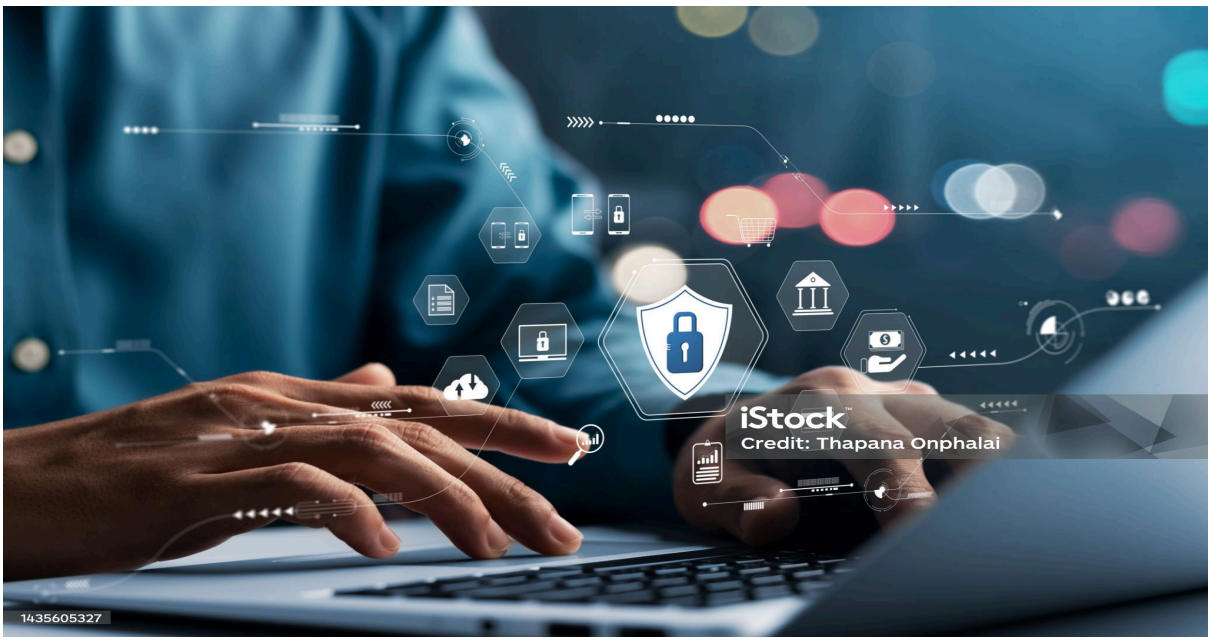

Comprehensive Analysis and Remediation of a Compromised Debian Server

Guillermo J. Costa H.
December, 9, 2024
4Geeks Academy

Introduction

This phase marks the initial step in analyzing the compromised Debian machine, focusing on uncovering critical vulnerabilities and identifying the techniques used by attackers. Through comprehensive forensic analysis, we systematically evaluated the machine's processes, network configurations, and services to detect potential risks. The findings outlined in this report provide the foundation for subsequent phases, where these vulnerabilities will be exploited, remediated, and secured. Below is a detailed breakdown of our methodology and key observations.

1. Active Processes

Command Executed:

ps aux | less

- **Explanation of Command:**
  - **a**: Lists processes of all users, not just the current session.
  - **u**: Displays detailed information, including user, CPU, memory usage, and runtime.
  - **x**: Includes processes not attached to a terminal.

```
debian@debian: ~
File  Edit  View  Search  Terminal  Help
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.3  0.6 102348 12248 ?        Ss   19:41   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    19:41   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   19:41   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   19:41   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   19:41   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   19:41   0:00 [netns]
root           7  0.0  0.0      0     0 ?        I    19:41   0:00 [kworker/0:0-ata_sff]
root           8  0.0  0.0      0     0 ?        I<   19:41   0:00 [kworker/0:0H-events_highpri]
root           9  0.4  0.0      0     0 ?        I    19:41   0:01 [kworker/u4:0-flush-8:0]
root          10  0.0  0.0      0     0 ?        I<   19:41   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    19:41   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    19:41   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    19:41   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    19:41   0:00 [ksoftirqd/0]
root          15  0.1  0.0      0     0 ?        I    19:41   0:00 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    19:41   0:00 [migration/0]
root          18  0.0  0.0      0     0 ?        S    19:41   0:00 [cpuhp/0]
:
```

Result: No suspicious processes were found. All running processes appeared to be legitimate system services.

2. Network Connections and Open Ports

Command Executed:

sudo netstat -antp

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      590/cupsd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      700/mariadbd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      626/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*                    LISTEN      626/sshd: /usr/sbin
tcp6       0      0 :::21                   :::*                    LISTEN      597/vsftpd
tcp6       0      0 :::80                   :::*                    LISTEN      701/apache2
tcp6       0      0 ::1:631                 :::*                    LISTEN      590/cupsd
debian@debian:~$
```

Result:

- **Port 21 (FTP)**: Open to all interfaces. This service does not encrypt credentials, posing a potential security risk.
- **Port 22 (SSH)**: Open to all interfaces, making it vulnerable to external brute-force attacks.
- **Port 80 (HTTP)**: Open to all interfaces, requiring further review of configurations to ensure proper security.
- **Port 3306 (MariaDB)**: Restricted to local IPs, minimizing external risks.
- **Port 631 (Printing)**: Restricted to local IPs; it can be disabled if not required.

3. Active Users and Previous Connections

Commands Executed:

who
last

```
debian@debian:~$ who
debian   tty7         2024-12-04 19:41 (:0)
debian@debian:~$
```

```
reboot   system boot  6.1.0-25-amd64   Wed Dec  4 19:20 - 19:35  (00:15)
debian   tty7         :0               Tue Oct  8 17:28 - crash (57+02:51)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 17:28 - 19:35 (57+03:07)
debian   tty7         :0               Tue Oct  8 16:48 - crash  (00:40)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 16:48 - 19:35 (57+03:47)
debian   tty7         :0               Tue Oct  8 16:44 - crash  (00:03)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 16:43 - 19:35 (57+03:52)
debian   tty7         :0               Mon Sep 30 15:13 - crash (8+01:29)
reboot   system boot  6.1.0-25-amd64   Mon Sep 30 15:09 - 19:35 (65+05:25)
debian   tty7         :0               Mon Sep 30 09:49 - 12:27  (02:38)
reboot   system boot  6.1.0-23-amd64   Mon Sep 30 09:48 - 12:28  (02:39)
debian   tty7         :0               Sat Sep 28 16:40 - crash (1+17:08)
reboot   system boot  6.1.0-23-amd64   Sat Sep 28 16:39 - 12:28 (1+19:48)
debian   tty7         :0               Wed Jul 31 16:45 - 18:18  (01:33)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 16:45 - 18:19  (01:34)
debian   tty7         :0               Wed Jul 31 16:04 - 16:44  (00:39)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 16:04 - 16:44  (00:40)
debian   tty7         :0               Wed Jul 31 15:57 - 15:59  (00:01)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 15:56 - 15:59  (00:02)
```

Result:

- The current session only has one active user (administrator).
- A review of previous logins showed historical connections, suggesting potential configuration weaknesses.

4. Command History and File Changes

Command Executed:

grep -r "" /root/.bash_history /home/*/.bash_history

```
/home/debian/.bash_history:cd /tmp
/home/debian/.bash_history:curl -O https://wordpress.org/latest.tar.gz
/home/debian/.bash_history:sudo apt install curl
/home/debian/.bash_history:curl -O https://wordpress.org/latest.tar.gz
/home/debian/.bash_history:tar xzvf latest.tar.gz
/home/debian/.bash_history:sudo cp -a /tmp/wordpress/. /var/www/html/
/home/debian/.bash_history:sudo chown -R www-data:www-data /var/www/html/
/home/debian/.bash_history:sudo chmod -R 755 /var/www/html/
/home/debian/.bash_history:cd /var/www/html/
/home/debian/.bash_history:sudo mv wp-config-sample.php wp-config.php
/home/debian/.bash_history:sudo nano wp-config.php
/home/debian/.bash_history:ip a
/home/debian/.bash_history:sudo systemctl restart apache2
/home/debian/.bash_history:sudo systemctl status apache2
/home/debian/.bash_history:sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring
 php-curl -y
/home/debian/.bash_history:cd ..
/home/debian/.bash_history:sudo nano /etc/apache2/sites-available/000-default.conf
```

Result: Changes in wordpress files were detected, indicating possible misconfigurations that require further investigation.

5. Installed Services and Versions

Command Executed:

dpkg -l | grep -E 'apache|mysql|vsftpd|ssh'

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ dpkg -l | grep -E "apache|mysql|vsftpd|ssh"
ii  apache2                              2.4.62-1~deb12u1                    amd64        Apache HTTP S
erver
ii  apache2-bin                          2.4.62-1~deb12u1                    amd64        Apache HTTP S
erver (modules and other binary files)
ii  apache2-data                         2.4.62-1~deb12u1                    all          Apache HTTP S
erver (common files)
ii  apache2-utils                        2.4.62-1~deb12u1                    amd64        Apache HTTP S
erver (utility programs for web servers)
ii  libapache2-mod-php                   2:8.2+93                            all          server-side,
HTML-embedded scripting language (Apache 2 module) (default)
ii  libapache2-mod-php8.2                8.2.20-1~deb12u1                    amd64        server-side,
HTML-embedded scripting language (Apache 2 module)
ii  libssh-gcrypt-4:amd64                0.10.6-0+deb12u1                    amd64        tiny C SSH li
brary (gcrypt flavor)
ii  libssh2-1:amd64                      1.10.0-3+b1                         amd64        SSH2 client-s
ide library
ii  mysql-common                         5.8+1.1.0                           all          MySQL databas
e common files, e.g. /etc/mysql/my.cnf
ii  openssh-client                       1:9.2p1-2+deb12u3                   amd64        secure shell
(SSH) client, for secure access to remote machines
```

```
(SSH) client, for secure access to remote machines
ii  openssh-server                       1:9.2p1-2+deb12u3                   amd64        secure shell
(SSH) server, for secure access from remote machines
ii  openssh-sftp-server                  1:9.2p1-2+deb12u3                   amd64        secure shell
(SSH) sftp server module, for SFTP access from remote machines
ii  php8.2-mysql                         8.2.20-1~deb12u1                    amd64        MySQL module
for PHP
ii  vsftpd                               3.0.3-13+b2                         amd64        lightweight,
efficient FTP server written for security
debian@debian:~$
```

Result:

- **Apache 2.4.62**: The default page is active, which could expose system information to attackers.
- **MariaDB 10.x**: Weak or default passwords may be present, representing a significant security concern.
- **vsftpd 3.0.3**: Allows anonymous access, increasing the risk of unauthorized actions.
- **OpenSSH 9.2p1**: Default configurations may present vulnerabilities.

From our Kali Linux machine, a scan was executed on the services running on our Debian system.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_  256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Apache2 Debian Default Page: It works
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
MAC Address: 08:00:27:75:E9:4E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

A search for suspicious files within the FTP directories was conducted, but no irregularities were found. Subsequently, a search for exploits based on the FTP version was performed, with the following results:

```
└─$ searchsploit vsftpd 3.0.3
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------------------------
vsftpd 3.0.3 - Remote Denial of Service                                          | multiple/remote/49719.py
---------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

An exploit search was also carried out for the OpenSSH service. The process was successful; however, no vulnerabilities were found.

```
└─$ searchsploit openssh 9.2
Exploits: No Results
Shellcodes: No Results
```

Within the same OpenSSH service, the configurations on our Debian machine were reviewed to check for potential weaknesses. The following command was used:

sudo nano /etc/ssh/ssh_config

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues
```

Lastly, a search was conducted for any available exploits related to the detected version of Apache.

```
└─$ searchsploit apache 2.4.62
---------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                             |  Path
---------------------------------------------------------------------------------------------------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                                            | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                                          | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                                                        | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                                       | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                                 | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                                 | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                                                        | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                                                          | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                                                        | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                                                  | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)              | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)              | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                                               | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                                           | linux/remote/34.pl
---------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

This systematic approach ensured a thorough review of each service for potential vulnerabilities.

6. MariaDB Weak Password Detection

Command Executed:

SELECT user, host FROM mysql.user;

```
MariaDB [(none)]> SELECT user, host FROM mysql.user;
+---------------+-----------+
| User          | Host      |
+---------------+-----------+
| mariadb.sys   | localhost |
| mysql         | localhost |
| root          | localhost |
| user          | localhost |
| wordpressuser | localhost |
+---------------+-----------+
5 rows in set (0.002 sec)
```

Result: Some MariaDB users are configured with potentially weak or short passwords. This creates a high risk for brute-force attacks, compromising the database and potentially the entire system.

7. Crontab Review

Commands Executed:

crontab -l
ls -la /etc/cron.*

Result: No suspicious scheduled tasks were identified in the crontab. Additional scans with grep confirmed the absence of malicious scripts or persistence mechanisms.

```
File  Edit  View  Search  Terminal  Help
debian@debian:~$ ls -la /etc/cron.*
/etc/cron.d:
total 36
drwxr-xr-x   2 root root  4096 Dec  6 19:11 .
drwxr-xr-x 127 root root 12288 Dec 10 21:37 ..
-rw-r--r--   1 root root   285 Jan 10  2023 anacron
-rw-r--r--   1 root root   201 Mar  4  2023 e2scrub_all
-rw-r--r--   1 root root   607 Aug 13  2022 john
-rw-r--r--   1 root root   712 Jul 13  2022 php
-rw-r--r--   1 root root   102 Mar  2  2023 .placeholder

/etc/cron.daily:
total 44
drwxr-xr-x   2 root root  4096 Sep 30 10:44 .
drwxr-xr-x 127 root root 12288 Dec 10 21:37 ..
-rwxr-xr-x   1 root root   311 Jan 10  2023 0anacron
-rwxr-xr-x   1 root root   539 Jul  1 08:57 apache2
-rwxr-xr-x   1 root root  1478 May 25  2023 apt-compat
-rwxr-xr-x   1 root root   123 Mar 26  2023 dpkg
```

8. Logs Review

Commands Executed:

```
journalctl -xe
tail -n 50 /var/log/auth.log
```

Result: No unauthorized login attempts were detected. The root user appears to have been the only one accessing the system during the review period.

Conclusion

The forensic analysis conducted during Phase 1 revealed several critical vulnerabilities in the compromised Debian machine, underscoring significant weaknesses in its current configuration. These findings emphasize the importance of proactive vulnerability management to minimize risks and secure the system against potential threats. Key findings include:

1. **FTP Service with Anonymous Access Enabled:** This poses a substantial risk, allowing attackers to upload or extract files without authentication, potentially compromising system integrity.
2. **SSH Service Open to All Interfaces:** This configuration leaves the service susceptible to brute-force attacks and unauthorized remote access, endangering sensitive operations.
3. **Apache Service with Default Page Active:** This exposes the system to reconnaissance activities, providing attackers with valuable information for future exploits.
4. **MariaDB Service with Weak Passwords:** Weak or default credentials increase the likelihood of brute-force attacks, risking databases and potentially system-wide compromise.

These vulnerabilities highlight systemic gaps that attackers could exploit to escalate privileges or compromise the system further. While this phase focused on identifying risks and analyzing their potential impact, it lays the groundwork for the critical steps that will follow in Phase 2.

In **Phase 2**, we will:

- Simulate exploitation attempts to validate the severity of the identified vulnerabilities.
- Implement targeted remediation strategies to address each weakness effectively.
- Enhance the overall security posture of the system by applying best practices and reinforcing configurations.

The systematic approach taken in Phase 1 underscores the value of detailed forensic analysis in understanding and addressing security challenges. By meticulously documenting these findings, we have established a robust foundation for securing the Debian machine and preventing future attacks. This process not only strengthens the immediate environment but also provides a replicable model for securing similar systems.