Vulnerability Assessment

Introduction

This task introduces the learner to the concept of Vulnerability Assessments. The learning objectives will take the learner through:

- the review of differences between vulnerability assessments and penetration tests
- how to carry out a vulnerability assessment
- how to interpret the assessment results
- how to deliver an effective vulnerability.

Activities

Security Assessment

The primary purpose of most types of security assessments is to find and confirm vulnerabilities are present, so – as Security Analyst, can work to patch, mitigate, or remove them.

Vulnerability Assessment

A vulnerability assessment is based on a particular security standard, and compliance with standards is analyzed and look for vulnerabilities in networks without simulating cyber attacks.

Penetration Tests

Evaluate the security of different assets and the impact of the issues present in the environment. Penetration tests can include manual and automated tactics to assess an organization's security posture. They also often give a better idea of how secure a company's assets are from a testing perspective.

A pentest is a simulated cyber attack to see if and how the network can be penetrated.

Types of Pentest

Black box pentesting is done with no knowledge of a network's configuration or applications. Typically a tester will either be given network access and nothing else (requiring them to perform their own discovery for IP addresses) if the pentest is internal, or nothing more than the company name if the pentest is from an external standpoint. This type of pentesting is usually conducted by third parties from the perspective of an external attacker.

Grey box pentesting is done with a little bit of knowledge of the network they're testing, from a perspective equivalent to an employee who doesn't work in the IT department.

White box pentesting is typically conducted by giving the penetration tester full access to all systems, configurations, build documents, etc., and source code if web applications are in-scope. The goal here is to discover as many flaws as possible that would be difficult or impossible to discover blindly in a reasonable amount of time.

Penetration testers must have knowledge of many different technologies but still will have a specialty.

Application pentesters assess web applications, thick-client applications, APIs, and mobile applications. They will often be well-versed in source code review and able to assess a given web application from a black box or white box standpoint (typically a secure code review).

Network or infrastructure pentesters assess all aspects of a computer network, including its networking devices such as routers and firewalls, workstations, servers, and applications. These types of penetration testers typically must have a strong understanding of networking, Windows, Linux, Active Directory, and at least one scripting language. Network vulnerability scanners, such as Nessus, can be used alongside other tools during network pentesting, but network vulnerability scanning is only a part of a proper pentest.

Physical pentesters try to leverage physical security weaknesses and breakdowns in processes to gain access to a facility such as a data center or office building.

Social engineering pentesters test human beings.

- Can employees be fooled by phishing, vishing (phishing over the phone), or other scams?
- Can a social engineering pentester walk up to a receptionist and say, "yes, I work here?"

Other Types of Security Assessments

Security Audits

They are typically requirements from outside the organization, and they're typically mandated by government agencies or industry associations to assure that an organization is compliant with specific security regulations.

Bug Bounties

Bug bounty programs are implemented by all kinds of organizations. They invite members of the general public, with some restrictions (usually no automated scanning), to find security vulnerabilities in their applications.

Red Team Assessment

Companies with larger budgets and more resources can hire their own dedicated red teams or use the services of third-party consulting firms to perform red team assessments. A red team consists of offensive security professionals who have considerable experience with penetration testing.

A red team is a type of evasive black box pentesting, simulating all kinds of cyber attacks from the perspective of an external threat actor. These assessments typically have an end goal (i.e., reaching a critical server or database, etc.).

Purple Team Assessment

A **blue team** consists of defensive security specialists. They are people who work in a SOC (security operations center) or a CSIRT (computer security incident response team). They have experience with digital forensics too. With blue teams being defensive and red teams offensive; **red** mixed with **blue** is **purple**.

Purple teams are formed when offensive and defensive security specialists work together with a common goal, to improve the security of their network.

Vulnerability Assessment

A Vulnerability Assessment aims to identify and categorize risks for security weaknesses related to assets within an environment. It is important to note that there is little to no manual exploitation during a vulnerability assessment. A vulnerability assessment also provides remediation steps to fix the issues.

The purpose of a Vulnerability Assessment is to understand, identify, and categorize the risk for the more apparent issues present in an environment without actually exploiting them to gain further access.

Methodology

As Security Analyst you must be well versed with vulnerability assessment methodology that most organizations could follow and find success with.

They are:

1. **Conduct Risk Identification and Analysis**
2. **Develop Vulnerability Scanning Policies**
3. **Identify The Types of Scans**
4. **Configure the Scan**
5. **Perform the Scan**
6. **Evaluate and Consider Possible Risks**
7. **Interpret The Scan Results**
8. **Create a Remediation & Mitigation Plan**

Vulnerability

A ***Vulnerability*** is a weakness or bug in an organization's environment, including applications, networks, and infrastructure, that opens up the possibility of threats from external actors. Vulnerabilities can be registered through MITRE's **Common Vulnerability Exposure database** and receive a **Common Vulnerability Scoring System (CVSS)** score to determine severity. This scoring system is frequently used

as a standard for companies and governments looking to calculate accurate and consistent severity scores for their systems' vulnerabilities.

Threat

A Threat is a process that amplifies the potential of an adverse event, such as a threat actor exploiting a vulnerability. Some vulnerabilities raise more threat concerns over others due to the probability of the vulnerability being exploited. For example, the higher the reward of the outcome and ease of exploitation, the more likely the issue would be exploited by threat actors.

Exploit

An Exploit is any code or resources that can be used to take advantage of an asset's weakness. Many exploits are available through open-source platforms such as Exploitdb or the Rapid7 Vulnerability and Exploit Database. We will often see exploit code hosted on sites such as GitHub and GitLab as well.

Risk

Risk is the possibility of assets or data being harmed or destroyed by threat actors.

Asset Management

When an organization of any kind, in any industry, and of any size needs to plan their cybersecurity strategy, they should start by creating an inventory of their data assets.

Asset Inventory

Asset inventory is a critical component of vulnerability management. An organization needs to understand what assets are in its network to provide the proper protection and set up appropriate defenses. The asset inventory should include information technology, operational technology, physical, software, mobile, and development assets.

Application and System Inventory

An organization should create a thorough and complete inventory of data assets for proper asset management for defensive security. Data assets include:

- All data stored on-premises. HDDs and SSDs in endpoints (PCs and mobile devices), HDDs & SSDs in servers, external drives in the local network, optical media (DVDs, Blu-ray discs, CDs), flash media (USB sticks, SD cards). Legacy technology may include floppy disks, ZIP drives (a relic from the 1990s), and tape drives.
- All of the data storage that their cloud provider possesses. *Amazon Web Services* (AWS), *Google Cloud Platform* (GCP), and *Microsoft Azure* are some of the most popular cloud providers,

Assessment Standards

Both penetration tests and vulnerability assessments should comply with specific standards to be accredited and accepted by governments and legal authorities. Such standards help ensure that the assessment is carried out thoroughly in a generally agreed-upon manner to increase the efficiency of these assessments and reduce the likelihood of an attack on the organization.

Compliance Standards

Each regulatory compliance body has its own information security standards that organizations must adhere to maintain their accreditation. The big compliance players in information security are PCI, HIPAA, FISMA, and ISO 27001.

These accreditations are necessary because it certifies that an organization has had a third-party vendor evaluate its environment. Organizations also rely on these accreditations for business operations since some companies won't do business without specific accreditations from organizations.

Payment Card Industry Data Security Standard (PCI DSS)

The *Payment Card Industry Data Security Standard (PCI DSS)* is a commonly known standard in information security that implements requirements for organizations that handle credit cards. While not a government regulation, organizations that store, process, or transmit cardholder data must still implement PCI DSS guidelines. This would include banks or online stores that handle their own payment solutions (e.g., Amazon).

PCI DSS requirements include internal and external scanning of assets. For example, any credit card data that is being processed or transmitted must be done in a Cardholder Data Environment (CDE). The CDE environment must be adequately segmented from normal assets. CDE environments are segmented off from an organization's regular environment to protect any cardholder data from being compromised during an attack and limit internal access to data.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is the Health Insurance Portability and Accountability Act, which is used to protect patients' data. HIPAA does not necessarily require vulnerability scans or assessments; however, a risk assessment and vulnerability identification are required to maintain HIPAA accreditation.

Federal Information Security Management Act (FISMA)

`The *Federal Information Security Management Act (FISMA)* is a set of standards and guidelines used to safeguard government operations and information. The act requires an organization to provide documentation and proof of a vulnerability management program to maintain information technology systems' proper availability, confidentiality, and integrity.

ISO 27001

It is a standard used worldwide to manage information security. It requires organizations to perform quarterly external and internal scans.

Although compliance is essential, it should not drive a vulnerability management program. Vulnerability management should consider the uniqueness of an environment and the associated risk appetite to an organization.

The International Organization for Standardization (ISO) maintains technical standards for pretty much anything you can imagine. The ISO 27001 standard deals with information security. ISO 27001 compliance depends upon maintaining an effective Information Security Management System. To ensure compliance, organizations must perform penetration tests in a carefully designed way.

Penetration Testing Standards

Penetration tests should not be performed without any rules or guidelines. There must always be a specifically defined scope for a pentest, and the owner of a network must have a signed legal contract

with pentesters outlining what they're allowed to do and what they're not allowed to do. Pentesting should also be conducted in such a way that minimal harm is done to a company's computers and networks. Penetration testers should avoid making changes wherever possible (such as changing an account password) and limit the amount of data removed from a client's network. For example, instead of removing sensitive documents from a file share, a screenshot of the folder names should suffice to prove the risk.

In addition to scope and legalities, there are also various pentesting standards, depending on what kind of computer system is being assessed. Here are some of the more common standards you may use as a pentester.

PTES

The **Penetration Testing Execution Standard** (PTES) can be applied to all types of penetration tests. It outlines the phases of a penetration test and how they should be conducted. These are the sections in the PTES:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

OSSTMM

It is the Open Source Security Testing Methodology Manual, another set of guidelines pentesters can use to ensure they're doing their jobs properly. It can be used alongside other pentest standards.

OSSTMM is divided into five different channels for five different areas of pentesting:

1. Human Security (human beings are subject to social engineering exploits)
2. Physical Security
3. Wireless Communications (including but not limited to technologies like WiFi and Bluetooth)
4. Telecommunications
5. Data Networks

NIST

The NIST (***National Institute of Standards and Technology***) is well known for their ***NIST Cybersecurity Framework***, a system for designing incident response policies and procedures. NIST also has a Penetration Testing Framework. The phases of the NIST framework include:

- Planning
- Discovery
- Attack
- Reporting

OWASP

OWASP stands for the **Open Web Application Security Project**. They're typically the go-to organization for defining testing standards and classifying risks to web applications.

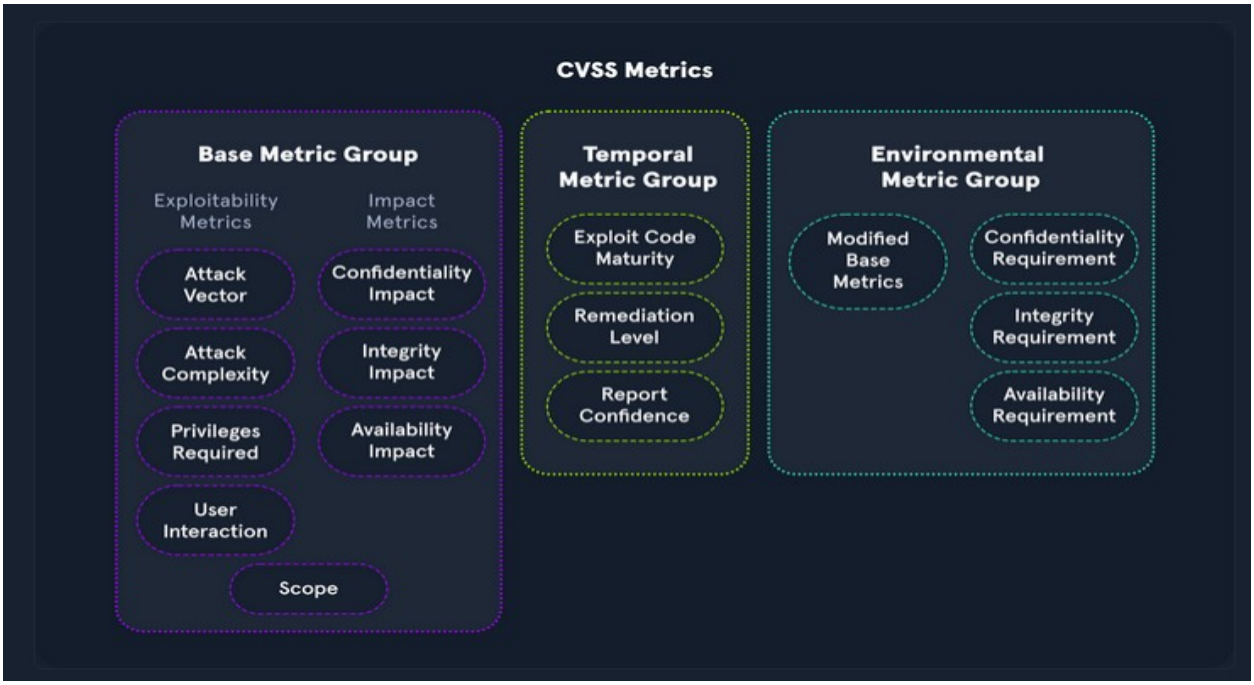
OWASP maintains a few different standards and helpful guides for assessment various technologies:

- **Web Security Testing Guide (WSTG)**
- **Mobile Security Testing Guide (MSTG)**
- **Firmware Security Testing Methodology**

Common Vulnerability Scoring System (CVSS)

The **Common Vulnerability Scoring System (CVSS)** is an industry standard for performing these calculations. The CVSS is often used together with the so-called **Microsoft DREAD**. DREAD is a risk assessment system developed by Microsoft to help IT security professionals evaluate the severity of security threats and vulnerabilities. It is used to perform a risk analysis by using a scale of 10 points to assess the severity of security threats and vulnerabilities. With this, a Security Analyst is able to calculate the risk of a threat or vulnerability based on five main factors:

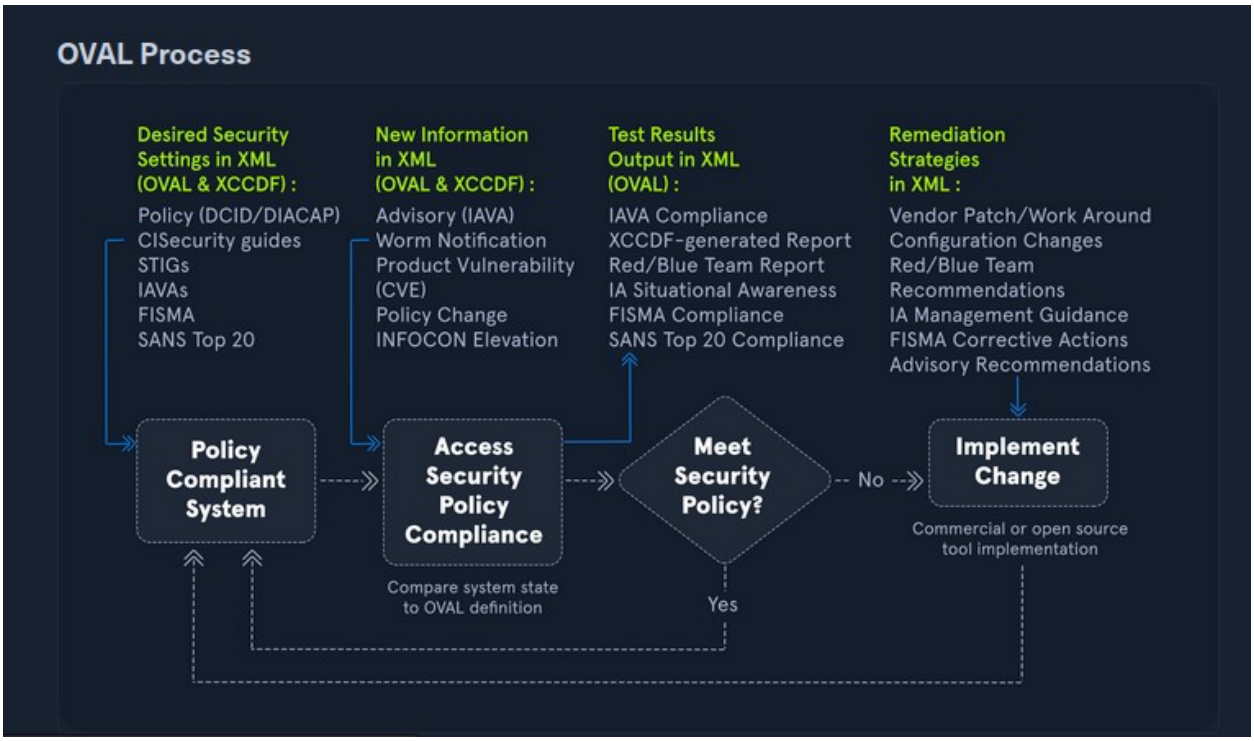
- *Damage Potential*
- *Reproducibility*
- *Exploitability*
- *Affected Users*
- *Discoverability*



Common Vulnerabilities and Exposures (CVE)

Open Vulnerability Assessment Language (OVAL)

Open Vulnerability Assessment Language (OVAL) is a publicly available information security international standard used to evaluate and detail the system's current state and issues.



The goal of the OVAL language is to have a three-step structure during the assessment process that consists of:

- Identifying a system's configurations for testing
- Evaluating the current system's state
- Disclosing the information in a report

OVAL Definitions

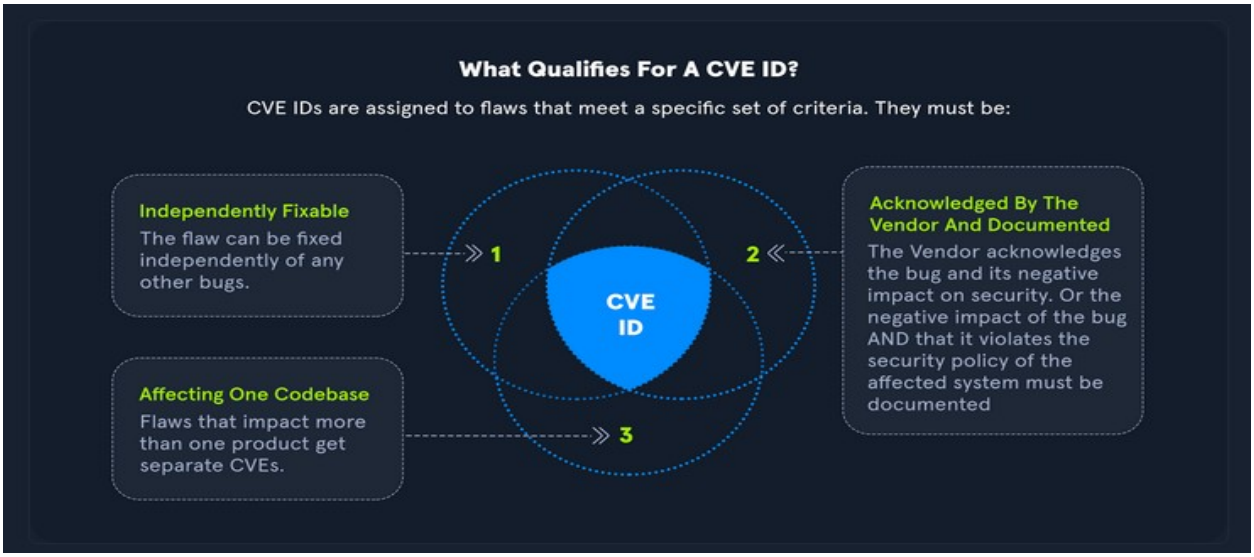
The OVAL definitions are recorded in an XML format to discover any software vulnerabilities, misconfigurations, programs, and additional system information taking out the need to exploit a system.

The four main classes of OVAL definitions consist of:

- OVAL Vulnerability Definitions: Identifies system vulnerabilities
- OVAL Compliance Definitions: Identifies if current system configurations meet system policy requirements
- OVAL Inventory Definitions: Evaluates a system to see if a specific software is present
- OVAL Patch Definitions: Identifies if a system has the appropriate patch

Additionally, **the OVAL ID Format** consist of a unique format that consists of "oval:Organization Domain Name:ID Type:ID Value". The ID Type can fall into various categories including: definition (def), object (obj), state (ste), and variable (var). An example of a unique identifier would be oval:org.mitre.oval:obj:1116.

Common Vulnerabilities and Exposures (CVE) - is a publicly available catalog of security issues sponsored by the United States Department of Homeland Security (DHS). Each security issue has a unique CVE ID number assigned by the CVE Numbering Authority (CNA). The purpose of creating a unique CVE ID number is to create a standardization for a vulnerability or exposure as a researcher identifies it.



Stages of Obtaining a CVE

Stage 1: Identify if CVE is Required and Relevant

Identify if the issue found is a vulnerability. According to the CVE Team, "A vulnerability in the context of the CVE Program is indicated by code that can be exploited, resulting in a negative impact to confidentiality, integrity, OR availability, and that requires a coding change, specification change, or specification deprecation to mitigate or address." Additionally, research should verify there is not a CVE ID already in the CVE database.

Stage 2: Reach Out to Affected Product Vendor

A researcher should ensure they have made a good faith effort to contact a vendor directly. Researchers can reference CVE's **Documents on Disclosure Practices** for additional information.

Stage 3: Identify if Request Should Be For Vendor CNA or Third Party CNA

If a company is a part of participating CNA's, they can assign a CVE ID for one of their products. If the vendor is not a participating CNA, a researcher should attempt to reach out to the vendor's third-party coordinator.

Stage 4: Requesting CVE ID Through CVE Web Form

The CVE Team has a form that can be filled out online if the methods above do not work for CVE requests.

Stage 5: Confirmation of CVE Form

Upon submitting the CVE Web Form mentioned in Stage 4, an individual will receive a confirmation email. The CVE team will contact the requestor if any additional information is required.

Stage 6: Receival of CVE ID

Upon approval, the CVE Team will notify the requestor of a CVE ID if the affected product's vulnerability is confirmed. Please note that the CVE ID is not public yet at this stage.

Stage 7: Public Disclosure of CVE ID

CVE IDs can be announced to the public as soon as appropriate vendors and parties are aware of the issue to prevent duplication of CVE IDs. This stage ensures that all associated parties are aware of the problem before being publicly disclosed.

Stage 8: Announcing the CVE

The CVE Team asks researchers who are sharing multiple CVEs to ensure each CVE indicates the different vulnerabilities.

Stage 9: Providing Information to The CVE Team

At this stage, the CVE Team asks that the researcher help provide additional information to be used in the official CVE listing on the website.

Vulnerability Scanning Overview

Scanning is automated and focuses on finding potential/known vulnerabilities on the network or at the application level.

Vulnerabilities scanners typically do not exploit vulnerabilities (with some exceptions) but need a human to manually validate scan issues to determine whether or not a particular scan returned real issues that need to be fixed or false positives that can be ignored and excluded from future scans against the same target.

Nessus, **Nexpose**, and **Qualys** are well-known vulnerability scanning platforms that also provide free community editions. There are also open-source alternatives such as OpenVAS.

Nessus Overview

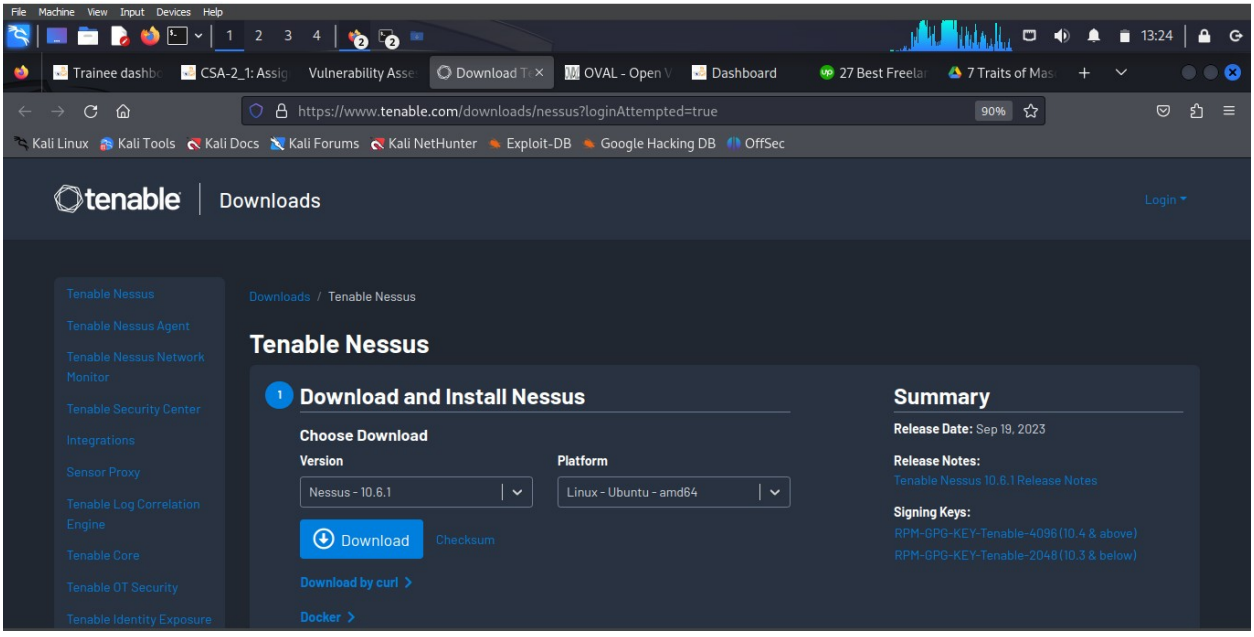
Nessus Essentials by Tenable is the free version of the official Nessus Vulnerability Scanner. Individuals can access Nessus Essentials to get started understanding Tenable's vulnerability scanner. The caveat is that it can only be used for up to 16 hosts. The features in the free version are limited but are perfect for someone looking to get started with Nessus. The free scanner will attempt to identify vulnerabilities in an environment.

OpenVAS Overview

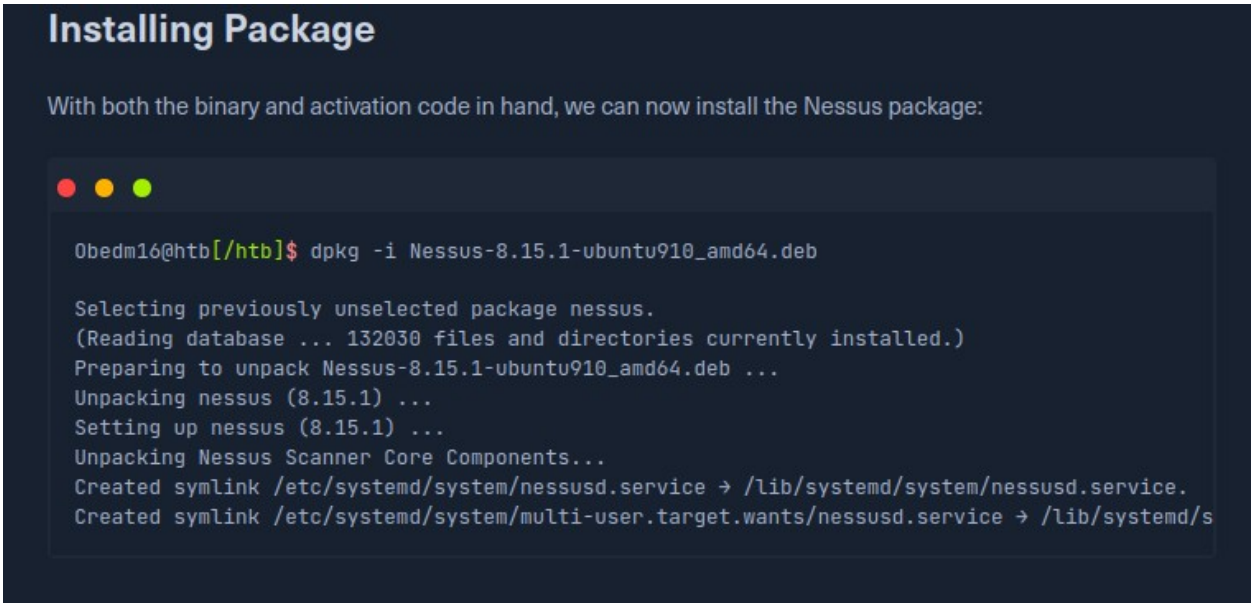
OpenVAS by Greenbone Networks is a publicly available open-source vulnerability scanner. OpenVAS can perform network scans, including authenticated and unauthenticated testing.

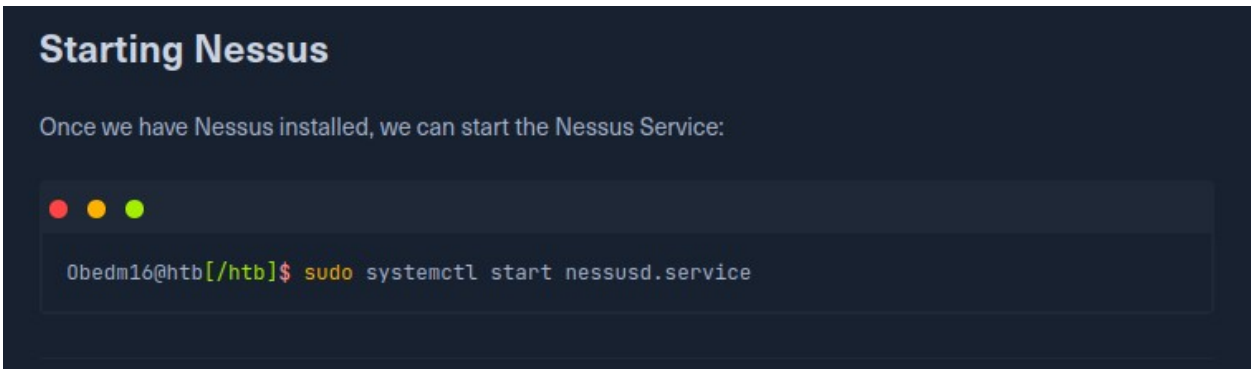
Getting Started with Nessus

The learner has an opportunity to interact with Nessus first by downloading it (the Debian package for **Ubuntu)**



After downloading it, the learner needs to acquire activation by visiting the Activation Code Page to request a Nessus Activation Code, which is necessary to get the free version of Nessus.





Nessus Scan

A new Nessus scan can be configured by clicking New Scan, and selecting a scan type. Scan templates fall into three categories: Discovery, Vulnerabilities, and Compliance.

New Scan

The learner has an option for a basic Host Discovery scan to identify live hosts/open ports or a variety of scan types such as the Basic Network Scan, Advanced Scan, Malware Scan, Web Application Tests, as well as scans targeted at specific CVEs and audit & compliance standards.

The learner will be able to demonstrate the usage of Nessus by targeting both Windows and Linux at ***172.16.16.100*** and ***172.16.16.160.***

Advanced Settings

The learner can configure a number of advanced settings for Nessus and its scans, like scan policies, plugins, and credentials.

Working with Nessus Scan Output

Nessus gives us the option to export scan results in a variety of report formats as well as the option to export raw Nessus scan results to be imported into other tools, archived, or passed to tools, such as EyeWitness, which can be used to take screenshots of all web applications identified by Nessus and greatly assist us with working through the results and finding more value in them.

Scanning Issues

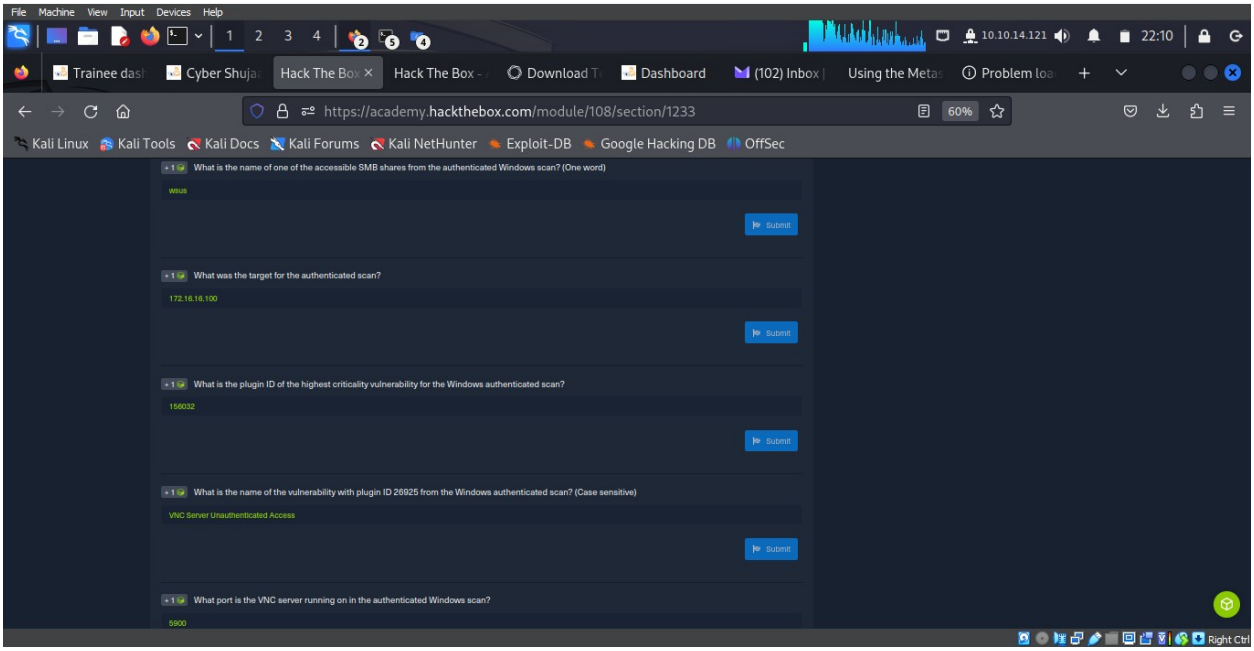
Nessus is a well-known and widely used vulnerability scanning platform. The learner a few best practices should be taken into consideration before starting a scan. Issues on sensitive networks and provide false positives, no results, or have an unfavorable impact on the network are to be kept into considerations.

Mitigating Issues

Firewalls will cause us to receive scan results showing either all ports open or no ports open. If this happens, a quick fix is often to configure an Advanced Scan and disable the Ping the remote host option. This will stop the scan from using ICMP to verify that the host is "live" and instead proceed with the scan. Some firewalls may return an "ICMP Unreachable" message that Nessus will interpret as a live host and provide many false-positive informational findings.

Network Impact

The potential impact of vulnerability scanning on a network, especially on low bandwidth or congested links can be tested using ***vnstat.***



Getting Started with OpenVAS

OpenVAS, by Greenbone Networks, is a publicly available vulnerability scanner. Greenbone Networks has an entire Vulnerability Manager, part of which is the OpenVAS scanner. Greenbone's Vulnerability Manager is also open to the public and free to use.

Installing Package

First, we can start by installing the tool:

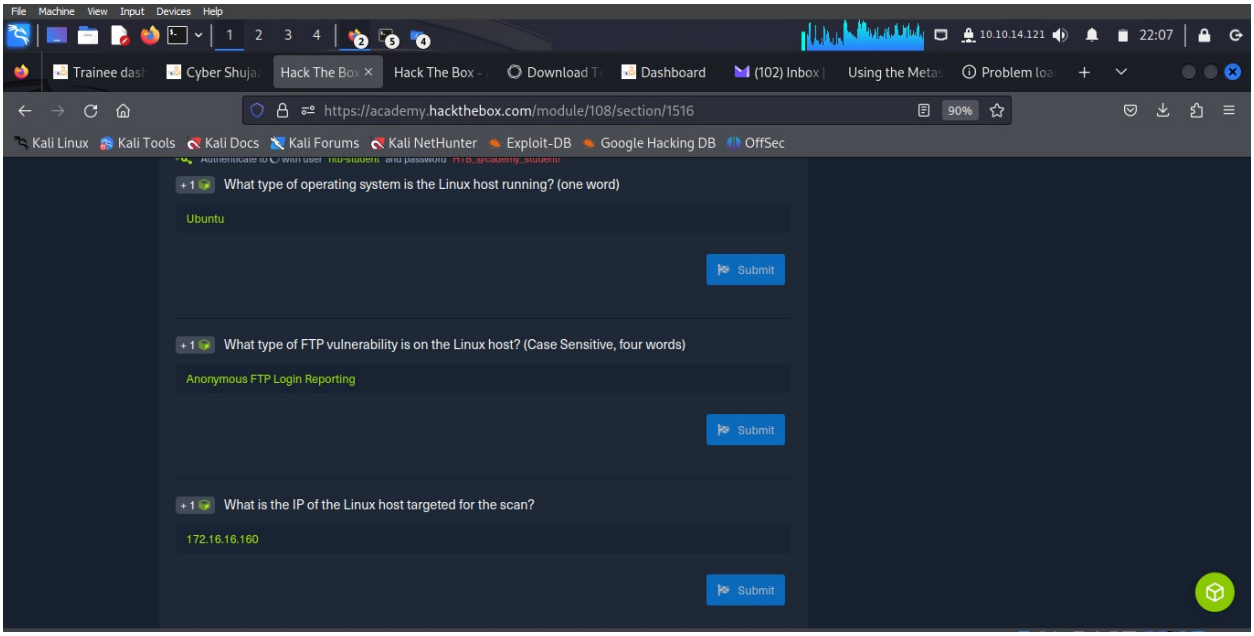
```
Obedm16@htb[/htb]$ sudo apt-get update && apt-get -y full-upgrade
Obedm16@htb[/htb]$ sudo apt-get install gvm && openvas
```

the installation process:

```
Obedm16@htb[/htb]$ gvm-setup
```

Start OpenVas:

Obedm16@htb[/htb]$ gvm-start



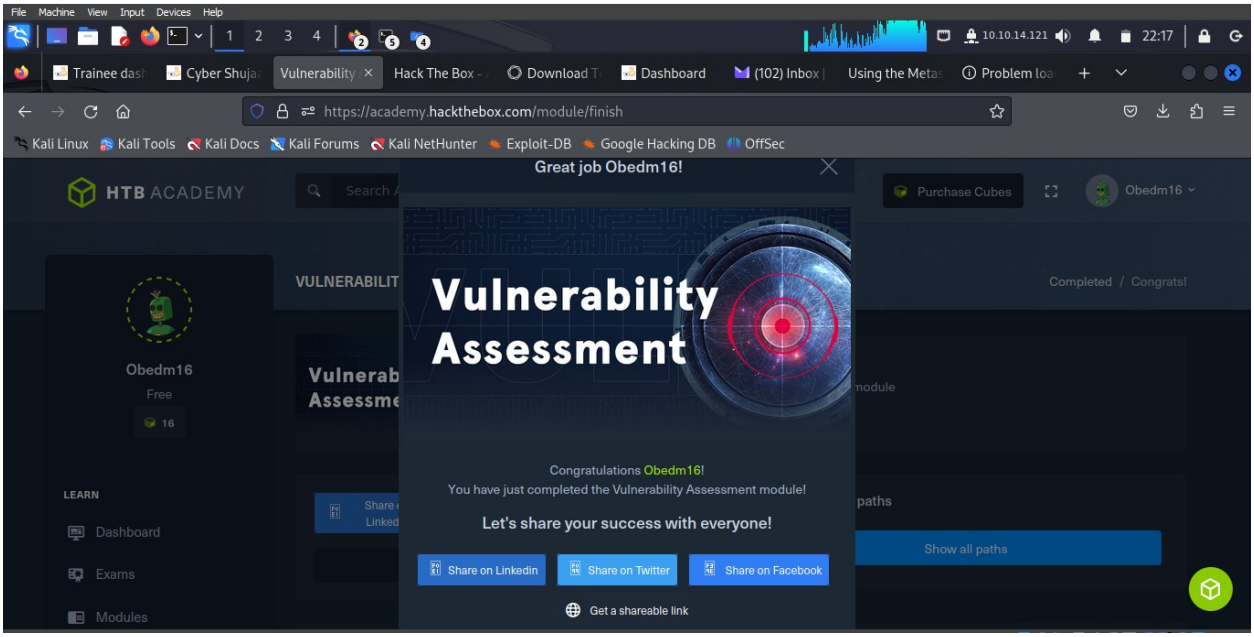
Conclusion

Reporting

Soft skills in information security are critical to being successful in your role.

The report should be readable by anyone ranging from a technical person to a non-technical person. A strong report consists of the following sections:

- Executive Summary
- Overview of Assessment
- Scope
- Vulnerabilities and Recommendations



Completion Link: https://academy.hackthebox.com/achievement/978332/108