What is Vulnerability Management?

Objectives:

At the end of this episode, I will be able to:

Understand what a vulnerability is.

Explain the difference between the various vulnerability classifications.

Identify what a vulnerability assessment is.

Define what the phases of the Vulnerability Management Life Cycle are.

External Resources:

Vulnerability Management

What is a Vulnerability? -

the existence of a weakness, design, or an implementation error that, when exploited, leads to an unexpected and undesirable event compromising the security of the system.

What are some common Vulnerability Research Websites? -

Common Vulnerability Scoring System (CVSS) (https://nvd.nist.gov)

The Common Vulnerability Scoring System (CVSS) is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

- Common Vulnerabilities and Exposures (CVE) (https://cve.mitre.org)
- National Vulnerability Database (NVD) (https://nvd.nist.gov)

Are there Vulnerability Classifications?: (9)

```
▪ Misconfigurations - the most common vulnerability that is mainly caused by
human error, which allows attackers to gain unauthorized access to the system.

▪ Default Installations - Not changing default settings on software or
hardware makes it much more likely that the attacker will be able to guess the
settings in order to break into the systems.

▪ Buffer Overflows - attackers try to take control of the system by writing
content beyond the allocated size of the buffer. Insufficient bounds checking
in the program is the root cause. Systems often crash or become unstable when
buffer overflow occurs.

▪ Unpatched Servers - These unpatched servers act as an entry point into the
network. This can lead to exposure of private data, financial loss,
discontinuation of operations, and so on.

▪ Design Flaws - Design vulnerabilities such as incorrect encryption or poor
validation of data refer to logical flaws in the functionality of the system
that are exploited by the attackers to bypass the detection mechanism and
acquire access to a secure system.

▪ Operating System Flaws - Patching of the OS, installing the minimum software
applications necessary, and the use of applications with firewall capabilities
are essential steps that an administrator needs to take to protect the OS from
attack.

▪ Application Flaws - Applications pose security threats such as data
tampering and unauthorized access to configuration stores. It is important for
developers to understand the anatomy of common security vulnerabilities and
develop highly secure applications by providing proper user validation and
authorization.

▪ Open Services - Open ports and services may lead to loss of data, DoS
attacks, and allow attackers to perform further attacks on other connected
devices. Administrators need to continuously check for unnecessary or insecure
ports and services to reduce the risk on the network.

▪ Default Passwords - make devices and systems vulnerable to various attacks
such as brute-force and dictionary attack. Passwords should be kept secret;
failing to protect the confidentiality of a password allows the system to be
compromised with ease.
```

What is a Vulnerability Assessment?

An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It seeks to identify, measure, and classify 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
```

Types of Vulnerability Assessments: (8)

```
▪ Active
▪ Passive
▪ External
▪ Internal
▪ Host-Based
▪ Network
▪ Application
▪ Wireless
```

What is the Vulnerability Management Life Cycle?

Helps in finding and remediating security weaknesses before they are exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are found.

The phases involved in vulnerability management are:

```
▪ Creating Baseline - critical assets are identified and prioritized.

▪ Vulnerability Assessment - the security analyst identifies the known
vulnerabilities in the organization infrastructure.

▪ Risk Assessment - summarizes the vulnerability and risk level identified for
each of the selected asset. It determines the risk level for a particular
asset, whether it is high, moderate, or low.

▪ Remediation - the process of reducing the severity of vulnerabilities.
```

NOTE: This phase is initiated after the successful implementation of baselining and assessment steps.

```
▪ Verification - allows the security team to check whether all the previous
phases have been properly executed.

▪ Monitor - Continuous monitoring identifies potential threats and any new
vulnerabilities that may arise.
```

What is the Post-Assessment Phase?

Also known as the recommendation phase, it is performed after the risk assessment. Post-assessment is based on the risk assessment.

Risk characterization is categorized by the key criteria, which helps to prioritize the list of recommendations.

The tasks performed in the post-assessment phase include:

```
▪ Making the priority list for assessment recommendations
▪ Developing an action plan to implement the proposed recommendation
▪ Capturing lessons learned to improve the complete process in the future
▪ Conducting training for the employees
```

NOTE: Post-assessment includes risk assessment, remediation, verification, and monitoring.

Steps for each phase:

Steps involved in creating a baseline:

```
1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes
3. Create an inventory of all assets, and prioritize/rank the critical assets
4. Map the network infrastructure
5. Identify the controls already in place
6. Understand policy implementation and standards compliance to the business processes
7. Define the scope of the assessment
8. Create information protection procedures to support effective planning, scheduling, coordination, and
logistics
```

Steps involved in Vulnerability Assessment phase:

```
1. Examine and evaluate physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Identify and prioritize vulnerabilities
5. Apply business and technology context to scanner results
6. Perform OSINT information gathering to validate the vulnerabilities
7. Create a vulnerability scan report
```

The tasks performed in the risk assessment phase include:

```
1. Perform risk characterization
2. Assess the level of impact
3. Determine the threat and risk level
```

The tasks performed in the remediation phase include:

```
1. Prioritize recommendations
2. Develop an action plan to implement the recommendation
3. Perform root-cause analysis
4. Apply patches/fixes
5. Capture lessons learned
6. Conduct awareness training
```

The tasks performed in the verification phase include:

```
1. Perform dynamic analysis
2. Attack surface review
```

The tasks performed in the monitoring phase include:

```
1. Monitoring intrusion detection and intrusion prevention logs
2. Implementation of policies, procedures, and controls
```