University of West London School of Computing & Engineering	UNIVERSITY OF WEST LONDON

Module	Security Operations and Assurance
Module Code	CP70044E
Module Leader:	Alireza Esfahani
Student Name:	Jash Vaidya
Student ID:	32126197

Contents

Introduction

This assignment is a comprehensive examination of the vulnerabilities in the network architecture of a small business called "SOA Enterprises, Inc." This project aims to improve our penetration testing skills and critically assess approaches for responding to security incidents.

This assignment entails carrying out a number of operational tasks that will be carried out strategically, including host discovery, port scanning, and vulnerability investigation. We'll strategically use tools like Nmap and OpenVAS to get these tasks done quickly and efficiently.

The assignment is divided into multiple tasks. The first task is to set up a structured environment in which to run two virtual machines (VMs): one for Windows 10 and the other for Metasploitable, which runs an uncertain web application called WebGoat. The analysis of fundamental vulnerabilities within these frameworks will be carried out with Kali Linux serving as a vital part of our toolkit.

In Task 2, the focus will be on identifying operational administrations and investigating defenseless virtual machines. OpenVAS will be used to test the Metasploitable virtual machine, and the results of the investigation will identify threats rated as medium or tall.

In summary, we will examine the outcomes from important project tasks. We'll start by going over the network configuration and the vulnerabilities found in the Windows 10 and Metasploitable virtual machines. Next, in order to highlight the open ports and services found, we'll enlarge on the results of the Nmap port scanning. The results of the OpenVAS vulnerability assessment will next be analyzed, with a focus on classifying and analyzing the vulnerabilities' severity. In addition, we'll offer a thorough analysis of a single high- or medium-risk vulnerability, outlining its characteristics, possible exploitation scenarios, and suggested solutions. In order to ensure a clear and effective presentation of the project's outcomes and insights into the security landscape of SOA Enterprises, Inc., we will emphasize the importance of thorough documentation and reporting in our final section.

Important tool information

Nmap:

Network Mapper is shortened to Nmap. It is an open-source Linux command-line utility for detecting installed applications and scanning IP addresses and ports within a network.
Network administrators can use Nmap to find out which devices are connected to their network, identify open ports and services, and identify security holes.
Nmap was created by Gordon Lyon, also known as Fyodor, as a tool to assist in quickly mapping a whole network and locating any open ports or services.

OpenVAS:

A vulnerability scanner called OpenVAS makes it possible to keep an eye out for security flaws in networks, systems, and applications. OpenVAS and other vulnerability management scanners locate and categorize potential weak points in your infrastructure, estimate potential risks, and suggest mitigations to fix the issue.

Metasploitable (Virtual Machine):

Metasploitable is a purposefully compromised Linux virtual machine that can be used for common penetration testing techniques, security tool testing, and security training. Any recent version of VMware software as well as other visualization tools like VirtualBox can run the virtual machine.

WebGoat (uncertain web application):

A purposefully insecure web application, the OWASP WebGoat project can be used to safely target common application vulnerabilities. It can also be used to practice scanning and identifying the different vulnerabilities built into WebGoat using application security tools like OWASP ZAP.

Penetration Testing (Pen Testing)

A method used by knowledgeable security professionals to pose as hackers and check for vulnerabilities in a computer system, network, or application is called penetration testing, or ethical hacking. The primary objective is to identify gaps in the security defenses so that companies can close them before actual attackers take advantage of them.

What Makes Penetration Testing Crucial:

Identifying Weaknesses

- Pen testing is a useful tool for organizations to identify vulnerabilities that hackers may exploit. This covers configuration errors, software bugs, and other security-related issues.

Cutting Down on Risks:

- Organizations can take action to reduce the likelihood of a security breach by identifying vulnerabilities. This keeps unauthorized individuals from accessing sensitive information. Why Penetration Testing is Important:

Demonstrating a dedication to security

- Penetration testing demonstrates to stakeholders, clients, and authorities alike that a company takes security seriously. It demonstrates their commitment to having robust security measures.

Respecting Guidelines and Standards:

- Certain sectors and regulations require periodic security audits, such as penetration testing, to ensure that all protocols are being followed. This is particularly valid for sectors like government, healthcare, and finance.

Teaching Security:

- Pen testing is an effective tool for organizations to learn about potential vulnerabilities and real-world threats. Having this knowledge is crucial for building a solid security culture inside an organization.

Preparing for Unexpected Events:

- Organizations can assess how well they can manage actual security issues by simulating attacks. They become more adept at handling situations when they arise as a result.

Keep Getting Better:

- In order to stay ahead of evolving security threats, penetration testing must be done on a regular basis. By doing this frequently, security measures are ensured to remain effective over time.

With explicit written consent from SOA Enterprises, Inc., the penetration testing procedure is conducted in a manner that closely adheres to the guidelines. This rigorous approach ensures the execution of a controlled and moral testing procedure.

Process of Penetration Testing:

Reconnaissance:

Gathering comprehensive data to gain a complete understanding of the target area is the first step.

Weakness Scanning:

Using advanced scanning techniques, vulnerabilities in the Windows 10 and Metasploitable virtual machines are systematically discovered.

Reporting:

A comprehensive report painstakingly records the findings and outcomes of the penetration testing operations. This document lists the vulnerabilities that were discovered, assesses their potential impact, and provides workable solutions.

Utilization:

The Kali Linux virtual machine (VM) is used to exploit vulnerabilities once they have been discovered, simulating potential real-world attack scenarios.

The testing report is one of SOA Enterprises, Inc.'s most important tools. It helps people make wise decisions that increase their security. They actively work to be incredibly safe and resilient against new cyberthreats rather than waiting for problems to happen.

Devices	IP ADDRESS	SUBNET MASK
Kali Linux	192.168.0.1	255.255.255.0
Metasploitable	192.168.0.3	255.255.255.0
Windows 10 + WebGoat	192.168.0.2	255.255.255.0

1 Network Scanning VM (NMAP)

"nmap <target ip address>" & "nmap -p- -A -sV -O -script=default <target ip address>"

are the commands used to do the Nmap scan.

Output for the target Windows 10 (192.168.0.2) & Metasploitable (192.168.0.3). The target system's open ports, services, operating system, and possible vulnerabilities are all detailed in the scan findings.

Synopsis of Results:

Open Ports:

- The target system's open ports are discovered by the scan. Every line in the output denotes a distinct open port and the corresponding service.

Services Detected:

- Nmap looks for services that are using open ports and, if it can, tells you the version of each one.

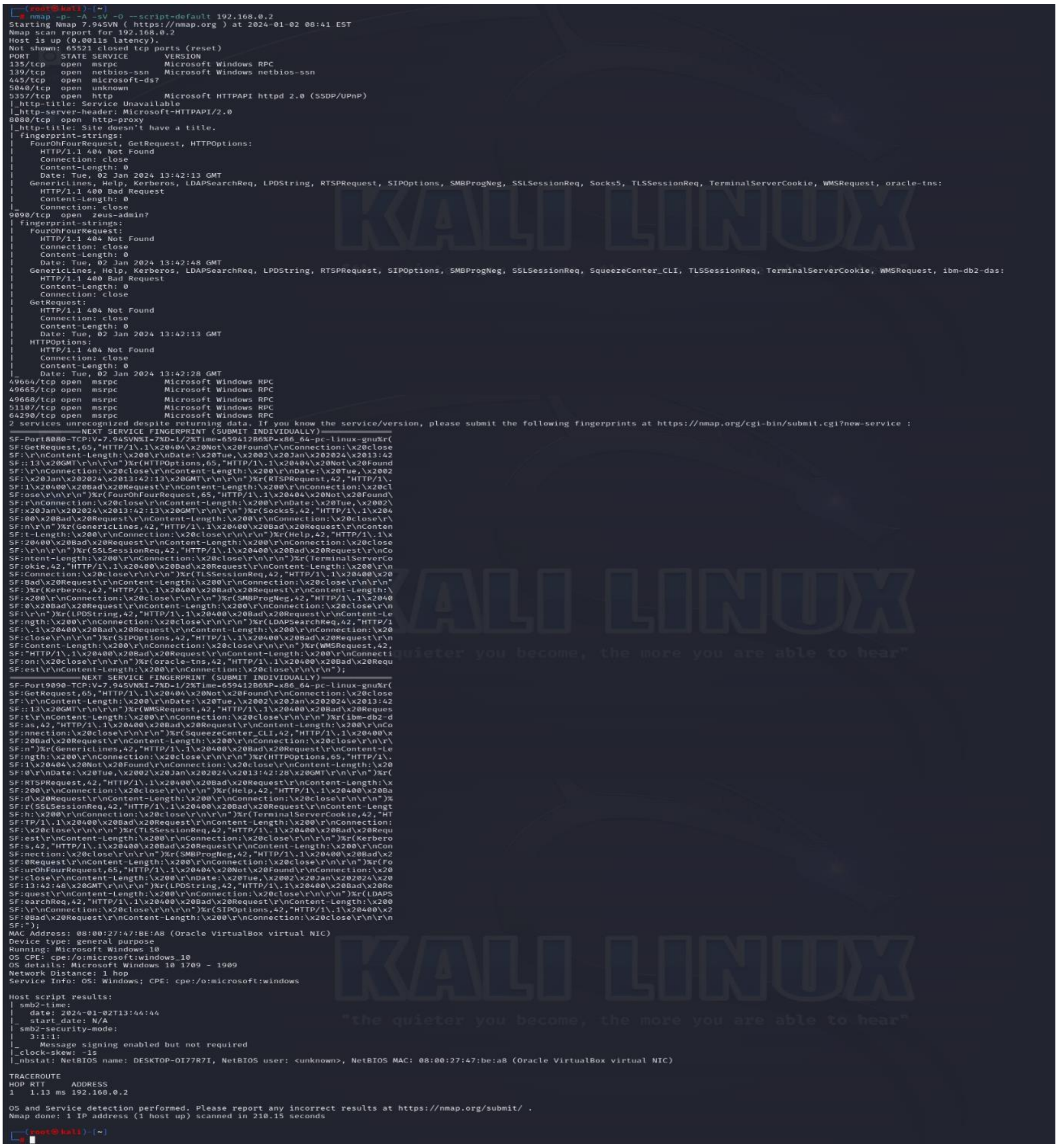
Nmap Scripting Engine (NSE) Scripts:

- Nmap's NSE scripts, which can carry out further checks and tests for potential vulnerabilities, are enabled via the --script=default option.

Operating System Detection:

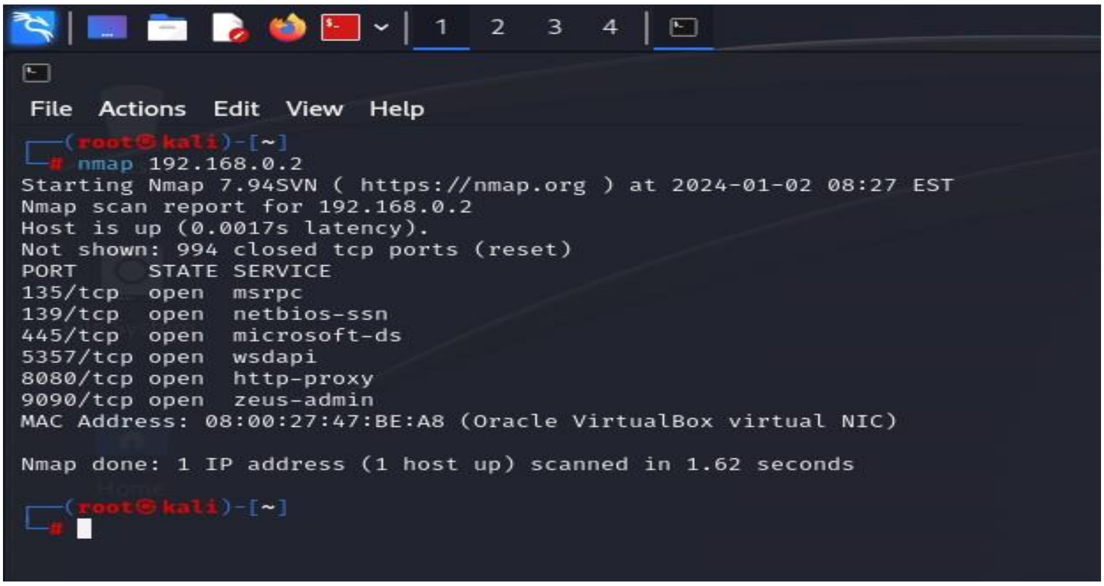
- Using a variety of fingerprinting approaches, the scan looks for the operating system that is currently installed on the target.

1.1 VM Windows 10 + WebGoat



```
┌──(root㉿kali)-[~]
└─# nmap -p- -A -sV -O --script-default 192.168.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 08:41 EST
Nmap scan report for 192.168.0.2
Host is up (0.0011s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http-proxy
|_http-title: Site doesn't have a title.
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 0
|     Date: Tue, 02 Jan 2024 13:42:13 GMT
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|_    Connection: close
9090/tcp  open  zeus-admin?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 0
|     Date: Tue, 02 Jan 2024 13:42:48 GMT
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, SqueezeCenter_CLI, TLSSessionReq, TerminalServerCookie, WMSRequest, ibm-db2-das:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|   GetRequest:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 0
|     Date: Tue, 02 Jan 2024 13:42:13 GMT
|   HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 0
|_    Date: Tue, 02 Jan 2024 13:42:28 GMT
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
51107/tcp open  msrpc         Microsoft Windows RPC
64290/tcp open  msrpc         Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.94SVN%I=7%D=1/2%Time=659412B6%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,65,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20close
SF:\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2002\x20Jan\x202024\x2013:42
SF::13\x20GMT\r\n\r\n")%r(HTTPOptions,65,"HTTP/1\.1\x20404\x20Not\x20Found
SF:\r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2002
SF:\x20Jan\x202024\x2013:42:13\x20GMT\r\n\r\n")%r(RTSPRequest,42,"HTTP/1\.
SF:1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl
SF:ose\r\n\r\n")%r(FourOhFourRequest,65,"HTTP/1\.1\x20404\x20Not\x20Found\
SF:r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2002\
SF:x20Jan\x202024\x2013:42:13\x20GMT\r\n\r\n")%r(Socks5,42,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\
SF:n\r\n")%r(GenericLines,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Help,42,"HTTP/1\.1\x
SF:20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close
SF:\r\n\r\n")%r(SSLSessionReq,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCo
SF:ntent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerCo
SF:okie,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\n
SF:Connection:\x20close\r\n\r\n")%r(TLSSessionReq,42,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n"
SF:)%r(Kerberos,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\
SF:x200\r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,42,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n
SF:\r\n")%r(LPDString,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Le
SF:ngth:\x200\r\nConnection:\x20close\r\n\r\n")%r(LDAPSearchReq,42,"HTTP/1
SF:\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20
SF:close\r\n\r\n")%r(SIPOptions,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Content-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(WMSRequest,42,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnecti
SF:on:\x20close\r\n\r\n")%r(oracle-tns,42,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9090-TCP:V=7.94SVN%I=7%D=1/2%Time=659412B6%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,65,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20close
SF:\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2002\x20Jan\x202024\x2013:42
SF::13\x20GMT\r\n\r\n")%r(WMSRequest,42,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(ibm-db2-d
SF:as,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCo
SF:nnection:\x20close\r\n\r\n")%r(SqueezeCenter_CLI,42,"HTTP/1\.1\x20400\x
SF:20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\
SF:n")%r(GenericLines,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Le
SF:ngth:\x200\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,65,"HTTP/1\.
SF:1\x20404\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x20
SF:0\r\nDate:\x20Tue,\x2002\x20Jan\x202024\x2013:42:28\x20GMT\r\n\r\n")%r(
SF:RTSPRequest,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x
SF:200\r\nConnection:\x20close\r\n\r\n")%r(Help,42,"HTTP/1\.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%
SF:r(SSLSessionReq,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Lengt
SF:h:\x200\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerCookie,42,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:
SF:\x20close\r\n\r\n")%r(TLSSessionReq,42,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Kerbero
SF:s,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCon
SF:nection:\x20close\r\n\r\n")%r(SMBProgNeg,42,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Fo
SF:urOhFourRequest,65,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20
SF:close\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2002\x20Jan\x202024\x20
SF:13:42:48\x20GMT\r\n\r\n")%r(LPDString,42,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(LDAPS
SF:earchReq,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200
SF:\r\nConnection:\x20close\r\n\r\n")%r(SIPOptions,42,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n
SF:");
MAC Address: 08:00:27:47:BE:A8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-02T13:44:44
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -1s
|_nbstat: NetBIOS name: DESKTOP-OI77R7I, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:47:be:a8 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.0.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.15 seconds

┌──(root㉿kali)-[~]
└─#
```

Fig. 1   Detailed Nmap Scan (Windows Virtual Machine)



```
┌──(root㉿kali)-[~]
└─# nmap 192.168.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 08:27 EST
Nmap scan report for 192.168.0.2
Host is up (0.0017s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
8080/tcp open  http-proxy
9090/tcp open  zeus-admin
MAC Address: 08:00:27:47:BE:A8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds

┌──(root㉿kali)-[~]
└─#
```

Fig. 2 Nmap Scan (Windows Virtual Machine)

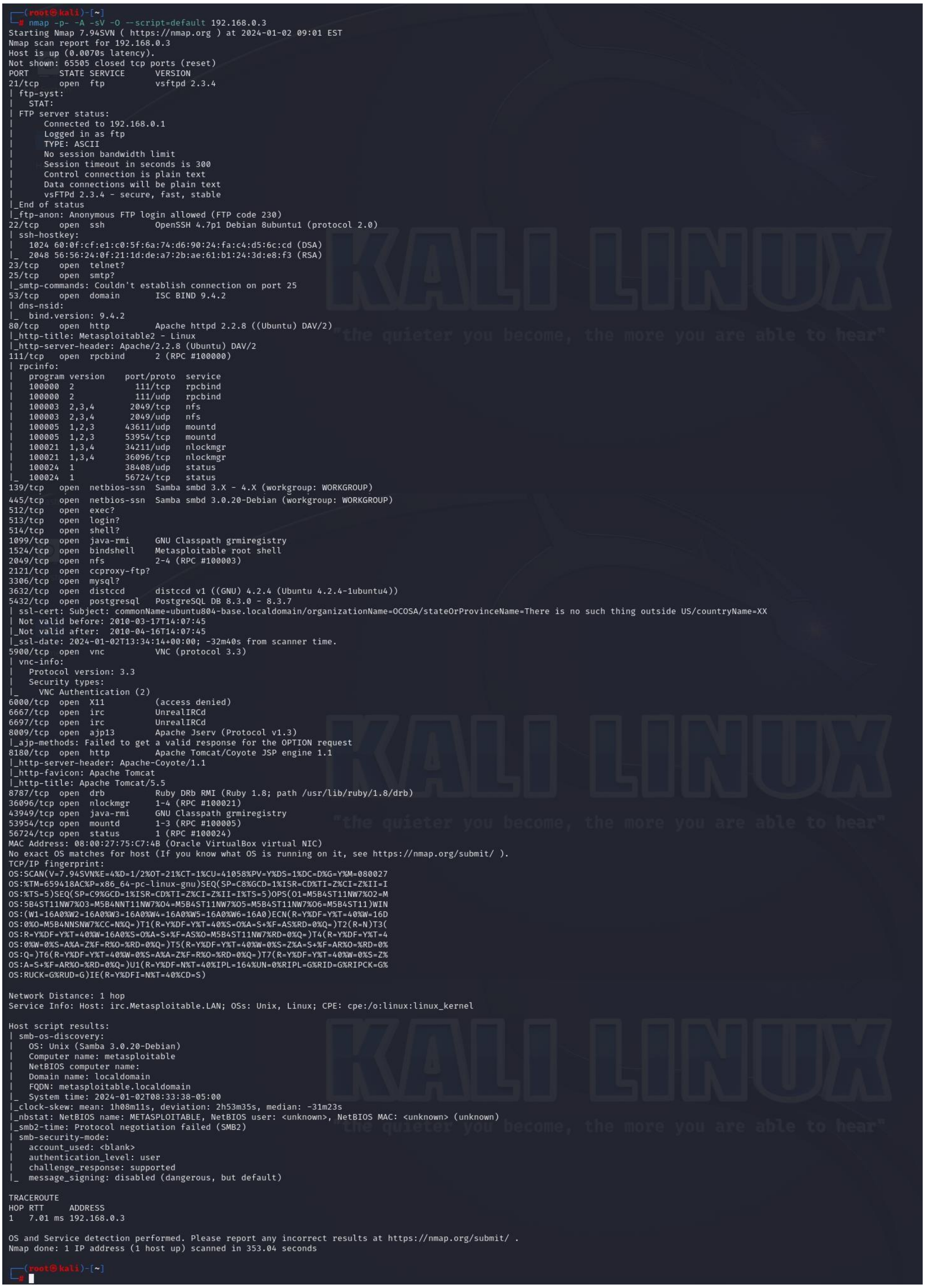
Detailed Explanation for Open Ports and Services:

- 135/tcp - msrpc: Port 135 is used by the Microsoft Windows RPC service.
- 139/tcp - netbios-ssn: Port 139 is being used by the Microsoft Windows netbios-ssn service.
- 445/tcp - microsoft-ds: Port 445 is used by Microsoft Windows Directory Services (microsoft-ds).
- 5040/tcp - unknown: This port is open, but it does not identify the service.
- 5357/tcp - http: Port 5357 is being used by Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP). It looks like the service isn't available.
- 8080/tcp - http-proxy: It appears that an HTTP proxy is operating on Port 8080, which is open. There is no title for the website.
- 9090/tcp - zeus-admin: It appears that there is activity on port 9090, which is connected to Zeus admin. The 404 Not Found error is returned by the service.

Operating System and Other Information:

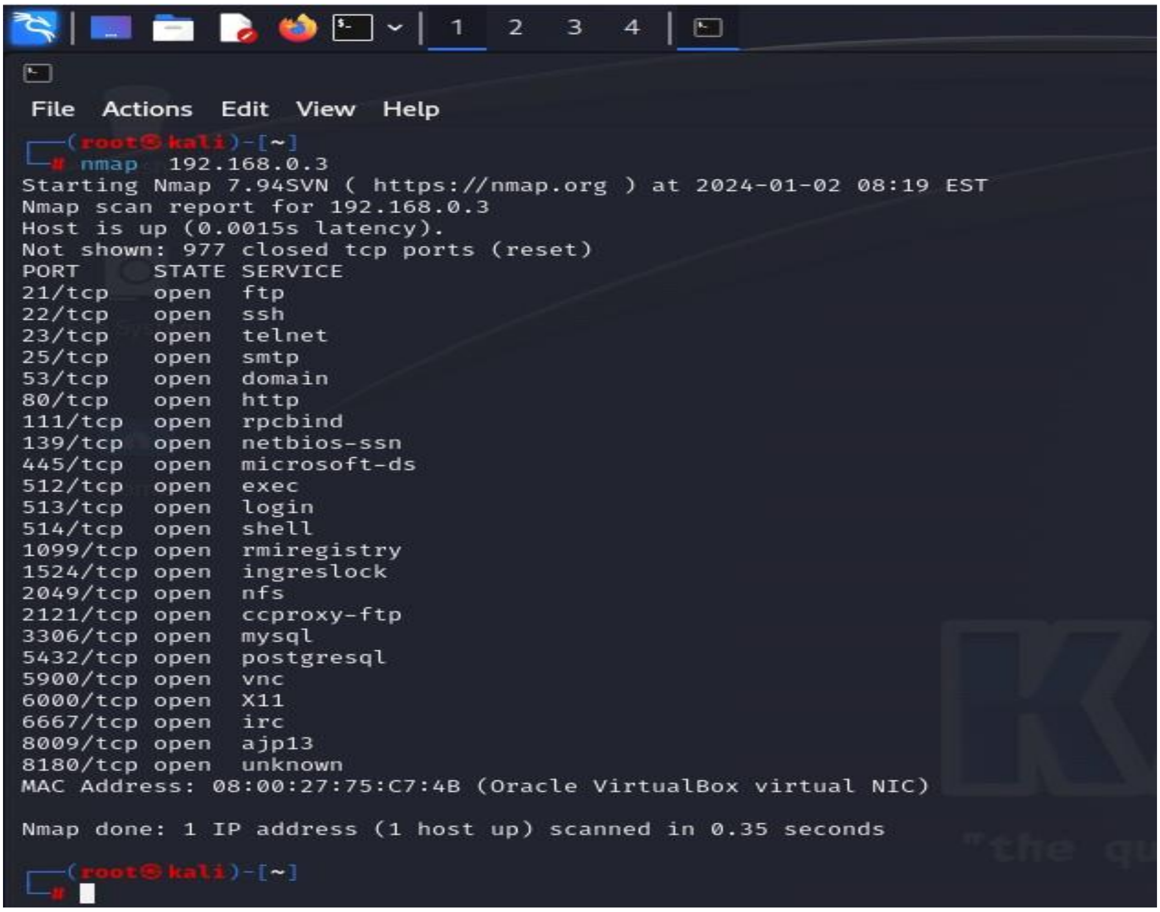
Operating System: Microsoft Windows 10 (versions 1709–1909) is the operating system that the scan successfully identifies.

Network Information: The host's virtual network interface (oracle virtualbox virtual NIC) is 08:00:27:47:BE:A8. 1.2 VM Metasploitable



```
┌──(root㉿kali)-[~]
└─# nmap -p- -A -sV -O --script=default 192.168.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 09:01 EST
Nmap scan report for 192.168.0.3
Host is up (0.0070s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      43611/udp   mountd
|   100005  1,2,3      53954/tcp   mountd
|   100021  1,3,4      34211/udp   nlockmgr
|   100021  1,3,4      36096/tcp   nlockmgr
|   100024  1          38408/udp   status
|_  100024  1          56724/tcp   status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-01-02T13:34:14+00:00; -32m40s from scanner time.
5900/tcp  open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
36096/tcp open  nlockmgr     1-4 (RPC #100021)
43949/tcp open  java-rmi     GNU Classpath grmiregistry
53954/tcp open  mountd       1-3 (RPC #100005)
56724/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:75:C7:4B (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/2%OT=21%CT=1%CU=41058%PV=Y%DS=1%DC=D%G=Y%M=080027
OS:%TM=659418AC%P=x86_64-pc-linux-gnu)SEQ(SP=C8%GCD=1%ISR=CD%TI=Z%CI=Z%II=I
OS:%TS=5)SEQ(SP=C9%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%TS=5)OPS(O1=M5B4ST11NW7%O2=M
OS:5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN
OS:(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D
OS:0%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(
OS:R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=4
OS:0%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%
OS:A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-01-02T08:33:38-05:00
|_clock-skew: mean: 1h08m11s, deviation: 2h53m35s, median: -31m23s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   7.01 ms 192.168.0.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 353.04 seconds

┌──(root㉿kali)-[~]
└─# 
```

Fig. 3   Detaild Nmap Scan (Metasploit Virtual Machine)



```
┌──(root㉿kali)-[~]
└─# nmap  192.168.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 08:19 EST
Nmap scan report for 192.168.0.3
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:75:C7:4B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

┌──(root㉿kali)-[~]
└─# █
```

Fig. 4   Nmap Scan (Metasploit VM)

Explanation on Open Ports & Services:

- ❖ • 21/tcp - ftp: Port 21 is being used by the FTP service (vsftpd 2.3.4). FTP code 230 allows anonymous logins.
- ❖ • 22/tcp - ssh: Port 22 is used by the SSH service (OpenSSH 4.7p1 Debian 8ubuntu1). Fingerprints for SSH keys are given.
- ❖ • 23/tcp - telnet: Port 23 appears to be operating a telnet service and is open. The precise service version is not identified.
- ❖ • 25/tcp - smtp: With port 25 open, an SMTP service is detected. On port 25, though, a connection could not be made.
- ❖ • 53/tcp - domain: Port 53 is used by the BIND DNS service (version 9.4.2).
- ❖ • 80/tcp - http: The Metasploitable2 web page is being served by the Apache HTTP server (version 2.2.8) on port 80.
- ❖ • 111/tcp-rpcbind: Various RPC programs are supported by the RPC service (rpcbind), which is operating on port 111.
- ❖ • 139/tcp - netbios-ssn: The Samba SMB server (version 3.X - 4.X) is running on port 139.

- • Netbios-ssn: 445/tcp: An additional Samba SMB server instance (version 3.0.20-Debian)
- • 512/tcp - exec: It appears that a "exec" service is operating on port 512, which is open.
- • 513/tcp - login: It appears that a "login" service is operating on port 513, which is open.
- • 514/tcp - shell: It appears that a "shell" service is operating on port 514, which is open.1524/tcp - bindshell: A bind shell service is running on port 1524.
- 2049/tcp - nfs: Port 2049 is being used by the Network File System (NFS).
- 3306/tcp - mysql: Port 3306 is used by the MySQL database server.
- 5432/tcp - postgresql: Port 5432 is used by the PostgreSQL database server (versions 8.3.0 - 8.3.7).
- 5900/tcp - vnc: Port 5900 is used by VNC (protocol 3.3).
- 6667/tcp and 6697/tcp - irc: These are the ports that UnrealIRCd is currently using.
- 8009/tcp - ajp13: Port 8009 is being used by Apache Jserv (Protocol v1.3).
- Port 8180 is being used by Apache Tomcat/Coyote JSP engine 1.1 on port 8180/tcp.
- 8787/tcp-drb: Ruby 1.8's DRb RMI is now operating on port 8787.

Operating System & Information:

- Network Information: The host's MAC address is 08:00:27:75:C7:4B (Oracle VirtualBox virtual NIC), and it is a member of the "WORKGROUP".
- Operating System: The scan couldn't detect the precise operating system, generating a TCP/IP fingerprint.

These results offer a thorough summary of the services that are operating on the target systems, facilitating more research and possible security enhancements.

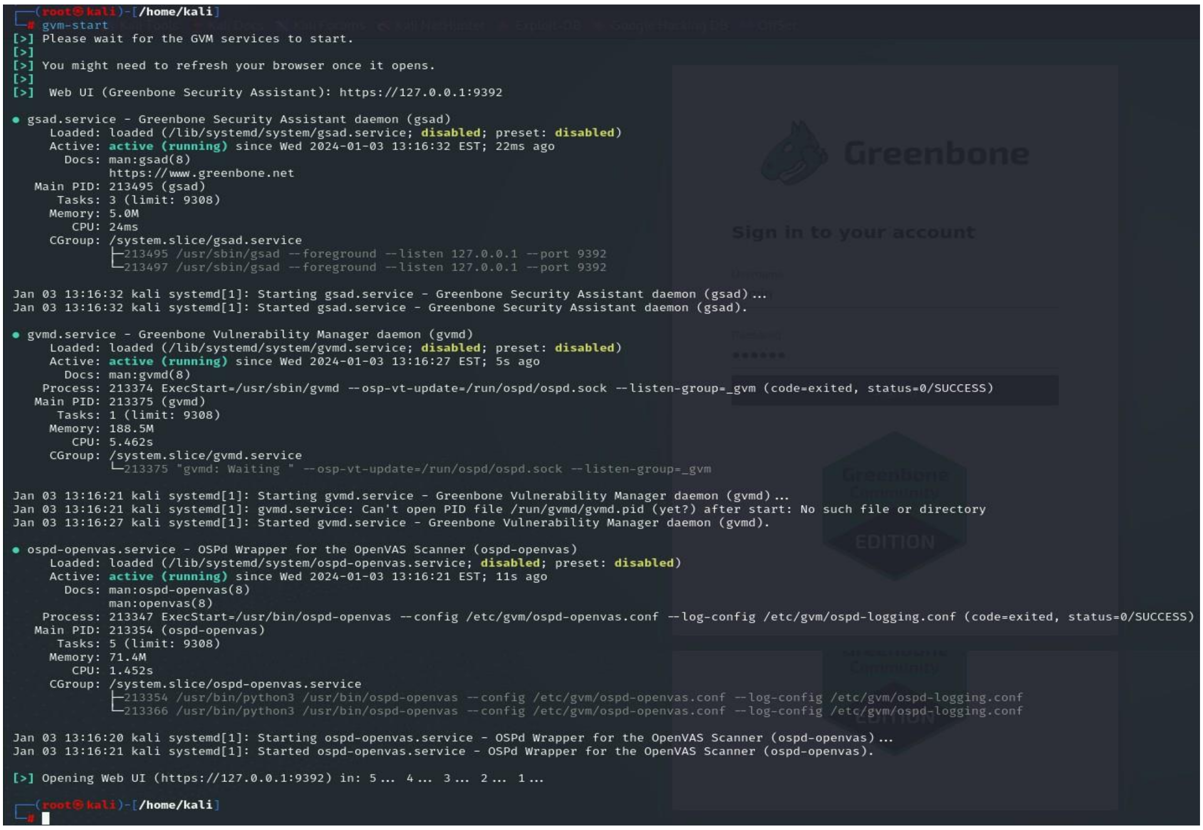
2 System Scanning (OpenVAS)

An essential open-source tool for vulnerability management and scanning is the Open Vulnerability Assessment System. OpenVAS aims to proactively identify and clarify any security risks by utilizing a technique based on thorough vulnerability assessments. Specifically designed to identify security flaws in computer systems and networks, this software is a key part of the Green bone Networks Vulnerability Management (GVM) solution.

Installation(Kali Linux):

Below are the commands which needs to run on a terminal.

```
sudo apt update
sudo apt upgrade -y
sudo apt dist-upgrade -y
sudo apt install openvas
gvm-setup
gvm-check-setup
gvmd --user=admin --new-password=********;
sudo gvm-start
```



```
┌──(root㉿kali)-[/home/kali]
└─# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Wed 2024-01-03 13:16:32 EST; 22ms ago
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 213495 (gsad)
      Tasks: 3 (limit: 9308)
     Memory: 5.0M
        CPU: 24ms
     CGroup: /system.slice/gsad.service
             ├─213495 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
             └─213497 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Jan 03 13:16:32 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Jan 03 13:16:32 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: active (running) since Wed 2024-01-03 13:16:27 EST; 5s ago
       Docs: man:gvmd(8)
    Process: 213374 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
   Main PID: 213375 (gvmd)
      Tasks: 1 (limit: 9308)
     Memory: 188.5M
        CPU: 5.462s
     CGroup: /system.slice/gvmd.service
             └─213375 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Jan 03 13:16:21 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Jan 03 13:16:21 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Jan 03 13:16:27 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
     Active: active (running) since Wed 2024-01-03 13:16:21 EST; 11s ago
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 213347 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)
   Main PID: 213354 (ospd-openvas)
      Tasks: 5 (limit: 9308)
     Memory: 71.4M
        CPU: 1.452s
     CGroup: /system.slice/ospd-openvas.service
             ├─213354 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
             └─213366 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf

Jan 03 13:16:20 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)...
Jan 03 13:16:21 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).

[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

┌──(root㉿kali)-[/home/kali]
└─# 
```

Fig. 5 GVM initiated(Kali)

you can also use the server's loopback IP, 127.0.0.1, in place of localhost. Launch a web browser and go to https://localhost:9392

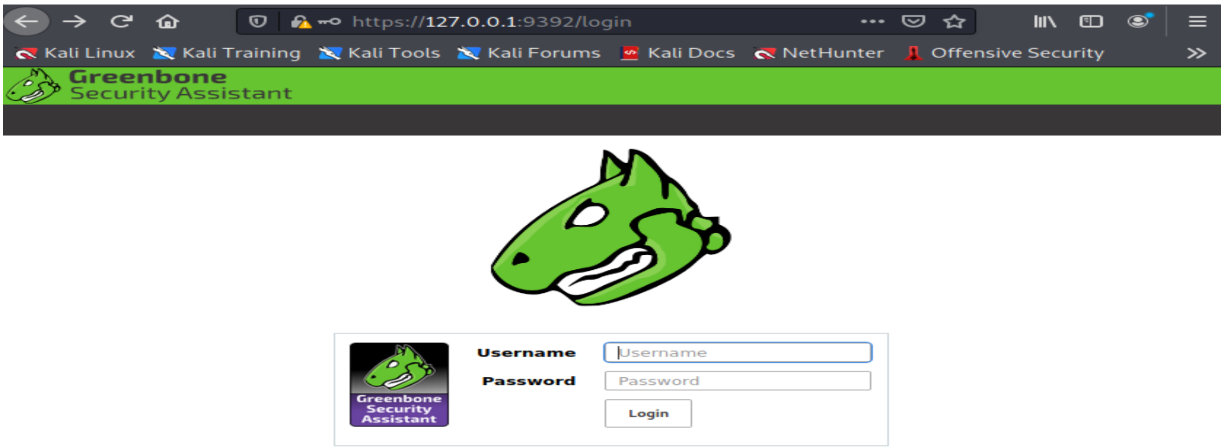


Fig. 6 OpenVAS(Login)

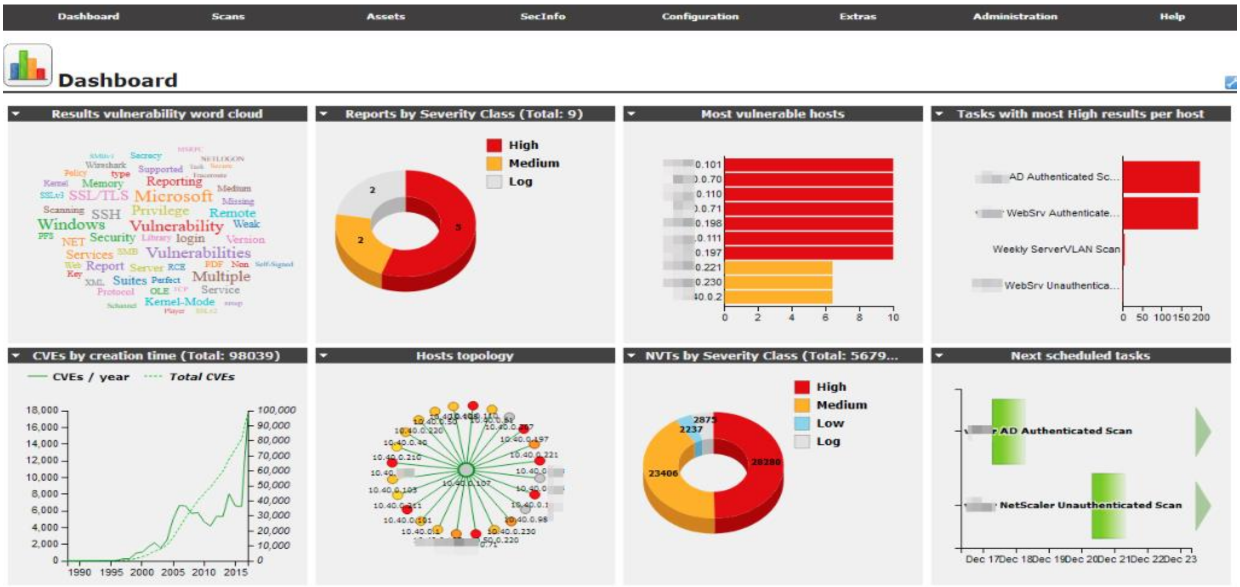
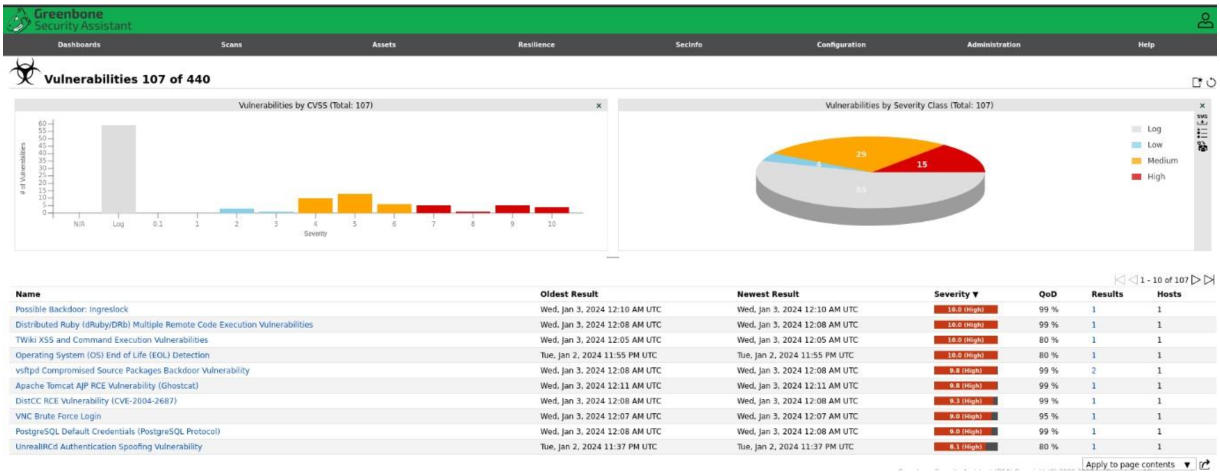


Fig. 7 OpenVAS Dashboard



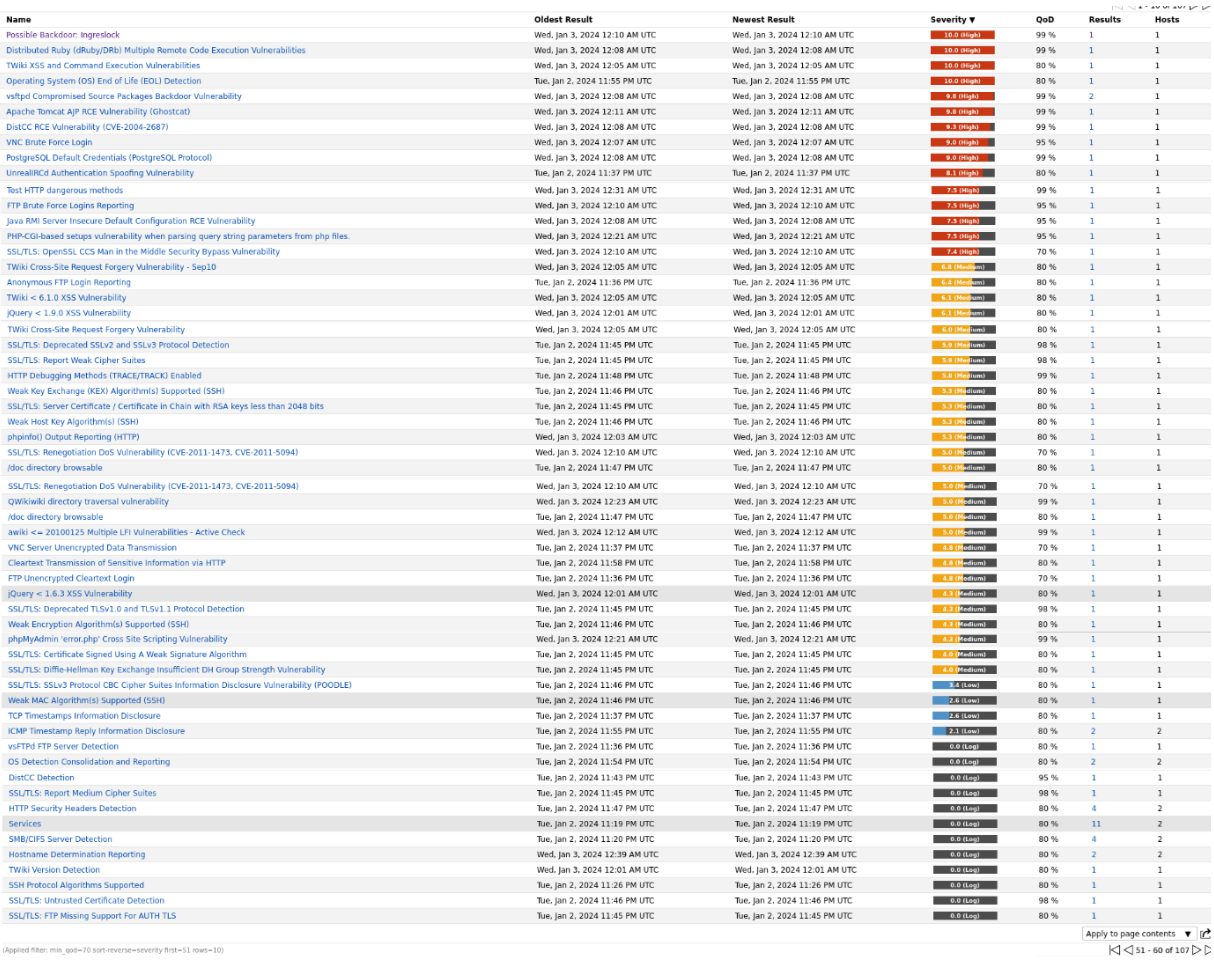
Vulnerabilities 107 of 440

Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
Possible Backdoor: Ingreslock	Wed, Jan 3, 2024 12:10 AM UTC	Wed, Jan 3, 2024 12:10 AM UTC	10.0 (High)	99 %	1	1
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	10.0 (High)	99 %	1	1
TWiki XSS and Command Execution Vulnerabilities	Wed, Jan 3, 2024 12:05 AM UTC	Wed, Jan 3, 2024 12:05 AM UTC	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	Tue, Jan 2, 2024 11:55 PM UTC	Tue, Jan 2, 2024 11:55 PM UTC	10.0 (High)	80 %	1	1
vsftpd Compromised Source Packages Backdoor Vulnerability	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	9.8 (High)	99 %	2	1
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	Wed, Jan 3, 2024 12:11 AM UTC	Wed, Jan 3, 2024 12:11 AM UTC	9.8 (High)	99 %	1	1
DistCC RCE Vulnerability (CVE-2004-2687)	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	9.3 (High)	99 %	1	1
VNC Brute Force Login	Wed, Jan 3, 2024 12:07 AM UTC	Wed, Jan 3, 2024 12:07 AM UTC	9.0 (High)	95 %	1	1
PostgreSQL Default Credentials (PostgreSQL Protocol)	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	9.0 (High)	99 %	1	1
UnrealIRCd Authentication Spoofing Vulnerability	Tue, Jan 2, 2024 11:37 PM UTC	Tue, Jan 2, 2024 11:37 PM UTC	8.1 (High)	80 %	1	1

Fig. 8 Vulnerable Hosts

After the two assigned hosts underwent a thorough vulnerability evaluation using OpenVAS, numerous security flaws were discovered in both systems. Notable is the Metasploit virtual machine, which became the center of increased vulnerability prevalence, highlighting how important this system vulnerability scan test is. The long list of vulnerabilities that have been found, along with the severity levels that correspond to them, is listed below. In addition to highlighting the complex nuances of the security environment, this painstaking analysis also highlights important issues that require careful consideration and corrective action as part of system defense and risk reduction

This thorough inventory not only offers a comprehensive view of the systems' security environment, but it also acts as a key source for determining the order in which to prioritize correction activities and strengthen the security posture as a whole. The inventory of all discovered vulnerabilities for both systems is provided below, arranged according to OpenVAS's severity ratings. This exhaustive inventory captures the wide range of possible dangers that were found during the vulnerability assessment.



1 - 10 of 107

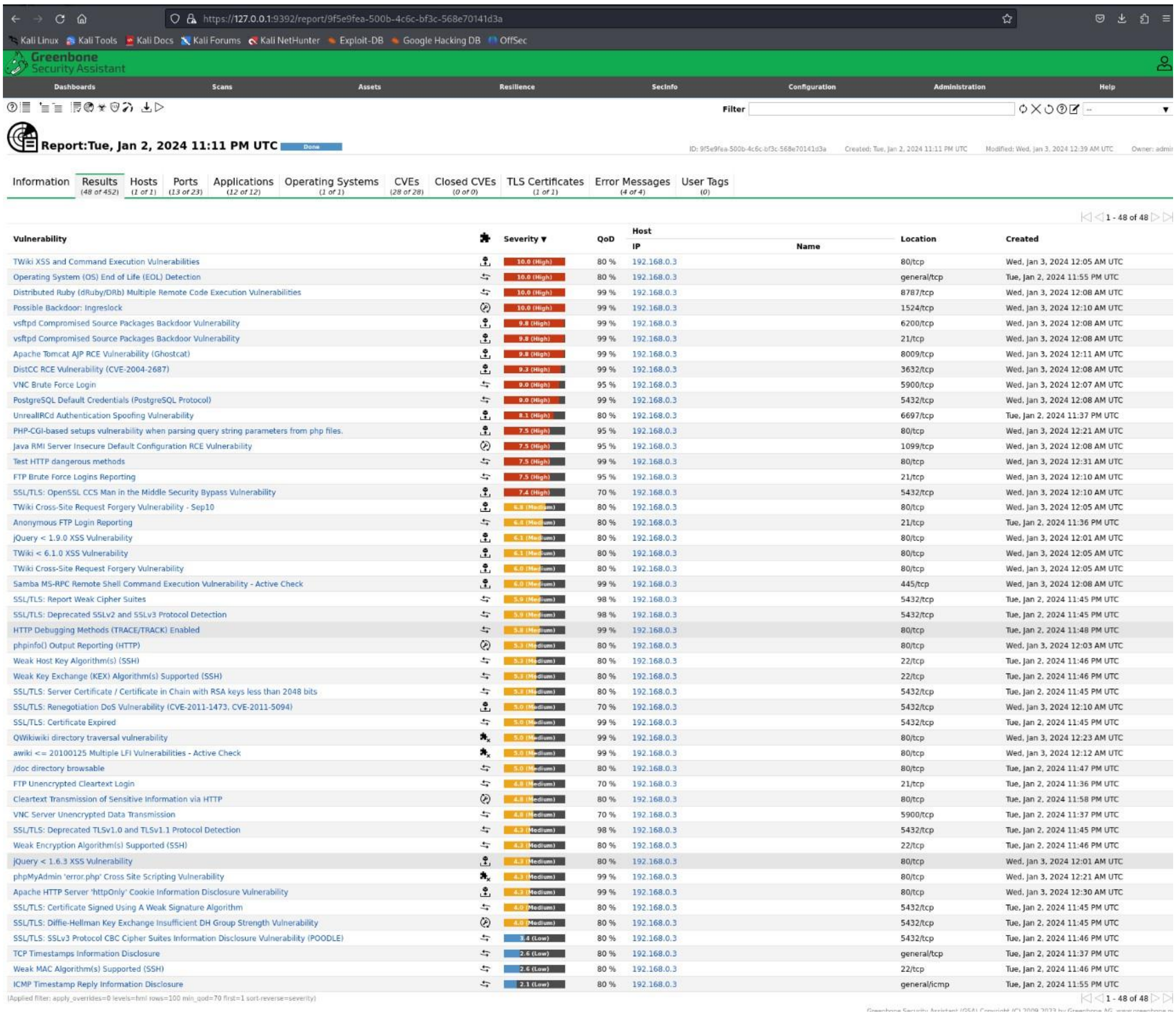
Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
Possible Backdoor: Ingreslock	Wed, Jan 3, 2024 12:10 AM UTC	Wed, Jan 3, 2024 12:10 AM UTC	10.0 (High)	99 %	1	1
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	10.0 (High)	99 %	1	1
TWiki XSS and Command Execution Vulnerabilities	Wed, Jan 3, 2024 12:05 AM UTC	Wed, Jan 3, 2024 12:05 AM UTC	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	Tue, Jan 2, 2024 11:55 PM UTC	Tue, Jan 2, 2024 11:55 PM UTC	10.0 (High)	80 %	1	1
vsftpd Compromised Source Packages Backdoor Vulnerability	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	9.8 (High)	99 %	2	1
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	Wed, Jan 3, 2024 12:11 AM UTC	Wed, Jan 3, 2024 12:11 AM UTC	9.8 (High)	99 %	1	1
DistCC RCE Vulnerability (CVE-2004-2687)	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	9.3 (High)	99 %	1	1
VNC Brute Force Login	Wed, Jan 3, 2024 12:07 AM UTC	Wed, Jan 3, 2024 12:07 AM UTC	9.0 (High)	95 %	1	1
PostgreSQL Default Credentials (PostgreSQL Protocol)	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	9.0 (High)	99 %	1	1
UnrealIRCd Authentication Spoofing Vulnerability	Tue, Jan 2, 2024 11:37 PM UTC	Tue, Jan 2, 2024 11:37 PM UTC	8.1 (High)	80 %	1	1
Test HTTP dangerous methods	Wed, Jan 3, 2024 12:31 AM UTC	Wed, Jan 3, 2024 12:31 AM UTC	7.5 (High)	99 %	1	1
FTP Brute Force Logins Reporting	Wed, Jan 3, 2024 12:10 AM UTC	Wed, Jan 3, 2024 12:10 AM UTC	7.5 (High)	95 %	1	1
Java RMI Server Insecure Default Configuration RCE Vulnerability	Wed, Jan 3, 2024 12:08 AM UTC	Wed, Jan 3, 2024 12:08 AM UTC	7.5 (High)	95 %	1	1
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	Wed, Jan 3, 2024 12:21 AM UTC	Wed, Jan 3, 2024 12:21 AM UTC	7.5 (High)	95 %	1	1
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	Wed, Jan 3, 2024 12:10 AM UTC	Wed, Jan 3, 2024 12:10 AM UTC	7.4 (High)	70 %	1	1
TWiki Cross-Site Request Forgery Vulnerability - Sep10	Wed, Jan 3, 2024 12:05 AM UTC	Wed, Jan 3, 2024 12:05 AM UTC	6.8 (Medium)	80 %	1	1
Anonymous FTP Login Reporting	Tue, Jan 2, 2024 11:36 PM UTC	Tue, Jan 2, 2024 11:36 PM UTC	6.4 (Medium)	80 %	1	1
TWiki < 6.1.0 XSS Vulnerability	Wed, Jan 3, 2024 12:05 AM UTC	Wed, Jan 3, 2024 12:05 AM UTC	6.1 (Medium)	80 %	1	1
jQuery < 1.9.0 XSS Vulnerability	Wed, Jan 3, 2024 12:01 AM UTC	Wed, Jan 3, 2024 12:01 AM UTC	6.1 (Medium)	80 %	1	1
TWiki Cross-Site Request Forgery Vulnerability	Wed, Jan 3, 2024 12:05 AM UTC	Wed, Jan 3, 2024 12:05 AM UTC	6.0 (Medium)	80 %	1	1
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	5.9 (Medium)	98 %	1	1
SSL/TLS: Report Weak Cipher Suites	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	5.9 (Medium)	98 %	1	1
HTTP Debugging Methods (TRACE/TRACK) Enabled	Tue, Jan 2, 2024 11:48 PM UTC	Tue, Jan 2, 2024 11:48 PM UTC	5.8 (Medium)	99 %	1	1
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	Tue, Jan 2, 2024 11:46 PM UTC	Tue, Jan 2, 2024 11:46 PM UTC	5.3 (Medium)	80 %	1	1
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	5.3 (Medium)	80 %	1	1
Weak Host Key Algorithm(s) (SSH)	Tue, Jan 2, 2024 11:46 PM UTC	Tue, Jan 2, 2024 11:46 PM UTC	5.3 (Medium)	80 %	1	1
phpinfo() Output Reporting (HTTP)	Wed, Jan 3, 2024 12:03 AM UTC	Wed, Jan 3, 2024 12:03 AM UTC	5.3 (Medium)	80 %	1	1
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	Wed, Jan 3, 2024 12:10 AM UTC	Wed, Jan 3, 2024 12:10 AM UTC	5.0 (Medium)	70 %	1	1
/doc directory browsable	Tue, Jan 2, 2024 11:47 PM UTC	Tue, Jan 2, 2024 11:47 PM UTC	5.0 (Medium)	80 %	1	1
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	Wed, Jan 3, 2024 12:10 AM UTC	Wed, Jan 3, 2024 12:10 AM UTC	5.0 (Medium)	70 %	1	1
QWikiwiki directory traversal vulnerability	Wed, Jan 3, 2024 12:23 AM UTC	Wed, Jan 3, 2024 12:23 AM UTC	5.0 (Medium)	99 %	1	1
/doc directory browsable	Tue, Jan 2, 2024 11:47 PM UTC	Tue, Jan 2, 2024 11:47 PM UTC	5.0 (Medium)	80 %	1	1
awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check	Wed, Jan 3, 2024 12:12 AM UTC	Wed, Jan 3, 2024 12:12 AM UTC	5.0 (Medium)	99 %	1	1
VNC Server Unencrypted Data Transmission	Tue, Jan 2, 2024 11:37 PM UTC	Tue, Jan 2, 2024 11:37 PM UTC	4.8 (Medium)	70 %	1	1
Cleartext Transmission of Sensitive Information via HTTP	Tue, Jan 2, 2024 11:58 PM UTC	Tue, Jan 2, 2024 11:58 PM UTC	4.8 (Medium)	80 %	1	1
FTP Unencrypted Cleartext Login	Tue, Jan 2, 2024 11:36 PM UTC	Tue, Jan 2, 2024 11:36 PM UTC	4.8 (Medium)	70 %	1	1
jQuery < 1.6.3 XSS Vulnerability	Wed, Jan 3, 2024 12:01 AM UTC	Wed, Jan 3, 2024 12:01 AM UTC	4.3 (Medium)	80 %	1	1
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	4.3 (Medium)	98 %	1	1
Weak Encryption Algorithm(s) Supported (SSH)	Tue, Jan 2, 2024 11:46 PM UTC	Tue, Jan 2, 2024 11:46 PM UTC	4.3 (Medium)	80 %	1	1
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	Wed, Jan 3, 2024 12:21 AM UTC	Wed, Jan 3, 2024 12:21 AM UTC	4.3 (Medium)	99 %	1	1
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	4.0 (Medium)	80 %	1	1
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	4.0 (Medium)	80 %	1	1
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	Tue, Jan 2, 2024 11:46 PM UTC	Tue, Jan 2, 2024 11:46 PM UTC	3.4 (Low)	80 %	1	1
Weak MAC Algorithm(s) Supported (SSH)	Tue, Jan 2, 2024 11:46 PM UTC	Tue, Jan 2, 2024 11:46 PM UTC	2.6 (Low)	80 %	1	1
TCP Timestamps Information Disclosure	Tue, Jan 2, 2024 11:37 PM UTC	Tue, Jan 2, 2024 11:37 PM UTC	2.6 (Low)	80 %	1	1
ICMP Timestamp Reply Information Disclosure	Tue, Jan 2, 2024 11:55 PM UTC	Tue, Jan 2, 2024 11:55 PM UTC	2.1 (Low)	80 %	2	2
vsFTPd FTP Server Detection	Tue, Jan 2, 2024 11:36 PM UTC	Tue, Jan 2, 2024 11:36 PM UTC	0.0 (Log)	80 %	1	1
OS Detection Consolidation and Reporting	Tue, Jan 2, 2024 11:54 PM UTC	Tue, Jan 2, 2024 11:54 PM UTC	0.0 (Log)	80 %	2	2
DistCC Detection	Tue, Jan 2, 2024 11:43 PM UTC	Tue, Jan 2, 2024 11:43 PM UTC	0.0 (Log)	95 %	1	1
SSL/TLS: Report Medium Cipher Suites	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	0.0 (Log)	98 %	1	1
HTTP Security Headers Detection	Tue, Jan 2, 2024 11:47 PM UTC	Tue, Jan 2, 2024 11:47 PM UTC	0.0 (Log)	80 %	4	2
Services	Tue, Jan 2, 2024 11:19 PM UTC	Tue, Jan 2, 2024 11:19 PM UTC	0.0 (Log)	80 %	11	2
SMB/CIFS Server Detection	Tue, Jan 2, 2024 11:20 PM UTC	Tue, Jan 2, 2024 11:20 PM UTC	0.0 (Log)	80 %	4	2
Hostname Determination Reporting	Wed, Jan 3, 2024 12:39 AM UTC	Wed, Jan 3, 2024 12:39 AM UTC	0.0 (Log)	80 %	2	2
TWiki Version Detection	Wed, Jan 3, 2024 12:01 AM UTC	Wed, Jan 3, 2024 12:01 AM UTC	0.0 (Log)	80 %	1	1
SSH Protocol Algorithms Supported	Tue, Jan 2, 2024 11:26 PM UTC	Tue, Jan 2, 2024 11:26 PM UTC	0.0 (Log)	80 %	1	1
SSL/TLS: Untrusted Certificate Detection	Tue, Jan 2, 2024 11:46 PM UTC	Tue, Jan 2, 2024 11:46 PM UTC	0.0 (Log)	98 %	1	1
SSL/TLS: FTP Missing Support For AUTH TLS	Tue, Jan 2, 2024 11:45 PM UTC	Tue, Jan 2, 2024 11:45 PM UTC	0.0 (Log)	80 %	1	1

(Applied filter: min_qod=70 sort-reverse=severity first=51 rows=10)

Fig. 9 Vulnerabilities total List

2.1 Metasploit VM Vulnerabilities

Many dangers are present in the system, according to the vulnerability scan that was done on the hosts. According to OpenVAS's classification, 16 of these have been categorized as severe vulnerabilities, 40 as medium-level vulnerabilities, and 4 as low severity vulnerabilities. This thorough examination highlights the variety and seriousness of the vulnerabilities found, requiring a planned and organized approach to remedial activities.



Report:Tue, Jan 2, 2024 11:11 PM UTC

ID: 9f5e9fea-500b-4c6c-bf3c-568e70141d3a Created: Tue, Jan 2, 2024 11:11 PM UTC Modified: Wed, Jan 3, 2024 12:39 AM UTC Owner: admin

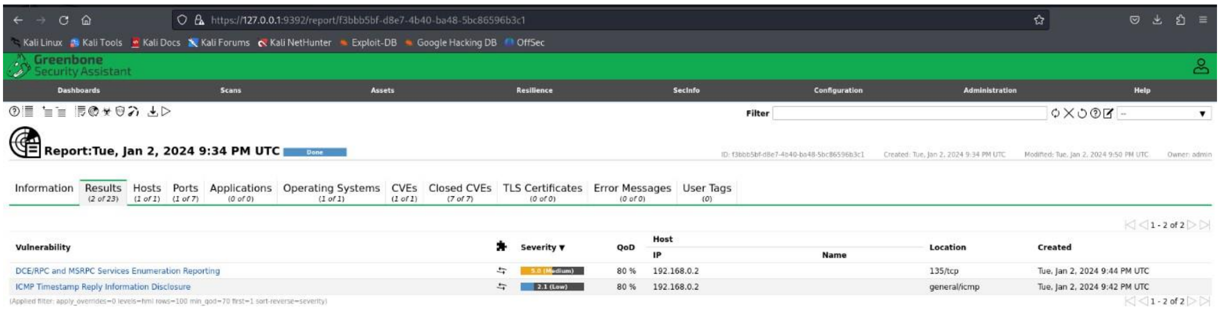
Vulnerability	Severity ▼	QoD	Host		Location	Created
			IP	Name		
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:05 AM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.0.3		general/tcp	Tue, Jan 2, 2024 11:55 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.0.3		8787/tcp	Wed, Jan 3, 2024 12:08 AM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.0.3		1524/tcp	Wed, Jan 3, 2024 12:10 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	9.8 (High)	99 %	192.168.0.3		6200/tcp	Wed, Jan 3, 2024 12:08 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	9.8 (High)	99 %	192.168.0.3		21/tcp	Wed, Jan 3, 2024 12:08 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	192.168.0.3		8009/tcp	Wed, Jan 3, 2024 12:11 AM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	9.3 (High)	99 %	192.168.0.3		3632/tcp	Wed, Jan 3, 2024 12:08 AM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.0.3		5900/tcp	Wed, Jan 3, 2024 12:07 AM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	9.0 (High)	99 %	192.168.0.3		5432/tcp	Wed, Jan 3, 2024 12:08 AM UTC
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.0.3		6697/tcp	Tue, Jan 2, 2024 11:37 PM UTC
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:21 AM UTC
Java RMI Server Insecure Default Configuration RCE Vulnerability	7.5 (High)	95 %	192.168.0.3		1099/tcp	Wed, Jan 3, 2024 12:08 AM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:31 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.0.3		21/tcp	Wed, Jan 3, 2024 12:10 AM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	7.4 (High)	70 %	192.168.0.3		5432/tcp	Wed, Jan 3, 2024 12:10 AM UTC
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:05 AM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.0.3		21/tcp	Tue, Jan 2, 2024 11:36 PM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:01 AM UTC
TWiki < 6.1.0 XSS Vulnerability	6.1 (Medium)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:05 AM UTC
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:05 AM UTC
Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	6.0 (Medium)	99 %	192.168.0.3		445/tcp	Wed, Jan 3, 2024 12:08 AM UTC
SSL/TLS: Report Weak Cipher Suites	5.9 (Medium)	98 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	192.168.0.3		80/tcp	Tue, Jan 2, 2024 11:48 PM UTC
phpinfo() Output Reporting (HTTP)	5.3 (Medium)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:03 AM UTC
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	192.168.0.3		22/tcp	Tue, Jan 2, 2024 11:46 PM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	192.168.0.3		22/tcp	Tue, Jan 2, 2024 11:46 PM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	192.168.0.3		5432/tcp	Wed, Jan 3, 2024 12:10 AM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
QWikiwiki directory traversal vulnerability	5.0 (Medium)	99 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:23 AM UTC
awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check	5.0 (Medium)	99 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:12 AM UTC
/doc directory browsable	5.0 (Medium)	80 %	192.168.0.3		80/tcp	Tue, Jan 2, 2024 11:47 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.0.3		21/tcp	Tue, Jan 2, 2024 11:36 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.0.3		80/tcp	Tue, Jan 2, 2024 11:58 PM UTC
VNC Server Unencrypted Data Transmission	4.8 (Medium)	70 %	192.168.0.3		5900/tcp	Tue, Jan 2, 2024 11:37 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	80 %	192.168.0.3		22/tcp	Tue, Jan 2, 2024 11:46 PM UTC
jQuery < 1.6.3 XSS Vulnerability	4.3 (Medium)	80 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:01 AM UTC
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	4.3 (Medium)	99 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:21 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99 %	192.168.0.3		80/tcp	Wed, Jan 3, 2024 12:30 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:45 PM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4 (Low)	80 %	192.168.0.3		5432/tcp	Tue, Jan 2, 2024 11:46 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	192.168.0.3		general/tcp	Tue, Jan 2, 2024 11:37 PM UTC
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %	192.168.0.3		22/tcp	Tue, Jan 2, 2024 11:46 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.0.3		general/icmp	Tue, Jan 2, 2024 11:55 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.n

Fig. 10 Vulnerabilities List on Metasploit.

2.2 Windows VM Vulnerabilities



https://127.0.0.1:9392/report/f3bbb5bf-d8e7-4b40-ba48-5bc86596b3c1

Report:Tue, Jan 2, 2024 9:34 PM UTC Done

ID: f3bbb5bf-d8e7-4b40-ba48-5bc86596b3c1 Created: Tue, Jan 2, 2024 9:34 PM UTC Modified: Tue, Jan 2, 2024 9:50 PM UTC Owner: admin

Information | Results (2 of 23) | Hosts (1 of 1) | Ports (1 of 7) | Applications (0 of 0) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (7 of 7) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 2 of 2

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	192.168.0.2		135/tcp	Tue, Jan 2, 2024 9:44 PM UTC
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)	80 %	192.168.0.2		general/icmp	Tue, Jan 2, 2024 9:42 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 2 of 2

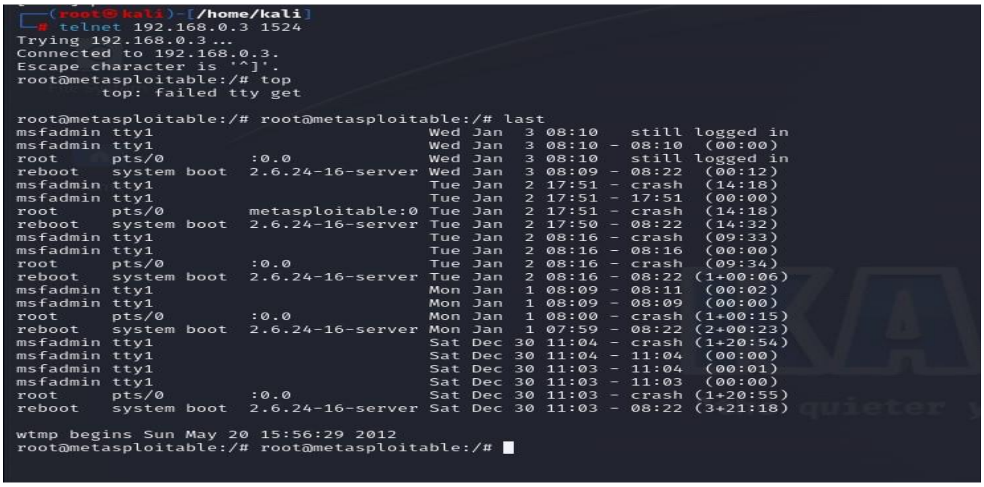
Fig 11 Windows System Vulnerabilities

A few dangers within the system have been found by the hosts' vulnerability assessment. One vulnerability among these has been assessed by OpenVAS as medium-level, and another as low severity. This comprehensive assessment highlights the range and severity of the vulnerabilities found, underscoring the necessity of a planned and methodical approach to resolving these problems.

Tools	Parameter	Hosts	Comments
OpenVAS	Full Scan	192.168.0.2	Only medium level vulnerabilities found
OpenVAS	Full Scan	192.168.0.3	Multiple severe level vulnerabilities found

3 Scanning Results

3.1 Possible Backdoor: Ingreslock



```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.0.3 1524
Trying 192.168.0.3 ...
Connected to 192.168.0.3.
Escape character is '^]'.
root@metasploitable:/# top
        top: failed tty get

root@metasploitable:/# root@metasploitable:/# last
msfadmin tty1                          Wed Jan  3 08:10   still logged in
msfadmin tty1                          Wed Jan  3 08:10 - 08:10  (00:00)
root     pts/0        :0.0             Wed Jan  3 08:10   still logged in
reboot   system boot  2.6.24-16-server Wed Jan  3 08:09 - 08:22  (00:12)
msfadmin tty1                          Tue Jan  2 17:51 - crash  (14:18)
msfadmin tty1                          Tue Jan  2 17:51 - 17:51  (00:00)
root     pts/0        metasploitable:0 Tue Jan  2 17:51 - crash  (14:18)
reboot   system boot  2.6.24-16-server Tue Jan  2 17:50 - 08:22  (14:32)
msfadmin tty1                          Tue Jan  2 08:16 - crash  (09:33)
msfadmin tty1                          Tue Jan  2 08:16 - 08:16  (00:00)
root     pts/0        :0.0             Tue Jan  2 08:16 - crash  (09:34)
reboot   system boot  2.6.24-16-server Tue Jan  2 08:16 - 08:22 (1+00:06)
msfadmin tty1                          Mon Jan  1 08:09 - 08:11  (00:02)
msfadmin tty1                          Mon Jan  1 08:09 - 08:09  (00:00)
root     pts/0        :0.0             Mon Jan  1 08:00 - crash (1+00:15)
reboot   system boot  2.6.24-16-server Mon Jan  1 07:59 - 08:22 (2+00:23)
msfadmin tty1                          Sat Dec 30 11:04 - crash (1+20:54)
msfadmin tty1                          Sat Dec 30 11:04 - 11:04  (00:00)
msfadmin tty1                          Sat Dec 30 11:03 - 11:04  (00:01)
msfadmin tty1                          Sat Dec 30 11:03 - 11:03  (00:00)
root     pts/0        :0.0             Sat Dec 30 11:03 - crash (1+20:55)
reboot   system boot  2.6.24-16-server Sat Dec 30 11:03 - 08:22 (3+21:18)

wtmp begins Sun May 20 15:56:29 2012
root@metasploitable:/# root@metasploitable:/# █
```

Fig. 12 Ingreslok Exploited.

The Ingreslock vulnerability is a potential security issue linked to the Ingreslock service, originally designed to secure parts of an Ingres database. However, when the database is not actively running, a vulnerability arises. Attackers can exploit an open port (usually port 1524) to gain unauthorized access. To do this, they manipulate a file called inetd.conf, inserting a line related to a backdoor shell script. Once this is done, connecting to the open port via Telnet provides unauthorized access, as shown in

Mitigating this vulnerability requires a few steps. First, inspect and remove the backdoor-related line from the inetd.conf file. Regularly check and control unnecessary services on the server, disabling those not actively needed. Ongoing vigilance involves continuously monitoring and inspecting system configurations, using robust tools to promptly identify and eliminate potential vulnerabilities.

In conclusion, organizations should prioritize understanding their system configurations, promptly addressing vulnerabilities, and conducting regular security audits. Continuous monitoring, following the principle of least privilege, and employee training on security best practices contribute to a stronger defense against potential threats. The Ingreslock vulnerability highlights the need for a collaborative effort in addressing cybersecurity challenges, combining technical solutions with a security-conscious organizational culture. Through these efforts, organizations can fortify their defenses and proactively protect against security breache.

4 Conclusion

Conducted a comprehensive examination of SOA Enterprises, Inc.'s security involved testing the network using the Metasploitable VM. The process included the identification of vulnerabilities, their exploitation, and the proposal of potential fixes.

Issues were identified on two virtual machines, one running Metasploitable and the other hosting an intentionally insecure web app on a Windows 10 system. Notably, the Ingreslock vulnerability raised concerns as it could serve as an entry point for attackers.

The focus was on exploiting the Ingreslock problem on the Metasploitable VM, accomplished straightforwardly through a Telnet connection, emphasizing the immediate need for fixes.

Solutions were explored, emphasizing the removal of the identified backdoor and the monitoring of unnecessary services. Recommendations were provided to enhance overall security following industry best practices.

Throughout the testing process, adherence to ethical guidelines was maintained, with explicit permission obtained from SOA Enterprises, Inc. This approach ensured a responsible and careful evaluation, documented comprehensively for the organization to address vulnerabilities.

The test results offer crucial insights into risks and vulnerabilities in the organization's network. The organization is encouraged to utilize this information to enhance security, addressing potential threats proactively. In summary, the penetration testing successfully identified vulnerabilities, explained potential exploits, and offered practical recommendations. The ethical and authorized approach ensures meaningful contributions to the resilience of SOA Enterprises, Inc.'s IT infrastructure.

5 References

1. Ingreslock vulnerability on the Metasploitable. https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
2. Service Management. https://www.atlassian.com/software/jira/service-management
3. Open port scanning. https://www.beyondtrust.com/blog/entry/what-is-an-open-port-what-are-the-security-implications
4. Nmap user guide. https://nmap.org/docs.html
5. OpenVAS Community forum. https://greenbone.github.io/docs/latest/22.4/source-build/troubleshooting.html#failed-to-find-config
6. Kali Linux Images. https://www.kali.org/get-kali/#kali-virtual-machines
7. Metasploitable image. https://docs.rapid7.com/metasploit/metasploitable-2/
8. Virtual Box Installation. https://www.virtualbox.org/wiki/Downloads
9. Vulnerability mitigation. https://hackertarget.com/sample-vulnerability-report/openvas-report-metasploitable.html
10. Ingreslock vulnerability on the Metasploitable https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

11. Service Management https://www.atlassian.com/software/jira/service-management

12. Open port scanning https://www.beyondtrust.com/blog/entry/what-is-an-open-port-what-are-the-security-implications