



Security Operations and Assurance Assignment

Vulnerability Assessment of SOA Enterprises, Inc.

NAME: Vahin Valliyur Sankar

STUDENT ID: 32121535

LECTURER: Alireza Esfahani

DATE: 30.12.2023

Table of Contents

Introduction:	2
Significance:.....	2
Objective:	2
Expected Outcomes:	3
Network set up for 'SOA Enterprises, Inc.:.....	3
Executive Summary of Results:.....	7
Vulnerability Assessment:	7
1. Scanning Metasploitable with Nmap:	7
Vulnerabilities Detected	8
Recommendations:	10
2. Scanning Windows 11 + WebGoat with Nmap:.....	10
Vulnerabilities Detected:	11
Recommendations:	12
Conclusion:	12
Reference list:.....	14

Introduction:

Penetration testing is an element of security assessments (such as audits) or certification processes (such as common criteria), with the aim of identifying and removing security flaws that an attacker could use to obtain access to the security target (system, device, or module). An attacker's goal in this situation is to breach or get around the security target's defences to access it. Put differently, the goal of a penetration tester is to find every vulnerability, whereas an attacker only needs to find one to successfully breach the security target (Caddy, 2006). The primary goal of penetration testing is to pinpoint vulnerabilities, analyse the potential threats connected with these weaknesses, and also offer recommendations for enhancing the general security of the organisation.

Significance:

Risk Mitigation: Identifies and mitigates potential security risks before malicious actors can exploit them.

Compliance: Assists in conference regulative and observance requirements by making certain of the implementation of adequate safety and security management.

Security Improvement: Provides insights, into vulnerabilities enabling companies to enhance their surveillance measures and protocols.

Incident Response Preparedness: Help businesses in getting ready for and attending to safety and security violations through understanding possible techniques of attack.

Objective:

The key objectives of the penetration testing work for SOA Enterprises, Inc. are diverse. The first objective is to completely explore vulnerabilities within the business's network facilities, focusing on two virtual machines (VM) targets-- a Metasploitable VM and a Windows 11 VM including an intentionally insecure web application. These targeted analyses help to recognize and identify possible weak points that may be made use of by an attacker.

To execute these tests, the job will certainly utilize the Kali Linux virtual machine, guaranteeing appropriate authorization from SOA Enterprises, Inc. to carry out penetration test activities. Making Use of the Kali Linux environment provides a specialized system outfitted with necessary resources for efficient safety and security screening.

The evaluation of penetration testing entails an extensive analysis, which includes uncovering hosts, scanning ports, and infiltrating vulnerabilities. Nmap will be utilized to clearly examine the network, identify available ports, and assess the degree of protection posed by the targeted digital types of equipment. This methodical technique is crucial for uncovering possible entrance points and vulnerabilities in the organization's electronic facilities.

Expected Outcomes:

- Identification of vulnerabilities on targeted VMs.
- Implementation of incident response strategies.
- Enhancement of penetration testing skills through practical application.

This penetration test intends to enhance proficiency in security operations and assurance, adding to the overall durability and preparedness of SOA Enterprises, Inc. against potential cybersecurity threats.

Network set up for 'SOA Enterprises, Inc.:

Device	IP Address	Subnet Mask
Kali Linux	192.168.64.3	255.255.255.0
Windows 11 + WebGoat	192.168.64.4	255.255.255.0
Metasploitable	192.168.64.5	255.255.255.0

Table 1: Network set-up

UTM is used in this demonstration by utilizing Apple's Hypervisor virtualization framework, enabling the operation of ARM64 operating systems on Apple Silicon devices at near-native speeds. On Intel-based Macs, UTM supports the virtualization of x86/x64 operating systems. Additionally, UTM offers lower-performance emulation options, allowing for the execution of x86/x64 on Apple Silicon and ARM64 on Intel platforms. For developers and enthusiasts, UTM supports emulation for various other processors, including ARM32, MIPS, PPC, and RISC-V, thereby providing extensive flexibility in virtualization capabilities (osy, 2020).

As illustrated in Table 1, all VMs are configured within the same network environment. Within the UTM settings, the network adapter is configured to utilize a shared network configuration, as depicted in Figures 1, 2, and 3. Subsequently, Figures 4, 5, and 6 display the respective IP addresses assigned to each VM. In this configuration, shared network traffic is routed directly by the host operating system, enabling the guest VMs to share a VLAN with the host. As a result, services running on both the guest and host systems can interact without requiring additional configuration. This shared network configuration is particularly recommended for new virtual machines, as it simplifies network setup and enhances compatibility.

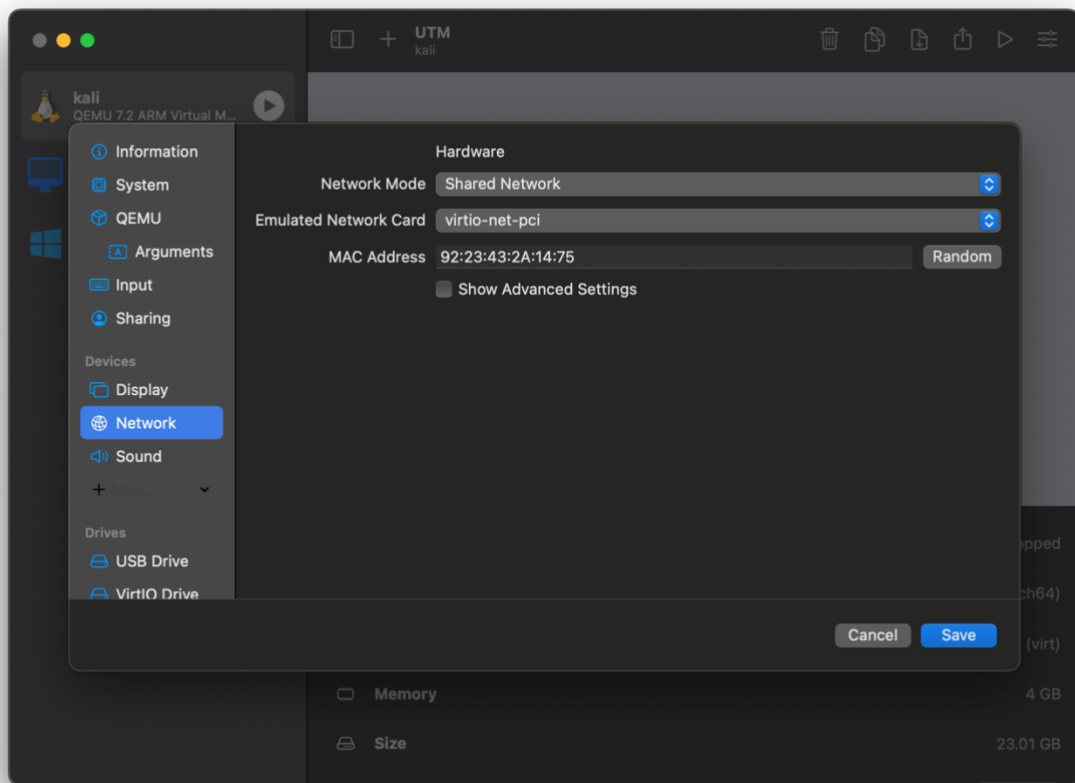


Figure 1: Network settings of Kali Linux

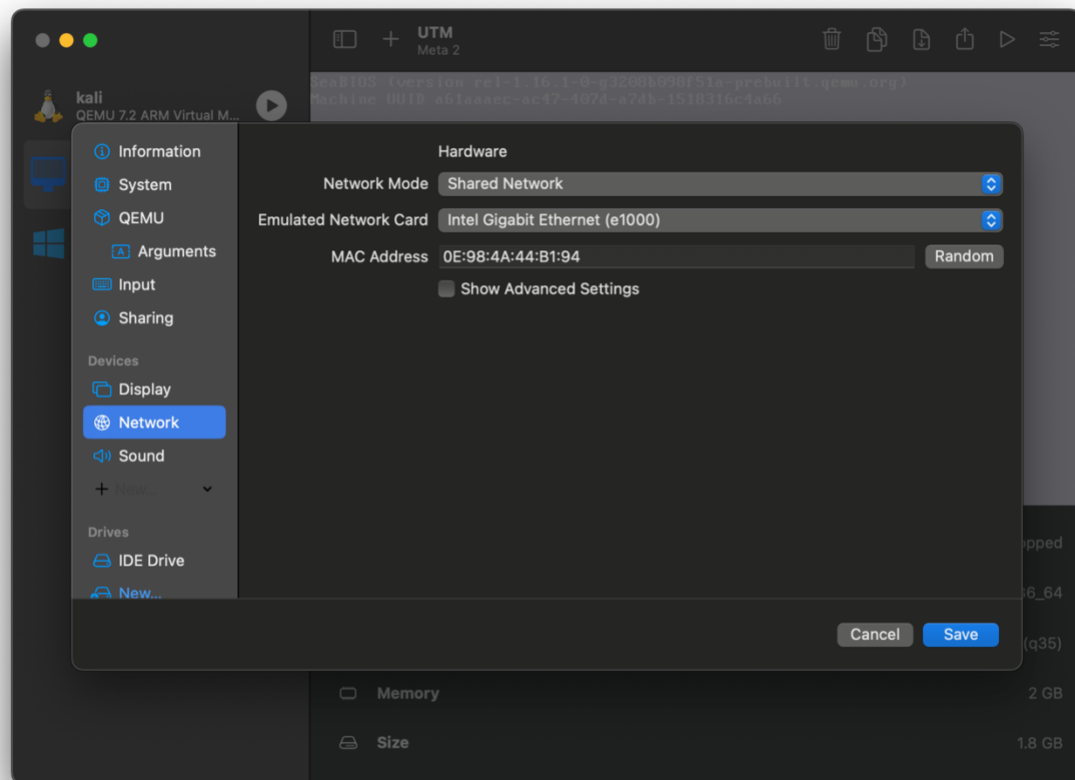


Figure 2: Network settings of Metasploitable

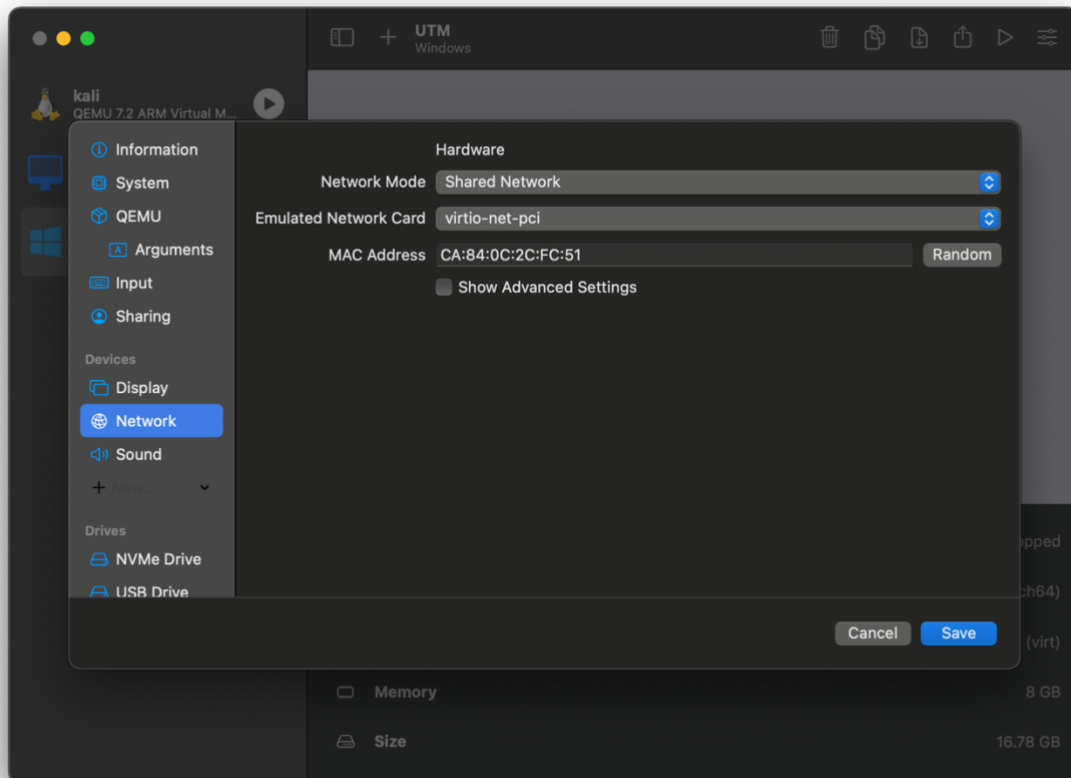


Figure 3: Network settings of Windows 11 + WebGoat

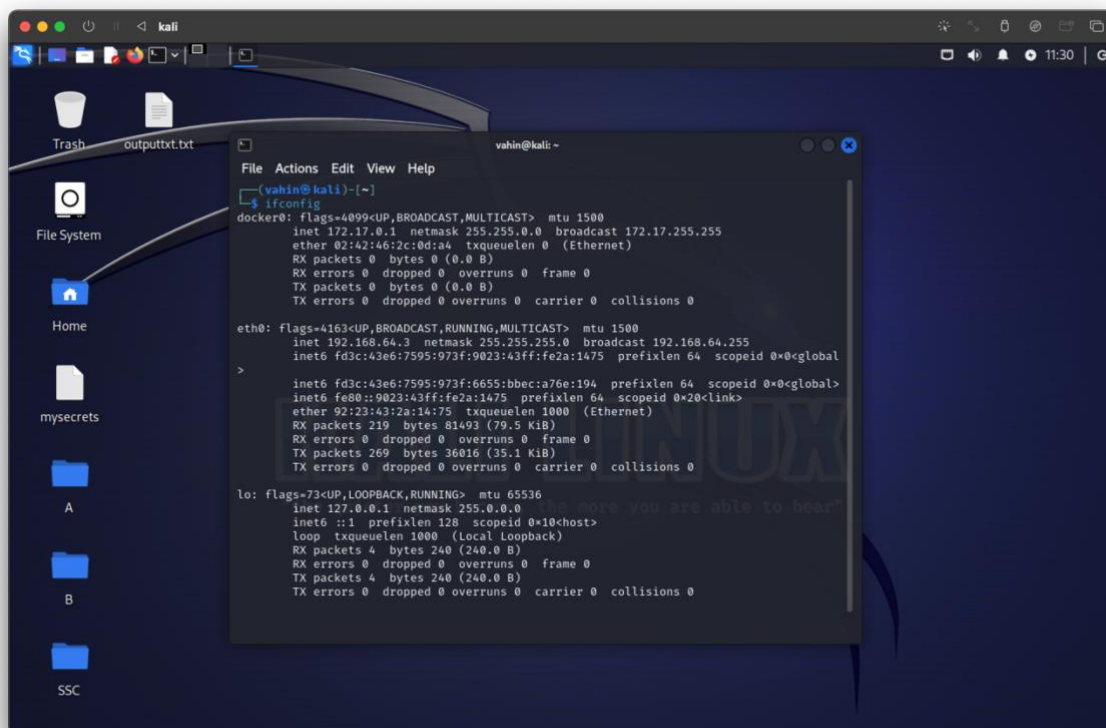


Figure 4: IP address of Kali Liniux

```
Meta 2
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0e:98:4a:44:b1:94
          inet addr:192.168.64.5  Bcast:192.168.64.255  Mask:255.255.255.0
          inet6 addr: fd3c:43e6:7595:973f:c98:4aff:fe44:b194/64 Scope:Global
          inet6 addr: fe80::c98:4aff:fe44:b194/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4448 (4.3 KB)  TX bytes:6923 (6.7 KB)
          Base address:0xc000 Memory:febc0000-febe0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Figure 5: IP address of Metasploitable

```
Windows
Command Prompt
Microsoft Windows [Version 10.0.25997.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vahin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : Home
    IPv6 Address. . . . . : fd3c:43e6:7595:973f:4691:5655:859e:375c
    Temporary IPv6 Address. . . . . : fd3c:43e6:7595:973f:2513:6b59:d39:ab22
    Link-local IPv6 Address . . . . . : fe80::3914:5239:2515:fb72%7
    IPv4 Address. . . . . : 192.168.64.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c435:d9ff:fe19:a964%7
                                192.168.64.1

C:\Users\vahin>
```

Figure 6: IP address of Windows 11 + WebGoat

Executive Summary of Results:

To identify vulnerabilities, the Nmap tool is implemented—a versatile utility designed for scanning a range of IP addresses. It serves the dual purpose of identifying active systems, determining open ports on those systems, and identifying the respective operating systems in use. This multifaceted tool can be wielded defensively by network managers to pinpoint weaknesses that require correction. Conversely, it can be utilized offensively by attackers probing for vulnerabilities to exploit (Corcoran, 2001).

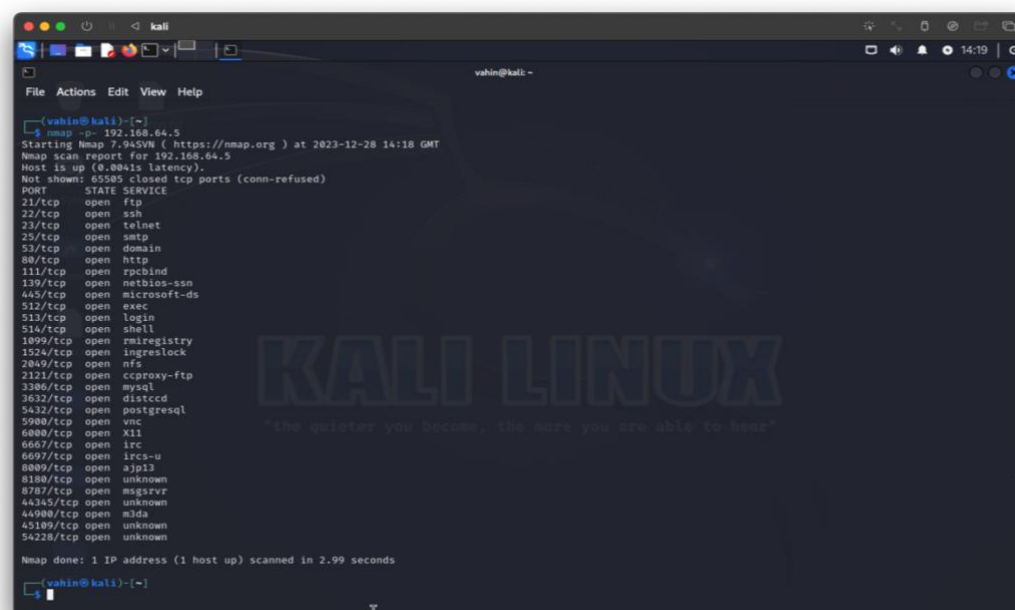
The targeted systems for this analysis include Windows machines running WebGoat—an intentionally insecure application designed for developers to test vulnerabilities commonly found in Java-based applications utilizing popular open-source components (OWASP, 2016). Additionally, the examination extends to Metasploitable, a deliberately vulnerable machine specifically created for learning and practicing Metasploit techniques. It's imperative to note that hacking or attacking any system without the owner's consent is illegal. However, the use of the Metasploitable machine provides users with a controlled environment for setting up a penetration testing scenario, allowing individuals to learn and practice ethical hacking (Simplilearn, 2021).

Vulnerability Assessment:

Tool	Parameters	Output
Nmap	nmap -p- 192.168.64.5	Figure 7
Nmap	nmap -p- 192.168.64.4	Figure 8

1. Scanning Metasploitable with Nmap:

Screenshot:



```
vahin@kali:~$ nmap -p- 192.168.64.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-28 14:18 GMT
Nmap scan report for 192.168.64.5
Host is up (0.0041s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6607/tcp  open  irc
6697/tcp  open  lrss-u
8009/tcp  open  ajp13
8100/tcp  open  unknown
8787/tcp  open  msgrvr
44345/tcp open  unknown
44980/tcp open  m3da
45109/tcp open  unknown
54228/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds
```

Figure 7: Nmap results of Metasploitable

Overview:

The Metasploitable VM, with IP address 192.168.64.5, was subjected to a comprehensive security assessment of SOA Enterprises using Nmap version 7.94SVN. The scan revealed several vulnerabilities across various services, ranging from outdated software versions to potential exploitation points.

Vulnerabilities Detected

1. Port 21/tcp (FTP):

Vulnerability: vsFTPD version 2.3.4 backdoor.

Exploitable: Yes

Explanation: VSFTPD (Very Secure FTP Daemon) is a prominent FTP web server program that enables documents transfers by means of the Documents Transfer Method (FTP) in between a client and a web server. Although VSFTPD is recognized for its security attributes, some vulnerabilities were discovered in version 2.3.4 of the software. These susceptibilities consist of buffer overflows, layout string weak points, and verification bypass concerns. attackers can make use of these susceptibilities to compromise the safety and security of the FTP web server. Among the most severe threats associated with the exploitation of VSFTPD 2.3.4 was the opportunity of remote code execution. This indicates that assailants could run destructive code on the server, leading to an overall system violation. The programmers of VSFTPD resolved these susceptibilities by releasing more recent variations of the software application with safety and security spots and solutions. Customers were strongly advised to update to the current variation to secure their servers from exploitation. (S3Curiosity, 2023)

2. Port 25/tcp (SMTP):

Vulnerability: SSL POODLE information leak.

Exploitable: Yes

Explanation: The POODLE susceptibility permits a cyberpunk to accessibility encrypted messages, possibly causing the burglary of delicate details such as session cookies or passwords. This can after that be made use of to pose the sufferer and gain control over online applications, especially if the assailant makes believe to be an administrator. The POODLE vulnerability affects cryptographic suites that utilize block cyphers and symmetric security, such as those using DES or AES formulas. In these cases, the client and web server establish a crooked file encryption secret (personal and public key) and utilize it for symmetrical file encryption of all communication. The data is encrypted in blocks of an established length, such as 8 or 16 bytes, utilizing block ciphers.

Making use of cipher-block chaining (CBC mode) is additionally found in cypher suites that can be manipulated by POODLE. This means that the value of each block is determined utilizing the XOR rational procedure, and each block's value depends on the one preceding it. In addition, an initialization vector, which is an arbitrary data block, is placed at the beginning. This is necessary to make certain that the encrypted information shows up various each time, making it impossible for an aggressor to analyze the information by determining similarities (CIA 2016).

3. Port 25/tcp (SMTP):

Vulnerabilities:

- Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
- Diffie-Hellman Key Exchange Insufficient Group Strength
- Diffie-Hellman Key Exchange Downgrade Attack (Logjam)

Exploitable: Yes

Explanation: A Diffie-Hellman cypher key can be cracked by an attacker using small key sizes and predictable prime numbers. The same common primes are used by some Diffie-Hellman keys. Attackers have been able to break these known primes through previous vulnerabilities, such as the logjam vulnerability. This has the potential to result in man-in-the-middle attacks (Postal, 2018).

4. Port 80/tcp (HTTP):

Vulnerability: Slowloris DOS attack.

Exploitable: Likely

Explanation: Slowloris is a denial-of-service strike tool that enables one maker to overload the web server of one more with very little bandwidth use and without affecting various other solutions or ports. Slowloris tries to maintain lots of open connections to the target internet server for as long as feasible. There are no trustworthy configurations of the at risk internet servers that can quit the Slowloris attack, yet there are methods to reduce or decrease its effect. Normally, these consist of increasing the maximum variety of customers the web server can handle, restricting the number of connections from a single IP address, enforcing restrictions on the minimum transfer speed of a connection, and restricting the duration of a connection.

To reduce the Slowloris strike on the Apache internet server, there are numerous modules readily available. These components, consisting of mod_limitipconn, mod_qos, mod_evasive, mod_security, mod_noloris, and mod_antiloris, have actually been recommended to reduce the probability of an effective Slowloris assault. Because Apache variation 2.2.15, the main option sustained by the programmers is the mod_reqtimeout module.

Other reduction techniques involve using reverse proxies, firewall programs, tons balancers or content switches. Administrators could additionally switch to a web server software program that is not affected by this sort of assault. For instance, lighttpd and nginx are not vulnerable to this certain strike. (Wikipedia, 2020)

5. Port 80/tcp (HTTP):

Detected possible SQL injection points in various URLs.

Example: <http://192.168.64.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

Exploitable: Potentially

Explanation: The technique of using malicious scripts to attack a database is known as SQL injection. When defining URL routes, ignorance could present a chance for SQL injection. These types of attacks are possible for any type of REST operation. For instance, there is a possibility that an attacker will append an incorrect string to parameters that the client is passing to the server. There might be a risk if we use

those variables or parameters straight into an SQL query that runs on our database (packt, 2014).

Recommendations:

Patch and Update:

- Update vsFTPD to eliminate the backdoor vulnerability.
- Apply patches for SSL POODLE vulnerability on the SMTP service.
- Address Diffie-Hellman vulnerabilities by configuring stronger key exchange methods.

Mitigate Slowloris Attack:

- Implement measures to mitigate Slowloris DOS attacks, such as rate limiting or deploying a web application firewall.

Secure SQL Injection Points:

- Conduct a detailed assessment of the SQL injection points identified in the HTTP service.
- Implement input validation and parameterized queries to prevent SQL injection attacks.

Regular Security Audits:

- Conduct periodic security audits to identify and remediate emerging vulnerabilities.

2. Scanning Windows 11 + WebGoat with Nmap:

Screenshot:

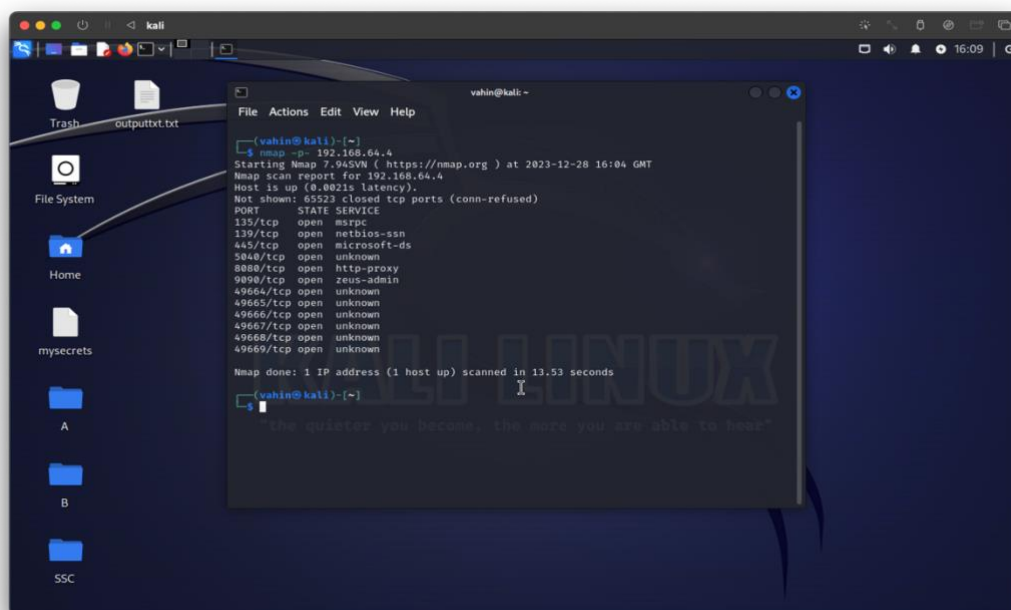


Figure 8: Nmap results of Windows 1 with WebGoat

Overview:

The Windows 11 with WebGoat in VM, with IP address 192.168.64.4, was subjected to a comprehensive security assessment of SOA Enterprises using Nmap version 7.94SVN. The scan revealed several vulnerabilities across various services, ranging from outdated software versions to potential exploitation points.

Vulnerabilities Detected:

1. Port135/tcp (msrpc):

Vulnerability: Denial of Service Attacks (331953)

Exploitable: Likely

Explanation: An attacker can manipulate a vulnerability in a susceptible server's RPC solution by sending out a maliciously crafted RPC message over TCP port 135, causing the service to stop working. To do this, they would certainly first develop a connection to the Endpoint Mapper process on the remote maker utilizing TCP/IP. They would certainly after that launch RPC connection settlement and send out the misshapen message, which would certainly make the process on the remote device fail. The Endpoint Mapper procedure keeps link details for RPC-using procedures, and considering that it runs within the RPC solution, manipulating this vulnerability would certainly also impact the RPC solution and cause the loss of RPC-based solutions and some COM features. (BetaFred, 2003).

2. 139/tcp (netbios-ssn):

Vulnerabilities: Inbound connection in port 139 (TCP) is not blocked in the Windows firewall

Exploitable: Likely

Explanation: The NetBIOS Session service uses port 139. If enable NetBIOS services, anyone connected to the internet can access shared resources, such as files and printers, in addition to network computers. As a result, blocking port 139 in the firewall is advised (Zoho Corp, 2014).

3. . Port 80/tcp (HTTP):

Vulnerability: Slowloris DOS attack.

Exploitable: Likely

Explanation: A particular kind of denial-of-service attack tool called slowloris enables one machine to bring down the web server of another with very little bandwidth usage and no negative impact on unrelated services or ports. Slowloris attempts to maintain numerous open connections for as long as possible to the target web server (Wikipedia, 2020).

4. Port 80/tcp (HTTP):

Detected possible SQL injection points in various URLs.

Example: <http://192.168.64.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

Exploitable: Potentially

Explanation: The technique of using malicious scripts to attack a database is known as SQL injection. When defining URL routes, ignorance could present a chance for SQL injection. These types of attacks are possible for any type of REST operation. For

instance, there is a possibility that an attacker will append an incorrect string to parameters that the client is passing to the server. There might be a risk if we use those variables or parameters straight into a SQL query that runs on our database (packt, 2014).

Recommendations:

- Configure the firewall to allow only essential services and ports while blocking unnecessary or potentially vulnerable ones.
- Block incoming traffic on port 139 to enhance security, especially considering the potential risks associated with NetBIOS services.
- Introduce rate-limiting mechanisms on the HTTP proxy (port 8080/tcp) to restrict the number of connections a single IP can establish within a specific timeframe.
- Deploy a Web Application Firewall to identify and block Slowloris-type attacks. WAFs can detect and prevent malicious activities targeting web applications.
- Implement measures to mitigate Slowloris DOS attacks, such as rate limiting or deploying a web application firewall.
- Conduct a detailed assessment of the SQL injection points identified in the HTTP service.
- Implement input validation and parameterized queries to prevent SQL injection attacks.
- Conduct periodic security audits to identify and remediate emerging vulnerabilities.

Conclusion:

The network infrastructure of SOA Enterprises, Inc. was evaluated for safety and security, which proved helpful for the firm. The assessment particularly targeted the vulnerabilities present in the Metasploitable and Windows 11 VMs with WebGoat. By making use of Nmap, a commonly identified network scanning device, the evaluation effectively recognized noteworthy security worries. If left neglected, these concerns might possibly be made use of by destructive individuals.

The protection analysis focused heavily on the firewall software setup, specifically in connection with the open ports and solutions that can be vulnerable to exploitation. Of certain problem was the visibility of NetBIOS services on port 139 in the Windows 11 VM, which considerably raised the probability of unapproved accessibility to shared resources. To solve this vulnerability, it is critical to develop a thorough firewall program configuration which includes activating a firewall to manage incoming connections and clearly obstructing port 139. By taking an aggressive method, the total safety and security of the network can be considerably enhanced, guaranteeing that just important services come and properly discouraging any type of unauthorized access efforts.

The safety and security evaluation additionally determined vulnerabilities connected to feasible denial-of-service attacks, particularly the Slowloris DoS strike identified on port 8080/tcp on both the Metasploitable and Windows 11 VMs. To counter this danger, the application of lasting actions such as price restricting and the release of

an Internet Application Firewall (WAF) is critical. These proactive procedures are utilized to recognize and reduce malicious activities targeting web applications, hence securing the honesty and accessibility of crucial resources.

In addition, the evaluation directed out possible SQL injection points within the HTTP services running on port 8080/tcp, presenting a severe risk to the underlying data source structure. To repair this vulnerability, a complete evaluation incorporated with the application of rigorous protection procedures, including input recognition and parameterized inquiries, is required. By adopting these finest practices, SOA Enterprises, Inc. can efficiently decrease the threat of SQL injection assaults, thus preserving the integrity, and accessibility of sensitive information.

To sum up, pen testing emphasizes the essential importance of taking steps to stop attacks and conducting routine audits to identify and attend to arising weak points efficiently. By adhering to the recommended approaches, such as repairing and updating vulnerable software, implementing durable and strong firewall arrangements, and taking on stringent security procedures, SOA Enterprises, Inc. can properly boost its ability to hold up against different possible cybersecurity attacks. In addition, it is important to stay careful, constantly display, and adjust to advancing safety obstacles in order to preserve a durable and dependable security approach, thus securing both business assets and the trust of stakeholders in today's interconnected digital atmosphere.

Reference list:

Zoho Corp (2014). *How to disable NetBIOS port 139 (TCP) | NetBIOS Session service*. [online] [www.manageengine.com](https://www.manageengine.com/vulnerability-management/misconfiguration/windows-firewall/how-to-disable-netbios-port-139-tcp-netbios-session-service.html#:~:text=Port%20139%20is%20utilized%20by). Available at: <https://www.manageengine.com/vulnerability-management/misconfiguration/windows-firewall/how-to-disable-netbios-port-139-tcp-netbios-session-service.html#:~:text=Port%20139%20is%20utilized%20by>.

BetaFred (2003). *Microsoft Security Bulletin MS03-010 - Important*. [online] [learn.microsoft.com](https://learn.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-010). Available at: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-010> [Accessed 30 Dec. 2023].

Caddy, T. (2006). *Penetration Testing*. Springer eBooks, pp.456–457. doi:https://doi.org/10.1007/0-387-23483-7_297.

CIA (2016). *SSL 3.0 Protocol Vulnerability and POODLE Attack | CISA*. [online] [www.cisa.gov](https://www.cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-poodle-attack#:~:text=The%20POODLE%20attack%20can%20be). Available at: <https://www.cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-poodle-attack#:~:text=The%20POODLE%20attack%20can%20be> [Accessed 29 Dec. 2023].

Corcoran, T. (2001). *An Introduction to NMAP | SANS Institute*. [online] [www.sans.org](https://www.sans.org/white-papers/72/). Available at: <https://www.sans.org/white-papers/72/>.

osy (2020). *UTM*. [online] UTM. Available at: <https://mac.getutm.app> [Accessed 28 Dec. 2023].

OWASP (2016). *OWASP WebGoat - Learn the Hack - Stop the Attack*. [online] [owasp.org](https://owasp.org/www-project-webgoat/#:~:text=WebGoat%20is%20a%20deliberately%20insecure). Available at: <https://owasp.org/www-project-webgoat/#:~:text=WebGoat%20is%20a%20deliberately%20insecure> [Accessed 28 Dec. 2023].

packt (2014). *Hands-On RESTful Web Services with Go - Second Edition*. [online] [subscription.packtpub.com](https://subscription.packtpub.com/book/web-development/9781838643577/2/ch02lvl1sec16/sql-injection-in-urls-and-ways-to-avoid-them#:~:text=SQL%20injection%20is%20a%20process). Available at: <https://subscription.packtpub.com/book/web-development/9781838643577/2/ch02lvl1sec16/sql-injection-in-urls-and-ways-to-avoid-them#:~:text=SQL%20injection%20is%20a%20process>.

Postal, C. (2018). *How Diffie-Hellman Key Exchange Provides Encrypted Communications | UpGuard*. [online] [www.upguard.com](https://www.upguard.com/blog/diffie-hellman#:~:text=Common%20Diffie%2DHellman%20prime%20used%20in%20key%2). Available at: <https://www.upguard.com/blog/diffie-hellman#:~:text=Common%20Diffie%2DHellman%20prime%20used%20in%20key%2>

0exchange&text=Previous%20vulnerabilities%2C%20like%20the%20logjam
[Accessed 29 Dec. 2023].

S3Curiosity (2023). *Understanding the Vulnerabilities in VSFTPD 2.3.4*. [online] Medium. Available at: <https://medium.com/@S3Curiosity/understanding-the-vulnerabilities-in-vsftpd-2-3-4-f5e0b8317af5> [Accessed 29 Dec. 2023].

Simplilearn (2021). *What Is Metasploit: Overview, Framework, and How Is It Used* / Simplilearn. [online] Simplilearn.com. Available at: <https://www.simplilearn.com/what-is-metasploit-article#:~:text=Metasploitable%20refers%20to%20a%20vulnerable> [Accessed 28 Dec. 2023].

Wikipedia (2020). *Slowloris (computer security)*. [online] Wikipedia. Available at: [https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](https://en.wikipedia.org/wiki/Slowloris_(computer_security)) [Accessed 29 Dec. 2023].