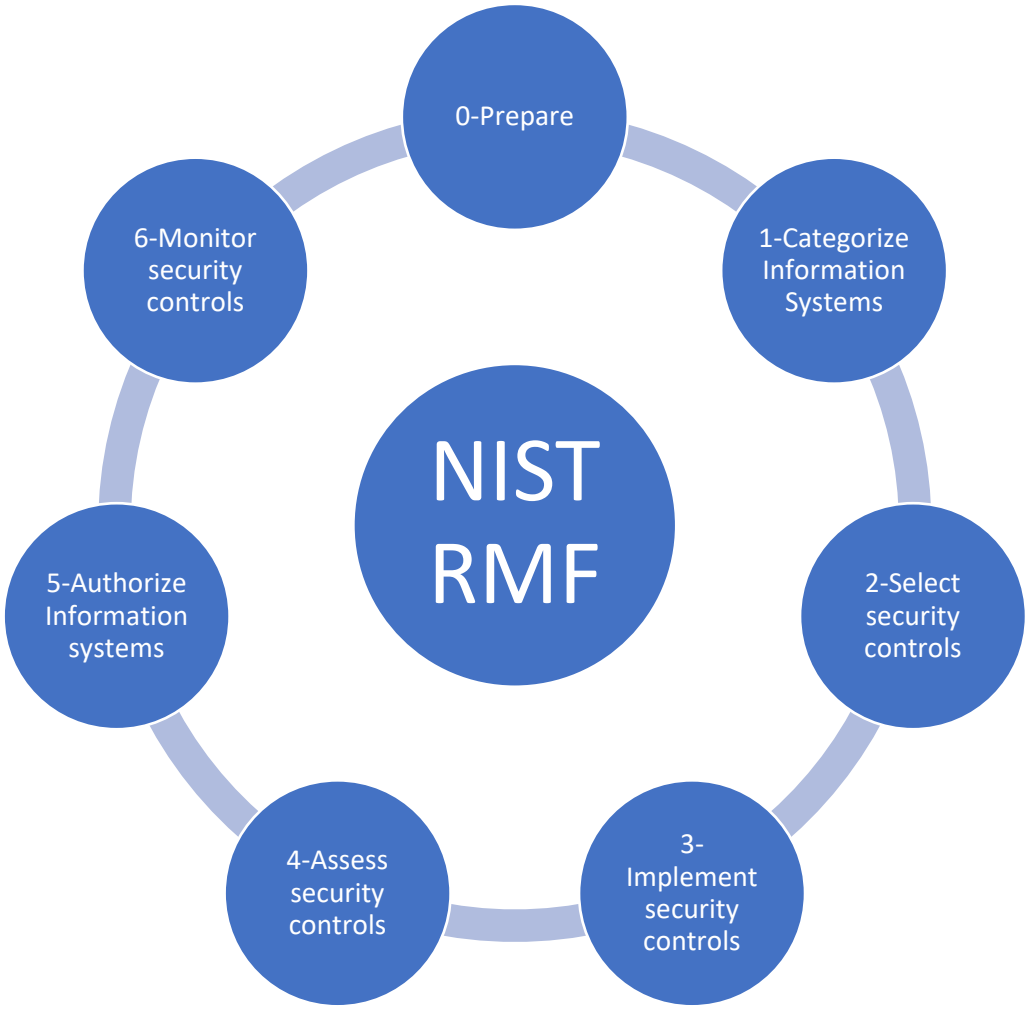
Cyber Risk – Management Framework

Risk Management Frameworks standardize the processes integrating security, supply chain risk management activities into the development lifecycle.

We will look at the NIST Risk Management Framework in detail.

Benefits of implementing an effective Risk Management Framework:

- ✓ Robust data and asset governance system
- ✓ Asset protection
- ✓ Compliance to standards
- ✓ IP Protection
- ✓ Reputation management



Cyber Risk – Resilience

Key components of cyber resilience strategy:

- Threat protection
- Recoverability
- Adaptability
- Durability

Benefits:

- Enhanced security
- Regulatory compliance
- Improved brand value
- Business development

Penetration Testing

Identifying vulnerabilities by simulating attacks on our infrastructure the same way in which an attacker would do. This helps in

- Proactively taking adequate measures in overcoming the weakness, technical flaws and vulnerabilities.
- Test and validate the efficiency of existing security protections and controls.
- Analyse the need for upgrading hardware resources.
- Classify severity on identified vulnerabilities.
- Assessing the security policy, its design, process and implementation.
- Relatively reduces the expense on IT security.
- Time to plan and prepare for any incident.
- Industry regulation.
- Best practices.

Penetration Testing

Key Elements

- Network Infrastructure Test
- Application-Based Test
- Cloud-Based Test

Testing Methods

- Unknown-Environment Test
- Known-Environment Test
- Partially Known - Environment Test

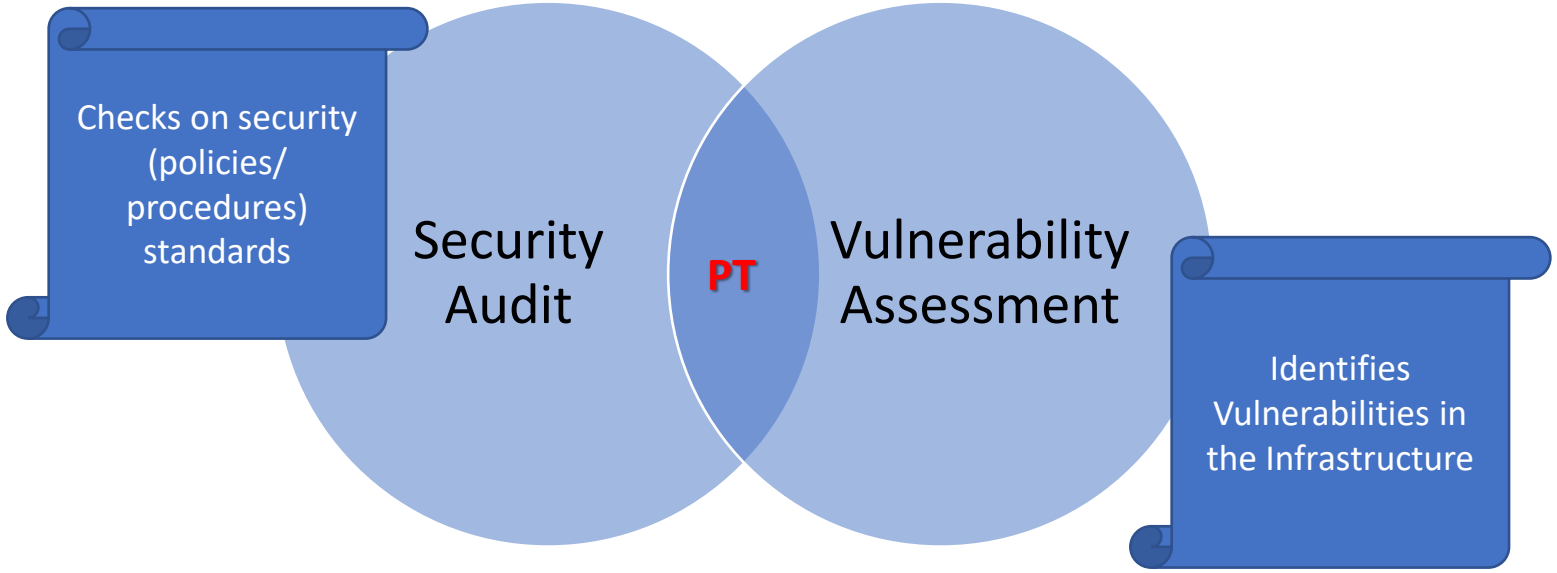
- Many penetration testers find the physical aspect of testing to be the most fun because they are essentially being paid to break into the facility of a target.
- This type of test can help expose any weaknesses in the physical perimeter as well as any security mechanisms that are in place, such as guards, gates, and fencing.
- The result should be an assessment of the external physical security controls.
- Most of the compromises today start with some kind of social engineering attack, such as a phone call, an email, a website, an SMS message, and so on.
- It is important to test how your employees handle these types of situations.
- This type of test is often omitted from the scope of a penetration testing engagement mainly because it primarily involves testing people instead of the technology.
- In most cases, management does not agree with this type of approach, but it is important to get a real-world view of the latest attack methods.
- The result of a social engineering test should be to assess the security awareness program so that you can enhance it.
- It should not be to identify individuals who fail the test.

Penetration Testing

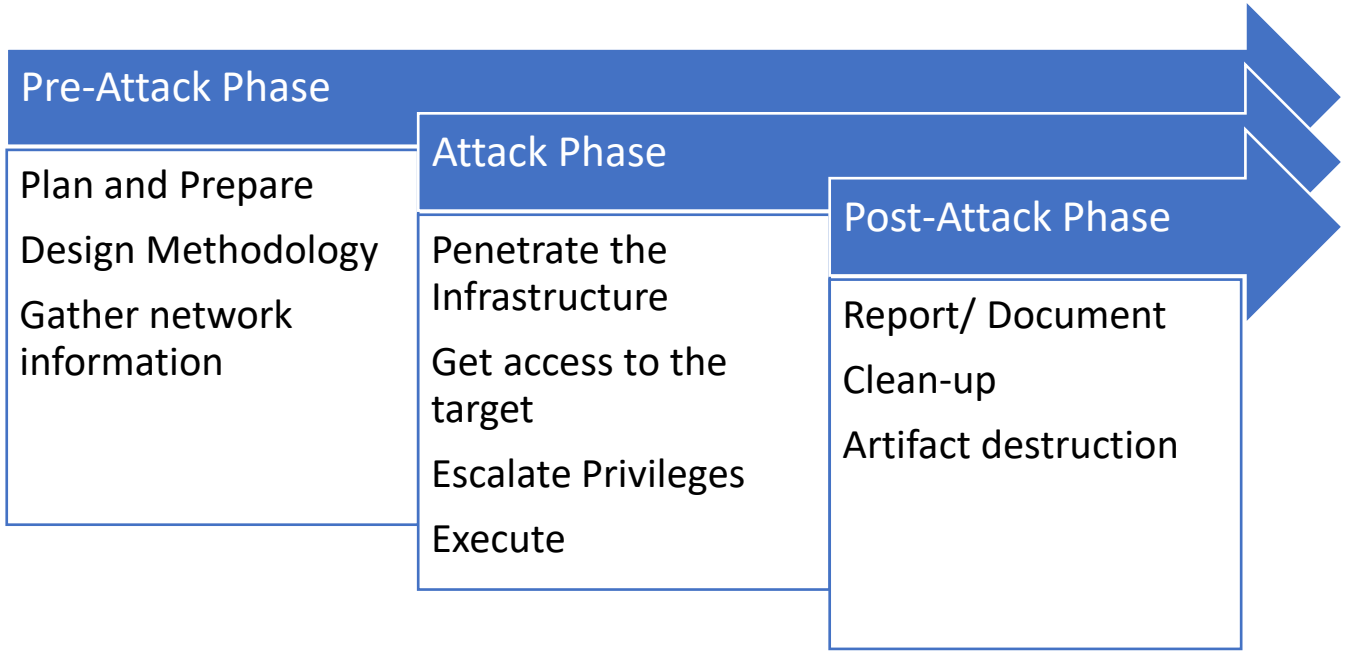
PT: It combines both security audits and vulnerability assessment. Helps in demonstrating the vuln. that could be successfully exploited.

Key Steps:

- Obtain Permission
- Document steps
- Write Report (Note that the Pen test report is most confidential and need to be discussed only with appropriate persons)



Penetration Testing

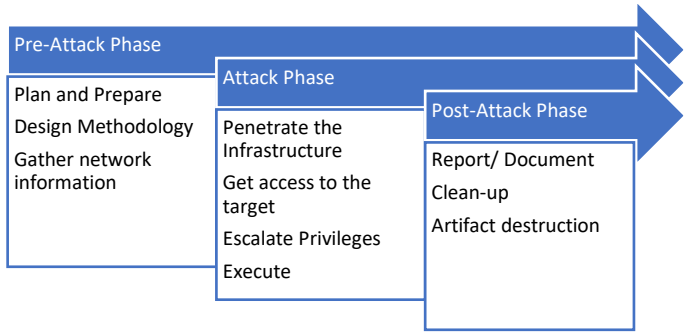


Types:

- Black-box: As its name says, it is a blind testing. Without any information about the infrastructure, the test will be executed.
- White-box: With the entire details about the infrastructure, test will be executed.
- Grey-box: With basic or limited knowledge, the test will be executed.

Penetration Testing

Any approach in assessing/ experimenting/ knowing new things need to adopt any proven methodology. A methodology is nothing but a proven approach to execute necessary steps.



- *The security testing method here leads to identify and check weak points in the aspect of security systems within an infrastructure.*
- *This process would help the authorities to initiate appropriate and adequate security measures ensuring safety of information and disruption of business*

OWASP (Open Web Application Security Project)

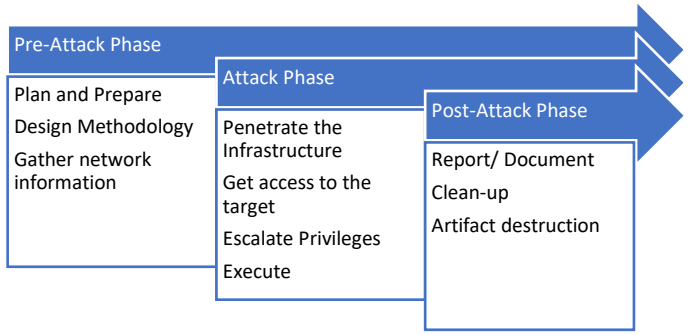
- *It is an open-source application security project. It helps to get, develop and maintain articles, methodologies, security tools, software applications and knowledge-based documentation for Web application security.*

OSSTMM (Open Source Security Testing Methodology Manual)

- *It is a methodology to test the operational security of physical locations, human interactions and all form of communications like wired, wireless, analog and digital. (data controls, fraud and social engineering control levels, physical security access controls, etc*
- *It is a peer and cross-disciplinary reviewed methodology.*

Penetration Testing

Any approach in assessing/ experimenting/ knowing new things need to adopt any proven methodology. A methodology is nothing but a proven approach to execute necessary steps.



- *The security testing method here leads to identify and check weak points in the aspect of security systems within an infrastructure.*
- *This process would help the authorities to initiate appropriate and adequate security measures ensuring safety of information and disruption of business*

MITRE ATT&CK

- *An amazing resource for learning about an adversary's tactics, techniques, and procedures (TTPs).*
- *Both offensive security professionals (penetration testers, red teamers, bug hunters, and so on) and incident responders and threat hunting teams use this framework today.*
- *It is a collection of different matrices of tactics, techniques, and subtechniques.*
- *These matrices–including the Enterprise ATT&CK Matrix, Network, Cloud, ICS, and Mobile–list the tactics and techniques that adversaries use while preparing for an attack, including gathering of information (open-source intelligence [OSINT], technical and people weakness identification, and more) as well as different exploitation and post-exploitation techniques.*

Penetration Testing

Penetration testing tools:

- Password crackers
- Wireless hacking, Network scanning and hacking
- Packet crafting, Packet sniffers
- Rootkit detectors
- Fuzzers to search vulnerabilities
- Forensic
- Debuggers
- Hacking operating systems
- Encryption
- Vulnerability exploitation, Vulnerability Scanners

Laws and Standards

- *PCI DSS (Payment Card Industry Data Security Standard) – proprietary information security standard for organisation to handle cardholder information (Debit/ Credit/ Prepaid/ ATM/ POS cards)*
- *ISO/IEC 27001:2013 – establishing, implementing, maintaining and improving information security management system*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Sarbanes Oxley Act (SOX) – 2002 – Protect investors and pubic by increasing the accuracy and reliability of corporate disclosures.*
- *UK Cyber Law*
  - *The Copyright, Trademarks (Offenses and Enforcement) Act 2002*
  - *Trademarks Act 1994 (TMA)*
  - *Computer Misuse Act 1990*
  - *The Data Protection Act 2018*

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

Advanced Cybersecurity

(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- EC-Council CEH
- Cisco Networking Academy
- Tevel Cyber Corps
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition

Advanced Cybersecurity

(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk