Cyber 357:

Thomas Saldari

Cyber357 - Mount St. Mary's University

4/9/2025

Table of Contents

Virtual Machines Assessment Report

Introduction

This report aims to identify vulnerabilities inherent in three virtual machines. The three virtual machines are Metasploitable 2, Mr. Robot, and an Ubuntu Server with Samba. To conduct this assessment, a Kali Linux virtual machine will use four tools which are, WPScan, nikto, nmap, and OpenVAS. Through utilizing these tools, an assessment of the virtual environment will be completed to determine the current threats. A remediation plan will thus be developed to remove these threats either tactically or through policy changes. Lastly, a budget will be enacted for the remediation plan to effectively manage resources and not overstep financial bounds.

Network in Depth:

This Virtual Environment is set up on the 192.168.10.0/24 network. The address space available on the DHCP server is 192.168.10.10-20.

1. The Kali Linux virtual machine (version: 2025.1) has an IP address of 192.168.10.15.
2. The Mr. Robot virtual machine (version: Linux 3.10-4.11) has an IP address of 192.168.10.14.
3. The Metaspolitable2 virtual machine (version: Ubuntu 8.04) has an IP address of 192.168.10.13.
4. The Ubuntu Server virtual machine (version: Ubuntu 24.04.2 LTS) has an IP address of 192.168.10.12.

Tools Used:

WPScan is an open source WordPress security scanner, that can identify vulnerabilities in systems using WordPress. The version used in this vulnerability assessment was WPScan 3.8.28. Utilizing this tool is simple as one needs to run the command “wpscan –url http://(ipaddress here)”

Nikto is an open source CLI web server vulnerability scanner. The version used in this vulnerability assessment was Nikto 2.5.0. Utilizing this tool is also simple as one needs to run the command “nikto -h (ipaddress here)”.

Nmap is an open source port scanner, wchich can detect open ports, and services leading to vulnerability discoveries. The version used in this vulnerability assessment was Nmap 7.95. This tool is a bit more versatile so its utilization can differ, however for this assessment the commands “nmap –open (ipaddress here)” and “nmap -sV (ipaddress here)” were used.

OpenVAS is an open source vulnerability scanner, with the capabilities of identifying vulnerabilities and matching them to a database of CVE’s. The version used in this vulnerability assessment was OpenVAS 23.16.1. This tool is easy to use once setup, to start the web application use the command (sudo gvm-start). After loggining into the web application, one could navigate to the scans tab, and create a new scan with the desired IP address they want to scan.

Assessment Results – OpenVAS

Item	System/ IP	CVE/Vulnerability	Risks	Criticality
1	Mr. Robot/ 192.168.10.14	CVE-2020-35489/ WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability	Attackers can upload files of any type, allowing attackers to inject malicious content.	High 10.0

2	Mr. Robot/ 192.168.10.14	CVE-2023-2996/ WordPress JetPack Plugin Arbitrary File Manipulation Vulnerability	Plugin does not validate uploaded files, allowing users with author roles to manipulate existing files and can rarely cause Remote Code Execution.	High 8.8
3	Mr. Robot/ 192.168.10.14	CVE-2022-3416 & 3417/ WordPress WPtouch Plugin < 4.3.45 Multiple Vulnerabilities	Plugin does not properly validate images, which allows privileged users to upload arbitrary files. Also, the plugin unserialises the content of an imported settings file, which leads to PHP object injections which can lead to an imported malicious settings file.	High 8.8
4	Mr. Robot/ 192.168.10.14	CVE-2021-24307/ WordPress All in One SEO Pack Plugin < 4.1.0.2 RCE Vulnerability	An authenticated attack might execute arbitrary code.	High 8.8
5	Metasploitable2/ 192.168.10.13	CVE-2008-5304 & 5305/ TWiki XSS and Command Execution Vulnerabilities	Variables "-%URLPARAM{}%" and "-%SEARCH{}%" are not properly sanitized allowing for XSS attacks and eval injection attack respectively.	High 10.0
6	Metasploitable2/ 192.168.10.13	CVE-1998-0618/ The rexec service is running	Rexec has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.	High 10.0
7	Metasploitable2/ 192.168.10.13	CVE-2012-1823 & 2311 & 2336 & 2335 /PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	Exploiting this issue allows remote attackers to view the source ode files in the context of the server process. It can allow attackers to obtain sensitive information and run arbitrary PHP code. Other attacks are also possible.	High 9.8
8	Metasploitable2/ 192.168.10.13	CVE-2001-0645/ MySQL / MariaDB Default Credentials (MySQL Protocol)	Remote MySQL was using default credentials.	High 9.8
9	Ubuntu Server/ 192.168.10.12	CVE-1999-0524/ ICMP Timestamp Reply Information Disclosure	This information could be used to exploit weak time-based random number generators in other services.	Low 2.1

OpenVAS Findings Summary: Through using the tool OpenVAS it was apparent that this was the strongest tool by far to find inherent vulnerabilities in all three virtual machines.

OpenVAS works by scanning a targets network, services, ports, OS, and applications. After identifying the versions of software, it matches those against the CVE database. Then finishes by printing out a report of the targeted system. As for Ubuntu Server, it was by far the least vulnerable system as there was only one CVE matched in the report. Both Metasploitable2 and Mr.Robot were both extremely vulnerable systems, showing severity scores of 10.0 (Highest possible). However, remediation efforts will find that Mr. Robot will be easier to secure as it has less vulnerabilities and they are mostly patch/ update-based solutions. Figure 1, will show the total vulnerabilities in each OpenVAS report.

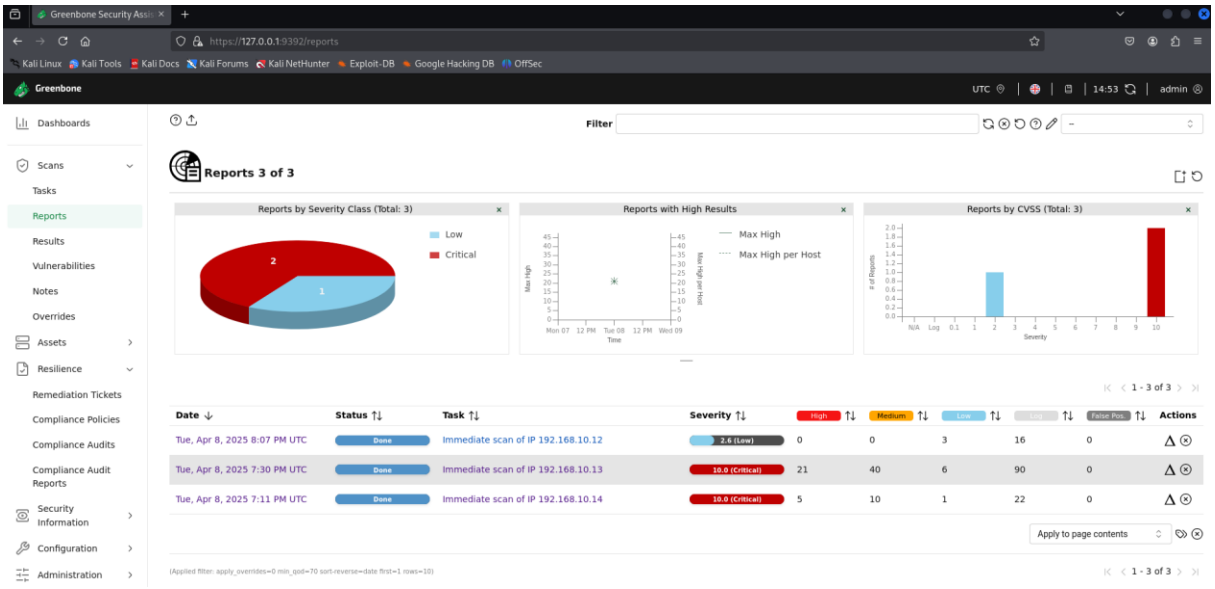

Figure 1 - OpenVAS Reports Dashboard

Assessment Results – Nmap

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.10.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-09 21:16 EDT
Nmap scan report for 192.168.10.12
Host is up (0.00026s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; pro
tocol 2.0)
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
MAC Address: 08:00:27:E6:73:37 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.54 seconds
```

Figure 2 - Nmap of Ubuntu Server

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.10.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-09 21:20 EDT
Nmap scan report for 192.168.10.13
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:56:BA:06 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.45 seconds
```

Figure 3 - Nmap of Metasploitable2

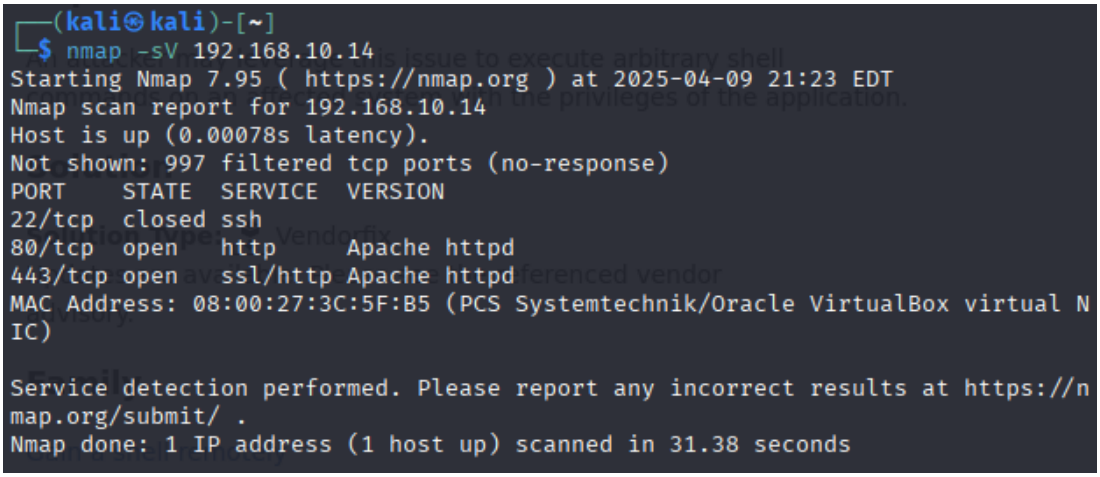

Figure 4 - Nmap of Mr. Robot

Nmap Findings Summary: Through the use of the tool Nmap and using the command "nmap -sV (ipaddress here)", Nmap would find the services and versions running on open ports of targeted machines. For the Ubuntu Server, it found that samba and OpenSSH were running, which could be potential threats if not secured. As for Metasploitable2, figure 3 shows a whole list of open ports with multiple services running on them, showing numerous vulnerabilities. Lastly for Mr. Robot, figure 4 shows that port 80 and 443 are open, which is typically normal.

Assessment Results – Nikto

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.10.12
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.10.13
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.10.13
+ Target Hostname:    192.168.10.13
+ Target Port:        80
+ Start Time:         2025-04-09 21:25:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows att
ackers to easily brute force file names. The following alternatives for 'inde
x' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d1
5,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Ap
ache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cau
se false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST
. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensiti
ve information via certain HTTP requests that contain specific QUERY strings.
 See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensiti
ve information via certain HTTP requests that contain specific QUERY strings.
 See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensiti
ve information via certain HTTP requests that contain specific QUERY strings.
 See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensiti
ve information via certain HTTP requests that contain specific QUERY strings.
 See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and
should be protected or limited to authorized hosts.
```

Figure 5 - Nikto of Ubuntu Server and part of Metasploitable 2

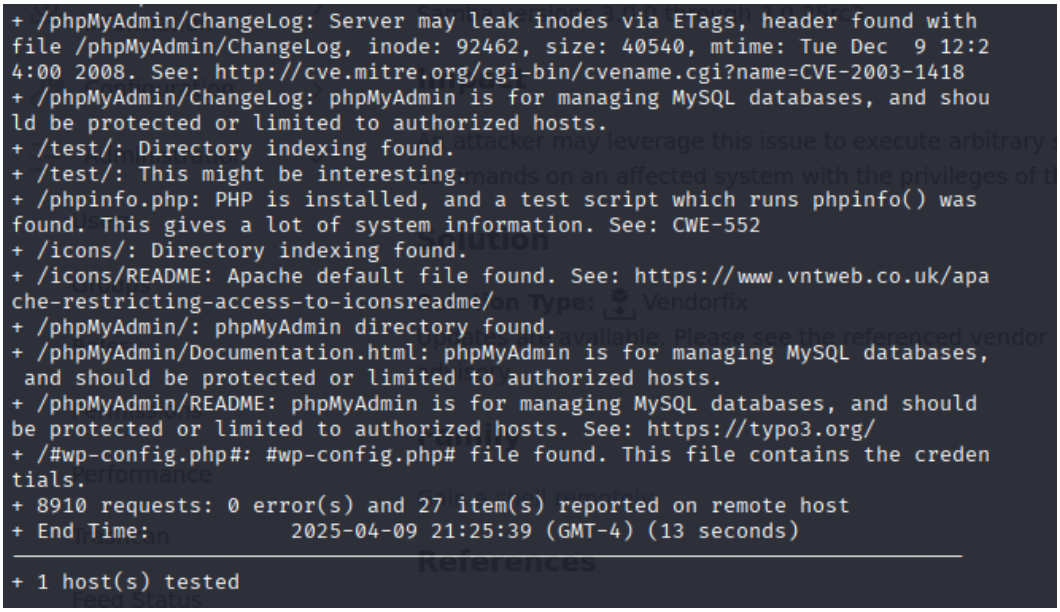

Figure 6 - Nikto of Metasploitable2 finished

Figure 7 - Nikto of Mr. Robot

Nikto Fidnings Summary: Through the use of the tool Nikto, it showed the present web server vulnerabilities in targeted systems. Of the systems, only Metasploitable2 and Mr. Robot had vulnerabilities. For Metasploitable2, the virtual machine had many vulnerabilities, such as an outdated Apache version, PHP admin login pages, enabled directory browsing, and enabled TRACE methods. As for Mr. Robot, it confirms that it is a wordpress site, it has multiple login pages available including admin login pages, and a WordPress config file which will contain credentials. Utilizing figures 5-7 one can find the full Nikto scans of both Metasploitable2 and Mr. Robot.

Assessment Results – WPScan

Figure 8- WPScan of Mr. Robot pt1

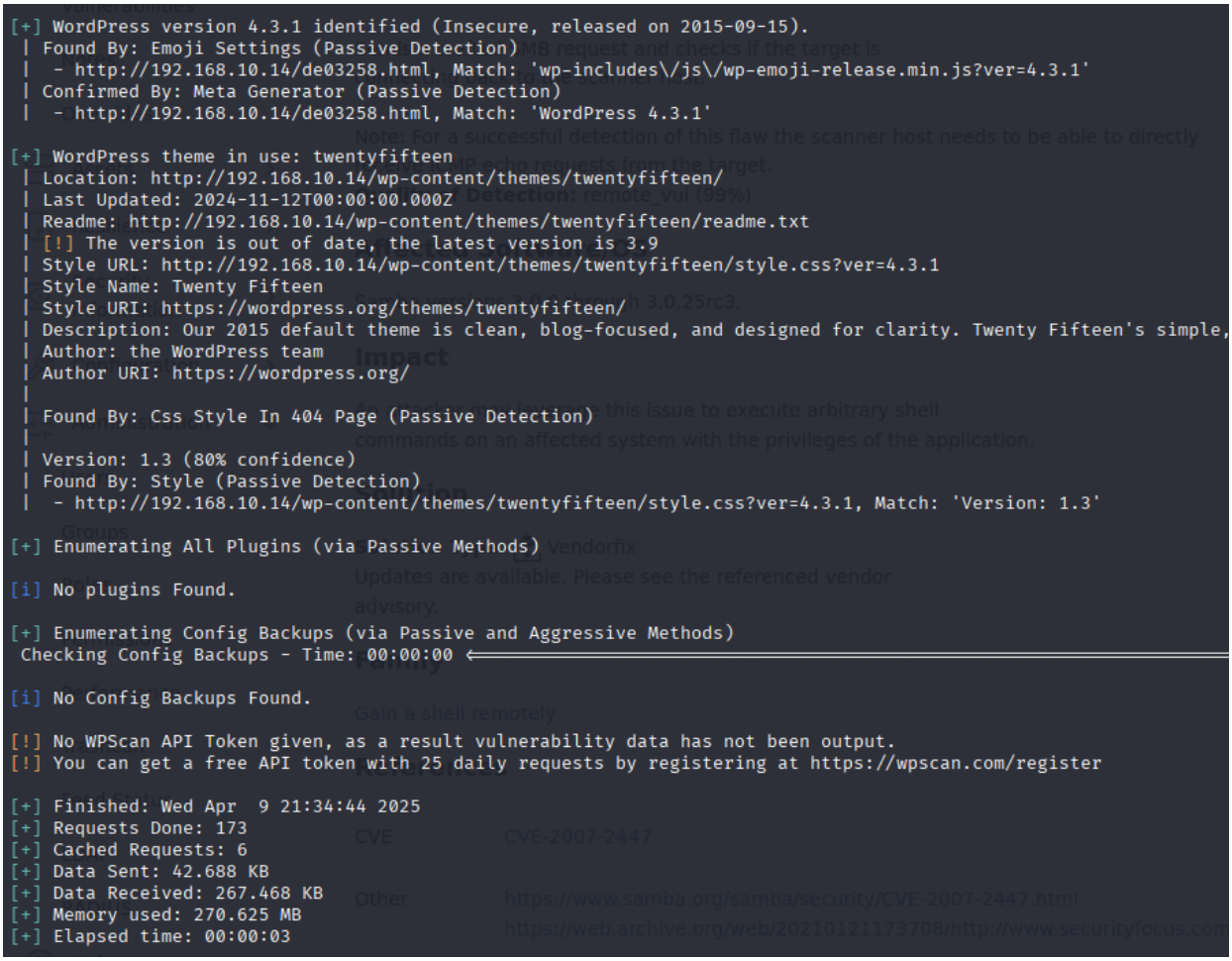

Figure 9 - WPScan of Mr. Robot pt2

WPScan Findsings Summary: WordPress was not present on either Metasploitable2 or Ubuntu Server virtual machines. However, it was found on Mr. Robot which revealed some critical information. Most notably was that WordPress is out of date, which is vulnerable and needs patched. Secondly, robots.txt is available, allowing attackers to find hidden files and directories. Lastly, it was not able to find plugins, however if it did it would find multiple vulnerable plugins like OpenVAS finds. Figures 8 and 9 show the full WPScan of Mr. Robot.

Remediation Recommendations Table

Item	System/ IP	CVE/Vulnerability	Solution/ Remediation	Budget = HxR+M
1	Mr. Robot/ 192.168.10.14	CVE-2020-35489/ WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability	Update WordPress Contact Form 7 plugin to version 5.3.2 or later.	1x50+0 = $50 budget
2	Mr. Robot/ 192.168.10.14	CVE-2023-2996/ WordPress JetPack Plugin Arbitrary File Manipulation Vulnerability	Update the WordPress Jetpack plugin with the new version at: https://jetpack.com/resources/jetpack-12-1-1-critical-security-update/	1x50+0 = $50 budget
3	Mr. Robot/ 192.168.10.14	CVE-2022-3416 & 3417/ WordPress WPtouch Plugin < 4.3.45 Multiple Vulnerabilities	Update WordPress WPtouch plugin to version 4.3.45 or later.	1x50+0 = $50 budget
4	Mr. Robot/ 192.168.10.14	CVE-2021-24307/ WordPress All in One SEO Pack Plugin < 4.1.0.2 RCE Vulnerability	Update WordPress All in One SEO Pack plugin to version 4.1.0.2 or later.	1x50+0 = $50 budget
5	Metasploitable2/ 192.168.10.13	CVE-2008-5304 & 5305/ TWiki XSS and Command Execution Vulnerabilities	Upgrade TWiki to version 4.2.4 or later.	3x50+0 = $150 budget
6	Metasploitable2/ 192.168.10.13	CVE-1998-0618/ The rexec service is running	Disable the rexec service. As an alternative use SSH instead.	2x50+0 = $100 budget
7	Metasploitable2/ 192.168.10.13	CVE-2012-1823 & 2311 & 2336 & 2335 /PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	Update PHP to version 5.3.13, 5.43 or later.	2x50+0 = $100 budget
8	Metasploitable2/ 192.168.10.13	CVE-2001-0645/ MySQL / MariaDB Default Credentials (MySQL Protocol)	Change the MySQL/ Maria DB password to a secure password.	1x50+0 = $50 budget
9	Ubuntu Server/ 192.168.10.12	CVE-1999-0524/ ICMP Timestamp Reply Information Disclosure	1. Disable the support for ICMP timestamp on the remote host. 2. Protect the remote host with a firewall, and block ICMP packets passing through the firewall from either direction.	1x50+0 = $100 budget
				Total: $700

Remediation Recommendations Information

The solution or remediation for each CVE was provided through the aid of NIST's National Vulnerability Database and OpenVAS's NVT. Through comparing and contrasting given solutions (most were the same) a final solution was developed to be implemented into the remediation process and was given a budget. The budget for each item was calculated by multiplying hours worked (H) by a rate (R) in USD. This calculation was then added with the cost of materials (M), creating the final equation (HxR)+M. Using this equation the budget was determined for each item. Since most of the vulnerabilities were simple fixes such as patches/updates, disabling services, or changing passwords, the total budget of all nine items was $700 to remediate.

Conclusion

This virtual network environment held 2 highly vulnerable machines on it in addition to 2 other machines. Of those machines Metasploitable 2 and Mr. Robot have severe vulnerabilities that need remediated immediately to become secure. This was determined through the use of four tools, OpenVAS, Nmap, Nikto, and WPScan which have all come to similar conclusions. Through utilizing OpenVAS's CVE matching against targeted systems it has found 61 medium to high vulnerabilities on the Metasploitable2 machine, and 15 medium to high vulnerabilities on the Mr. Robot system (most WordPress related). Of the most four most severe vulnerabilities on each system it will cost upwards of $600 to remediate in total. These findings highlight the need for remediation efforts and demonstrate the importance of vulnerability assessments to maintain secure network environments.