IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 3, Ser. 2 (May. – June. 2024), PP 05-20
www.iosrjournals.org

A Comparative Study on Network Exploration and Performance Evaluation Techniques for Vulnerability Assessment Tools in Security Systems

Saffanah Abdulaziz Alkhathlan[1], Lina Hasan Alzahrani[2], Shumukh Hamad Alfulayj[3], Sherif Kamel Hussein [4]

[1]*Arab East Colleges for Graduate Studies, Degree of Bachelor of Cyber Security, AlQirawan, Riyadh, Kingdom of Saudi Arabia*

[2] *Arab East Colleges for Graduate Studies, Degree of Bachelor of Cyber Security, AlQirawan, Riyadh, Kingdom of Saudi Arabia*

[3] *Arab East Colleges for Graduate Studies, Degree of Bachelor of Cyber Security, AlQirawan, Riyadh, Kingdom of Saudi Arabia*

[4] *Associate Professor, Department of Communications and Computer Engineering ,October University for Modern Sciences and Arts, Giza- Egypt,*
Associate Prof. Computer Science Department,- Arab East Collrges - AlQirawan, Riyadh, KSA

Abstract:
This study outlines a comparative studies on Vulnerabilities Assessment tools in security systems, the Research deepen into network reconnaissance and vulnerability assessment methodologies within Windows environments. Its core aim is to increase comprehension and practical profinciency by outlining structured objectives about network tracerouting, host discovery, port and service identification, OS profiling, and vulnerability analysis. Within the dynamic circumstances of cyber threats, the research underscores the urgency of practical defense measures and the fundamental role of defensive identification and mitigation of vulnerabilities. It serves as a significant step towards providing individuals with essential cybersecurity expertise, addressed towards protecting network infrastructures against any potential exploits.

Keywords: *Vulnerability Assessment, Network Reconnaissance, Vulnerability Scanning Tools, Practical Implementation.*

Date of Submission: 07-05-2024 Date of Acceptance: 17-05-2024

I. Introduction

In an increasingly interconnected world driven by internet technologies, network security has become crucial. With the widespread of cloud computing and the accessibility of various amounts of information through public networks, safeguarding personal, economic, and organizational data is imperative. This paper deepen into the importance of network security measures such as vulnerability assessment, penetration testing, and antivirus software to prevent unauthorized access and potential harm to sensitive information. As cyber threats grow in complexity and development, the need for cybersecurity professionals becomes more pressing. Our project aims to enhance understanding and practical skills in network reconnaissance and vulnerability assessment, particularly focusing on Windows operating systems. It serves both academic enrichment and practical application, equipping individuals with essential cybersecurity expertise to defend against evolving threats.(1)

II. Literature Review

This section is dedicated to a comparative study on three recent research papers specialized in using different Vulnerabilities Assessment tools.

1. The Emergence of Vulnerability Assessment and Scanning Tools for Network Security

The emergence of vulnerability assessment and scanning tools for network security represents a significant progress in cybersecurity practices. This development entails a thorough examination of such tools to enhance understanding of Cyber Defense Technology to safeguard network security.

Traditionally, network security strategies relied on reactive measures, addressing vulnerabilities only post-exploitation. However, with the rise of advanced cyber threats, proactive approaches became vital.

Vulnerability assessment tools enable organizations to systematically evaluate networks, systems, and applications, identifying and mitigating vulnerabilities before exploitation. This proactive stand has reshaped network security practices, empowering organizations to defend against evolving cyber threats more effectively.(2)

2. The Comparative Evaluation of Vulnerability Assessment Methods

This study is based on applying four distinct algorithms in vulnerability assessment, are:

1. POMDP (Partially Observable Markov Decision Process): It offers a mathematical framework for decision-making under uncertainty, particularly applicable in robotics and autonomous systems.
2. MIPSA (Mixed Initiative Planning and Scheduling Agent): Combining human and automated decision-making, MIPSA enhances task planning and scheduling efficiency, fostering collaboration.
3. RL (Reinforcement Learning): As a subset of machine learning, RL empowers agents to make decisions through interactions with the environment, with successful applications across various domains.
4. Host Clustering: This technique categorizes hosts based on specific criteria, assist in network management and security tasks, such as load balancing and resource allocation.

By using Vulnerability Assessment and Penetration Testing (VAPT) accuracy analysis, it revealed that POMDP and RL techniques outperform MIPSA and Host Clustering in terms of accuracy and effectiveness. As shown in the **Figure 1** below; POMDP particularly overtake in ensuring confidentiality.(2)

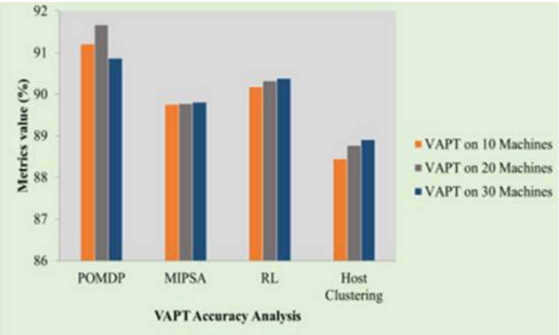


Figure 1: VAPT Accuracy Analysis of various methods

3. IT Support Website Security Evaluation Using Vulnerability Assessment Tools

This study is based on the evaluation of IT Support website security through vulnerability assessment tools, along with a thorough analysis of its pros and cons. Which is;

A. Pros:

1. Risk Reduction: Vulnerability assessments enable proactive addressing of security risks, minimizing the likelihood of successful attacks.
2. Comprehensive Assessment: Following the VAPT Life Cycle method ensures a thorough evaluation of the website's vulnerabilities.
3. Continuous Improvement: Regular assessments enhance website security by addressing emerging vulnerabilities for ongoing protection.
4. Clear Reporting: The final report provides a detailed overview of vulnerabilities found, aiding organizations in prioritizing and addressing security issues.
5. Identification of Vulnerabilities: The research offers a systematic approach to identify and assess vulnerabilities, allowing organizations to understand their security weaknesses.

B. Cons:

1. Limited Scope: The focus on assessing vulnerabilities in the IT Support website of XYZ Institution may not cover all possible vulnerabilities or address specific issues of other websites or institutions.
2. Incomplete Coverage: The research may not cover all potential attack vectors or novel exploitation techniques used by sophisticated attackers.
3. Real-time Gap: Periodic assessments may miss new vulnerabilities, posing a risk until the next evaluation.
4. Cost Implications: Implementing necessary security measures to address identified vulnerabilities may involve additional costs for organizations.

5. Lack of Real-time Assessment: Vulnerability assessments are typically conducted at specific points in time, meaning that new vulnerabilities may remain undetected until the next assessment.

Additionally, an analysis of the usability of the OpenVAS vulnerability scanner evaluates OpenVAS 9.0 through expert-based and user-based testing, identifying critical usability flaws and issues that affect the tool's effectiveness in providing security. **Table 1** outlines the main pros and cons of this usability evaluation, emphasizing the tool's open-source nature, comprehensive library of vulnerability detection plugins, and wide usage among cyber security practitioners, while also acknowledging potential challenges such as user-friendliness and technical skill requirements.(3)

Table 1: Usability Evaluation Pros and Cons

Pros	***Cons***
Open-source tool	May is not user-friendly for some users
Comprehensive library of vulnerability detection plugins	May require advanced technical skills for installation and setup
Widely used among cybersecurity practitioners	Can generate large and complex scan reports
Capable of detecting vulnerabilities across a wide range of systems and applications	May have limitations in accurately detecting certain vulnerabilities
Provides comprehensive and detailed scan results	May require configuration and customization to meet specific needs

III. Methods : Virtual Environments and Cloud-Based Labs

This Section is dedicated to apply two Scenarios for Vulnerability Scanning.The first scenario implies conducting vulnerability scanning between a client and a server within virtual environments. This dynamic exploration deepen into the complications of simulating these devices, understanding their roles, functions, and the accurate interactions within this digital space. Virtualization simplifies the creation of a controlled yet comprehensive environment for vulnerability scanning between the client and server.

In the second scenario, the focus shifts to using cloud computing-based labs available on the EC-Council platform as a crucial component. These labs provide a practical platform for applying theoretical knowledge, filling the gap between concepts and real-world implementation.

A. First Scenario:

In the first scenario, vulnerability scanning between a client and a server is conducted in virtual environments using the VirtualBox program. This dynamic exploration delves into the intricacies of VirtualBox, where the server downloads the vulnerability scanning program for the client. This process involves a closer examination of VirtualBox's features and capabilities, enabling the creation of a controlled yet comprehensive environment for vulnerability scanning between the client and server. As shown in **Figure 2** First Scenario Block Diagram.

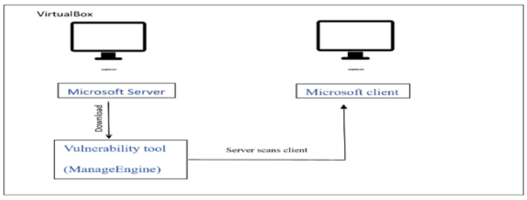


Figure 2: First Scenario Block Diagram

Regarding the tools configured for the Virtual Machine's first scenario:
1. VirtualBox: Is a powerful virtualization product for enterprise and home use, supporting various guest operating systems and platforms. It provides features for creating controlled virtual environments for vulnerability scanning. (4)
2. Vulnerability Tool (ManageEngine):Offers a suite of IT management software solutions, including network monitoring, server and application management, help desk services, and security management. Its tools streamline IT operations and enhance network security. (5)
3. Microsoft Server (2019 version): Is a comprehensive operating system designed for server infrastructure, offering advanced security features, hybrid cloud integration, virtualization capabilities, and software-defined storage solutions.(6)

4. Microsoft Client (2019 version): Is an advanced operating system designed for client devices, providing enhanced security, productivity features, compatibility enhancements, and centralized device management through cloud-based solutions like Microsoft Intune. (7)

B. Second Scenario:

In the second scenario, EC-Council cloud computing-based labs play a central role as participants engage in purposefully crafted exercises aligned with project objectives. These activities involve diverse tasks like network tracerouting, host discovery, port identification, operating system profiling, and vulnerability analysis. The incorporation of EC-Council labs marks a crucial juncture, converting theoretical knowledge into tangible skills. This integration serves as a transformative step, equipping individuals to effectively address the complexities of real-world cybersecurity challenges. **Figure 3** shows the Second Scenario Lab Environment Block Diagram.(8)

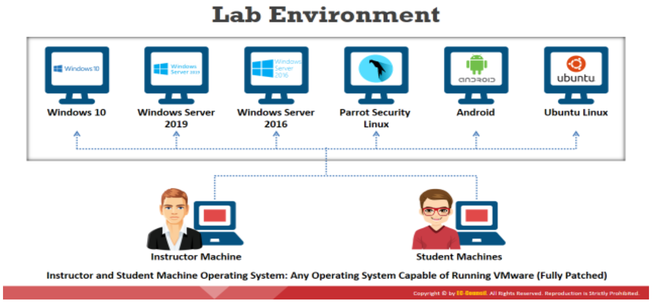

Lab Environment
Windows 10
Windows Server 2019
Windows Server 2016
Parrot Security Linux
Android
Ubuntu Linux
Instructor Machine
Student Machines
Instructor and Student Machine Operating System: Any Operating System Capable of Running VMware (Fully Patched)
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 3: Second Scenario Lab Enviroment (Block Diagram)

Regarding the tools configured of EC-Council cloud computing-based labs for the Second Scenario:
The tools have been organized with the following configurations:

1. Windows 10 (client station): Is an operating system developed by Microsoft, designed to provide a user-friendly interface and a wide range of features and functionalities for personal computers. It emphasizes security and productivity, offering tools for file management, application installation, and customization.
2. Microsoft Server (2016 version): Is a server operating system developed to run networked applications. It prioritizes security and includes features like identity management and enhanced security capabilities to safeguard data.
3. Microsoft Server (2019 version):Is a comprehensive operating system designed for server infrastructure, offering advanced security features, hybrid cloud integration, virtualization capabilities, and software-defined storage solutions.
4. Parrot Security Linux: Provides a comprehensive suite of tools for IT and security professionals to test and assess the security of their assets. It offers flexibility and reliability from information gathering to reporting, making it a valuable asset in cybersecurity assessments.
5. Android: Is a mobile operating system widely adopted for smartphones and tablets. It offers a wide range of applications and customization options, making it versatile for various user needs.
6. Ubuntu Linux: Is a free and open-source operating system known for its user-friendly interface, security features, and stability. It supports a diverse range of software applications and hardware architectures, making it suitable for different use cases.

IV. Practical Implementation and Insights for Exploring Vulnerability Scanning

Practical applications presented in a detailed step-by-step manner, showcasing the results and insights derived from two scenarios. Microsoft Server 2019 is a comprehensive operating system designed for server infrastructure, offering advanced security features, hybrid cloud integration, virtualization capabilities, and software-defined storage solutions.

A. First Scenario:

In the first scenario, a vulnerability scan was conducted between a client and a server, using VMware, Server 2019, and Client 2019. ManageEngine was downloaded onto the server to start the vulnerability scan. The steps of the first scenario is shown in the block diagram of Figure 4.

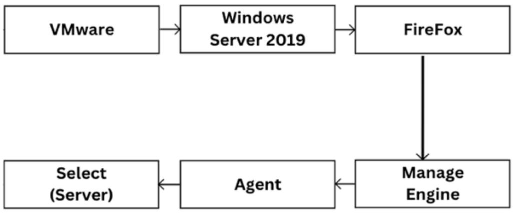
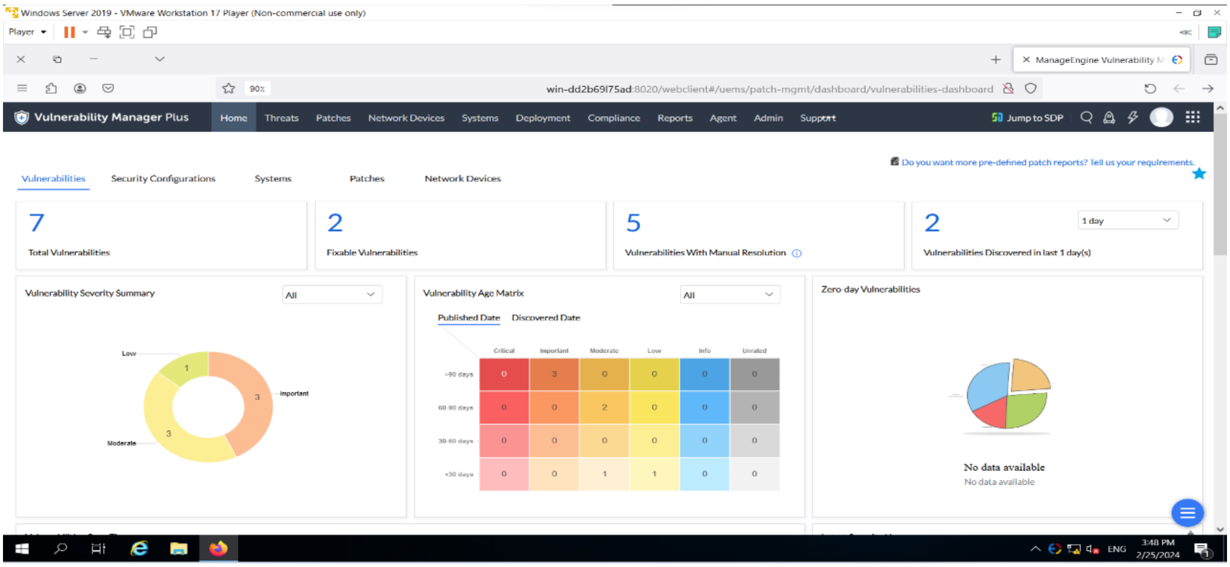


Figure 4: First scenario Block Diagram

1. First Scenario Steps

It contains all the steps and information that was recorded to help describing the implementation processes.

Step 1: As shown in screenshot of **figure 5,** User mouse drag on (tool bar) and click "Home".


Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
ManageEngine Vulnerability M
90%
win-dd2b69l75ad:8020/webclient#/uems/patch-mgmt/dashboard/vulnerabilities-dashboard
Vulnerability Manager Plus
Home
Threats
Patches
Network Devices
Systems
Deployment
Compliance
Reports
Agent
Admin
Support
Jump to SDP
Do you want more pre-defined patch reports? Tell us your requirements.
Vulnerabilities
Security Configurations
Systems
Patches
Network Devices
1 day
Vulnerability Severity Summary
All
Low
1
Important
3
Moderate
3
Zero-day Vulnerabilities
No data available
No data available
3:48 PM
2/25/2024
ENG

7 Total Vulnerabilities

2 Fixable Vulnerabilities

5 Vulnerabilities With Manual Resolution

2 Vulnerabilities Discovered in last 1 day(s)

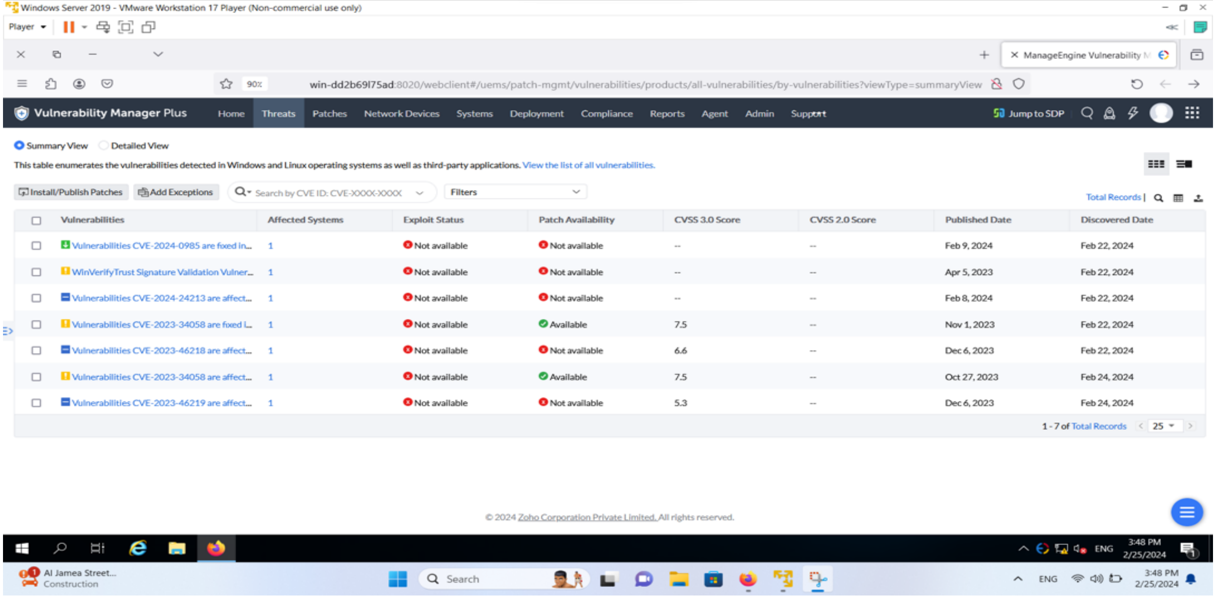
Vulnerability Age Matrix — All

Published Date | Discovered Date

	Critical	Important	Moderate	Low	Info	Unrated
>90 days	0	3	0	0	0	0
60-90 days	0	0	2	0	0	0
30-60 days	0	0	0	0	0	0
<30 days	0	0	1	1	0	0

Figure 5 :Vulnerability Manager Plus Home Page

Step 2: As shown in screenshot of **figure 6**, User mouse drag on (tool bar) and click "Threats".


Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
ManageEngine Vulnerability M
90%
win-dd2b69l75ad:8020/webclient#/uems/patch-mgmt/vulnerabilities/products/all-vulnerabilities/by-vulnerabilities?viewType=summaryView
Vulnerability Manager Plus
Home
Threats
Patches
Network Devices
Systems
Deployment
Compliance
Reports
Agent
Admin
Support
Jump to SDP
Install/Publish Patches
Add Exceptions
Search by CVE ID: CVE-XXXX-XXXX
Filters
Total Records
Al Jamea Street... Construction
Search
ENG
3:48 PM
2/25/2024

● Summary View ○ Detailed View

This table enumerates the vulnerabilities detected in Windows and Linux operating systems as well as third-party applications. View the list of all vulnerabilities.

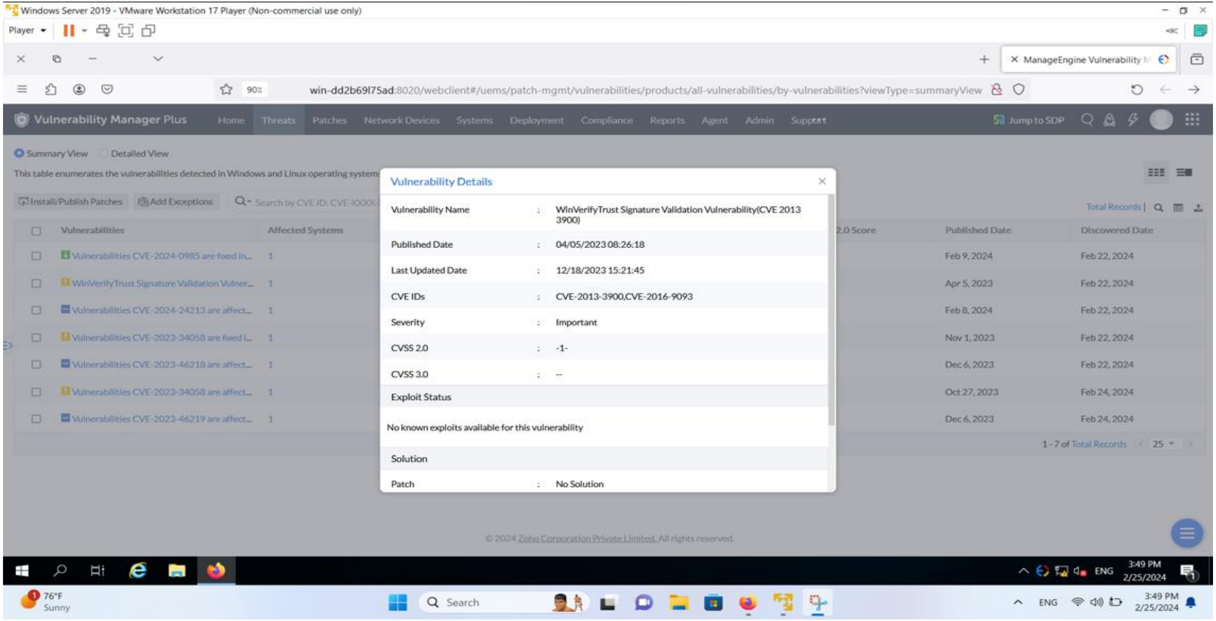
Vulnerabilities	Affected Systems	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score	Published Date	Discovered Date
Vulnerabilities CVE-2024-0985 are fixed in...	1	Not available	Not available	--	--	Feb 9, 2024	Feb 22, 2024
WinVerifyTrust Signature Validation Vulner...	1	Not available	Not available	--	--	Apr 5, 2023	Feb 22, 2024
Vulnerabilities CVE-2024-24213 are affect...	1	Not available	Not available	--	--	Feb 8, 2024	Feb 22, 2024
Vulnerabilities CVE-2023-34058 are fixed i...	1	Not available	Available	7.5	--	Nov 1, 2023	Feb 22, 2024
Vulnerabilities CVE-2023-46218 are affect...	1	Not available	Not available	6.6	--	Dec 6, 2023	Feb 22, 2024
Vulnerabilities CVE-2023-34058 are affect...	1	Not available	Available	7.5	--	Oct 27, 2023	Feb 24, 2024
Vulnerabilities CVE-2023-46219 are affect...	1	Not available	Not available	5.3	--	Dec 6, 2023	Feb 24, 2024

1 - 7 of Total Records 25

© 2024 Zoho Corporation Private Limited. All rights reserved.

Figure 6: Vulnerability Manager Plus Threats Page

Step 3: As shown in screenshot of **figure 7,** User mouse drag on (Vulnerabilities) and click on Vulnerability Name "WinVerifyTrust Signature Validation Vulnerability (CVE 2013 3900)", then the details will appear.



Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)

win-dd2b69l75ad:8020/webclient#/uems/patch-mgmt/vulnerabilities/products/all-vulnerabilities/by-vulnerabilities?viewType=summaryView

Vulnerability Manager Plus

○ Summary View ○ Detailed View

This table enumerates the vulnerabilities detected in Windows and Linux operating system

□	Vulnerabilities	Affected Systems	Published Date	Discovered Date
□	Vulnerabilities CVE-2024-0985 are fixed in...	1	Feb 9, 2024	Feb 22, 2024
□	WinVerifyTrust Signature Validation Vulner...	1	Apr 5, 2023	Feb 22, 2024
□	Vulnerabilities CVE-2024-24213 are affect...	1	Feb 8, 2024	Feb 22, 2024
□	Vulnerabilities CVE-2023-34058 are fixed i...	1	Nov 1, 2023	Feb 22, 2024
□	Vulnerabilities CVE-2023-46218 are affect...	1	Dec 6, 2023	Feb 22, 2024
□	Vulnerabilities CVE-2023-34058 are affect...	1	Oct 27, 2023	Feb 24, 2024
□	Vulnerabilities CVE-2023-46219 are affect...	1	Dec 6, 2023	Feb 24, 2024

1 - 7 of Total Records

Vulnerability Details

Vulnerability Name	:	WinVerifyTrust Signature Validation Vulnerability(CVE 2013 3900)
Published Date	:	04/05/2023 08:26:18
Last Updated Date	:	12/18/2023 15:21:45
CVE IDs	:	CVE-2013-3900,CVE-2016-9093
Severity	:	Important
CVSS 2.0	:	-1-
CVSS 3.0	:	--

Exploit Status

No known exploits available for this vulnerability

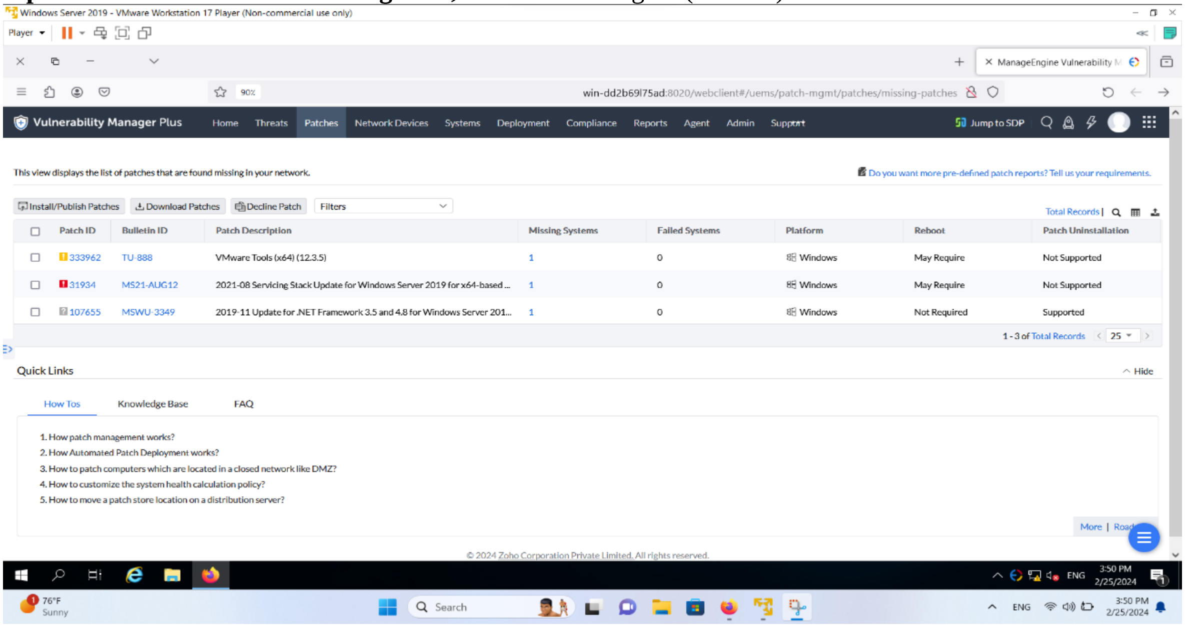
Solution

Patch	:	No Solution

© 2024 Zoho Corporation Private Limited. All rights reserved.

Figure 4.4 Figure 7: Vulnerability Manager Plus Vulnerability Details

Step 4: As shown in screenshot of **figure 8,** User mouse drag on (tool bar) and click on Patches.



Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)

win-dd2b69l75ad:8020/webclient#/uems/patch-mgmt/patches/missing-patches

Vulnerability Manager Plus

This view displays the list of patches that are found missing in your network.

Do you want more pre-defined patch reports? Tell us your requirements.

□	Patch ID	Bulletin ID	Patch Description	Missing Systems	Failed Systems	Platform	Reboot	Patch Uninstallation
□	333962	TU-888	VMware Tools (x64) (12.3.5)	1	0	Windows	May Require	Not Supported
□	31934	MS21-AUG12	2021-08 Servicing Stack Update for Windows Server 2019 for x64-based ...	1	0	Windows	May Require	Not Supported
□	107655	MSWU-3349	2019-11 Update for .NET Framework 3.5 and 4.8 for Windows Server 201...	1	0	Windows	Not Required	Supported

1 - 3 of Total Records

Quick Links

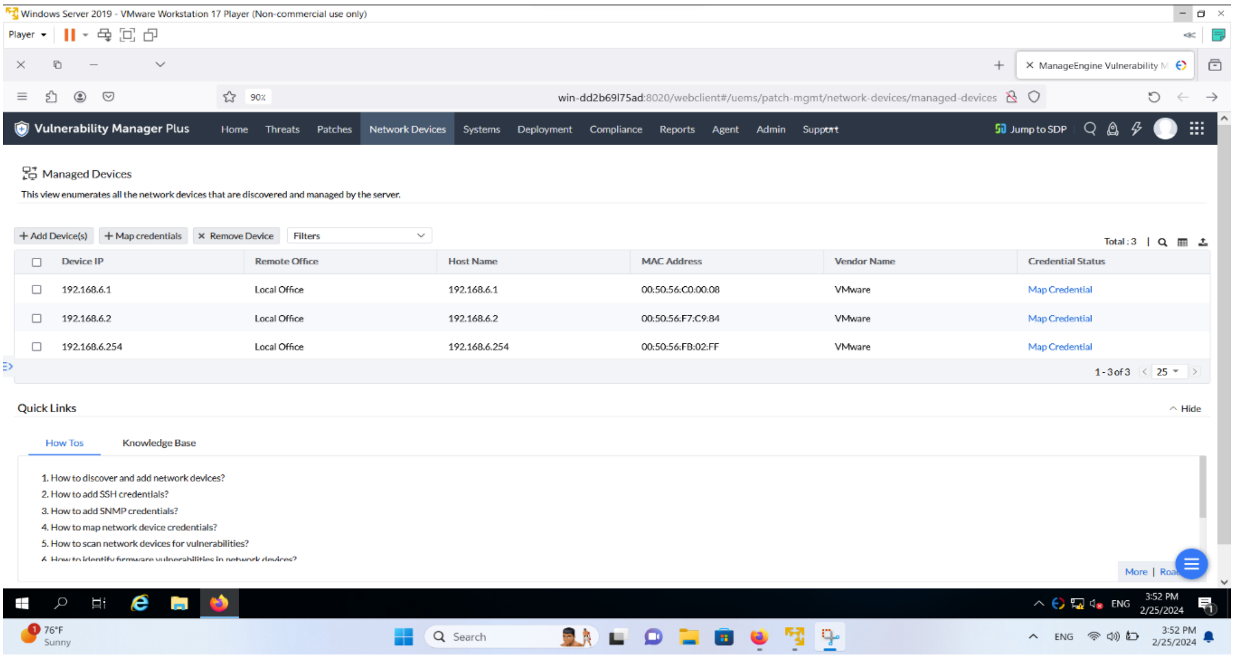
How Tos Knowledge Base FAQ

1. How patch management works?
2. How Automated Patch Deployment works?
3. How to patch computers which are located in a closed network like DMZ?
4. How to customize the system health calculation policy?
5. How to move a patch store location on a distribution server?

© 2024 Zoho Corporation Private Limited. All rights reserved.

Figure 8 :Vulnerability Manager Plus Patches

Step 5: As shown in screenshot of **figure 9,** User mouse drag on (tool bar) and click on Network Devices.



Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
ManageEngine Vulnerability M
90%
win-dd2b69l75ad:8020/webclient#/uems/patch-mgmt/network-devices/managed-devices
Vulnerability Manager Plus
Home
Threats
Patches
Network Devices
Systems
Deployment
Compliance
Reports
Agent
Admin
Support
Jump to SDP

Managed Devices

This view enumerates all the network devices that are discovered and managed by the server.

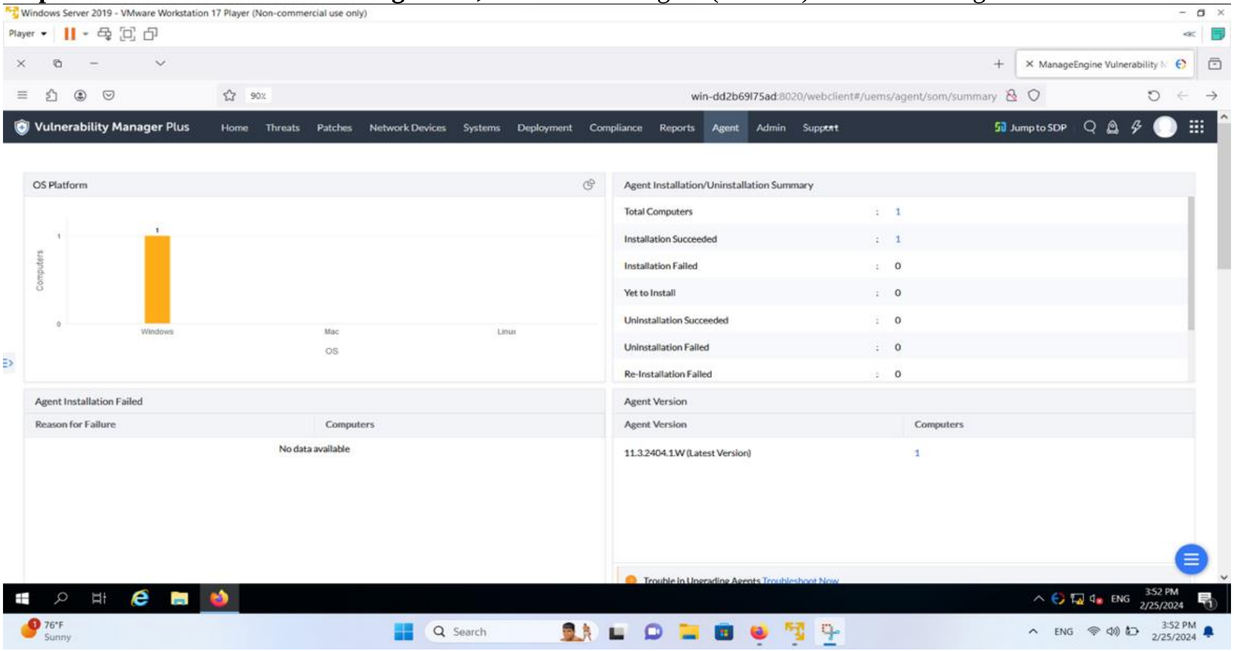
+ Add Device(s)
+ Map credentials
× Remove Device
Filters
Total : 3

□	Device IP	Remote Office	Host Name	MAC Address	Vendor Name	Credential Status
□	192.168.6.1	Local Office	192.168.6.1	00.50.56.C0.00.08	VMware	Map Credential
□	192.168.6.2	Local Office	192.168.6.2	00.50.56.F7.C9.84	VMware	Map Credential
□	192.168.6.254	Local Office	192.168.6.254	00.50.56:FB:02:FF	VMware	Map Credential

1. How to discover and add network devices?
2. How to add SSH credentials?
3. How to add SNMP credentials?
4. How to map network device credentials?
5. How to scan network devices for vulnerabilities?
6. How to identify firmware vulnerabilities in network devices?

Figure 9 : Vulnerability Manager Plus Network Devices

Step 6: As shown in screenshot of **figure 10,** User mouse drag on (tool bar) and click on Agent.



Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
ManageEngine Vulnerability M
90%
win-dd2b69l75ad:8020/webclient#/uems/agent/som/summary
Vulnerability Manager Plus
Home
Threats
Patches
Network Devices
Systems
Deployment
Compliance
Reports
Agent
Admin
Support
Jump to SDP
OS Platform
Computers
1
0
1
Windows
Mac
Linux
OS

Agent Installation/Uninstallation Summary

Total Computers	:	1
Installation Succeeded	:	1
Installation Failed	:	0
Yet to Install	:	0
Uninstallation Succeeded	:	0
Uninstallation Failed	:	0
Re-Installation Failed	:	0

Agent Installation Failed

Reason for Failure	Computers
No data available	

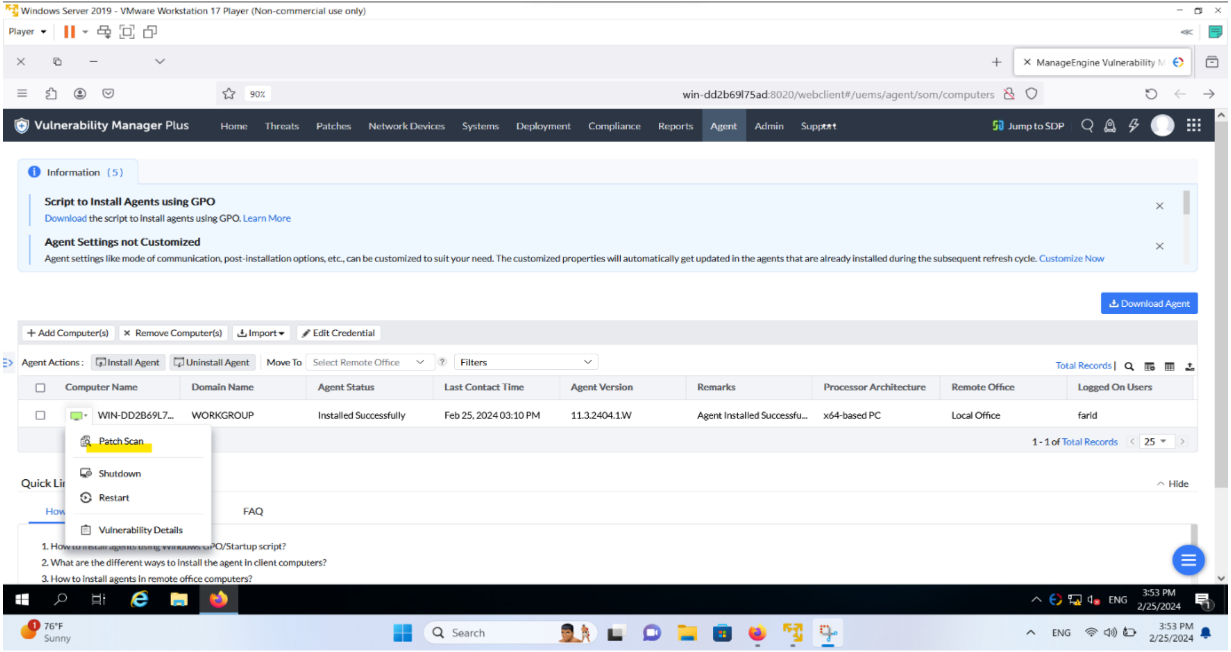
Agent Version

Agent Version	Computers
11.3.2404.1.W (Latest Version)	1

Trouble in Upgrading Agents Troubleshoot Now

Figure 10: Vulnerability Manager Plus Agent

Step 7: As shown in screenshot of **figure 11**, Agent shows Agent Actions; you can find the Vulnerability to Patch Scan it by right clicking then choosing Patch Scan.



Windows Server 2019 - VMware Workstation 17 Player (Non-commercial use only)
Player
ManageEngine Vulnerability M
90%
win-dd2b69l75ad:8020/webclient#/uems/agent/som/computers
Vulnerability Manager Plus
Home
Threats
Patches
Network Devices
Systems
Deployment
Compliance
Reports
Agent
Admin
Support
Jump to SDP
Information (5)

Script to Install Agents using GPO

Download the script to install agents using GPO. Learn More

Agent Settings not Customized

Agent settings like mode of communication, post-installation options, etc., can be customized to suit your need. The customized properties will automatically get updated in the agents that are already installed during the subsequent refresh cycle. Customize Now

☐	Computer Name	Domain Name	Agent Status	Last Contact Time	Agent Version	Remarks	Processor Architecture	Remote Office	Logged On Users
☐	WIN-DD2B69L7...	WORKGROUP	Installed Successfully	Feb 25, 2024 03:10 PM	11.3.2404.1.W	Agent Installed Successfu...	x64-based PC	Local Office	farid

1. How to install agents using Windows GPO/Startup script?
2. What are the different ways to install the agent in client computers?
3. How to install agents in remote office computers?

Figure 11 :Vulnerability Manager Plus Agent Actions

B. Second Scenario: Perform Network Scanning to Identify Live Hosts, Open Ports and Services and Target OS in the Network

Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine. It is one of the most important phases of intelligence gathering for an attacker, which enables him/her to create a profile of the target organization. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

Lab Objectives

Perform Host Discovery using Nmap
Perform Port and Service Discovery using MegaPing
Perform OS Discovery using Unicornscan

Task 1: Perform Host Discovery using Nmap

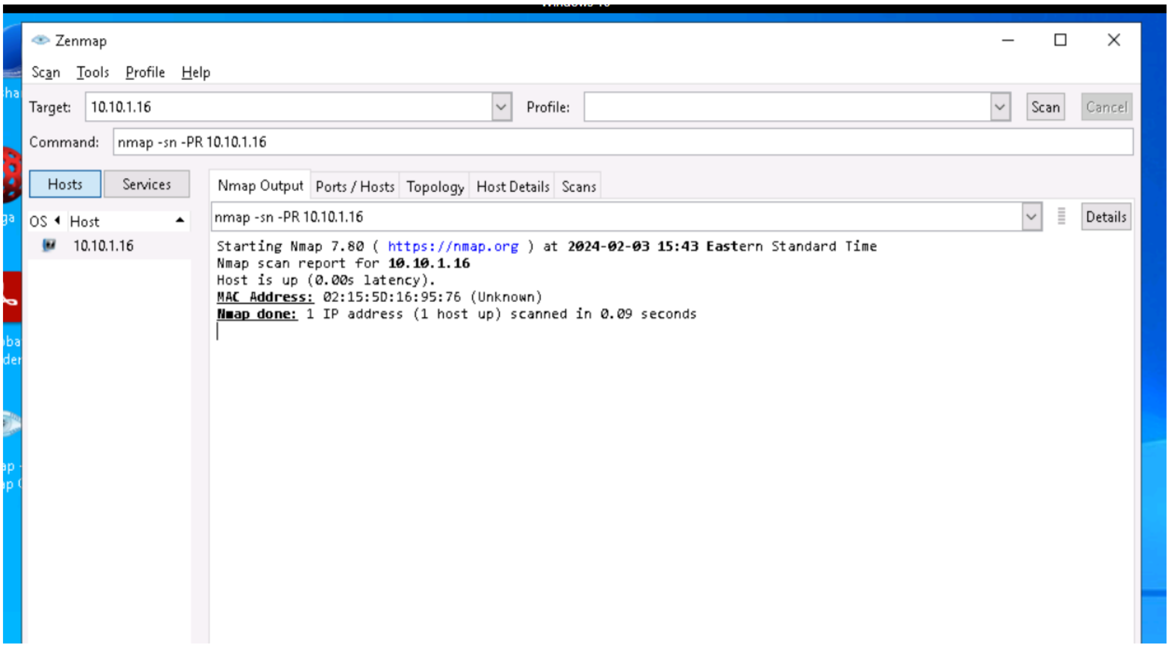
Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

This task uses Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc. Here, consider EC-Council as a target organization.

1- Navigate to the Desktop and double-clik Nmap - Zenmap GUI shortcut.

2- The Nmap - Zenmap GUI appears; in the Command field, type the command nmap -sn -PR [Target IP Address] (here, the target IP address is 10.10.1.16) and click Scan.

3- The scan results appear, indicating that the target Host is up, as shown in the screenshot of **figure 12**.



Target: 10.10.1.16
Profile:
Command: nmap -sn -PR 10.10.1.16

10.10.1.16

```
nmap -sn -PR 10.10.1.16
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 15:43 Eastern Standard Time
Nmap scan report for 10.10.1.16
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:76 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

FiF

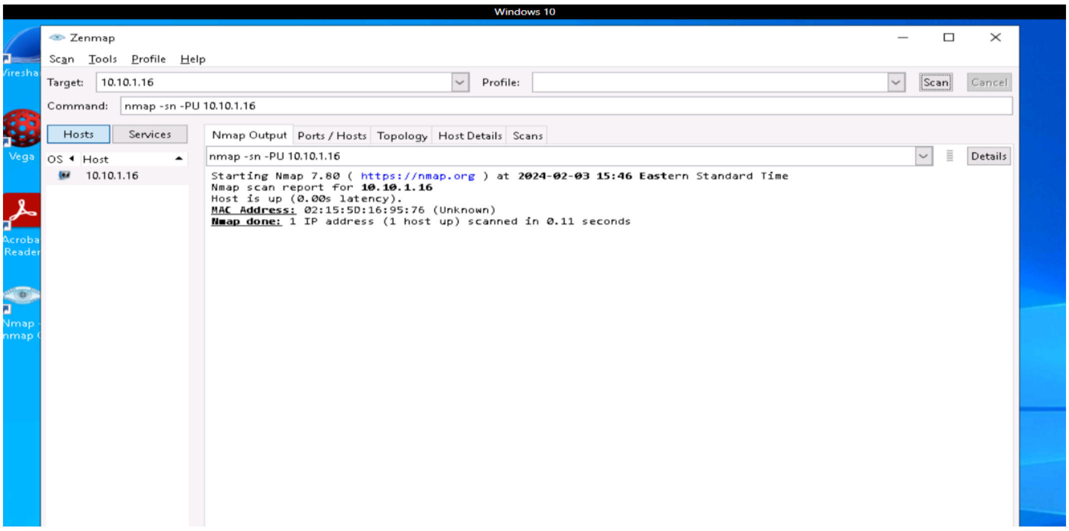
Figure 12: (nmap -sn -PR) Command Output

In this lab, targeting the Windows Server 2016 (10.10.1.16) machine.

The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

4- In the Command field, type nmap -sn -PU [Target IP Address], (here, the target IP address is 10.10.1.16) and click Scan. The scan results appear, indicating the target Host is up, as shown in the screenshot of **figure 13.**

5-



Target: 10.10.1.16
Profile:
Command: nmap -sn -PU 10.10.1.16

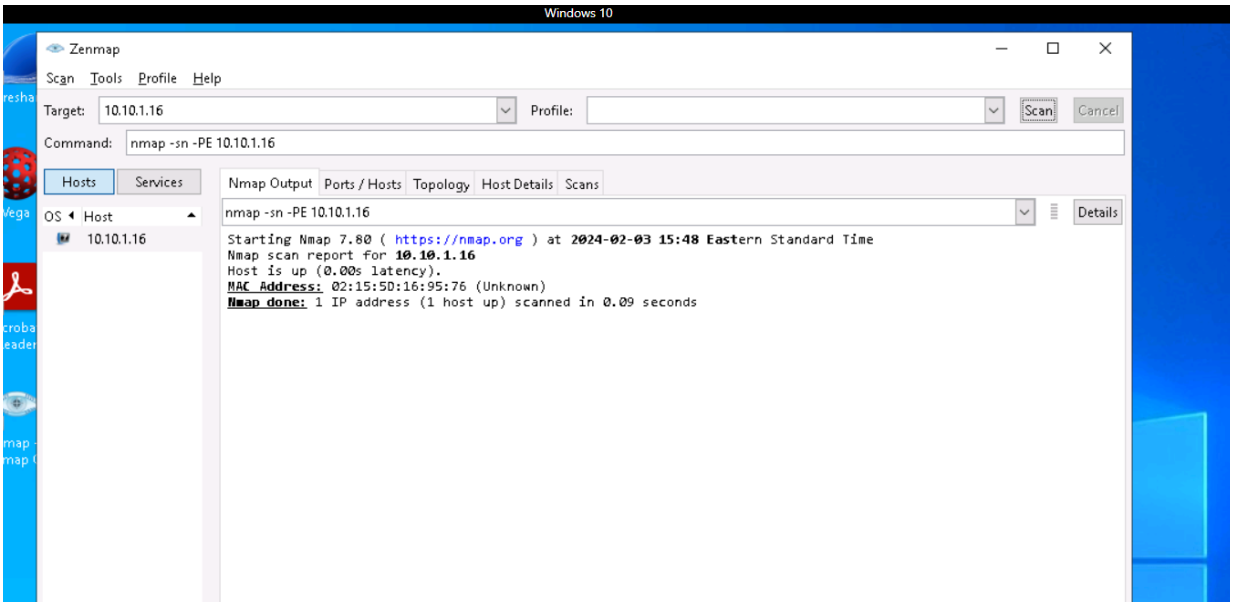
10.10.1.16

```
nmap -sn -PU 10.10.1.16
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 15:46 Eastern Standard Time
Nmap scan report for 10.10.1.16
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:76 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Figure13: (nmap -sn -PU) Command Output

The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as “host/network unreachable” or “TTL exceeded” could be returned.

6- Now, perform the ICMP ECHO ping scan. In the Command field, type nmap -sn -PE [Target IP Address], (here, the target IP address is 10.10.1.16) and click Scan. The scan results appear, indicating that the target Host is up, as shown in the screenshot of figure **14.**



Target: 10.10.1.16

Profile:

Command: nmap -sn -PE 10.10.1.16

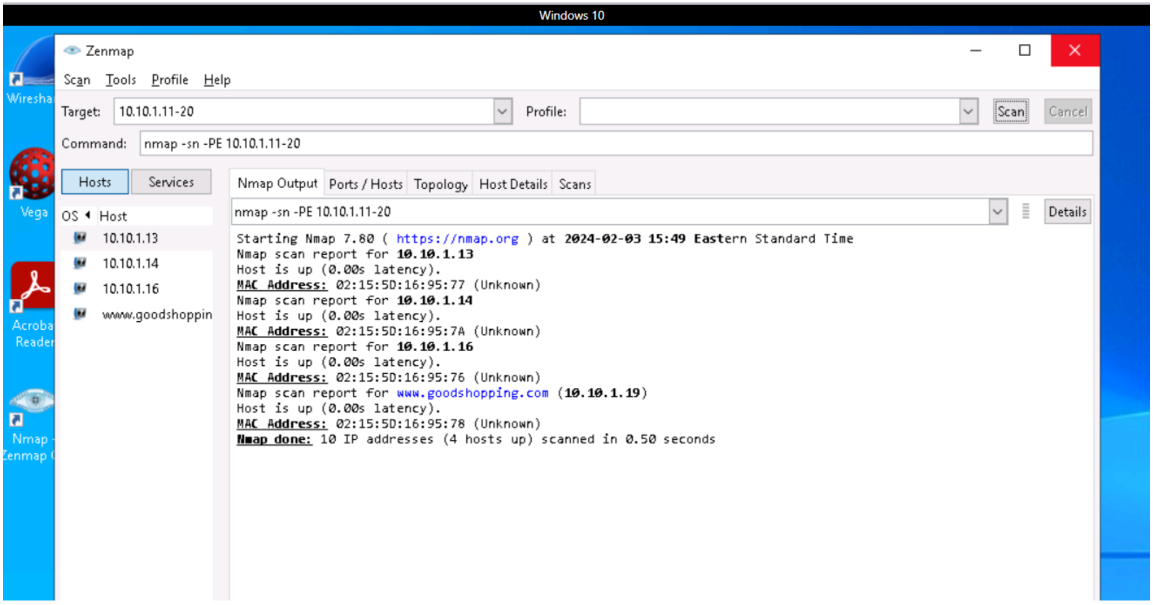
10.10.1.16

```
nmap -sn -PE 10.10.1.16
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 15:48 Eastern Standard Time
Nmap scan report for 10.10.1.16
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:76 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Figure 14: (nmap -sn -PE) Command Output

The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.

7- Now, perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the Command field, type nmap -sn -PE [Target Range of IP Addresses] (here, the target range of IP addresses is 10.10.1.11-20) and click Scan. The scan results appear, indicating the target Host is up, as shown in the screenshot of **figure 15.**



Target: 10.10.1.11-20

Profile:

Command: nmap -sn -PE 10.10.1.11-20

10.10.1.13
10.10.1.14
10.10.1.16
www.goodshoppin

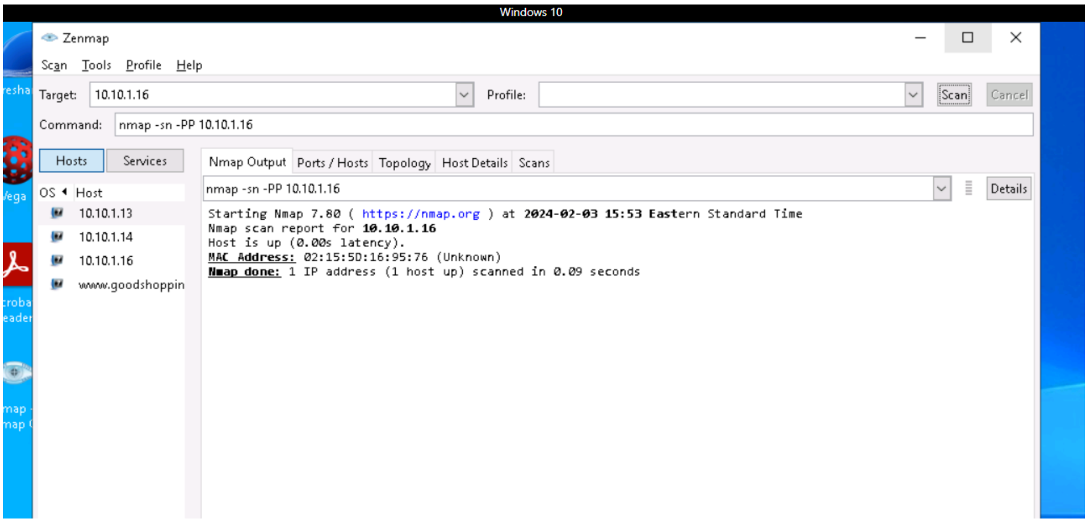
```
nmap -sn -PE 10.10.1.11-20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 15:49 Eastern Standard Time
Nmap scan report for 10.10.1.13
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:77 (Unknown)
Nmap scan report for 10.10.1.14
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:7A (Unknown)
Nmap scan report for 10.10.1.16
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:76 (Unknown)
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:78 (Unknown)
Nmap done: 10 IP addresses (4 hosts up) scanned in 0.50 seconds
```

Figure 15: (nmap -sn -PE) Command Output

In this lab task, we are scanning Windows Server 2019, Windows Server 2016, Parrot Security and Android machines.

The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.

8- Now, perform the ICMP timestamp ping scan. In the Command field, type nmap -sn -PP [Target IP Address], (here, the target IP address is 10.10.1.16) and click Scan. The scan results appear, indicating that the target Host is up, as shown in the screenshot of figure **16.**



Target: 10.10.1.16

Command: nmap -sn -PP 10.10.1.16

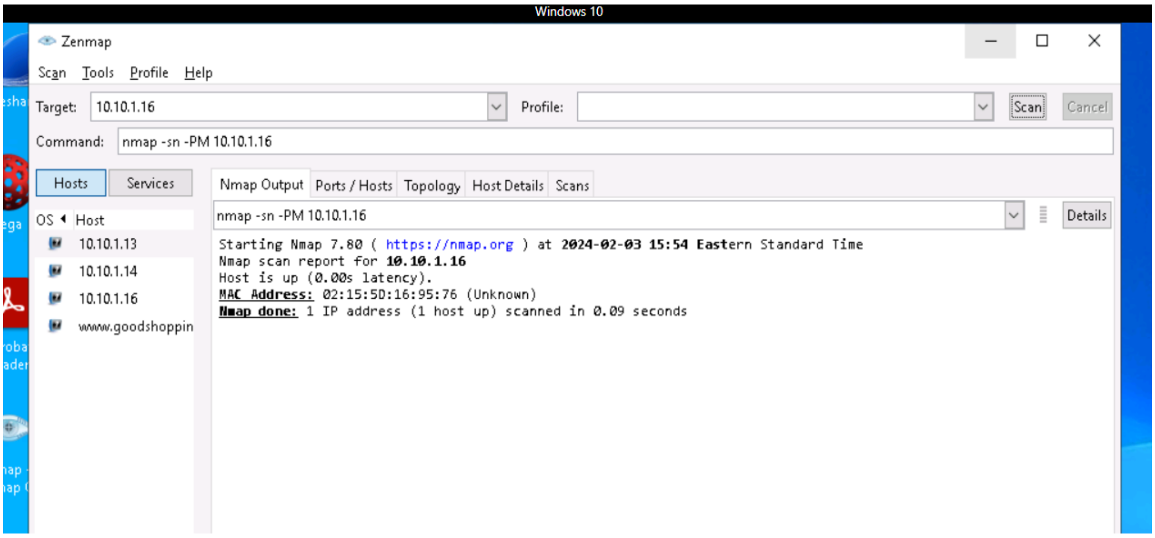
```
nmap -sn -PP 10.10.1.16
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 15:53 Eastern Standard Time
Nmap scan report for 10.10.1.16
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:76 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Figure 16: (nmap -sn -PP) Command Output

In ICMP timestamp ping scan the target machine responds with a timestamp reply to each timestamp query that is received. It is an optional and additional type of ICMP ping whereby a timestamp message can be queried to acquire the information related to the current time from the target host machine.

9- Now, perform the ICMP address mask ping scan. In the Command field, type nmap -sn -PM [Target IP Address], (here, the target IP address is 10.10.1.16) and click Scan. The scan results appear, indicating that the target Host is up, as shown in the screenshot of **figure 17**

10-



Target: 10.10.1.16

Command: nmap -sn -PM 10.10.1.16

```
nmap -sn -PM 10.10.1.16
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-03 15:54 Eastern Standard Time
Nmap scan report for 10.10.1.16
Host is up (0.00s latency).
MAC Address: 02:15:5D:16:95:76 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

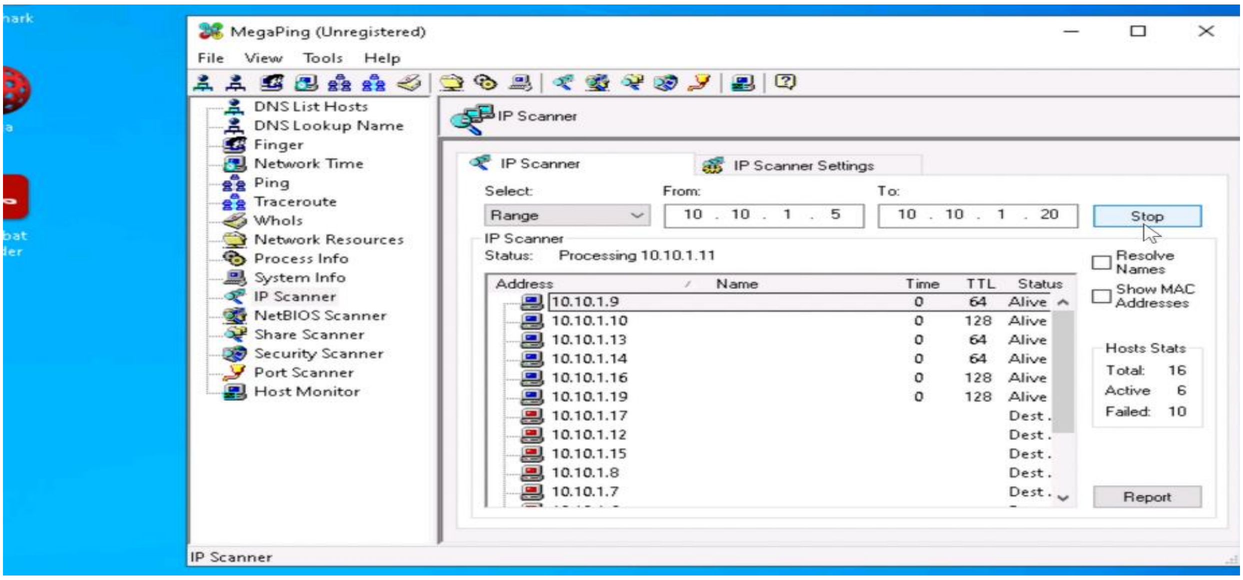
Figure 17: (nmap -sn -PM) Command Output

In ICMP address mask ping scan ICMP address mask query is sent to the target host to acquire information related to the subnet mask. This type of ping method is also effective in identifying the active hosts similarly to the ICMP timestamp ping, specifically when the administrator blocks the traditional ICMP Echo ping.

Task 3: Perform Port and Service Discovery using MegaPing

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

1- The MegaPing (Unregistered) GUI appears displaying the System Info.
2- Select the IP Scanner option from the left pane. In the IP Scanner tab in the right-hand pane, enter the IP range in the From and To fields; in this lab, the IP range is 10.10.1.5 to 10.10.1.20; then, click Start.
3- MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot of figure **18.**



Select: Range
From: 10 . 10 . 1 . 5
To: 10 . 10 . 1 . 20

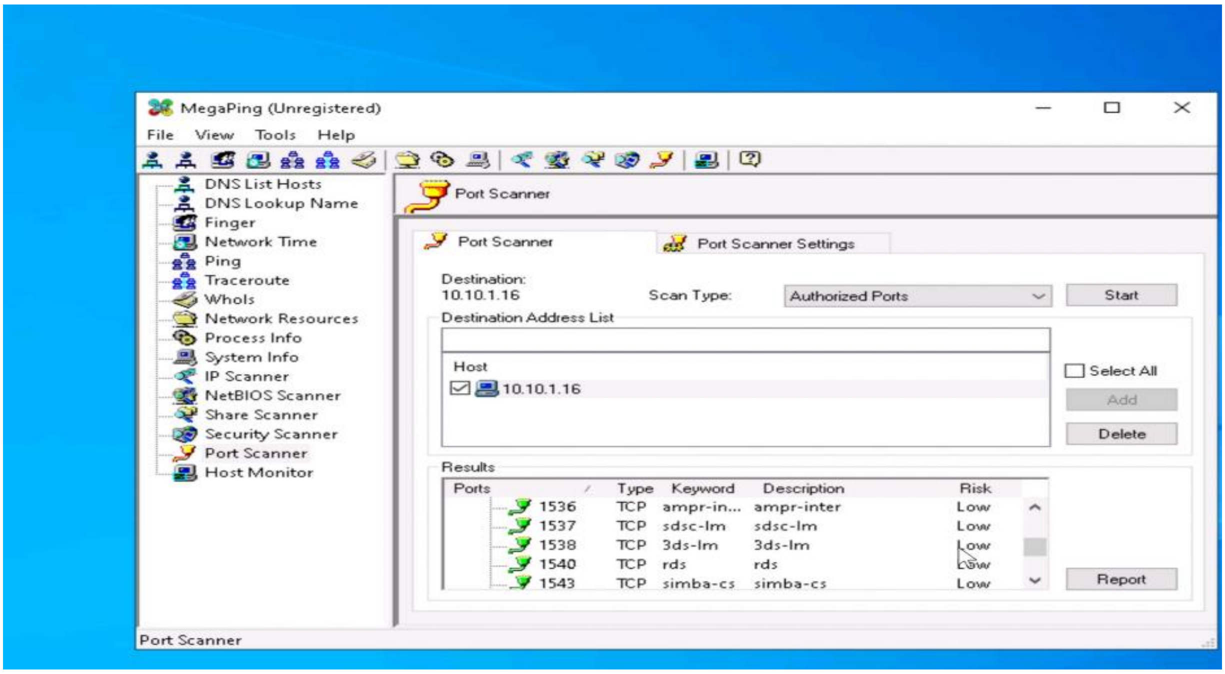
IP Scanner
Status: Processing 10.10.1.11

Address	Name	Time	TTL	Status
10.10.1.9		0	64	Alive
10.10.1.10		0	128	Alive
10.10.1.13		0	64	Alive
10.10.1.14		0	64	Alive
10.10.1.16		0	128	Alive
10.10.1.19		0	128	Alive
10.10.1.17				Dest .
10.10.1.12				Dest .
10.10.1.15				Dest .
10.10.1.8				Dest .
10.10.1.7				Dest .

Hosts Stats
Total: 16
Active 6
Failed: 10

Figure 18: IP Scanner

4- Select the Port Scanner option from the left-hand pane. In the Port Scanner tab in the right-hand pane, enter the IP address of the Windows Server 2016 (10.10.1.16) machine into the Destination Address List field and click Add.
5- Select the 10.10.1.16 checkbox and click the Start button to start listening to the traffic on 10.10.1.16.
6- MegaPing lists the ports associated with Windows Server 2016 (10.10.1.16), with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot of **figure 19.**



Destination:
10.10.1.16
Scan Type: Authorized Ports

Destination Address List

Host
☑ 10.10.1.16

Results

Ports	Type	Keyword	Description	Risk
1536	TCP	ampr-in...	ampr-inter	Low
1537	TCP	sdsc-lm	sdsc-lm	Low
1538	TCP	3ds-lm	3ds-lm	Low
1540	TCP	rds	rds	Low
1543	TCP	simba-cs	simba-cs	Low

Figure 19: Port Scanner

Task 4: Perform OS Discovery using Unicornscan

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

1- Click Parrot Security

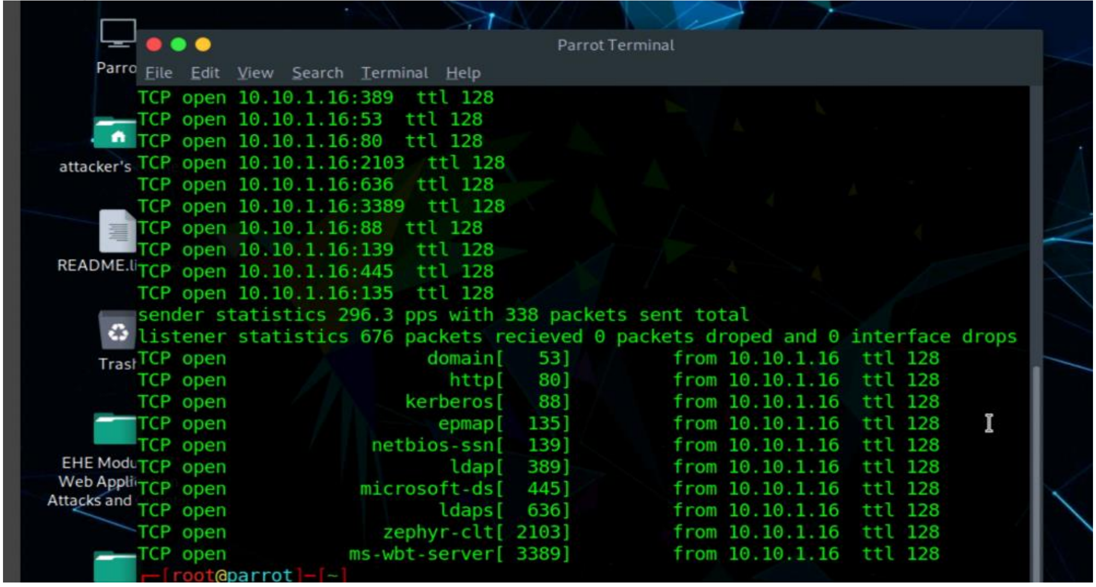
2- Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

3- In the terminal window, type unicornscan [Target IP Address] -Iv (here, the target machine is Windows Server 2016 [10.10.1.16]) and press Enter.

a. In this command, -I specifies an immediate mode and v specifies a verbose mode.

b. As shown in Figure 20 , the scan results appear, displaying the open TCP ports along with the obtained TTL value of 128. As shown in the figure, the ttl values acquired after the scan are 128; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16)

Here, the target machine is Windows Server 2016 (10.10.1.16).

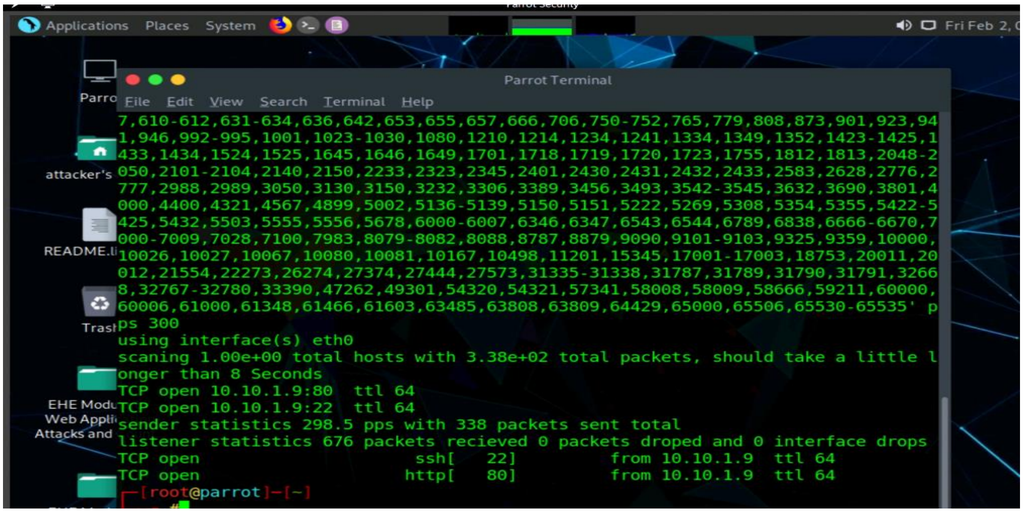


```
TCP open 10.10.1.16:389  ttl 128
TCP open 10.10.1.16:53  ttl 128
TCP open 10.10.1.16:80  ttl 128
TCP open 10.10.1.16:2103  ttl 128
TCP open 10.10.1.16:636  ttl 128
TCP open 10.10.1.16:3389  ttl 128
TCP open 10.10.1.16:88  ttl 128
TCP open 10.10.1.16:139  ttl 128
TCP open 10.10.1.16:445  ttl 128
TCP open 10.10.1.16:135  ttl 128
sender statistics 296.3 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets droped and 0 interface drops
TCP open                     domain[   53]         from 10.10.1.16  ttl 128
TCP open                       http[   80]         from 10.10.1.16  ttl 128
TCP open                   kerberos[   88]         from 10.10.1.16  ttl 128
TCP open                      epmap[  135]         from 10.10.1.16  ttl 128
TCP open                netbios-ssn[  139]         from 10.10.1.16  ttl 128
TCP open                       ldap[  389]         from 10.10.1.16  ttl 128
TCP open               microsoft-ds[  445]         from 10.10.1.16  ttl 128
TCP open                      ldaps[  636]         from 10.10.1.16  ttl 128
TCP open                 zephyr-clt[ 2103]         from 10.10.1.16  ttl 128
TCP open              ms-wbt-server[ 3389]         from 10.10.1.16  ttl 128
┌─[root@parrot]─[~]
```

Figure 20: TCP Ports Output for Windows

4- In the Parrot Terminal window, type unicornscan [Target IP Address] -Iv (here, the target machine is Ubuntu [10.10.1.9]) and press Enter.

a- The scan results appear, displaying the open TCP ports along with a TTL value of 64. As shown in the **figure 21**, the ttl values acquired after the scan are 64; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali).



Applications Places System
Parrot Terminal
File Edit View Search Terminal Help

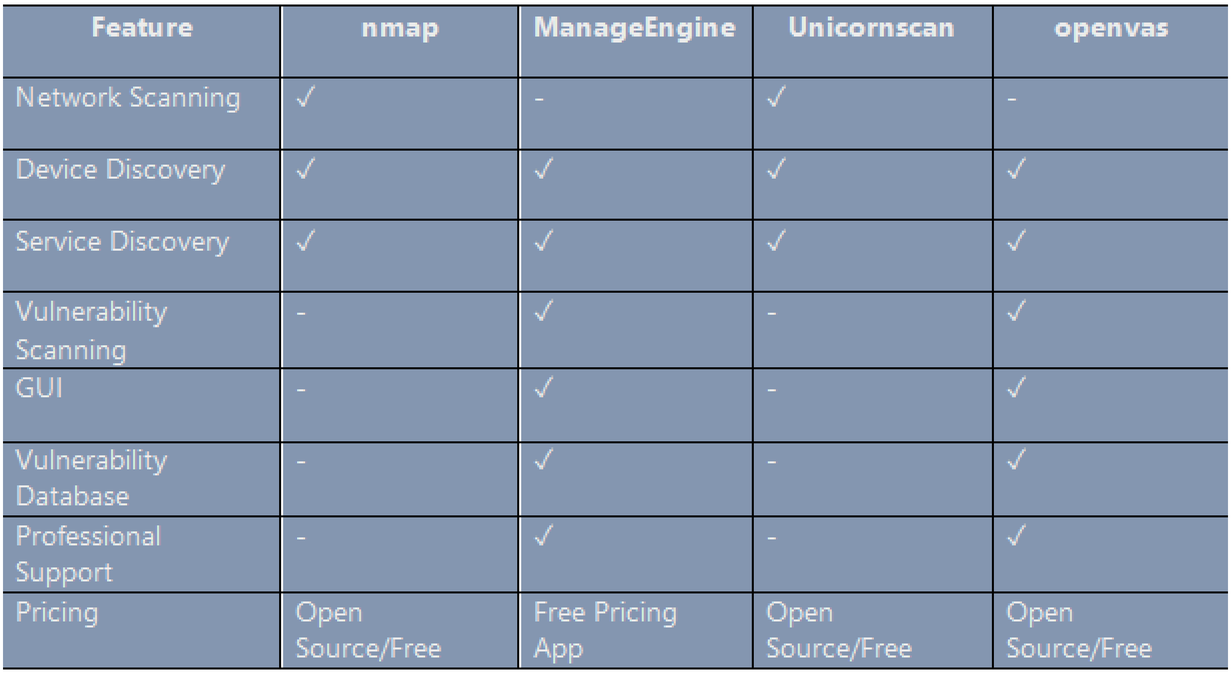
```
7,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,94
1,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1
433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2
050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2
777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4
000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5
425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7
000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,
10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20
012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,3266
8,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,
60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' p
ps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little l
onger than 8 Seconds
TCP open 10.10.1.9:80  ttl 64
TCP open 10.10.1.9:22  ttl 64
sender statistics 298.5 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets droped and 0 interface drops
TCP open                        ssh[   22]         from 10.10.1.9  ttl 64
TCP open                       http[   80]         from 10.10.1.9  ttl 64
┌─[root@parrot]─[~]
```

Figure 21: TCP Ports Output for Linux

V.Comparison of Scenarios Tools: Nmap, ManageEngine, Unicornscan, and OpenVAS

This comparative analysis aims to evaluate and contrast the features of four prominent scenario tools: nmap, ManageEngine, Unicornscan, and OpenVAS. Each tool offers distinct functionalities tailored to network scanning, device discovery, service detection, and vulnerability assessment.

Table 2: Comparison of Scenarios Tools: Nmap, ManageEngine, Unicornscan, and OpenVAS



Feature	nmap	ManageEngine	Unicornscan	openvas
Network Scanning	✓	-	✓	-
Device Discovery	✓	✓	✓	✓
Service Discovery	✓	✓	✓	✓
Vulnerability Scanning	-	✓	-	✓
GUI	-	✓	-	✓
Vulnerability Database	-	✓	-	✓
Professional Support	-	✓	-	✓
Pricing	Open Source/Free	Free Pricing App	Open Source/Free	Open Source/Free

As shown in Table 2 ,Each network security tool offers unique strengths and capabilities, catering to diverse user requirements and preferences. While Nmap excels in network reconnaissance and service detection, ManageEngine and OpenVAS provide comprehensive solutions for vulnerability management and assessment. Unicornscan, on the other hand, prioritizes speed and efficiency in network scanning but may require additional tools for comprehensive vulnerability assessment. Selecting the most suitable tool depends on factors such as the organization's security objectives, budget constraints, and technical expertise.

VI. Feasibility Study

This section is offering insights into both technical and economic aspects essential for any successful implementation.

A. Technical Feasibility Study:

It explores the tools available for the execution. Such as:

1. VirtualBox, an open-source virtualization platform, enables precise simulation and testing.
2. ManageEngine provides advanced vulnerability assessment and patch management tools for meticulous scanning and efficient management.
3. Microsoft Server 2019 and Client 2019 versions offer advanced security features, enhancing reliability and providing a secure computing environment.
4. The second scenario is based on the EC-Council cloud-based lab, focusing on network scanning, host discovery, and vulnerability analysis.

B. Operational Feasibility:

Operational feasibility involves the identification of two distinct scenarios and the establishment of specific tools for their execution.

have been established for their execution.

- **First Scenario**

The first scenario is based on using VirtualBox, utilizing the Server version 2019 and the Client version 2019. Additionally, it involves downloading the ManageEngine tool onto the server and implementing it on the client. The process is explained in figure 22

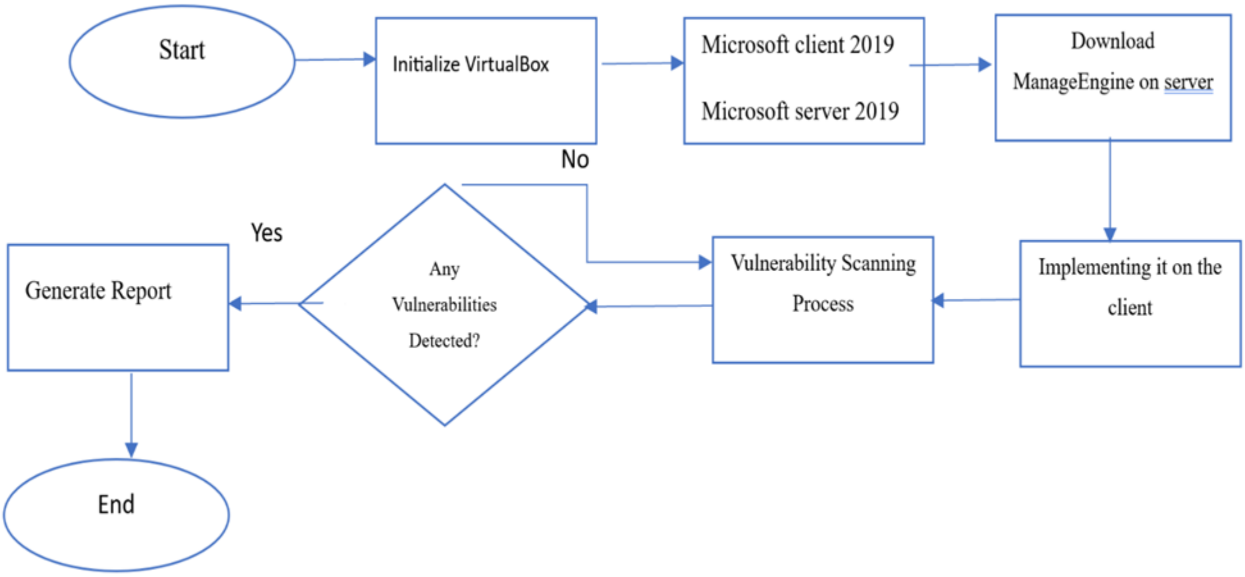


Figure 22 Flow chart First scenario

- **Second Scenario**

It is based on using the EC-Council Cloud Computing-based lab to run the following tasks:
1. Perform Network Scanning to Identify Live Hosts, Open Ports and Services and Target OS in the Network.
2. Perform Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network.

C. Economic Feasibility Study:

The economic feasibility study assesses the financial viability of the project, considering various costs associated with implementation. The costs are detailed in Table 3.

Table 3: Economic Feasibility Study

Items	*Description*	*Cost*
Virtualization Software	Licensing for VirtualBox, a virtualization platform	Free
Vulnerability Tool	18mm	Free
Internet Subscription	High-speed Internet subscription for the project 100 GB	$90.00
EC-Council Kit	Ethical Hacking Essentials (EHE) Kit	$80.00
Dell Laptop	LAPTOP DELL G15 5530/Core i7-13650HX/ RAM 32GB/1TB SSD/15.6" FHD 120Hz/GeForce RTX 3050 6GB/Cam & Mic/WLAN + BT/Backlit Kb/3	$1360.87

VI. Conclusion

In conclusion, this Comparative study provides a comprehensive overview of network reconnaissance and vulnerability assessment, emphasizing the critical need for powerful cybersecurity measures in our interconnected world. Through an extensive exploration of existing literature and research, The light had been shed on the significance of vulnerability assessment tools and methodologies in protecting digital infrastructures.

The goal is to outline two distinct scenarios, each offering valuable insights into practical implementation and hands-on experience. The first scenario involves the use of VirtualBox, ManageEngine's Vulnerability Tool, and Microsoft Server and Client versions for vulnerability scanning in virtual environments. In return, the second scenario focuses on using EC-Council intelligent cloud computing-based labs for network scanning and vulnerability assessment.

Careful consideration is given to the selection of tools and methodologies, ensuring a balanced approach to both knowledge enrichment and practical application. Additionally, the feasibility study conducted underscores the technical, operational, and economic aspects crucial for the successful execution of vulnerability detection initiatives.

Looking ahead, the implementation phase will continue to prioritize the translation of theoretical knowledge into significant skills through practical applications. By providing detailed step-by-step processes for each scenario, this study aims to serve as a valuable resource for cyber security specialists seeking to enhance their proficiency in vulnerability assessment practices.

In summary, this study paper underscores the importance of proactive cybersecurity measures and the critical role played by vulnerability assessment in safeguarding digital assets. Through ongoing research and collaborative efforts, we aim to contribute to the continuous improvement of cybersecurity practices and methodologies.

In future work, a real implementation will be using ManageEngine on a real network. This will allow us to gather valuable data and insights from real systems, aiding in the evaluation of the effectiveness and efficiency of our vulnerability scanning techniques.

References

[1]. Kyriakos Kritikos, Kostas Magoutis, Manos Papoutsakis, Sotiris Ioannidis, “A survey on vulnerability assessment tools and databases for cloud-based web applications,” Elsevier.com, [Online]. Available: www.elsevier.com/journals/array/2590-0056/open-access-journal.

[2]. Dipali N Railkar, Shubhalaxmi Joshi "A Study on Vulnerability Scanning Tools for Network Security", February 2022.

[3]. Rio Armando, Igagkom Agnam Melyantara, Rizma Elfariani, Desy Fitri Aulia Latuconsina, Muhammad Nasrullah "IT Support Website Security Evaluation Using Vulnerability Assessment Tools", December 2022.

[4]. https://www.virtualbox.org/

[5]. https://www.manageengine.com/

[6]. https://www.microsoft.com/en-us/cloud platform/windows-server.

[7]. https://www.microsoft.com/en-us/windows

[8]. https://www.microsoft.com/en-us/cloud platform/windows-server

[9]. Ugur Aksu, Enes Altuncu, Kemal Bicakci "First Look at the Usability of OpenVAS Vulnerability Scanner", TOBB University of Economics and Technology Ankara, Turkey, 2019.