Questions about Phase-0

1. Which is the most appropriate filter that allows you to display only traffic belonging to the FTP session? To answer this question, consider that there are multiple filters that you can adopt to achieve such goal, but one of those filters is the most suitable one.

Il filtro più appropriato per evidenziare un traffico ftp è: *tcp.port == 21*, perchè permette di evidenziare le comunicazioni verso la well-known port del server dove tutte le richieste dei client vengono spedite. Grazie a questo filtro è possibile individuare l’indirizzo ip del server, che filtrandolo con *ip.addr == indirizzo\_server* permette di analizzare tutti i pacchetti scambiati durante la sessione ftp.

# Questions about Phase-1

1. Which is the IP address of the Ubuntu FTP server?

L'indirizzo del server ftp Ubuntu che ha risposto alla richiesta di connessione è 91.189.88.149.

2. Which is the TCP port adopted by your FTP client in order to start the TCP three-way-handshake to the Ubuntu FTP server?

La porta utilizzata dal client per iniziare la connessione con il server ftp Ubuntu è la 54958.

3. Which are the messages, Request and Response, exchanged during this Phase? Describe who sends this message to who (i.e., from client to server, or vice-versa).   
Also, indicate:   
 i) if those messages belongs to the command or to the data connection;

ii) which TCP ports are used during this exchange.

Siccome una sessione FTP utilizza TCP, per prima cosa viene effettuato un tree-way-handshake per instaurare la connessione, cioè: il client invia un pacchetto di SYN alla well-known port del server, cioè la 21; il server risponde con un pacchetto di SYNACK al client e infine il client invia un pacchetto di ACK al server.

Una volta effettuata la connessione con successo, il server si identifica al client come FTP Server e il client richiede che venga utilizzata la codifica dei caratteri UTF8; il server risponde che possiede sempre codifica UTF8.

Infine viene effettuato il login al server: il client richiede l’accesso come USER *anonymous*; il server risponde richiedendo la password dell’utente; il client effettua una richiesta al server dove inserisce la sua password e infine il server risponde che il login è avvenuto con successo.

Tutti questi messaggi appartengono alla “*command connection*”, infatti le porte coinvolte sono la 54958 per il client e la 21 per il server.

Immagine che contiene parete

Descrizione generata automaticamente

4. Is there any message exchanged on the data connection? Hint: to answer this question, consider to change your filter in ip.addr == <ubuntu\_ftp\_server\_IP\_Addr>

Durante la fase di connessione al server non viene scambiato nessun messaggio sulla “data connection”, infatti non viene mai aperta.

# Questions about Phase-2

**Step 1: ?**, the question mark allows to display which command can be performed on the FTP server.

1. Which messages, if any, are exchanged between client and server?

Per questo comando non vengono inviati messaggi al server. Le informazioni relative ai comandi utilizzabili sul server FTP sono contenute nell’applicazione ftp dell’utente, che quindi può direttamente rispondere senza dover fare richieste al server.

**Step 2: ls**, this command allows to display the content of the current folder.

1. Which messages, if any, are exchanged between client and server?

Il client richiede una connessione attiva al server tramite il comando PORT comunicandogli la porta disponibile per effettuare la connessione e il server risponde che ha preso in carico la richiesta.

Il client effettua la richiesta di ricevere le informazioni sul contenuto della directory del server, cioè invia il comando NLST.

Il server comunica che procede all’invio delle informazioni richieste e infine invia una conferma per dire che il trasferimento è terminato.

2. On which connection, command or data, are those message exchanged?

IDK

3. In case messages are exchanged on data connection:

1. Is data connection opened in ACTIVE or PASSIVE mode? Please, motivate your answer by telling your consideration
2. Whether connection is ACTIVE or PASSIVE, which TCP port is used to establish the connection?

La connessione dati è aperta in modo ***attivo***, cioè il server effettua la prima richiesta di connessione verso la porta designata dal client nel comando PORT (cioè la 54959). Infatti si nota che nel momento della richiesta da parte del client, è l’indirizzo IP del server che effettua la richiesta di SYN. La porta utilizzata per stabilire la connessione è la 46793 del server.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Immagine che contiene parete

Descrizione generata automaticamente

Packet No. :

1. COMMAND CONNECTION: Il client effettua una richiesta di connessione attiva al server tramite il comando PORT all’interno del quale comunica la porta sulla quale il server deve effettuare la richiesta.
2. COMMAND CONNECTION: Il server risponde che ha accettato la richiesta di connessione attiva alla porta specificata.
3. COMMAND CONNECTION: Il client effettua la richiesta al server del comando NLST
4. DATA CONNECTION: Il server inizializza la connessione dati con un pacchetto di SYN sulla porta specificata in PORT.
5. DATA CONNECTION: Il client risponde con un SYNACK, confermando di aver ricevuto il messaggio di richiesta di apertura di una connessione.
6. COMMAND CONNECTION: Il server manda un ACK per aver ricevuto correttamente il messaggio di richiesta di NLST
7. DATA CONNECTION: Il server risponde con un ACK per confermare di aver ricevuto il messaggio di SYNACK del client
8. COMMAND CONNECTION: Il server comunica al client che sta trasmettendo sulla connessione dati le informazioni richieste.
9. DATA CONNECTION: Il server invia i dati sulla connessione dati con un PSH
10. DATA CONNECTION: il server comunica che ha intenzione di chiudere il collegamento perché ha terminato il trasferimento delle informazioni, infatti specifica FIN nel pacchetto.
11. DATA CONNECTION: il client invia un ACK per il primo pacchetto dati inviato dal server.
12. DATA CONNECTION: il client invia un FIN ACK per chiudere la connessione dati.
13. COMMAND CONNECTION: il client invia un ACK per il messaggio del server che gli comunicava l’arrivo delle informazioni richieste.
14. COMMAND CONNECTION: il server informa il client che le informazioni sono state inviate con successo.
15. DATA CONNECTION: il server invia un ACK per confermare la chiusura del collegamento dati.
16. COMMAND CONNECTION: il client invia un ACK per confermare di aver ricevuto il messaggio di consegna delle informazioni precedentemente inviato sulla command connection.

**Step 3: cd <folder>**, adopt this command to enter the folder displayed at step 2.

1. Which messages, if any, are exchanged between client and server?

Vengono scambiati quattro messaggi sulla connessione di controllo per richiedere al server di cambiare la directory corrente in una differente e il server risponde dando la conferma di aver effettuato la modifica.

2. On which connection, command or data, are those message exchanged?

I messaggi per questo comando sono trasferiti tutti sulla connessione di controllo tra server e client.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Immagine che contiene screenshot

Descrizione generata automaticamente

Packet No. :

1. COMMAND CONNECTION: Il client richiede al server di cambiare la directory corrente con ./ubuntu tramite il comando CWD
2. COMMAND CONNECTION: Il server risponde con un ACK di conferma per aver ricevuto il messaggio contenente la richiesta.
3. COMMAND CONNECTION: Il server comunica al client che la directory è stata cambiata con successo con quella desiderata
4. COMMAND CONNECTION: Il client invia un ACK per confermare di aver ricevuto il messaggio contenente la comunicazione da parte del server.

**Step 4: ls**, enter again this command.

1. Which messages, if any, are exchanged between client and server?

I messaggi FTP scambiati tra client e server sono gli stessi che sono avvenuti durante lo Step 2.

2. On which connection, command or data, are those message exchanged?

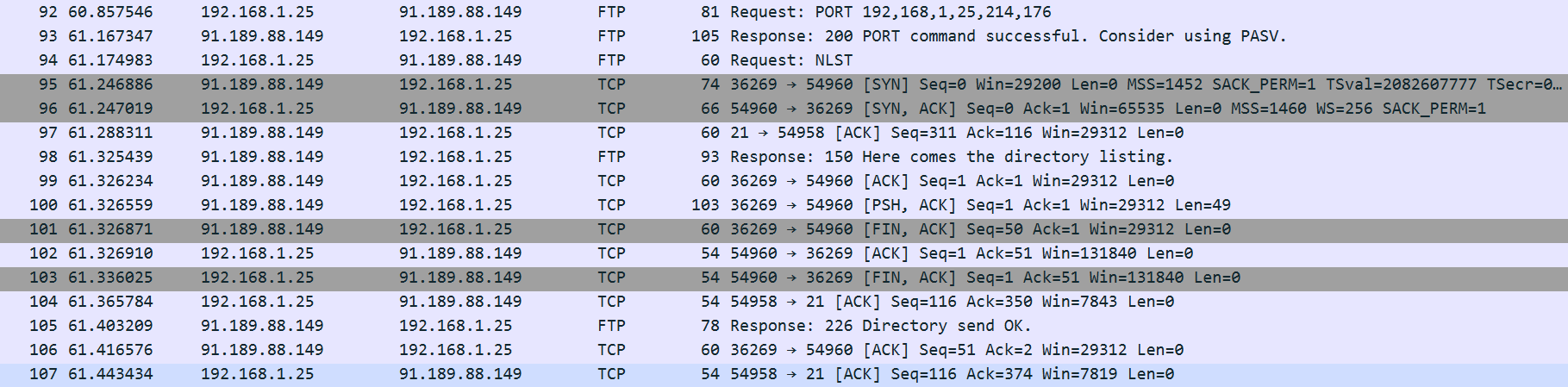
Le connessioni utilizzate sono le stesse che sono state utilizzate per lo Step 2.

3. In case messages are exchanged on data connection:

1. Is data connection opened in ACTIVE or PASSIVE mode? Please, motivate your answer by telling your consideration
2. Whether connection is ACTIVE or PASSIVE, which TCP port is used to establish the connection?

La connessione dati è aperta in modo attivo, perchè il server effettua la prima richiesta di connessione verso la porta designata dal client nel comando PORT (cioè la 54960). Infatti si nota che nel momento della richiesta da parte del client, è l’indirizzo IP del server che effettua la richiesta di SYN. La porta utilizzata per stabilire la connessione è la 36269 del server.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.



Packet No. :

1. COMMAND CONNECTION: Il client effettua una richiesta di connessione attiva al server tramite il comando PORT all’interno del quale comunica la porta sulla quale il server deve effettuare la richiesta.
2. COMMAND CONNECTION: Il server risponde che ha accettato la richiesta di connessione attiva alla porta specificata.
3. COMMAND CONNECTION: Il client effettua la richiesta al server del comando NLST
4. DATA CONNECTION: Il server inizializza la connessione dati con un pacchetto di SYN sulla porta specificata in PORT.
5. DATA CONNECTION: Il client risponde con un SYNACK, confermando di aver ricevuto il messaggio di richiesta di apertura di una connessione.
6. COMMAND CONNECTION: Il server manda un ACK per aver ricevuto correttamente il messaggio di richiesta di NLST
7. COMMAND CONNECTION: Il server comunica al client che sta trasmettendo sulla connessione dati le informazioni richieste.
8. DATA CONNECTION: Il server risponde con un ACK per confermare di aver ricevuto il messaggio di SYNACK del client
9. DATA CONNECTION: Il server invia i dati sulla connessione dati con un PSH
10. DATA CONNECTION: il server comunica che ha intenzione di chiudere il collegamento perché ha terminato il trasferimento delle informazioni, infatti specifica FIN nel pacchetto.
11. DATA CONNECTION: il client invia un ACK per il primo pacchetto dati inviato dal server.
12. DATA CONNECTION: il client invia un FIN ACK per chiudere la connessione dati.
13. COMMAND CONNECTION: il client invia un ACK per il messaggio del server che gli comunicava l’arrivo delle informazioni richieste.
14. COMMAND CONNECTION: il server informa il client che le informazioni sono state inviate con successo.
15. DATA CONNECTION: il server invia un ACK per confermare la chiusura del collegamento dati.
16. COMMAND CONNECTION: il client invia un ACK per confermare di aver ricevuto il messaggio di consegna delle informazioni precedentemente inviato sulla command connection.

**Step 5: get ls-lR.gz**, this command allows the download of ls-lR.gz.

1. Which messages, if any, are exchanged between client and server?

Il client richiede una connessione attiva tramite il comando PORT, il server prende in considerazione la richiesta e, quando il client effettua la request di RETR, apre la connessione nella porta desiderata dal client.

Il server invia poi un messaggio per comunicare al client che sta avvenendo il trasferimento del file richiesto e, quando questo viene ultimato, comunica che il trasferimento è avvenuto con successo.

2. On which connection, command or data, are those message exchanged?

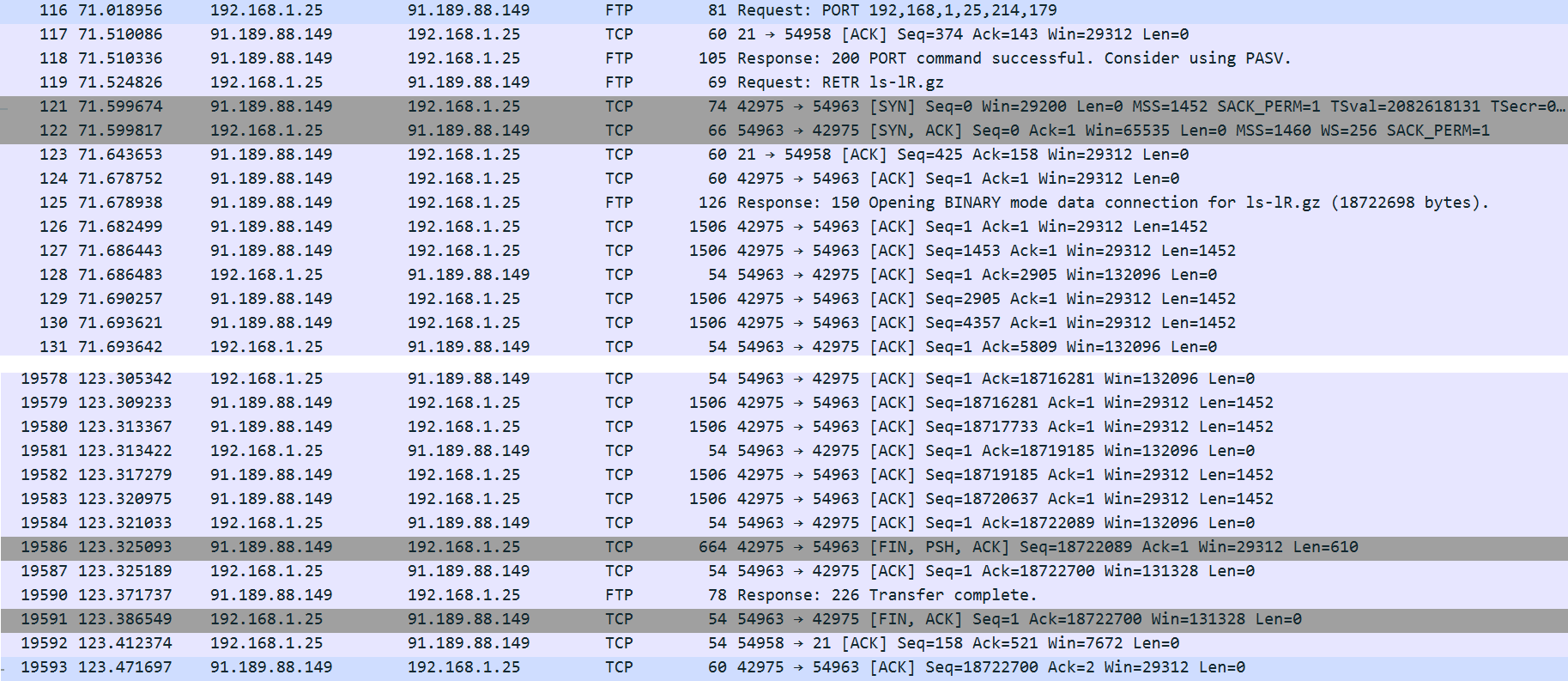
IDK

3. In case messages are exchanged on data connection:

1. Is data connection opened in ACTIVE or PASSIVE mode? Please, motivate your answer by telling your consideration
2. Whether connection is ACTIVE or PASSIVE, which TCP port is used to establish the connection?

La connessione dati viene aperta in modalità attiva, perché è il server che invia il pacchetto di SYN al client per aprire la connessione. Le porte utilizzate in questa connessione dati sono la 42975 per il server e la 54963 per il client.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.



Packet No. :

1. COMMAND CONNECTION: Il client richiede al server una connessione attiva tramite il comando POST e gli comunica la porta sulla quale deve aprire la connessione.
2. COMMAND CONNECTION: Il server invia un ACK per confermare di aver ricevuto il messaggio precedente.
3. COMMAND CONNECTION: il server comunica al client che il comando PORT è andato a buon fine.
4. COMMAND CONNECTION: Il client effettua la richiesta al server di scaricare il file ls-lR.gz tramite il comando RETR.
5. DATA CONNECTION: Il server apre una connessione TCP con il client con il messaggio di SYN per effettuare un three-way handshake
6. DATA CONNECTION: Il client risponde al server con un messaggio di SYNACK per dirgli che sta allocando le strutture per la connessione
7. COMMAND CONNECTION: Il server invia un ACK al client per dirgli che ha ricevuto il messaggio contenente la richiesta di effettuare RETR
8. DATA CONNECTION: Il server invia un ACK per completare il three-way handshake
9. COMMAND CONNECTION: Il server invia al client un messaggio di conferma di presa in carico dell’operazione RETR.
10. -> 19584. DATA CONNECTION: Viene trasferito il file richiesto.
11. DATA CONNECTION: Il server comunica al client che ha completato la trasmissione dei pacchetti tramite un flag FIN
12. DATA CONNECTION: Il client invia un ACK per comunicare al server che ha ricevuto il messaggio.
13. COMMAND CONNECTION: Il server comunica al client che il trasferimento del messaggio è terminato.
14. DATA CONNECTION: il client comunica al server che sta per chiudere la connessione.
15. COMMAND CONNECTION: Il client invia un ACK per confermare di aver ricevuto il messaggio del server che comunica il trasferimento avvenuto.
16. DATA CONNECTION: Il server comunica al client che ha ricevuto il messaggio precedente e si chiude la connessione dati.

**Step 6: exit (or bye)**, this command allows terminate FTP session.

1. Which messages, if any, are exchanged between client and server?

Il client chiede al server di chiudere la sessione FTP inviandogli il comando QUIT, il server risponde con Goodbye e poi si procede alla chiusura della connessione di controllo.

2. On which connection, command or data, are those messageexchanged?

IDK

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Immagine che contiene screenshot

Descrizione generata automaticamente

1. COMMAND CONNECTION: Il client invia al server un messaggio in cui effettua la richiesta dell’operazione QUIT
2. COMMAND CONNECTION: Il server invia un ACK per confermare di aver ricevuto il messaggio.
3. COMMAND CONNECTION: Il server invia il messaggio Goodbye al client
4. COMMAND CONNECTION: Il server invia al client un messaggio di FIN ACK per comunicare che vuole chiudere il collegamento
5. COMMAND CONNECTION: Il client invia un ACK per confermare di aver ricevuto il messaggio correttamente
6. COMMAND CONNECTION: Il client invia un messaggio di FIN ACK al server per comunicargli che sta per chiudere la connessione.
7. COMMAND CONNECTION: Il server invia un ACK per confermare di aver ricevuto il messaggio.