FTP

Cos’è FTP

FTP (File Transfer Protocol) è un protocollo di rete che consente il trasferimento di file tra un client e un server. È uno dei protocolli più antichi e ampiamente utilizzati per lo scambio di file su Internet. FTP opera su due canali: il canale di controllo per la comunicazione tra il client e il server e il canale dati per il trasferimento effettivo dei file.

A cosa serve FTP

FTP viene utilizzato per una varietà di scopi, tra cui:

- Caricamento e download di file su server web.
- Trasferimento di file tra computer locali e server.
- Backup e sincronizzazione di file.
- Condivisione di file in modo pubblico o privato.
- Gestione remota di server.

Connessione Client - Server

La connessione FTP si basa su un modello client-server. Ecco come avviene la connessione:

1. Il client si connette al server FTP sulla porta 21 (porta di controllo) utilizzando il protocollo TCP/IP.
2. Il client e il server stabiliscono una connessione di controllo per scambiare comandi e risposte. Questo canale è utilizzato per operazioni come l'autenticazione, la navigazione tra le directory e l'invio di comandi FTP.
3. Durante il trasferimento di file, può essere aperto un secondo canale dati. La modalità di apertura di questo canale (attiva o passiva) varia in base alla configurazione del server e alle impostazioni del client.

Modalità di accesso:

Le modalità di accesso FTP includono:

1. **Accesso anonimo**: In questa modalità, gli utenti possono connettersi a un server FTP senza fornire credenziali. Tuttavia, l'accesso anonimo è spesso limitato alle directory pubbliche.
2. **Autenticazione utente**: Gli utenti devono fornire un nome utente e una password per accedere al server. Questa modalità offre un maggiore livello di sicurezza rispetto all'accesso anonimo.
3. **Accesso tramite chiavi SSH (SFTP)**: Questa modalità utilizza chiavi crittografiche per l'autenticazione, rendendo il trasferimento dei file più sicuro rispetto all'uso di password.

Vulnerabilità

Alcune vulnerabilità comuni associate a FTP includono:

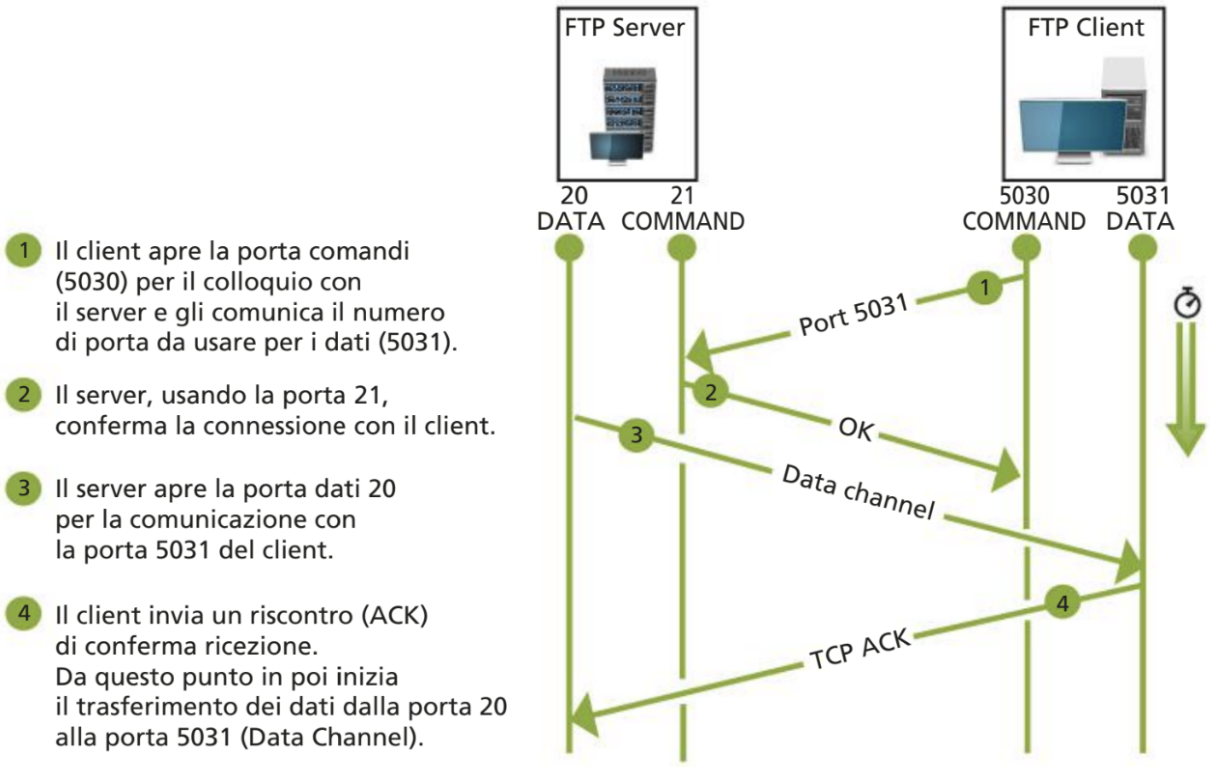
1. **Trasmissione non crittografata**: FTP tradizionale trasmette dati, inclusi nomi utente e password, in chiaro, rendendo vulnerabili le informazioni a intercettazioni da parte di terzi. Questo è stato mitigato con l'uso di FTPS (FTP over SSL/TLS) o SFTP (SSH File Transfer Protocol), che crittografano le comunicazioni.
2. **Atacchi di forza bruta**: Gli attaccanti possono tentare di indovinare le credenziali di accesso tramite attacchi di forza bruta, cercando di indovinare la password.
3. **Atacchi DoS**: I server FTP possono essere soggetti a attacchi di tipo Denial of Service (DoS) che cercano di sovraccaricare il server, impedendo l'accesso legittimo.
4. **Accesso non autorizzato**: La compromissione delle credenziali di accesso o delle autorizzazioni dei file sul server può consentire l'accesso non autorizzato ai file sensibili.
5. **Versioni obsolete di FTP**: L'uso di versioni obsolete del software FTP espone il server a vulnerabilità conosciute. È importante mantenere il software aggiornato.

Active Mode

Nella modalità attiva, il client inizia il trasferimento dei dati aprendo una porta locale ad alto numero (generalmente nell'intervallo da 1024 a 65535) e comunica questa porta al server attraverso il canale di controllo. Il server successivamente si connette alla porta del client per inviare i dati. Ecco come funziona in dettaglio:

1. Il client invia un comando PORT al server, specificando l'indirizzo IP e la porta in cui è in ascolto.
2. Il server si connette alla porta specificata dal client per avviare il trasferimento dei dati. Questo significa che il client deve essere in grado di ricevere connessioni in ingresso da qualsiasi indirizzo IP.

La modalità attiva può causare problemi in scenari in cui il client si trova dietro un firewall o un router NAT, poiché il server remoto potrebbe non essere in grado di connettersi direttamente al client.



Passive Mode

Nella modalità passiva, il server apre una porta locale ad alto numero (simile a quanto fa il client nella modalità attiva) e comunica questa porta al client tramite il canale di controllo. Il client quindi si connette al server su questa porta per avviare il trasferimento dei dati. Ecco come funziona:

1. Il client invia un comando PASV al server, chiedendo al server di entrare in modalità passiva.
2. Il server risponde con un messaggio contenente il suo indirizzo IP e il numero di porta su cui è in ascolto per la connessione dei dati.
3. Il client stabilisce una connessione separata al server su questa porta per il trasferimento dei dati.

La modalità passiva è spesso preferita in situazioni in cui il client è dietro un firewall o un router NAT, poiché consente al server di aprire una porta e attendere le connessioni in ingresso dal client.

1. Il client apre la porta comandi (5030) per il colloquio con il server richiedendo di usare la modalità passiva (comando PASV).
2. Il server apre la porta 2545 (numero casuale) per il trasferimento dei dati e ne comunica il numero al client.
3. Il client apre la porta dati 5031 per la comunicazione con la porta 2545 del server.
4. Il server invia un riscontro (ACK) di conferma ricezione. Da questo punto in poi inizia il trasferimento dei dati dalla porta 2545 alla porta 5031 (Data Channel).