Informe de Incidente de Seguridad

Análisis Forense

El análisis forense realizado en el sistema comprometido (IP: 192.168.1.139, máquina Debian) reveló una serie de actividades maliciosas y configuraciones inseguras que permitieron la explotación del sistema. A continuación, se detallan los hallazgos principales:

Acceso no autorizado mediante SSH:

- Se identificó que el servicio SSH permitía el acceso directo como root (*PermitRootLogin yes*), lo que facilitó intentos de acceso no autorizado.
- La autenticación por contraseña estaba habilitada (*PasswordAuthentication yes*), lo que aumentó el riesgo de ataques de fuerza bruta, especialmente si las contraseñas eran débiles.
- El historial de comandos (*~/.bash_history*) mostró actividades sospechosas, como la instalación de servicios (Apache2, MariaDB, WordPress) y modificaciones en archivos críticos como *wp-config.php*. También se observaron intentos de escalación de privilegios al agregar el usuario *debian* al grupo *sudo*.

Servicios expuestos y configuraciones inseguras:

El servidor tenía varios puertos abiertos, incluyendo el puerto 21 (FTP), 22 (SSH) y 80 (HTTP). Estos servicios presentaban configuraciones inseguras:

- **FTP (vsftpd 3.0.3)**: Permitía accesos inseguros, exponiendo archivos y servicios.
- **SSH (OpenSSH 9.2p1)**: Aunque no se detectaron vulnerabilidades críticas, la configuración permitía autenticación por contraseña, lo que representaba un riesgo.
- **HTTP (Apache 2.4.62)**: El servidor web estaba expuesto en todas las interfaces, lo que lo hacía vulnerable a ataques de denegación de servicio (DoS) y explotación de vulnerabilidades conocidas.

Posible instalación de malware o rootkits:

Se realizó un escaneo con herramientas como *chkrootkit* y *Nmap* para detectar rootkits o malware. Aunque no se encontraron evidencias concluyentes, se identificaron actividades sospechosas en el historial de comandos que sugerían la posible instalación de servicios no autorizados.

Explotación de vulnerabilidades:

- Se detectó una posible vulnerabilidad de denegación de servicio (DoS) en el servicio Apache (CVE-2011-1002), que podría ser explotada para sobrecargar el servidor.

- También se identificaron posibles vulnerabilidades de CSRF (Cross-Site Request Forgery) en las rutas */wp-admin/* y */wp-login.php*, lo que permitiría a un atacante realizar acciones maliciosas en nombre de usuarios autenticados.

Cambios en la configuración de SSH:

Se identificó que el puerto SSH estaba configurado en el puerto 22, lo que lo hacía vulnerable a ataques automatizados. Además, se permitía el acceso root y la autenticación por contraseña, lo que aumentaba el riesgo de compromiso.

Acciones Correctivas

Para mitigar las vulnerabilidades identificadas y restaurar la seguridad del sistema, se implementaron las siguientes acciones correctivas:

Cierre de puertos y desactivación de servicios innecesarios:

- Se cerró el puerto 80 (HTTP) y se redirigió el tráfico web al puerto 443 mediante HTTPS para mejorar la seguridad.
- Se desactivaron servicios no esenciales como *Exim4* (correo), *CUPS* (impresión) y *avahi-daemon* (descubrimiento de red) para reducir la superficie de ataque.
- Se detuvo el servicio FTP en el puerto 21 y se recomendó reemplazarlo por SFTP para una transmisión segura de archivos.

Refuerzo de configuraciones en SSH y Apache:

- Se modificó la configuración de SSH (*/etc/ssh/sshd_config*) para deshabilitar el acceso root (*PermitRootLogin no*) y forzar la autenticación por clave (*PasswordAuthentication no*).
- Se cambió el puerto SSH del puerto 22 al puerto 2222 para evitar ataques automatizados.
- En Apache, se configuraron límites en las solicitudes HTTP para prevenir ataques de denegación de servicio (DoS).
- Se habilitó SSL/TLS (HTTPS) para cifrar el tráfico web y se redirigió el tráfico HTTP a HTTPS.

Actualización de software y parches de seguridad:

- Se actualizaron todos los paquetes del sistema para corregir vulnerabilidades conocidas.
- Se aplicaron parches de seguridad en servicios críticos como Apache y OpenSSH.

Cambio de contraseñas y refuerzo de autenticación:

- Se cambiaron las contraseñas de los usuarios *root* y *debian* para garantizar el uso de credenciales seguras.
- Se recomendó implementar autenticación de dos factores (2FA) en servicios críticos como SSH.

Implementación de reglas de firewall:

Se configuraron reglas de firewall para restringir el acceso a puertos críticos y bloquear tráfico no autorizado:

```
debian@debian:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  any    any     anywhere             anywhere
tcp dpt:http reject-with icmp-port-unreachable
    0     0 DROP       tcp  --  any    any     anywhere             anywhere
tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere
tcp dpt:2222

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Instalación de Fail2Ban:

Se instaló Fail2Ban para prevenir ataques de fuerza bruta en SSH:

Medidas Preventivas Aplicadas

Para prevenir futuros incidentes de seguridad, se implementaron las siguientes medidas preventivas:

Refuerzo de políticas de autenticación:

- Se deshabilitó la autenticación por contraseña en SSH y se implementó la autenticación basada en claves.
- Se recomendó el uso de contraseñas fuertes y la implementación de autenticación de dos factores (2FA) en todos los servicios críticos.

Monitoreo y auditoría continua:

- Se activaron registros detallados para monitorear intentos de acceso no autorizados y actividades sospechosas.
- Se recomendó la implementación de un sistema de detección de intrusos (IDS) para detectar y mitigar posibles ataques en tiempo real.

Cierre de puertos y servicios no esenciales:

- Se desactivaron servicios no esenciales como *Exim4*, *CUPS* y *avahi-daemon* para reducir la superficie de ataque.
- Se recomendó mantener solo los puertos y servicios necesarios abiertos y asegurarlos adecuadamente.

Actualización periódica del sistema:

- Se estableció un ciclo de actualización periódica para mantener el sistema y los servicios actualizados con los últimos parches de seguridad.
- Se recomendó la implementación de un proceso automatizado para la aplicación de actualizaciones de seguridad.

Capacitación y concienciación del personal:

- Se recomendó capacitar al equipo de administración en buenas prácticas de seguridad, como la gestión de contraseñas, la configuración segura de servicios y la detección de actividades sospechosas.
- Se sugirió realizar simulaciones de incidentes para mejorar la respuesta ante futuros ataques.

Configuración de Fail2Ban:

Se configuró Fail2Ban para monitorear los intentos de acceso no autorizados y bloquear direcciones IP sospechosas automáticamente.

Conclusión

El análisis forense y las acciones correctivas implementadas han permitido identificar y mitigar las vulnerabilidades que permitieron la explotación del sistema. Las medidas preventivas aplicadas, como el refuerzo de configuraciones de seguridad, el monitoreo continuo y la actualización periódica del sistema, contribuirán a reducir el riesgo de futuros incidentes. Se recomienda mantener un enfoque proactivo en la gestión de la seguridad, incluyendo auditorías regulares y la implementación de tecnologías avanzadas de protección.

*Para más información, detalles y evidencias, ver el archivo anexo: “Informe de Pentesting”.