Filesystem Security Audit – Izveštaj

1. Uvod

Svrha ovog alata je da izvrši **sveobuhvatnu proveru sigurnosti fajl sistema** na Linux sistemima, sa fokusom na:

- pregled montiranih particija i opcija montiranja,
- dozvole za osjetljive fajlove i backup fajlove,
- setuid fajlove,
- world-writable fajlove i direktorijume,
- backup direktorijume i sadržaj.

Skripta generiše **`system_audit.log`** fajl sa detaljnim rezultatima i klasifikuje nalaze u:

- **SECURITY ISSUES** – kritični problemi koji zahtevaju hitnu reakciju,
- **WARNINGS** – potencijalni problemi koji treba proveriti,
- **INFO FINDINGS** – informacije i uspešno izvršene provere.

2. Pregled montiranih particija

Alat koristi komande `mount` i čita `/etc/fstab` kako bi proverio trenutne i trajne opcije montiranja fajl sistema.

Zašto je ovo bitno:

- Opcija `noatime` sprečava update vremena poslednjeg pristupa fajlovima. U slučaju kompromitovanja sistema, zadržavanje ove informacije je ključno za forenzičku analizu.
- Za direktorijume poput `/tmp` i `/home`, opcije `noexec` i `nosuid` smanjuju rizik od izvršenja neautorizovanih binarnih fajlova i zloupotrebe setuid fajlova.

Nalazi iz loga:

- Detektovana je opcija `noatime` na više montiranih particija (`/usr/lib/wsl/drivers`, `/sys`, `/proc` itd.), što predstavlja sigurnosni problem jer uklanja evidenciju pristupa fajlovima.

3. Provera osjetljivih fajlova

Skripta proverava dozvole za fajlove koji sadrže kritične informacije, poput:

- `/etc/shadow` i `/etc/gshadow` – sadrže hashirane lozinke korisnika,
- `/etc/mysql/my.cnf` – konfiguracioni fajl sa pristupom MySQL-u,
- SSL privatni ključevi i `.ssh` direktorijumi.

Zašto je ovo bitno:

- Fajlovi koji su čitljivi ili modifikovani od strane neautorizovanih korisnika ugrožavaju sigurnost sistema.
- Backup fajlovi (`*.bak`, `*.backup`) sa lošim dozvolama predstavljaju dodatni rizik, jer mogu sadržati osjetljive podatke.

Nalazi iz loga:

- `/etc/passwd` i `/etc/group` su world-readable, što je sigurnosni problem jer omogućava svakom korisniku pristup informacijama o korisnicima i grupama.
- Backup fajlovi nisu uspešno pronađeni zbog timeout-a, što ukazuje na moguće probleme sa performansama ili previše fajlova u sistemu.

4. Setuid fajlovi

Alat pretražuje sve fajlove sa setuid bitom (`find / -perm -4000`) i analizira:

- da li su legitimni (npr. `/bin/su`, `/usr/bin/passwd`, `/usr/bin/sudo`),
- da li se nalaze u sumnjivim direktorijumima (`/tmp`, `/var/tmp`, `/dev/shm`, `/home`, `/var/www`).

Zašto je ovo bitno:

- Setuid fajlovi omogućavaju izvršenje sa privilegijama vlasnika fajla (najčešće root). Maliciozni setuid fajlovi u nepravilnim direktorijumima mogu omogućiti eskalaciju privilegija.

Nalazi iz loga:

- Zbog timeout-a, setuid fajlovi nisu detektovani, što može biti posledica velike količine fajlova ili restrikcija pristupa.

5. World-writable fajlovi i direktorijumi

Skripta pronalazi fajlove i direktorijume koji su **world-writable** (`chmod o+w`).

Zašto je ovo bitno:

- World-writable fajlovi omogućavaju neautorizovanim korisnicima modifikaciju kritičnih fajlova, što može dovesti do kompromitovanja sistema.
- Posebna pažnja se obraća na sistemske fajlove (`/etc/`, `/bin/`, `/usr/bin/`) i web direktorijume (`/var/www/`).

6. Backup direktorijumi

Alat proverava direktorijume koji služe za backup (`/backup`, `/var/backups`) i dozvole fajlova u njima.

Zašto je ovo bitno:

- Backup fajlovi često sadrže osjetljive podatke i lozinke. Ako nisu pravilno zaštićeni, predstavljaju visok rizik.

Nalazi iz loga:

- Backup direktorijumi nisu detaljno skenirani zbog timeout-a pretrage.

7. Zaključak i preporuke

Na osnovu loga, detektovana je opcija `noatime` na više particija, a `/etc/passwd` i `/etc/group` su world-readable, što su ključni problemi koje je potrebno ispraviti. Neke pretrage, poput backup i setuid fajlova, nisu završene zbog timeout-a, što pokazuje da skripta može da se optimizuje za veće sisteme. Generalno, alat omogućava **automatsku identifikaciju sigurnosnih problema**, jasno ih klasifikuje i daje preporuke za poboljšanje bezbednosti sistema.