Logo

Description automatically generated

Assignment (30%) (Proposal – Task 1)

|  |  |  |
| --- | --- | --- |
| **Module Code** | **:** | CT119-3-3-VAPT (Vulnerability Assessment and Penetration Testing) |
| **Intake Code** | **:** | APD3F2411CS(CYB) |
| **Lecturer Name** | **:** | TS. DR. MANIMEGALAI A/P RAJENDERAN |
| **Date Assigned** | **:** | 1st January |
| **Date Submitted** | **:** | 24th March |

|  |  |
| --- | --- |
| **Student Name** | **TP Number** |
| Abdulrahman Gamil Mohammed Ahmed | TP071012 |

Contents

[1.0 INTRODUCTION 4](#_Toc193630836)

[1.1 Overview 4](#_Toc193630837)

[1.2 Targeted System 6](#_Toc193630838)

[1.3 Overview of the machine source – Vulnhub 7](#_Toc193630839)

[1.4 PTS Type, Importance and Scope 8](#_Toc193630840)

[1.4.1 Scope of Penetration Testing 8](#_Toc193630841)

[1.4.2 Importance of Penetration Testing 9](#_Toc193630842)

[2.0 VULNERBILITY ASSESSMENT APPROCH & TOOLS TO USE 10](#_Toc193630843)

[2.1 Vulnerability Assessment Approach 10](#_Toc193630844)

[2.1.1 Asset Discovery 11](#_Toc193630845)

[2.1.2 Asset Prioritization 12](#_Toc193630846)

[2.1.3 Vulnerability Scanning 12](#_Toc193630847)

[2.1.4 Result Analysis & Remediation 13](#_Toc193630848)

[2.1.5 Continuous Cyber Security 13](#_Toc193630849)

[2.2 Vulnerability Assessment Tools Used 14](#_Toc193630850)

[2.2.1 Nmap 14](#_Toc193630851)

[2.2.2 SNMPwalk 15](#_Toc193630852)

[3.0 EXPLIOATION & ATTACKING METHODS & TOOLS TO USE 16](#_Toc193630853)

[3.1 Penetration Testing (PTS) Methods 16](#_Toc193630854)

[3.1.1 Planning and Reconnaissance 16](#_Toc193630855)

[3.1.2 Scanning 17](#_Toc193630856)

[3.1.3 Gaining System Access 17](#_Toc193630857)

[3.1.4 Persistent Access 17](#_Toc193630858)

[3.1.5 Analysis and Reporting 18](#_Toc193630859)

[3.2 Penetration Testing (PTS) Tools 19](#_Toc193630860)

[3.2.1 Knock Tool 19](#_Toc193630861)

[3.2.2 Metasploit 20](#_Toc193630862)

[4.0 CONCLUSION 21](#_Toc193630863)

[5.0 REFERENCES 22](#_Toc193630864)

Table of Figures[*1 Vulnerability Assessment & Penetration Testing (VAPT) 4*](#_Toc193630747)

[*2 Vulnerability Assessment Phases 10*](#_Toc193630748)

[*3 Nmap 14*](#_Toc193630749)

[*4 SNMPwalk 15*](#_Toc193630750)

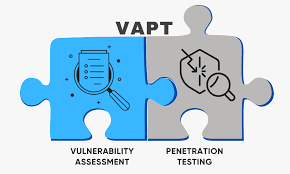
[*5 Penetration Testing Phases 16*](#_Toc193630751)

[*6 Knock Tool 19*](#_Toc193630752)

[*7 Metasploit 20*](#_Toc193630753)

# INTRODUCTION

## 1.1 Overview



1 Vulnerability Assessment & Penetration Testing (VAPT)

A security vulnerability is a system or software weakness whereby malicious attacks exploit vulnerabilities to harm computer networks or systems. These issues compromise operation and integrity, leading to data breaches or denial-of-service attacks. There are two critical processes companies utilize to examine and prevent such complications. These two critical processes are Vulnerability Assessment and Penetration Testing (VAPT). They complement each other in order to secure one system's edge from more advanced security threats in the future. For instance, vulnerability assessment is the method of finding, measuring, and researching weaknesses and deficiencies in relation to a system's environment (Ammar Bin Vahab, 2024).

The goal of the vulnerability assessment is to compile an extensive inventory of vulnerabilities along with relative risk for subsequent remediation. Whereas penetration testing (pen testing) goes a step further and attempts to achieve the cyber-attack. In a controlled setting, security professionals attempt to breach those weaknesses to discover exactly how far an attacker can go. It reveals the architecture of security from inside and whether systems are truly safe from breaches. This VAPT report is generated from a server operating with an Ubuntu version 4.4 x86\_64. The penetration testing firm has assessed a cloud hosting company.

The recent security assessment was due to a security breach a few weeks ago where an unsuccessful threat actor breached the assessed company's server, and it now believes an undetectable backdoor has been installed for future access. The assessment's intent is to discover vulnerabilities, attempt to breach to see if any backdoors exist, and provide investigative findings and recommendations of best practices to ensure this server environment is adequately secured in the foreseeable future.

## 1.2 Targeted System

The system to be analyzed and investigated is a server running ‎Ubuntu version 4.4 x86\_64, which plays a very critical role in the ‎infrastructure of the cloud hosting company for key services and ‎business operations. Recently, following a security incident, there are ‎fears that a backdoor might have been planted by an attacker. It might provide a certain backdoor, allowing unauthorized access to the system and letting the attacker re-enter the environment unnoticed, or do anything possible for malice.

The company has shared user credentials, milton:thelaststraw, to facilitate a deeper test. This is solely for controlled and secured testing of the system's defenses. With this access, the testing team will be able to safely simulate different scenarios to find existing vulnerabilities and confirm whether there is still a backdoor within the server.

On the server, a number of security mechanisms are configured in a layered manner to safeguard its operation. Among the most important ones is a kind of advanced security feature called port knocking. By default, this technique keeps the communication ports closed and opens them only when a specific, predefined sequence of connection attempts is performed correctly. Port knocking works by hiding entry points from unauthorized users, thereby reducing the attack surface.‎

**Key Characteristics of the Target System:**

|  |  |
| --- | --- |
| **Operating System**: | Ubuntu 4.4 x86\_64 |
| **IP Address**: | 192.168.47.178 |
| **Services**: | SSH, Telnet, SNMP, HTTP (on port 8) |
| **Security Mechanisms**: | Port knocking, firewalls, and intrusion prevention systems. |

## 1.3 Overview of the machine source – Vulnhub

This research paper sets out to draw attention to a clear, step-by-step process of conducting vulnerability scanning and penetration testing (VAPT) via access to the functionality of VulnHub a great open-source platform where virtual machines (VMs) can be obtained free of charge download. These pre-installed virtual machines come with deliberate security vulnerabilities along with them, which is just ideal as a sandbox platform to any individual looking to practice one's cybersecurity skills in a manner that's legal and ethical. It's an experiment ground for aspiring ethical hackers where they can experiment and learn in a safe environment.

With VulnHub, you can boot these VMs using software like VirtualBox or VMware and experience a virtual world of systems that is equivalent to the original. With the tools and methods of VAPT, you get to detect and leverage vulnerabilities think of it as an interactive boot camp for penetration testing. It's all about living the kind of skills you'd be performing out in the wild, but without going over the edge of the law and actually causing harm.

What sets VulnHub apart is the way it promotes hands-on learning. As a new user or veteran expert, the site dishes up all sorts of scenarios to put your skills in detecting and fixing security vulnerabilities to the test. It's not about hacking in—it's about gaining confidence and competence. And with pre-prepared vulnerable systems and a tip-and-solution-sharing community, it's a friendly environment that promotes cooperation and ethical hacking principles.

But it doesn’t stop there. VulnHub keeps things fresh by regularly updating its collection with new VMs that reflect the latest threats and vulnerabilities popping up in the cybersecurity world. This means you’re always learning skills that are relevant and up-to-date. The community-driven vibe is a bonus, too peer-reviewed content keeps the quality high and the lessons practical. In doing so through this research, VulnHub is more than just a means; it is a learning platform for the basics of VAPT and getting ready for the unpredictable caprices of the current world of cybersecurity.

## 1.4 PTS Type, Importance and Scope

In this penetration test, the approach of grey box testing will be applied. Grey box testing is the balance between black box and white box; the tester researching the target system has limited but valuable knowledge. This usually involves access to partial information, such as system credentials or other selected technical details, without full insight into the inner structure or full working of the system. This approach emulates a ‎scenario where an attacker has some insider knowledge, thus allowing a focused, realistic, and ‎effective security assessment (Nicholls, 2023). ‎

### 1.4.1 Scope of Penetration Testing

The penetration test will focus on achieving a few key objectives that are of significance to the in-depth evaluation of the server's security posture:‎

• **Objective 1:** Identify and exploit vulnerabilities: The first step is to discover potential weaknesses or misconfigurations in the server's architecture and services. These vulnerabilities could provide entry points for unauthorized access or exploitation.

• **Objective 2:** Identify the backdoor: One of the critical parts of this ‎assessment would be to find out if an attacker has planted a hidden backdoor. ‎In a situation where there is such a backdoor, the attacker will be capable of‎‎re-entering the system at his will without being detected.

• **Objective 3:** Obtain root: Another key objective is to determine whether it is possible to escalate privileges and gain root-level control of the server. This would help assess the full extent of the system compromise .‎

**• Objective 4:** Provide security recommendations: After identification of vulnerabilities and assessment of the risk, we will provide actionable suggestions to strengthen the security posture of the system and mitigate the identified threats (Mitnick Security, 2023). ‎

### 1.4.2 Importance of Penetration Testing

Practice of penetration testing is vital to maintaining cybersecurity at its best. Its importance can be emphasized with respect to the following aspects: ‎

**• Identifying vulnerabilities:** Penetration testing is effective in uncovering security ‎weaknesses that might not be discovered through regular security checks. Such flaws, if not fixed, may be further exploited by malicious actors.‎

**• Preventing data breaches:** Organizations can protect themselves against unauthorized access, data leaks, and other cyber threats by proactively finding and patching vulnerabilities. Breach prevention is considered one of the most critical tasks in protecting sensitive customer and business information.

**• Customer trust and organizational reputation:** A secure system reassures customers that their data is safe, hence maintaining their trust and confidence in the organization. Besides this, it shields the company from the negative publicity effect associated with breaches (Malik, 2021). ‎

# 2.0 VULNERBILITY ASSESSMENT APPROCH & TOOLS TO USE

## 2.1 Vulnerability Assessment Approach

With the proper mechanisms in place, the penetration test can be developed through the means of the application of ‎the ‎following methods as presented below:‎

A group of icons with text

Description automatically generated

2 Vulnerability Assessment Phases

### 2.1.1 Asset Discovery

Identification of assets in a target system is normally the first or most important step in the whole process of penetration testing. This generally includes gathering necessary information such as the server's IP address, open communications ports, and what services are running on the identified ports. With mapping into the network environment, it is supposed that a good knowledge of digital footprints gives testers grounds whereon they could make an effective and focused security assessment (*Asset Discovery and Assessment*, 2023).‎

Active network scanning utilizes custom tools like NetDiscover, which is extremely effective at performing reconnaissance. It discovers live hosts on the local network by ARP-pinging them and waiting for responses, performing especially well in DHCP environments.

This test is aimed at Nmap, which is a network discovery and security auditing tool. Nmap does detailed scans to find active systems, open ports, and the services running on each port, along with versions. This reveals potential entry points for attackers and highlights high-risk services for further analysis.

|  |  |
| --- | --- |
| **NetDiscover:** | This tool is utilized to scan the network to locate the IP ‎address of the server, 192.168.47.178 |
| **Nmap:** | Nmap will be utilized to conduct an initial scan for the identification of open ports and ‎services.‎ |

### 2.1.2 Asset Prioritization

Once the assets of the system have been identified, prioritization based on criticality and potential impact from a successful compromise is the next step. This prioritization ensures that testing efforts are focused on portions that attackers are most likely to reach and on portions whose compromise would result in severe consequences to the organization (Firch, 2023).

The critical factors that go into the prioritization process are the asset's purpose at the ‎infrastructure level, data sensitivity, and exposure to external networks. Applications that allow remote access, system operations management, and those used for critical ‎communication streams usually pose higher risks and are usually tagged in the highest order of ‎this priority list for assessment (Firch, 2023).

|  |  |
| --- | --- |
| **High Priority:** | SSH and Telnet, as they provide access to the server remotely.‎ |
| **Medium Priority:** | SNMP, since it is able to give out valuable system whether misconfigured.‎ |

### 2.1.3 Vulnerability Scanning

Vulnerability scanning will use Nmap and SNMP walk to identify security weaknesses. Tests will target open ports, identify service versions, and look for configuration weaknesses. This scans the network to reveal exposed services (Scarfone et al., 2008) and provides in-depth SNMP data for analysis. These tools will scan for weaknesses, exposure of the system, and identify areas that need security improvements for the target system.

|  |  |
| --- | --- |
| **Nmap Advanced Scanning**: | Advanced Nmap scanning for filtered ‎ports and services identification will be conducted, including TCP SYN ‎scans and UDP scans.‎ |
| **SNMPwalk**: | It's a tool that sends a query against the SNMP running service on ‎port 161 for retrieving system information, configuration, and ‎maybe credentials.‎ |

### 2.1.4 Result Analysis & Remediation

Additional analysis will determine the significant security weaknesses from the vulnerability scanning. These will be based on vulnerabilities that can be exploited, misconfigurations, and services that need to be updated. The analysis will be followed by recommendations to enhance system defenses. These include patching software, closing unnecessary ports to reduce vulnerabilities, and locking down service configurations to prevent unauthorized access. This will increase overall security as a result, protecting the system from future attack (StrongBox IT, 2024).

|  |  |
| --- | --- |
| **Critical Vulnerabilities**: | The SNMP service is misconfigured, and the open Telnet port may be ‎‎backdoored.‎ |
| **Remediation**: | Disable all the unnecessary services; upgrade the software for better access control. |

### 2.1.5 Continuous Cyber Security

Vulnerability scanning is a continuous process that guarantees the security of systems. Since vulnerabilities are found on a daily basis, regular scanning identifies potential threats or weaknesses to guarantee safety from evolving attacks. Vulnerability to exploitation and sensitive data contamination may be minimized if organizations updated vulnerabilities, patched security configurations, and made regular checks in a timely manner. Checks are a necessary part of a comprehensive cyber-security posture, enabling systems to be resilient and evolve with best practices amidst dynamic technology environments (Gowsika, 2024).

|  |  |
| --- | --- |
| **Continuous Monitoring**: | Establish procedures that allow for continuous monitoring of the system security posture. |
| **Regular Updates**: | Ensure that the system is kept updated regularly with all security patches. |

## 2.2 Vulnerability Assessment Tools Used

### 2.2.1 Nmap



**3** Nmap

Nmap, or Network Mapper, is an advanced, award-winning open-source tool for network ‎discovery, vulnerability scanning, and security auditing. It would come in great importance for use in ‎scanning the target server for opened ports, active services, and other possible vulnerabilities that ‎the attacker could possibly take advantage of. Equipped with strong powers like TCP SYN scans and UDP ‎scans, Nmap will deeply scan the system. These techniques are of great importance to discover the ports and services hidden by firewalls or filtering devices, which show in detail the network exposure of a server (CompTIA, 2024).

**Key Features:**

**• Enumerate open ports and services:** Nmap port-scans the network to identify open ports and running services.

**• Detect service versions and system details:** Nmap identifies service versions and adds detailed system environment information.

**‎• Scanning:** Nmap can execute SYN scans, also referred to as half-open ‎scans, and ‎UDP scans to determine filtered or hidden ports and services. This is significant ‎in testing the ‎system for potential vulnerabilities that have not been found.

.

### 2.2.2 SNMPwalk



**4** SNMPwalk

SNMPwalk is a specialized command-line utility that interacts with devices and systems using the Simple Network Management Protocol. As such, this tool is supposed to query devices enabled with SNMP, which are supposed to enable detailed system information, network data, and possibly misconfigurations. SNMPwalk will be performed in order to assess the configuration of the target server. More precisely, any weaknesses or vulnerabilities regarding the SNMP service will be identified using this tool. This is a handy tool for retrieving sensitive information from poorly configured or insecure SNMP services, which might be entry points to an attacker (*What Is SNMP Walk? How Does It Work? - IT Glossary | SolarWinds*, 2025).

**Key Features:**

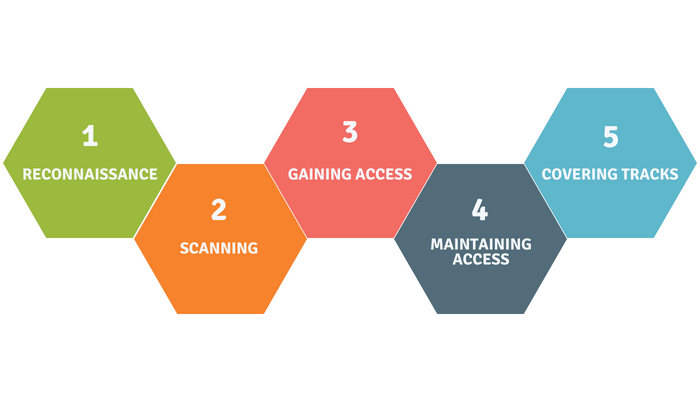
• **Using SNMPwalk to query SNMP-enabled devices for system information:** it queries SNMP-‎enabled systems for detailed insights into their configuration, performance, and ‎health.‎

**• Configuration Information and Potential Credentials Extraction:** It can extract sensitive ‎configuration details, including community strings or other authentication credentials, ‎which may expose vulnerabilities if misconfigured.‎

**• Identification of misconfiguration of SNMP services:** SNMPwalk identifies the weak or default ‎configurations of SNMP settings that may inadvertently expose critical data or open ‎security gaps.‎

# 3.0 EXPLIOATION & ATTACKING METHODS & TOOLS TO USE

## 3.1 Penetration Testing (PTS) Methods



Penetration Testing Phases

### 3.1.1 Planning and Reconnaissance

Information gathering of the target system's IP address, open ‎ports, and running services would be a good start. NetDiscover and Nmap tools will ‎be used for reconnaissance and will let us know about active systems, open ports, and ‎services, which are very important for our investigation and penetration test (Praveen, 2022).‎

|  |  |
| --- | --- |
| **NetDiscover**: | This was used to know the IP address of the server, which is 192.168.47.178‎. |
| **Nmap**: | This was used to run a preliminary scan to identify running ports and ‎services.‎. |

### 3.1.2 Scanning

Scanning for vulnerabilities will be the next step on the target system. Advanced Nmap scans and ‎SNMPwalk will be conducted to identify opened ports, running services, and potential ‎vulnerabilities for a detailed security assessment of the system and identifying possible entry points ‎for exploitation (Praveen, 2022).‎

|  |  |
| --- | --- |
| **Nmap Advanced Scanning**: | Used to identify filtered ports and services.‎ |
| **SNMPwalk**: | To enumerate system information from the SNMP ‎service. |

### 3.1.3 Gaining System Access

Identification of the vulnerabilities, the next task will be exploitation of the identified vulnerabilities to access the system; this includes how port knocking has been exploited and how SNMPwalk is used in extracting sensitive ‎information, then exploiting vulnerabilities like those in services such as Telnet (Praveen, 2022).‎

|  |  |
| --- | --- |
| **Port Knocking**: | The Knock Tool will be used in sending the right sequence of ‎‎"**knocks**" that will open the required ports for access.‎ |
| **SNMP Exploitation**: | SNMPwalk will be used to extract sensitive information such as ‎credentials from this SNMP service.‎ |
| **Telnet Exploitation**: | The attacker will access the system using Telnet service.‎ |

### 3.1.4 Persistent Access

After gaining access, the aim is for persistent access to the system, including adding SSH keys to the authorized\_keys file, modification of system configurations for continued access (Praveen, 2022). ‎

|  |  |
| --- | --- |
| **SSH Key Addition**: | The pentester will add his SSH public key into the ‎authorized\_keys file to allow password-less SSH access.‎ |
| **System Configuration**: | System settings will be changed to maintain access, such as permitting ‎root login via SSH‎. |

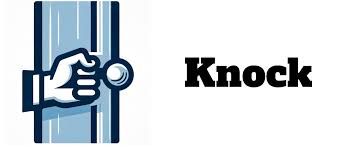
### 3.1.5 Analysis and Reporting

The last step will be analyzing the results of a penetration test and giving recommendations about securing the system. This will include pinpointing critical vulnerabilities, detailing steps taken to exploit them, and providing remediation advice (Praveen, 2022).‎

|  |  |
| --- | --- |
| **Critical Vulnerabilities**: | Misconfigured SNMP service, open Telnet port with a possible ‎backdoor‎. |
| **Remediation**: | Turn off superfluous services, update software packages, and use ‎more stringent access controls‎. |

## 3.2 Penetration Testing (PTS) Tools

### 3.2.1 Knock Tool



**6** Knock Tool

Knock talks to the server port knocking software. Port knocking is a security system that closes all the ports and opens them only after a specific sequence of connection attempts, hence making them invisible to attackers. The Knock Tool sends a sequence of "knocks" to the server in a way that some ports are only opened with correct execution to prevent normal port blocking (GeeksforGeeks, 2021). ‎

**Key Features:‎**

**• Send a series of connection attempts to open the ports:** Knock Tool sends ‎a series of predefined, specific connection attempts to the target server in an attempt to "knock" on the right ‎sequence of ports.‎

**• Bypass firewalls and intrusion prevention systems:** It will enable the tester to bypass firewalls and intrusion prevention systems, which would block or filter unauthorized traffic, not allowing access to a legitimate service.

### 3.2.2 Metasploit



**7** Metasploit

Metasploit is a very powerful, popular, and feature-rich penetration testing framework that will be used to exploit the target system's identified weaknesses. With its comprehensive library of exploits, payloads, and modules, Metasploit will enable the penetration tester to mimic a real-world attack by compromising systems through known vulnerabilities. Here, Metasploit ‎will be used for the exploitation of vulnerabilities in such services like Telnet and SSH, unauthorized ‎access, escalation of privileges, and ensure post-exploited persistent access to the server for further testing ‎and analysis (Buckbee, 2020).‎

**Key Features:**

**• Attack the known vulnerabilities of services such as Telnet and SSH:** Using the comprehensive pre-built exploit database of Metasploit, a tester can pinpoint and attack particular vulnerabilities of Telnet- or SSH-like services for unauthorized system access.

**• Privilege Escalation:** This is an advance to root access when Metasploit gains initial access. It allows taking complete control over the target system at administrative or root levels.

**• Continue having access to the system:** Metasploit enables testers in creating backdoors ‎and other persistence mechanisms, allowing them to have continued access even after systems reboot or start security.

# 4.0 CONCLUSION

The subsequent paper describes the detailed VAPT process of a server running on Ubuntu 4.4 x86\_64. The scanning for vulnerabilities shall include searching out the open ports, services running on them, and their associated vulnerabilities by making use of various tools such as Nmap and SNMPwalk. Further, penetration testing shall be done by making use of the identified vulnerabilities to gain system access, privilege escalation, and gaining persistent access with tools such as the Knock Tool and Metasploit.‎

# 5.0 REFERENCES

* Ammar Bin Vahab. (2024, August 9). *What is VAPT? | Wattlecorp Cybersecurity Labs*. Wattlecorp. https://www.wattlecorp.com/what-is-vapt/
* Nicholls, M. (2023, December 10). *Types of Penetration Testing | Black Box vs White Box vs Grey Box*. Redscan. https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/

‌

* Mitnick Security. (2023). Understanding the Scope of A Penetration Test. *Mitnicksecurity.com*. https://doi.org/1056769960/1713452321153

‌

* Malik, K. (2021, October 12). *Why Penetration Testing is Important - Astra Security*. Astra Security. https://www.getastra.com/blog/security-audit/why-penetration-testing-is-important/#:~:text=Penetration%20testing%20helps%20in%20validating,attacks%20to%20find%20security%20holes.

‌

* *Asset Discovery and Assessment*. (2023). Tenable.com. https://docs.tenable.com/cyber-exposure-studies/cyber-exposure-insurance/Content/DiscoveryAssessment.htm

‌

* Firch, J. (2023, March 24). *How To Prioritize Vulnerabilities For Remediation*. PurpleSec. https://purplesec.us/learn/vulnerability-prioritization/

‌

* Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Special Publication 800-115 Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*. NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

‌

* StrongBox IT. (2024, December 19). *The Importance of Vulnerability Remediation after VAPT*. StrongBox IT | Cybersecurity Consulting Services. https://www.strongboxit.com/the-importance-of-vulnerability-remediation-after-vapt/

‌

* Gowsika. (2024, October 10). *Sprinto Compliance Software*. Sprinto. https://sprinto.com/blog/continuous-security-monitoring/

‌

* CompTIA. (2024, March 6). *What Is Nmap?* CompTIA. https://www.comptia.org/blog/what-is-nmap

‌

* *What Is SNMP Walk? How Does It Work? - IT Glossary | SolarWinds*. (2025). Solarwinds.com. https://www.solarwinds.com/resources/it-glossary/snmp-walk

‌

* Praveen. (2022, March 28). *5 Essential Penetration Testing Phases You Can’t Ignore in 2025*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

‌

* GeeksforGeeks. (2021). Knock Subdomain Scanner Tool in Kali Linux. *GeeksforGeeks*. https://doi.org/10704233954/11

‌

* Buckbee, M. (2020, March 29). *What is Metasploit? The Beginner’s Guide*. Varonis.com; Varonis. https://www.varonis.com/blog/what-is-metasploit

‌

---Word Count: 3657---