Forensics analyses report

TABLE OF CONTENTS

Executive Summary

4 Geeks commissioned a comprehensive forensic analysis following a cybersecurity breach of a Debian 12 (Bookworm) virtual machine. The objective was to ascertain the details of the compromise, determine the attack vector, address identified vulnerabilities, and establish enhanced security measures to prevent recurrence.

Incident Overview

A virtual machine running Debian 12 was compromised, and unauthorized access was detected. Services operational on the host included Apache HTTP server (2.4.62), MySQL/MariaDB databases, Wordpress web applications, OpenSSH, and vsFTPd.

Methods and Tools

The following tools and methodologies were utilized:

- **Autopsy**: For comprehensive forensic file and log analysis.
- **Powershell and QEMU**: Employed to convert provided VMDK files into RAW images for analysis.

The forensic process involved:

1. Conversion of VM disk images using Powershell and QEMU.
2. Acquisition and documentation of hashes to ensure integrity and maintain a secure chain of custody.
3. Creation and detailed analysis of the forensic case using Autopsy.

Forensic Analysis Findings

Analysis indicated several suspicious activities, specifically on October 8, 2024. The notable activities included:

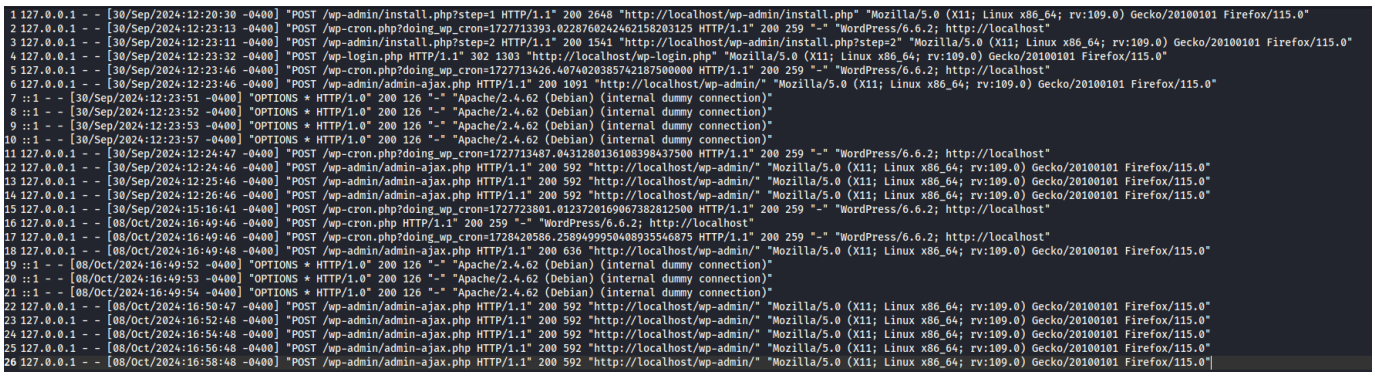
- Modification of Wordpress and SSH configuration files.
- I

```
Oct 08 16:08:57 debian sudo[4687]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install vsftpd
Oct 08 16:09:00 debian groupadd[4757]: group added to /etc/group: name=ftp, GID=122
Oct 08 16:09:00 debian groupadd[4757]: group added to /etc/gshadow: name=ftp
Oct 08 16:09:00 debian groupadd[4757]: new group: name=ftp, GID=122
Oct 08 16:09:00 debian useradd[4766]: new user: name=ftp, UID=113, GID=122, home=/srv/ftp, shell=/usr/sbin/nologin, from=none
Oct 08 16:09:00 debian chfn[4786]: changed user 'ftp' information
Oct 08 16:09:38 debian sudo[4886]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/vsftpd.conf
Oct 08 16:12:13 debian sudo[5104]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install openssh-server
Oct 08 16:12:13 debian sudo[5104]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:12:14 debian sudo[5104]: pam_unix(sudo:session): session closed for user root
Oct 08 16:12:55 debian sudo[5157]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
Oct 08 16:12:55 debian sudo[5157]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:14:03 debian sudo[5157]: pam_unix(sudo:session): session closed for user root
Oct 08 16:14:16 debian sudo[5335]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart ssh
Oct 08 16:14:16 debian sshd[5341]: Server listening on 0.0.0.0 port 22.
Oct 08 16:14:16 debian sshd[5341]: Server listening on :: port 22.
Oct 08 16:14:59 debian sudo[5376]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/apt install net-tools
Oct 08 16:14:59 debian sudo[5376]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:15:01 debian sudo[5376]: pam_unix(sudo:session): session closed for user root
Oct 08 16:15:16 debian sudo[5442]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/netstat -tuln
Oct 08 16:17:59 debian sudo[5532]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod -R 777 /var/www/html
Oct 08 16:17:59 debian sudo[5532]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:18:00 debian sudo[5532]: pam_unix(sudo:session): session closed for user root
Oct 08 16:20:04 debian sudo[5592]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/chmod 777 /var/www/html/wp-config.php
Oct 08 16:20:04 debian sudo[5592]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 16:20:04 debian sudo[5592]: pam_unix(sudo:session): session closed for user root
Oct 08 16:21:23 debian sudo[5646]:   debian : TTY=pts/1 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/nano /etc/apache2/apache2.conf
Oct 08 16:43:30 debian lightdm[859]: pam_unix(lightdm:auth): check pass; user unknown
Oct 08 16:43:30 debian lightdm[859]: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=
Oct 08 16:43:39 debian lightdm[867]: pam_unix(lightdm:auth): check pass; user unknown
Oct 08 16:43:39 debian lightdm[867]: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=
Oct 08 16:43:47 debian lightdm[875]: pam_unix(lightdm:auth): check pass; user unknown
Oct 08 16:43:47 debian lightdm[875]: pam_unix(lightdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=
Oct 08 16:44:04 debian lightdm[682]: pam_unix(lightdm-greeter:session): session closed for user lightdm
Oct 08 16:44:04 debian lightdm[902]: pam_unix(lightdm:session): session opened for user debian(uid=1000) by (uid=0)
Oct 08 16:48:01 debian systemd-journald[241]: Time spent on flushing to /var/log/journal/41b6de202c3f48fdaa490411748aaaff is 3.718ms for 545 entries.
Oct 08 16:48:01 debian systemd-journald[241]: System Journal (/var/log/journal/41b6de202c3f48fdaa490411748aaaff) is 55.4M, max 2.8G, 2.8G free.
Oct 08 16:48:01 debian systemd-journald[241]: Received client request to flush runtime journal.
Oct 08 16:48:01 debian systemd-journald[241]: File /var/log/journal/41b6de202c3f48fdaa490411748aaaff/system.journal corrupted or uncleanly shut down, renaming and replacing.
Oct 08 17:23:01 debian sudo[2851]:   debian : TTY=pts/2 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/sbin/ip a
Oct 08 17:23:01 debian sudo[2851]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 17:25:42 debian sudo[2960]:   debian : TTY=pts/2 ; PWD=/home/debian ; USER=root ; COMMAND=/usr/bin/systemctl restart networking
Oct 08 17:25:42 debian sudo[2960]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Oct 08 17:28:53 debian lightdm[886]: pam_unix(lightdm:session): session opened for user debian(uid=1000) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: Accepted password for root from 192.168.0.134 port 45623 ssh2
Oct 08 17:40:59 debian sshd[1650]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian systemd[1]: Created slice user-0.slice - User Slice of UID 0.
Oct 08 17:40:59 debian systemd[1]: Starting user-runtime-dir@0.service - User Runtime Directory /run/user/0...
Oct 08 17:40:59 debian systemd-logind[488]: New session 6 of user root.
Oct 08 17:40:59 debian (systemd)[1653]: pam_unix(systemd-user:session): session opened for user root(uid=0) by (uid=0)
Oct 08 17:40:59 debian sshd[1650]: pam_env(sshd:session): deprecated reading of user environment enabled
Oct 08 17:57:51 debian NetworkManager[498]: <info>  [1728424671.0885] dhcp6 (enp0s3): state changed new lease, address=2800:810:458:173:8879:c1b2:f8ba:ceb5
Oct 08 17:58:38 debian NetworkManager[498]: <info>  [1728424718.3542] dhcp4 (enp0s3): state changed new lease, address=192.168.0.137
```

- I

dant or unnecessary services such as an additional OpenSSH service and vsFTPd.

- Irregular Apache HTTP POST and OPTIONS requests to the Wordpress site, suggesting potential



  malicious activity.

Attack Identification

Log analysis identified unauthorized root-level SSH access from IP address 192.168.0.134 via port 45623 on October 8, 2024, at 17:40:59. Additionally, suspicious local installations using root privileges and earlier root login failures indicated a possible internal compromise or credential leakage.

Critical misconfigurations were also identified, notably unrestricted permissions (chmod 777) on sensitive configuration files, potentially exposing database credentials.

Impact Assessment

The unauthorized access presented substantial threats, including:

- Exposure and possible exfiltration of sensitive personal, financial, or operational data.
- Potential disruption to critical services (servers, databases, internal applications).

- Economic damage due to direct theft or the financial burden of incident response and recovery.
- Legal and reputational risks resulting from non-compliance with cybersecurity regulations.

Remedial Actions

Immediate corrective actions recommended include:

- Revocation of compromised credentials, particularly root-level access.
- Removal of unauthorized and unnecessary services.
- Comprehensive malware and rootkit scans.
- Audit and correction of file permissions, especially critical configurations.
- System reinstallation in scenarios where integrity is uncertain.
- Integrity verification through known-good file hashes.

Preventative Recommendations

Future security posture enhancements advised include:

- Implementation of strict SSH policies (disabling root login, enforcing key-based authentication).
- Deployment of advanced logging, monitoring, and intrusion detection solutions.
- Enforcement of least-privilege principles.
- Regular vulnerability assessments and system audits.
- Consistent software updates and security patches.
- Ongoing forensic readiness training and anomaly monitoring.

Conclusion

Forensic evidence strongly indicates unauthorized root-level intrusion, misuse of system privileges, and critical misconfiguration exploitation. Immediate mitigation steps have been recommended and partially implemented to contain the incident. Long-term recommendations provide a structured approach to reinforce security and significantly reduce future vulnerability to similar breaches.