Unit 2: Attack Vectors, Threat, Risk And Vulnerability

2

Unit Structure

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand various terminology related to security
- Understand of relationship between different terminologies
- Understand how risk management is done to handle the potential risk associated with the threats

2.1 INTRODUCTION

This chapter we will introduce some of the key terms which will be usedthroughout the book and also will be used in different topics for the rest of the chapters. Also, we will see what kind of relationship is there between different terminologies. Different attack vectors, threats, associated risks, vulnerability, and consequences.

Also, we will see how risk management is done to handle the potential risk associated with the threats.

2.3KEY TERMINOLOGIES

Attack OR Attack Vector

An attack vector is defined as the technique by which unauthorized access is gained inside the computer or network for a criminal purpose by exploiting the vulnerabilities in the system.

Risk

It can be defined as the probability of the loss from any particular threat from the threat landscape, which can exploit the system and gain the benefits from it such as loss of private and confidential information such as username and password, sensitive organization data, also the loss of the reputation which has occurred can be considered. Also, the loss occurred in terms of damage or destruction of hardware and software assets can be considered as Risk.

Threat

Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Vulnerability

Weaknesses or gaps in a systems security program, design policies and implementation that can be exploited by different threats to gain unauthorized access of a computer system or network.

Asset

People, property, and information. People may include employees and customers. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, or by minimizing the harm it can cause, or by discovering and reporting it so that corrective and proactive action can be taken.

Here in the below image, we will the relationship between all the different terminologies we have seen.

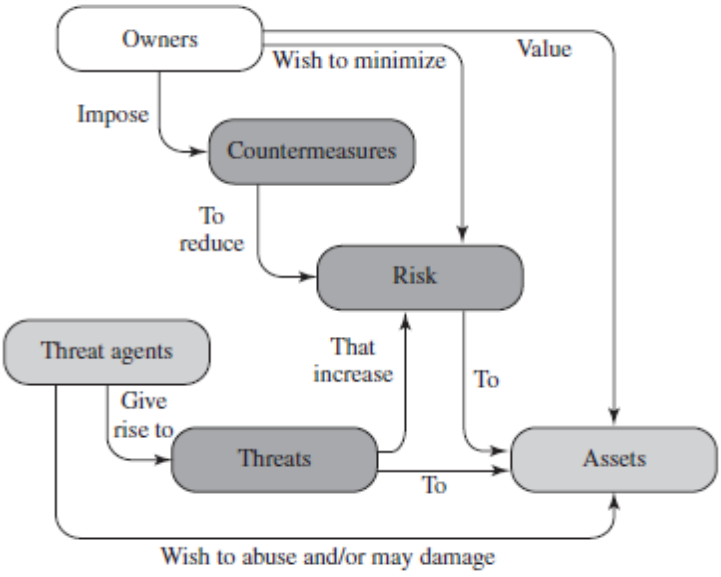

Figure 2.1 Security Concepts and Relationships

Let us start looking at each concept in details. But before that let us look key terminologies into the equation form which is given below and we will look at them in detail.

2.4ATTACK

We have already seen the definition of the attack on the previous page, we will look here the subtypes of attack and they are Active Attacks and Passive Attacks.

- **Active Attacks:** In an active attack, the attacker intercepts the connection and then modifies information.

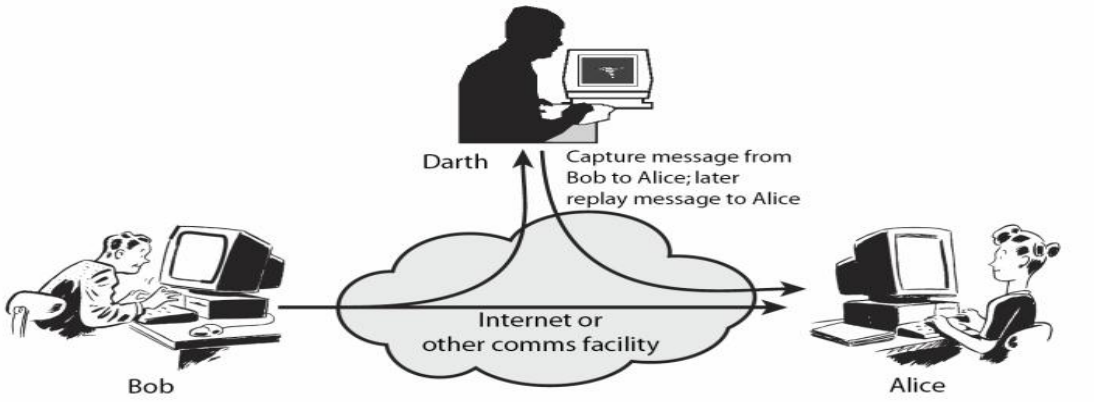

Figure 2.2 Active Attack Source:techdifferences.net

An active attack can be divided further into Masquerade, Replay attack, Modification of messages.

- **Passive Attack:** In a passive attack, the attacker intercepts the information but with the intent of reading the information and not modifying it. It can further be divided as Traffic Analysis and Release of Message content.

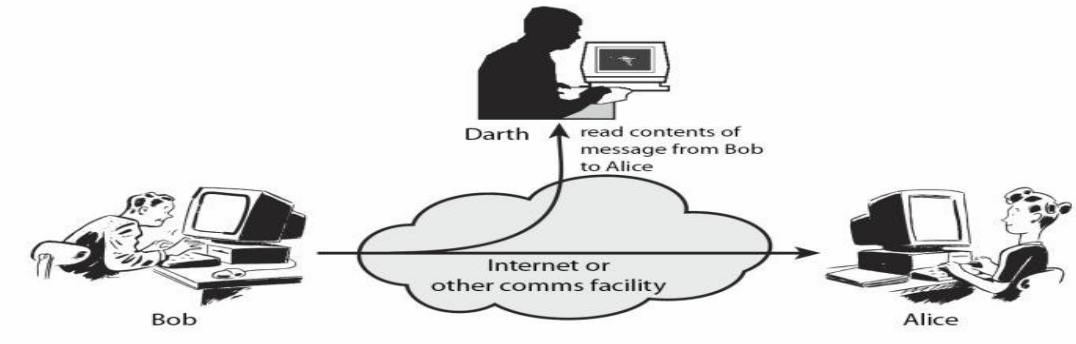

Figure 2.3 Passive Attack

We can also classify the attack based on its origin.

- **Inside Attack:** If the origin of the threat agent is from the inside the organization, which may have the authorization and access granted to the resources, but uses it with the criminal intent.
- **Outside Attack:** Origin or source of the attack is from the outside of the organization and gains the unauthorized access to the system or resources with the criminal intent.

A Cyberattack can destroy the business overnight, a proper security defense is required to stop such attacks. The main focus is to compromise the systems and gain access to sensitive data. Let us see the top cybersecurity attack and what do they do.

- **Phishing Attack:** It is a type of security attack that tricks the user to divulge the sensitive and personal/confidential information which is sometimes referred to as “Phishing Scam” also. Definitely, every user will not click the links provided in the email id for providing the details, but the attackers are smart they will perform the social engineering and will send the emails to the users with the similar content which user is already looking or interested in it.

  The most targeted business sectors are Payment Platforms, Financial and Banking organizations, Webmail services and Cloud storage/hosting providers.

  Phishing attacks engage users with a specific message and very solicit way for the response from the user which is ideally to click on the link is known as “Call To Action”. Which means the attacker wants the user action on the link provided in the email to perform the action.

    - **Spearphishing:** When a phishing attack is targeted to the specific individuals of the organization, it is known as spearphishing. Attackers use the solicit company logo, footer and all other style information which is present in the legit email to trick the user. The content of the email mainly focuses on the password reset email or, account reset activity.

For the prevention of the phishing, the user has to check clearly the from address and email content, along with the links present in the email body. Apart from this,

employees awareness using various teaching method is the most important as major data breach occurs due to human error which cannot be ignored.

- **SQL Injection Attack:** SQL which is pronounced as “squeal” stands for the structured query language. it’s a programming language used to communicate with databases. It is used to store critical data of websites/users/services in their databases which can contain personal and sensitive information such as username and password, transaction details.

  SQL Injection attack targets the database using specifically crafted SQL statements to trick the system into unexpected and undesired outputs.

  SQL Injection attack can be carried out in different ways which can be decided after the attacker identifies system behavior.

  If the web application is building a SQL query string dynamically with the account number the user will provide, it might look something like this:

  “SELECT * FROM customers WHERE account = ‘“ +
  userProvidedAccountNumber +”’;”

  While this works for users who are properly entering their account number, it leaves the door open for attackers. For example, if someone decided to provide an account number of “‘ or ‘1’ = ‘1”, that would result in a query string of:

  “SELECT * FROM customers WHERE account = ‘’ or ‘1’ = ‘1’;”

  Due to the ‘1’ = ‘1’ always evaluates to TRUE, sending this statement to the database will result in the data for all customers being returned instead of just a single customer.

  The above query might not work for all the database, but it can work where there are less or no security measures taken to filter such SQL injection queries.

Other types of SQL injection attacks include Blind SQL Injection, Out of Bound SQL Injection. SQL Injection attack can be prevented by avoiding the use of dynamic SQL, sanitize user inputs, don’t store data in plaintext, provide access control and privileges also use of web application firewall is a must.

- **Denial-of-service(DOS) and Distributed Denial of Service(DDOS):** Denial-of-Service attack focus on disrupting or preventing legitimate users from accessing

the websites or application or any other resources by sending flood of messages, packets, & connection requests, causing the target to slow down or “crash”, rendering it unavailable to its users. Attacker mostly targets high-end value organizations such as media houses, banking, and financial organization, E-Commerce to disrupt their services.

When the majority of present-day DoS attacks involve a number of systems (even into the hundreds of thousands) under the attacker’s control which are installed with the bots, all simultaneously attacking the target. This coordination of attacking systems is referred to as a “**Distributed Denial-of-Service**” **(DDoS).**

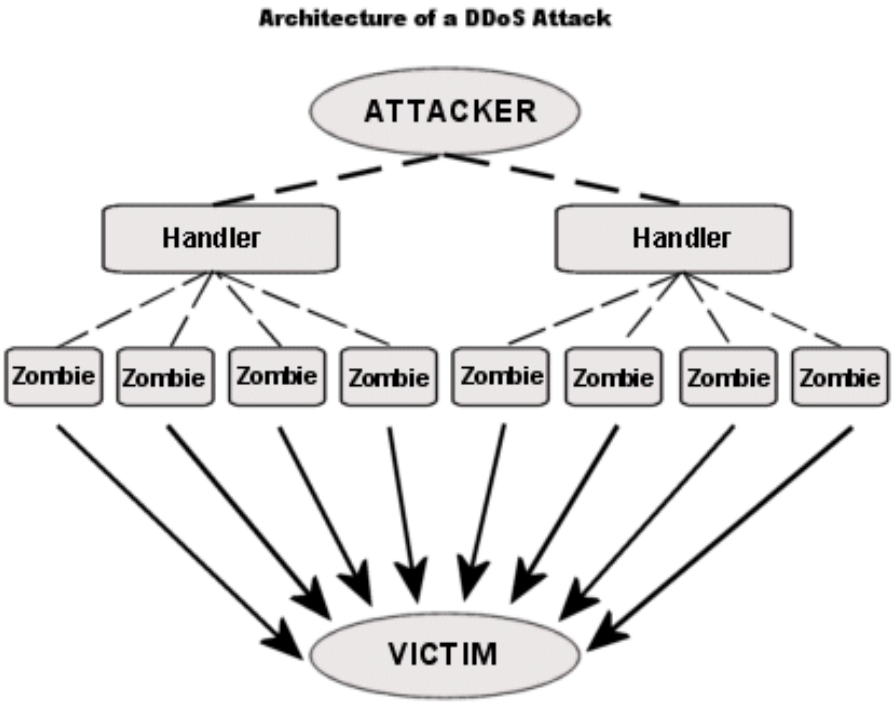

Figure 2.4 DDOS Architecture Source:Wikimedia.com

- **Man-In-The-Middle Attack and Session Hijacking:** Man-in-the-middle attacks are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen.

  When a user is using the internet and our computer performs a lot back and forth transaction, the application generates and uses a session ID which will be unique and to make the transactions private between user and application. The attacker

hijacks the session ID to eavesdrop the communication between user and application.

There are various types of Man-In-The-Middle Attack such as Rogue access points, ARP Spoofing, DNS Spoofing, Packet Injection, SSL Striping.

We can prevent such attacks by using strong WEP/WAP encryption on access points, using a virtual private network(VPN), enforce https and using a strong combination of the public key pair authentication.

- **BruteForce Attack(Password Attack):** The theory behind such an attack is that if you take an infinite number of attempts to guess a password, you are bound to be right eventually. The term brute-force means overpowering the system through repetition. A brute force attack is among the simplest and least sophisticated hacking method. Brute Force attacks often use automated systems or tools to perform the attack in which different password combinations are used to try to gain entry to a network, such as a dictionary attack list or using rainbow tables.

  The attacker aims to forcefully gain access to a user account by attempting to guess the username/email and password. Usually, the motive behind it is to use the breached account to execute a large-scale attack, steal sensitive data, shut down the system, or a combination of the three.

  We can prevent it by using a strong password combination policy and require to change a password on regular intervals, locking out accounts on a certain number of incorrect password attempts, use captcha, two-factor authentication, monitoring server logs, limit logins from the single IP/Range.

- **Malware Attack:** Malware can be described as Malicious software that is installed in your system without your consent. It can attach itself to the legitimate process or replicate itself or can put itself to startup. The objective of the malware could be to exfiltrate information, disrupt business operations, demand payment, There are many types of malware below are some of the commonly known types:
  - **Macro Virus:** These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes

instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.

- **Trojans:** A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers
- **Logic bombs:** A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
- **Worms:** Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm can result in denial-of-service attacks against nodes on the network.
- **Dropper:** A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.
- **Ransomware:** Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion and asks for the payment in bitcoin. Which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key or using the decryptor if it is available.
- **Adware:** Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up

windows or through a bar that appears on the computer screen automatically.

- **Spyware:** Spyware is a type of program that is installed to collect information about users, their computers or their browsing history. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.
- **Zero-Day Exploit:** A zero-day exploit hits after a vulnerability has been announced, but before a patch or solution is implemented. Attacker targets the disclosed vulnerability during this window of time.

To prevent such attack we need to ensure that the anti-virus product is up-to-date with the latest signatures, continues user education, performing regular audits, regular backup of the websites, application, and databases at multiple locations.Now we will start with understanding the complete Risk Rating Methodology. It will also include different steps such as Risk Analysis, Risk Assessment, and Risk Management.

Check Your Progress 1

1. What kind of malware encrypts the file and ask for ransom to decrypt the file

   _____

2. Mention any two types of SQL injection attacks

   _____

3. Which type of malicious software captures the user data and history

   _____

2.5RISK ASSESSMENT

Identifying threats and vulnerabilities is very important to build a robust security architecture. It always starts with identifying what are the important assets which need to be secured from threats. So the first and foremost task is to define the scope

of the cybersecurity Risk Assessment. Being able to estimate the associated risk to the business is very important.

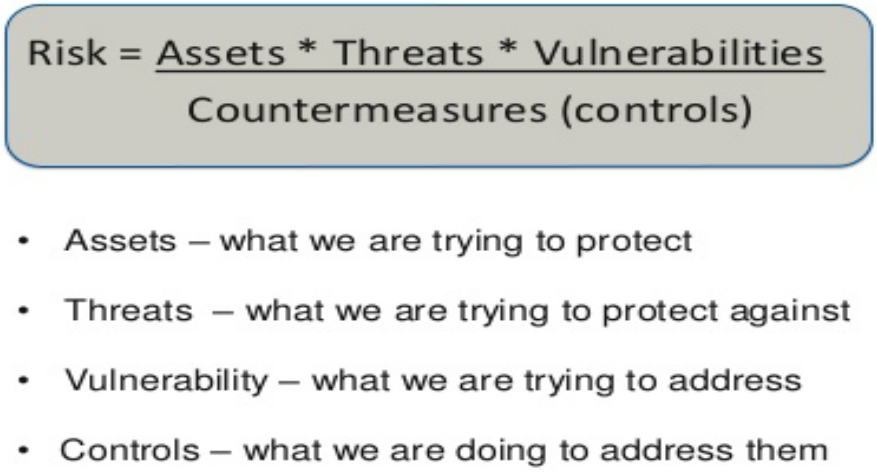

Figure 2.5 Risk Equation

- **Assets:** We have seen the definition of the Assets in the first section under key terminologies. Now we will understand the assets in relation to threat actions and will map with the CIA triad.

  Assets can be categorized in various types such as hardware, software, Data, and communication channel(different devices including communication cables). In details if we go it can be described as follow:

  Physical assets such as Computer, Laptop, Networking Devices, Storage Devices, etc..Software such as Operating system, Application Running on the system, services running, port scanning, API services, protocols used, and policies.

  All this can be considered as an important asset and are part of the scope of the Risk Assessment. One may identify security concerns in architecture or design. By using this process it is possible to estimate the severity of all of these risks to the business and make an informed decision about what to do about those risks. Having a system in place for rating risks will save time when there is a situation arise to take the critical business decision to reduce the impact.

  - **Asset Value Assessment:** This would be the first involved in measuring the asset value which is part of the critical business process. An asset can be the people, process, hardware, software, data, any tangible or intangible(can include the reputation of the

organization, loss of customer and services) things which are part of the critical business process.

In order to achieve greater control in risk and with effective least cost, identifying and prioritizing the assets are a critical part of the process from top priority to least priority.

This can be achieved by identifying the core functions and the process of the organization. Along with this identifying the physical infrastructure, assets which can be critical hardware or software related to the business functions and safety measures which are preinstalled for the emergency situations need to be also considered.

- **Threats actions and its Consequences:** As per the RFC 2828 we will see some terminologies related to the threat, we have already seen the definition of the threat in the first section of key terminologies.

  After identifying the asset value assessment and quantifying it, next step is to conduct the Threat assessment where the potential threats are identified.

  There is another relative term “Hazard” is also used for the threats which are natural or not man-made, such as earthquake, flood or wind disaster which also needs to be considered and the man-made hazard can be either technological threats or terrorism which we can refer as “Threats” for simplicity.

  - **Threat Action:** It is an assault on system security.
  - **Threat Analysis:** An analysis of the probability of occurrences and consequences of damaging actions to a system.
  - **Threat Consequence:** A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation.

Threat Action (attack)	**Threat Consequence**
Exposure: Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive	**Unauthorized Disclosure:** A circumstance or event whereby an entity gains access to data for which the entity is not authorized.

data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.	
Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.	**Deception:** A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
Incapacitation: Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.	**Disruption:** A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Misappropriation: An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.	**Usurpation:** A circumstance or event that results in control of system services or functions by an unauthorized entity.

Table 2.1 Threat Action and Consequences Source: RFC 2828

Check Your Progress 2

1. What kind of threat action can cause the unauthorized disclosure of data _____
2. What kind of event authorized user can receive false data _____
3. What do we call if due to undesirable action data is altered _____

- **Threat Analysis:** Our next goal here is to estimate the likelihood of a successful attack by this group of threat agents for this we will use the OWASP risk rating methodology for preparing severity of the Risk Assessment Model.

  Skill level: How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9),

  Motive: How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

  Opportunity: What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

Size: How large is this group of threat agents? Developers (2), system admins (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

The use of a rating system will help in the quantification of risk. There is always difficulty in justifying the protection of assets. Management is better able to understand the implications of the threat and vulnerabilities when they are presented in the form of numbers and statistics which means quantifiable and measurable.

- **Vulnerability Analysis:**A vulnerability is a weakness that a threat can exploit to breach security and harm your organization. Vulnerabilities can be identified through vulnerability analysis, audit reports, the NIST vulnerability database, vendor data. The problem faced within many organizations is the ability to effectively filter out the false positives from assessment applications.

  The result of the various manual and automated tools must be verified in order to accurately determine the reliability of the tools in use and to avoid protecting an area that in reality does not exist. False positive results can be mitigated by ensuring that the assessment applications are up to date with the latest stable signatures and patches.

  There are two ways penetration testing and vulnerability analysis can be done, one with having the knowledge of the systems and topology, another with zero knowledge which is mostly conducted externally known as black box testing.

  Examples of vulnerabilities:

  - Lack of sufficient logging mechanism
  - Input validation vulnerability
  - Sensitive data protection vulnerability
  - Session management vulnerability
  - Cryptographic vulnerability
  - Memory leak Issue
  - Cross-site request forgery
  - Remote Code Execution
  - Business logic vulnerability

  For more similar issues refer to OWASP Top Ten Project

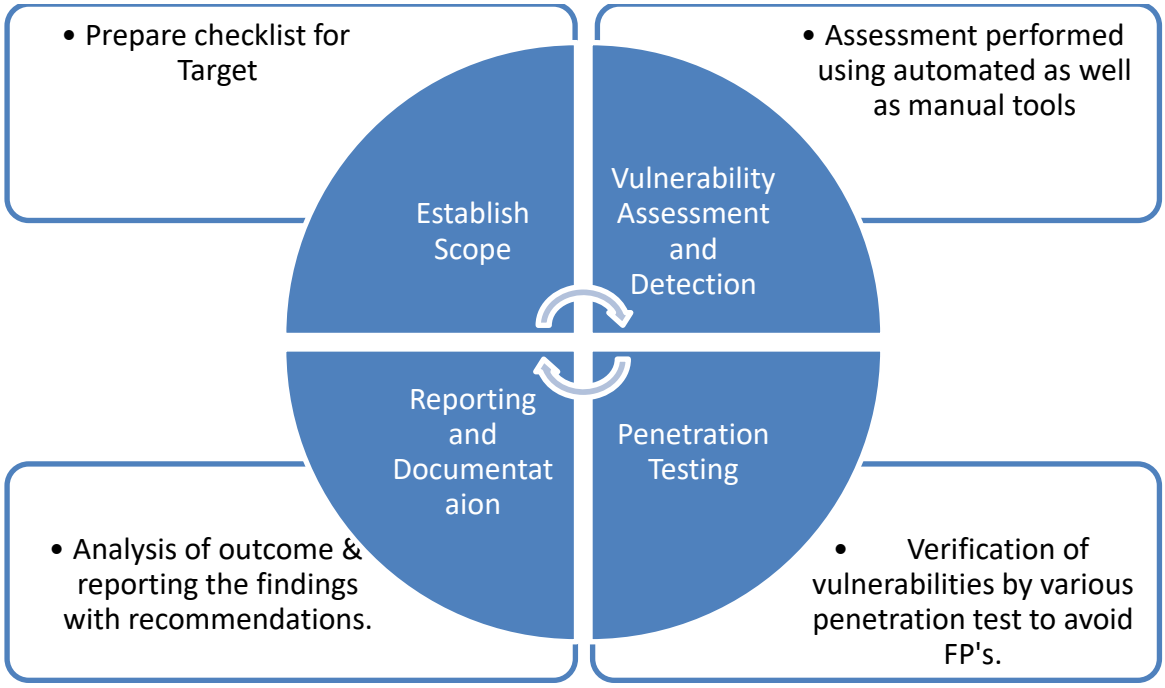

Figure 2.6 VAPT Process

- **Vulnerability Factors:** The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

  Ease of discovery: How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

  Ease of exploit: How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

  Awareness: How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

  Intrusion detection: How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

- **Estimating Impact:** When estimating the impact of the successful attack, it is important to consider the technical impact and business impact.

Ultimately the business impact would be more important. So by providing the appropriate technical risk details which will enable management to make the decision about the business risk.

- **Technical Impact Factors:** The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

  Loss of confidentiality: How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

  Loss of integrity: How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

  Loss of availability: How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)

  Loss of accountability: Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

- **Business Impact Factors:** Business impact requires a deep understanding of the different operations on which the company is working and gets maximum return on investment.

There are many factors and also may not be the same for all organization, but we will see some of the common impact factors.

- **Financial damage:** How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- **Reputation damage:** Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)

- **Non-compliance:** How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
- **Privacy violation:** How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

➢ **The severity of RISK:** We will now prepare the severity of the risk which can be obtained by combining the different impact factors.

It is divided into three parts from a 0-9 scale, low medium or high as shown below.

Impact Scale	Impact Levels
0-<3	LOW
3-<6	MEDIUM
6-9	HIGH

Table 2.2 Severity Matrix

➢ **Countermeasures(Control):** In this step, we have to identify the existing security policies and protocols which are placed. Are they are adequate with the current threat landscape? Or it needs to modify and update the security posture of the organization. What level of risk is acceptable to the organization. This will help the security team and top management to understand the risk levels and they can focus on more high-level risks.

➢ **Documentation:** This is the final step in which risk assessment report is prepared to support the management to take appropriate decision on policies, procedures, budget allocation. For each threat, the report should have corresponding vulnerabilities, assets at risk, impact, and control remediation.

2.6LET US SUM UP

In this chapter, we have seen what all different types of attacks and what it can cause. Next is we have seen threats and consequences. Which is followed by Risk Assessment procedure which includes threat assessment, vulnerability assessment

and how to prepare the severity matrix to report the threat to management. Also based on the identified risk in the report we have to recommend the security policy and procedure to rebuild the security posture of the organization from the current threats and attacks.

2.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. Ransomware
2. Blind SQL Injection & Out of bound SQL Injection
3. Spyware

Check Your Progress 2

1. Exposer
2. Deception
3. Corruption