Born2beRoot - Domande e Risposte per la Defense

Sistema Operativo

Perché hai scelto Debian invece di Rocky?

Debian è più semplice da configurare, ha una community enorme, documentazione vasta, ed è consigliato per chi è nuovo alla system administration. Rocky è basato su Red Hat, più usato in ambito enterprise ma più complesso.

Cos'è una macchina virtuale?

È un computer simulato dentro un altro computer. Un software (VirtualBox/UTM) crea un ambiente isolato dove puoi installare un sistema operativo separato. Utile per testare, sviluppare, o isolare servizi senza toccare il sistema principale.

Cos'è AppArmor?

È un sistema di sicurezza per Linux che limita cosa possono fare i programmi. Anche se un programma viene compromesso, AppArmor gli impedisce di fare danni al resto del sistema.

Comando per verificare: `aa-status`

Cos'è SELinux? (per Rocky)

Simile ad AppArmor ma più complesso. Usa etichette di sicurezza per controllare l'accesso tra processi e file.

Apt vs Aptitude

Qual è la differenza tra apt e aptitude?

Entrambi gestiscono i pacchetti su Debian.

- **apt** = command-line semplice, più diretto
- **aptitude** = ha anche interfaccia grafica testuale, gestisce meglio le dipendenze, può suggerire soluzioni ai conflitti

apt è più usato oggi, aptitude è più "intelligente" nella risoluzione dei conflitti.

LVM

Cos'è LVM?

Logical Volume Manager — permette di gestire lo storage in modo flessibile. Puoi ridimensionare, spostare, aggiungere partizioni senza reinstallare.

I dischi fisici diventano "Physical Volumes" (PV), raggruppati in "Volume Groups" (VG), divisi in "Logical Volumes" (LV).

Perché usare LVM?

Flessibilità: puoi espandere o ridurre partizioni al volo, aggiungere dischi, fare snapshot.

Come verificare LVM?

`lsblk` — mostra "lvm" nel tipo

SSH

Cos'è SSH?

Secure Shell — protocollo per connettersi a un computer remoto in modo sicuro (crittografato). Ti permette di controllare un server via terminale da un altro computer.

Perché porta 4242 e non 22?

Sicurezza: la porta 22 è standard e viene scansionata dagli attaccanti. Usare una porta diversa riduce gli attacchi automatizzati.

Perché disabilitare root login via SSH?

Sicurezza: root ha tutti i privilegi, se qualcuno indovina la password ha controllo totale. Meglio entrare come utente normale e poi usare sudo.

Come verificare SSH?

```bash
systemctl status sshd
```

Deve essere active.

```bash
ss -tulpn | grep 4242
```

Deve mostrare sshd sulla porta 4242.

UFW (Firewall)

Cos'è UFW?

Uncomplicated Firewall — strumento semplice per gestire il firewall su Debian. Blocca connessioni non autorizzate, tu decidi quali porte aprire.

Cos'è firewalld? (per Rocky)

L'equivalente di UFW per Rocky Linux, con concetto di "zone" di sicurezza.

Come verificare UFW?

```bash
ufw status
```

Mostra le porte aperte (solo 4242).

Sudo

Cos'è sudo?

"Super User DO" — ti permette di eseguire comandi come root temporaneamente, senza essere loggato come root. Più sicuro perché devi inserire la password e i comandi vengono loggati.

Perché limitare sudo a 3 tentativi?

Sicurezza: impedisce attacchi brute-force sulla password.

Perché TTY mode?

Sicurezza: sudo funziona solo da un terminale reale, non da script automatizzati malevoli.

Perché limitare il PATH?

Sicurezza: impedisce l'esecuzione di programmi da cartelle non sicure.

Dove sono i log di sudo?

`/var/log/sudo/sudo.log`

Password Policy

Quali sono le regole della password?

- Minimo 10 caratteri
- Almeno 1 maiuscola, 1 minuscola, 1 numero
- Max 3 caratteri identici consecutivi
- No nome utente nella password
- Almeno 7 caratteri diversi dalla vecchia (non per root)
- Scade ogni 30 giorni
- Minimo 2 giorni prima di cambiarla
- Avviso 7 giorni prima della scadenza

Dove si configura?

- Scadenza: `/etc/login.defs`
- Qualità: `/etc/pam.d/common-password`

Hostname

Cos'è l'hostname?

Il nome della macchina sulla rete. Nel tuo caso: `rarriola42`

Come cambiarlo?

```bash
hostnamectl set-hostname nuovonome
```

Poi modifica anche `/etc/hosts` per sostituire il vecchio nome.

Utenti e Gruppi

Come creare un nuovo utente?

```bash
adduser nomeutente
```

Come aggiungerlo a un gruppo?

```bash
usermod -aG nomegruppo nomeutente
```

Come verificare i gruppi di un utente?

```bash
groups nomeutente
```

Come creare un nuovo gruppo?

```bash
groupadd nomegruppo
```

Script Monitoring

Come funziona lo script?

Raccoglie info di sistema usando vari comandi (`uname`, `free`, `df`, `who`, ecc.) e le manda a tutti i terminali con `wall`.

Come si esegue ogni 10 minuti?

Tramite **cron** — uno scheduler che esegue comandi automaticamente a intervalli regolari.

Configurato con `crontab -e`, riga:

```
*/10 * * * * /usr/local/bin/monitoring.sh
```

Come fermarlo senza modificare lo script?

```bash
systemctl stop cron
```

Oppure:

```bash
crontab -e
```

E commenta la riga con # davanti.

Comandi Utili da Ricordare

```bash
# Verifica AppArmor
aa-status

# Verifica partizioni LVM
lsblk

# Verifica SSH
systemctl status sshd

# Verifica UFW
ufw status

# Verifica gruppi utente
groups rarriola

# Verifica password policy
chage -l rarriola

# Verifica cron
crontab -l

# Cambia hostname
hostnamectl set-hostname nuovonome

# Crea utente
adduser nomeutente

# Aggiungi a gruppo
usermod -aG gruppo utente
```

Checklist Pre-Defense

- [ ] VM funzionante
- [ ] Signature corrisponde
- [ ] So cambiare hostname
- [ ] So creare utente e aggiungerlo a gruppo
- [ ] So spiegare password policy
- [ ] So spiegare configurazione sudo
- [ ] So dimostrare SSH funzionante
- [ ] So spiegare e fermare lo script monitoring
- [ ] So spiegare UFW/firewall
- [ ] So la differenza apt vs aptitude
- [ ] So cos'è LVM e AppArmor

Buona fortuna per la defense! 💪