SSH: Sicurezza e Amministrazione Remota

Analisi e Risoluzione dei Casi d'Esame (2016-2024)

Prof. Capolupo

3 marzo 2026

Il Ruolo di SSH nelle Tracce d'Esame

Le prove di Sistemi e Reti degli ultimi anni pongono sfide comuni:

- **Accessibilità:** Gestire sistemi distanti (MyStart 2018).
- **Privacy:** Proteggere dati sensibili e personali (Sanità 2024).
- **Limiti Infrastrutturali:** Accedere a reti private con un solo IP pubblico (Residenziale 2016).

SSH (Secure Shell) risolve queste criticità operando al livello Applicazione della pila TCP/IP, garantendo un canale cifrato su reti insicure.

Riferimenti Normativi: Gli Standard RFC

SSH non è un semplice software, ma un protocollo standardizzato dall'IETF:

- **RFC 4251:** Architettura generale del protocollo.
- **RFC 4252:** Protocollo di autenticazione (Password vs Chiavi).
- **RFC 4253:** Protocollo del livello di Trasporto (Cifratura e Integrità).
- **RFC 4254:** Gestione dei canali (Sessioni interattive e Tunneling).

Configurazione di Base: Il Server

In qualsiasi traccia (es. il Web Server della prova 2024), il primo passo è l'installazione e l'attivazione del demone:

Comandi di sistema

```
sudo apt update && sudo apt install openssh-server
sudo systemctl enable --now ssh
```

Il servizio resta in ascolto di default sulla **porta TCP 22**.

Configurazione di Base: Autenticazione RSA

Per eliminare la vulnerabilità delle password, si utilizzano le coppie di chiavi asimmetriche (Standard RSA):

1. **Generazione sul Client:**

   ```
   ssh-keygen -t rsa -b 4096
   ```

2. **Invio della chiave pubblica al Server:**

   ```
   ssh-copy-id utente@ip_server
   ```

Da questo momento, l'accesso avviene tramite scambio di chiavi, immune ad attacchi di forza bruta.

Caso 1: Gestione Multi-tenant (MyStart 2018)

Il Problema: L'incubatore ospita diverse start-up indipendenti che condividono lo stesso hardware (server fisici).

La Soluzione SSH per il Multi-tenancy:

- **Isolamento Logico:** Ogni start-up ha la propria Macchina Virtuale (VM) con un'istanza SSH separata.
- **Gestione Credenziali:** MyStart fornisce l'infrastruttura, ma solo la start-up possiede la *chiave privata* per accedere alla propria VM.
- **Autonomia:** Ogni azienda gestisce i propri servizi web e DB in remoto come se fosse su un server dedicato, senza interferire con le altre.

Caso 2: Trasferimento Dati Medici (Sanità 2024)

Contesto: Invio di referti e immagini diagnostiche al Data Center Regionale.

Uso di SFTP (SSH File Transfer Protocol):

- Sostituisce il vecchio FTP (che invia dati in chiaro).
- Sfrutta il tunnel SSH per cifrare l'intero trasferimento.
- **Punto chiave:** Garantisce la conformità normativa per il trattamento dei dati sanitari durante il transito su rete pubblica.

Caso 3 (A): Accesso Remoto e Limiti del NAT

Contesto: Un Centro Residenziale (2016) o un'Azienda (2024) con molti apparati interni (Server, DVR, Switch) ma un **solo IP Pubblico** sul router.

La Criticità:

- Dall'esterno, la rete privata (LAN) è invisibile.
- Il router riceve le richieste sull'IP pubblico ma non sa a quale dispositivo interno inoltrare la richiesta di gestione.
- Esporre ogni dispositivo direttamente su internet sarebbe un rischio di sicurezza enorme.

Caso 3 (B): Port Forwarding e Tunneling

Per risolvere il limite dell'IP singolo si agisce su due livelli:

1. **Port Forwarding (DNAT) sul Router:**
   - Si mappa una porta esterna non standard (es. 2222) verso l'IP interno del server sulla porta 22.
   - Richiesta: `IP_PUBBLICO:2222` $\rightarrow$ `192.168.1.10:22`.
2. **SSH Local Port Forwarding (Tunneling):**
   - Una volta stabilita la connessione SSH, si può creare un tunnel per vedere servizi non cifrati (es. interfaccia web del DVR).
   - `ssh -L 8080:ip_dvr:80 utente@ip_pubblico -p 2222`.

Sicurezza Avanzata (Hardening)

Per una risoluzione eccellente della prova, citare le modifiche al file `sshd_config`:

- `PermitRootLogin no`: Obbliga l'uso di un utente standard (minimo privilegio).
- `PasswordAuthentication no`: Accetta solo chiavi RSA.
- `MaxAuthTries 3`: Chiude la connessione dopo 3 tentativi errati.

Conclusioni

L'integrazione di SSH nelle soluzioni d'esame permette di:

1. Soddisfare i requisiti di **gestione remota** chiesti dalle tracce.
2. Implementare la **sicurezza del dato** (Cifratura).
3. Superare i limiti di indirizzamento (**NAT**) in modo professionale e standardizzato.