SSH

Introduzione

SSH (Secure Shell, ovvero shell sicura) è un protocollo che permette di stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host di una rete informatica.
In passato, esisteva un protocollo analogo chiamato Telnet ma è stato poi sostituito in quanto non garantiva alcuna sicurezza durante la trasmissione dei dati.
Il comando su sistemi UNIX è:

```
ssh [opzioni] nomeutente@host [comando]
```

Come è strutturato?

Questo protocollo si basa su un'architettura a 3 livelli: TLP (Transfer Layer Protocol), UAP (User Authentication Protocol) e CLP (Connection Layer Protocol).
Dunque, avremo un livello per il trasporto (come devono essere trasportati i dati), uno per l'autenticazione dei due utenti e uno per la connessione.
Questa divisione ci permette di avere molta elasticità in questo protocollo. Infatti, se per esempio dovessimo cambiare il protocollo di autenticazione, gli altri due non saranno minimamente toccati.

Come funziona?

Analizziamo ora i passaggi.

1. **Negoziazione degli algoritmi**: è il primo passaggio che avviene quando un client e un server vogliono comunicare. In questa fase, vengono scambiate delle liste in cui ci sono scritti gli algoritmi supportati da uno e dall'altro, mettendoli in ordine di preferenza. Una volta fatto, vengono scelti anche i protocolli da usare.
2. **Scambio delle chiavi**: dopo aver scelto gli algoritmi, avviene lo scambio delle chiavi di cifratura. Questo passaggio è importantissimo in quanto le chiavi garantiscono la riservatezza dei dati che verranno trasmessi. L'algoritmo di scambio di chiavi più usato è quello di Diffie-Hellman, il quale è considerato il più sicuro.
3. **Autenticazione del server**: mentre avviene lo scambio di chiavi, il server deve autenticarsi, evitando così che ci sia qualche malintenzionato al posto suo. Per farlo, il server crea un messaggio cifrato con la propria chiave privata e la invia al client, il client la decifra con la chiave pubblica del server verificando l'identità del server, se la decifrazione del messaggio avviene correttamente il client procede con l'instaurazione della connessione, in caso contrario interrompe la procedura.
4. **Crittografia della connessione**: dopo aver definito la chiave condivisa, si può utilizzare un protocollo di crittografia per cifrare la comunicazione. Gli algoritmi più usati sono l'AES e il 3DES. Una volta fatto, è possibile instaurare la connessione.
5. **Compressione delle informazioni**: vengono applicati algoritmi di compressione delle informazioni. Attualmente viene usata la libreria zlib.
6. **Integrità dei pacchetti**: è un processo che verifica che non ci siano stati errori di trasmissione nei dati spediti. Questa fase è consigliata ma non obbligatoria.

7. **Autenticazione**: dopo aver instaurato la connessione, l’utente deve autenticarsi. Per farlo, il server genera una stringa casuale di 256 bit, la cifra usando la chiave pubblica dell'utente e l'algoritmo di cifratura corrispondente alla chiave e la invia al client. Il client decifra il messaggio utilizzando la propria chiave privata e invia l'hash della stringa ricevuta al server, se l'hash della stringa del client corrisponde all'hash della stringa del server l'utente viene autenticato. Solo chi possiede la chiave privata dell'utente è in grado di decifrare correttamente il messaggio cifrato del server, in questo modo il server è in grado di verificare l'identità del client. Un altro metodo più semplice è quello in cui il client da un nome utente e una password.
8. **Uso dei canali**: ogni terminale interattivo aperto e ogni connessione inoltrata attraverso la connessione SSH può occupare un canale di comunicazione. Essendo possibile l'instaurazione di canali multipli ogni canale possiede un numero identificativo, tale numero viene utilizzato per distinguere pacchetti appartenenti a canali diversi permettendo all'applicativo SSH di ricostruire le diverse comunicazioni aperte attraverso il tunnel criptato. L'apertura di un canale avviene quando entrambe le parti concordano la sua creazione, se una delle due parti rifiuta, il canale non viene creato. Fintanto che uno degli host non ha ancora confermato l'apertura del canale nessun pacchetto è autorizzato ad utilizzare tale canale.