25 December 2025

Created by: Neetrox

Difficulty: Very Easy

Scenario

You’re a SOC analyst at Sfax-Tech. Your team lead rushes in: “A client server triggered multiple alerts. The system isolated it and saved the traffic.” She hands you a USB with a PCAP file. Find out what happened. Time is critical.

Artifacts Provided

Net-Traffic.PCAP

SHA256 Hash:
3f57bbe369f78c92d79b22c31c6c7d93d30fabf8d95409c28d6db98828d06bb1

Initial Analysis

To begin the analysis, the password-protected ZIP file was unlocked using the password `hacktheblue`

Questions

Q1: How many decoy hosts are randomized in this reconnaissance evasion technique ?
Answer: `11`

Q2: What is the real attacker ip address ?
Answer: `192.168.1.23`

Q3: how many open ports did the attacker find ?
Answer: `4`

Q4: What web enumeration tool did the attacker use?
Answer: `gobuster`

Q5: what is the first endpoint discovered by the attacker ?
Answer: `/about`

Q6: What was the first file extension tested during the enumeration?
Answer: `html`

Q7: what is the full vulnerable request parameter used in the attack ?
Answer: `file`

Q8 : what is the username discovered by the attacker?
Answer: `zoro`

Q9: What SSH-related file did the attacker try to access, enter the full path ?
Answer: `/home/zoro/.ssh/authorized_keys`

Q10: when were the first brute force attempts occurred by the attacker to get the right password ?
Answer: `09:02:47,19`

Writeup

Solve Q1:

Wireshark Filter Used:

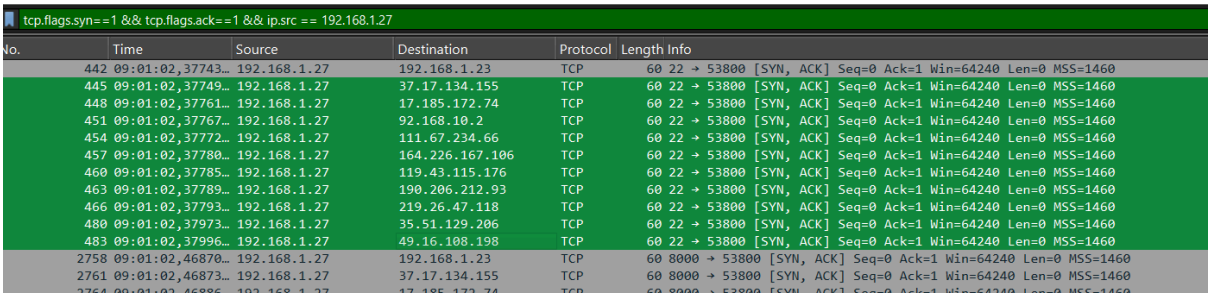
```
tcp.flags.syn==1 && tcp.flags.ack==1 && ip.src == 192.168.1.27
```

This shows SYN-ACK packets from 192.168.1.27

- I see 11 decoy hosts used
- Evidence:
    - Same source (192.168.1.27) contacts many different destination IPs
    - All packets share the same timestamp (09:01:02)

Conclusion: Likely a **decoy scan** (`nmap --randomize-hosts -D RND:10`) attacker hides the real scan by mixing many fake targets.

Destinations: 192.168.1.23, 37.17.134.155, 17.185.172.74, 92.168.10.2, 111.67.234.66, 164.226.167.106, 119.43.115.176, 190.206.212.93, 219.26.47.118, 35.51.129.206, 49.16.108.198



So the response is **11**

Solve Q2:

Navigate to: Statistics → Conversations → IPv4 tab
This shows all communication pairs between IP addresses with traffic statistics.

Looking at the conversation statistics there is massive Traffic Volume:

- 192.168.1.23 ↔ 192.168.1.27: 235,790 packets, 26 MB
- 192.168.1.23 ↔ 172.19.0.2: 463,476 packets, 52 MB

Also this IP is included with the **decoy scan** from the Question 1

Ethernet | IPv4 · 66 | IPv6 · 13 | TCP · 50248 | UDP · 58

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.23	172.19.0.2	463,476	52 MB	29	270,162	23 MB	193,314	29 MB	23.433138	445.0477	420 kbps	521 kbps
192.168.1.23	192.168.1.27	235,790	26 MB	18	137,098	12 MB	98,692	15 MB	23.431443	445.0493	212 kbps	262 kbps
17.185.172.74	192.168.1.27	2,020	119 kB	20	1,000	62 kB	1,020	57 kB	23.431444	32.4634	15 kbps	14 kbps
35.51.129.206	192.168.1.27	2,020	119 kB	27	1,000	62 kB	1,020	57 kB	23.432576	32.4615	15 kbps	14 kbps
37.17.134.155	192.168.1.27	2,020	119 kB	19	1,000	62 kB	1,020	57 kB	23.431444	32.4635	15 kbps	14 kbps
49.16.108.198	192.168.1.27	2,020	119 kB	28	1,000	62 kB	1,020	57 kB	23.432576	32.4611	15 kbps	14 kbps
92.168.10.2	192.168.1.27	2,020	119 kB	21	1,000	62 kB	1,020	57 kB	23.431444	32.4633	15 kbps	14 kbps
111.67.234.66	192.168.1.27	2,020	119 kB	22	1,000	62 kB	1,020	57 kB	23.431444	32.4633	15 kbps	14 kbps
119.43.115.176	192.168.1.27	2,020	119 kB	24	1,000	62 kB	1,020	57 kB	23.432576	32.4620	15 kbps	14 kbps
164.226.167.106	192.168.1.27	2,020	119 kB	23	1,000	62 kB	1,020	57 kB	23.432576	32.4621	15 kbps	14 kbps
190.206.212.93	192.168.1.27	2,020	119 kB	25	1,000	62 kB	1,020	57 kB	23.432576	32.4619	15 kbps	14 kbps
219.26.47.118	192.168.1.27	2,020	119 kB	26	1,000	62 kB	1,020	57 kB	23.432576	32.4617	15 kbps	14 kbps
192.168.1.27	34.160.90.233	72	18 kB	4	38	4 kB	34	13 kB	0.386212	171.1790	207 bits/s	619 bits/s
192.168.1.27	34.36.137.203	51	16 kB	58	25	9 kB	26	7 kB	151.977651	170.2925	417 bits/s	340 bits/s
192.168.1.27	151.101.1.91	41	14 kB	2	21	3 kB	20	11 kB	0.298048	171.3130	118 bits/s	521 bits/s
192.168.1.27	151.101.193.91	46	12 kB	5	24	3 kB	22	9 kB	0.721009	208.8937	105 bits/s	350 bits/s

So the response is **192.168.23**

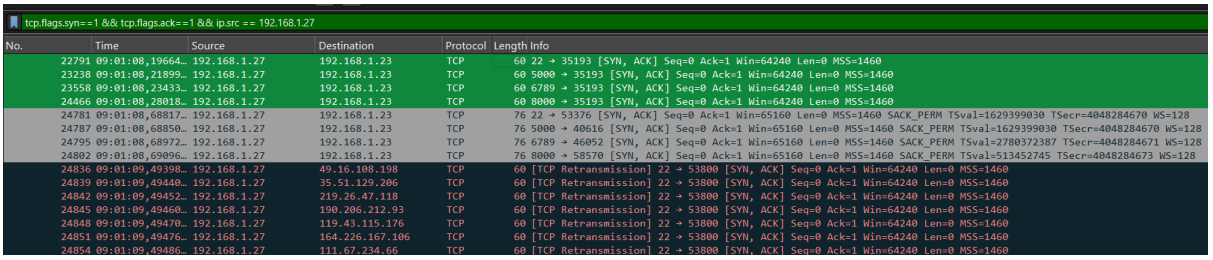
Solve Q3:

Wireshark Filter Used:

```
tcp.flags.syn==1 && tcp.flags.ack==1 && ip.src == 192.168.1.27
```

After scrolling through the network traffic, The attacker sends SYN packets to initiate a TCP handshake. If a port is open, the target responds with a SYN-ACK packet

So we Find out that he find 4 open port 22, 5000, 6789, 8000



tcp.flags.syn==1 && tcp.flags.ack==1 && ip.src == 192.168.1.27

No.	Time	Source	Destination	Protocol	Length	Info
22791	09:01:08,19664…	192.168.1.27	192.168.1.23	TCP	60	22 → 35193 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
23238	09:01:08,21899…	192.168.1.27	192.168.1.23	TCP	60	5000 → 35193 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
23558	09:01:08,23433…	192.168.1.27	192.168.1.23	TCP	60	6789 → 35193 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24466	09:01:08,28018…	192.168.1.27	192.168.1.23	TCP	60	8000 → 35193 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24781	09:01:08,68817…	192.168.1.27	192.168.1.23	TCP	76	22 → 53376 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1629399030 TSecr=4048284670 WS=128
24787	09:01:08,68850…	192.168.1.27	192.168.1.23	TCP	76	5000 → 40616 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1629399030 TSecr=4048284670 WS=128
24795	09:01:08,68972…	192.168.1.27	192.168.1.23	TCP	76	6789 → 46052 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2780372387 TSecr=4048284671 WS=128
24802	09:01:08,69096…	192.168.1.27	192.168.1.23	TCP	76	8000 → 58570 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=513452745 TSecr=4048284673 WS=128
24836	09:01:09,49398…	192.168.1.27	49.16.108.198	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24839	09:01:09,49440…	192.168.1.27	35.51.129.206	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24842	09:01:09,49452…	192.168.1.27	219.26.47.118	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24845	09:01:09,49460…	192.168.1.27	190.206.212.93	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24848	09:01:09,49470…	192.168.1.27	119.43.115.176	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24851	09:01:09,49476…	192.168.1.27	164.226.167.106	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
24854	09:01:09,49486…	192.168.1.27	111.67.234.66	TCP	60	[TCP Retransmission] 22 → 53800 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

So the response is **4**

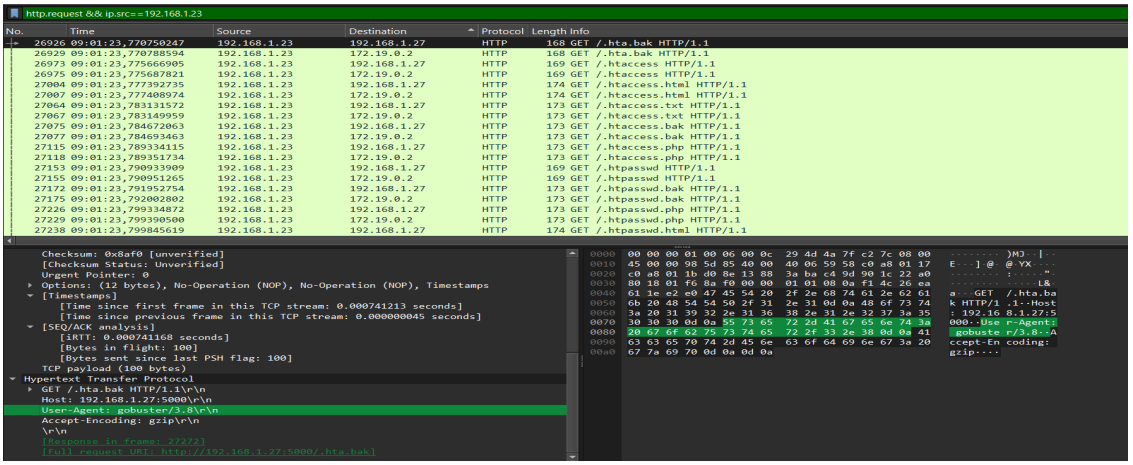
Solve Q4:

Wireshark Filter Used:

```
http.request && ip.src == 192.168.1.23
```

User-Agent String:

- `User-Agent: gobuster/3.8`
- Clearly visible in the HTTP request headers (highlighted in green in the packet details)



Web Enumeration Tool Used: **Gobuster**

Solve Q5:

Wireshark Filter Used:

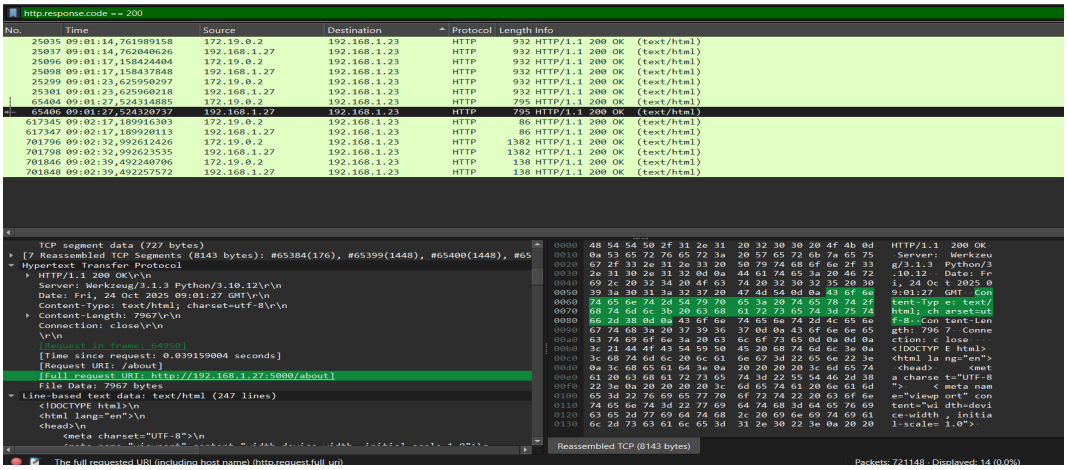
```
http.response.code == 200
```

This filter shows all HTTP responses with status code 200 (OK), indicating successful requests to existing endpoints.

Request Details (from packet details at bottom):

- **Request URI**: `/about`
- **Full request URI**: `http://192.168.1.27:5000/about`

Timeline Analysis: Looking at the timestamps, `/about` appears at **09:01:27 and it was the first endpoint discovred**



So the response is **/about**

Solve Q6:

Wireshark Filter Used:

```
http.request && ip.src==192.168.1.23
```

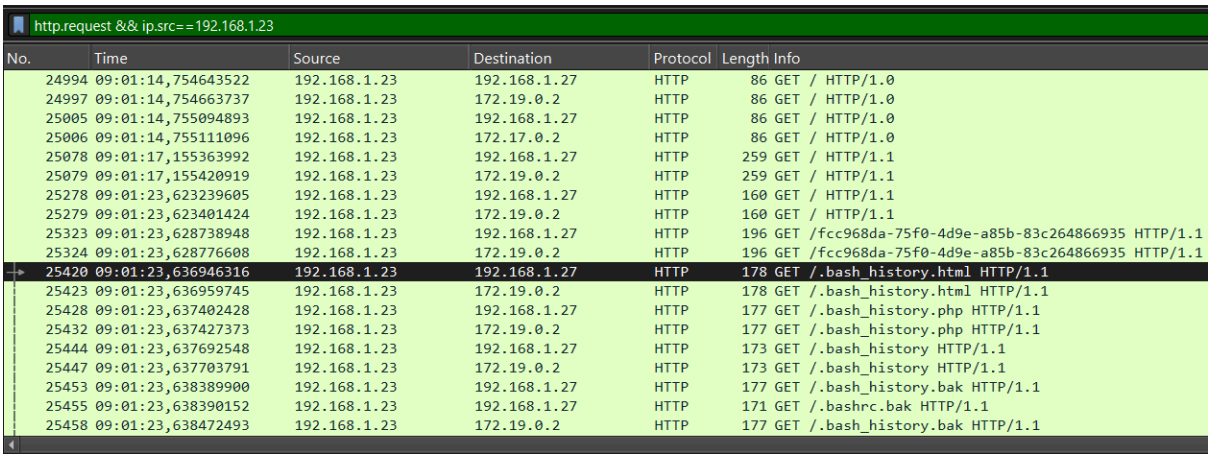
This filter shows HTTP requests from the attacker's source IP 192.168.1.23.

First File Extension Tested: `html`

Evidence:

Timeline Analysis - Looking at the earliest packets:

- Packet #25423 at 09:01:23: `GET /.bash_history.html`


http.request && ip.src==192.168.1.23

No.	Time	Source	Destination	Protocol	Length	Info
24994	09:01:14,754643522	192.168.1.23	192.168.1.27	HTTP	86	GET / HTTP/1.0
24997	09:01:14,754663737	192.168.1.23	172.19.0.2	HTTP	86	GET / HTTP/1.0
25005	09:01:14,755094893	192.168.1.23	192.168.1.27	HTTP	86	GET / HTTP/1.0
25006	09:01:14,755111096	192.168.1.23	172.17.0.2	HTTP	86	GET / HTTP/1.0
25078	09:01:17,155363992	192.168.1.23	192.168.1.27	HTTP	259	GET / HTTP/1.1
25079	09:01:17,155420919	192.168.1.23	172.19.0.2	HTTP	259	GET / HTTP/1.1
25278	09:01:23,623239605	192.168.1.23	192.168.1.27	HTTP	160	GET / HTTP/1.1
25279	09:01:23,623401424	192.168.1.23	172.19.0.2	HTTP	160	GET / HTTP/1.1
25323	09:01:23,628738948	192.168.1.23	192.168.1.27	HTTP	196	GET /fcc968da-75f0-4d9e-a85b-83c264866935 HTTP/1.1
25324	09:01:23,628776608	192.168.1.23	172.19.0.2	HTTP	196	GET /fcc968da-75f0-4d9e-a85b-83c264866935 HTTP/1.1
25420	09:01:23,636946316	192.168.1.23	192.168.1.27	HTTP	178	GET /.bash_history.html HTTP/1.1
25423	09:01:23,636959745	192.168.1.23	172.19.0.2	HTTP	178	GET /.bash_history.html HTTP/1.1
25428	09:01:23,637402428	192.168.1.23	192.168.1.27	HTTP	177	GET /.bash_history.php HTTP/1.1
25432	09:01:23,637427373	192.168.1.23	172.19.0.2	HTTP	177	GET /.bash_history.php HTTP/1.1
25444	09:01:23,637692548	192.168.1.23	192.168.1.27	HTTP	173	GET /.bash_history HTTP/1.1
25447	09:01:23,637703791	192.168.1.23	172.19.0.2	HTTP	173	GET /.bash_history HTTP/1.1
25453	09:01:23,638389900	192.168.1.23	192.168.1.27	HTTP	177	GET /.bash_history.bak HTTP/1.1
25455	09:01:23,638390152	192.168.1.23	192.168.1.27	HTTP	171	GET /.bashrc.bak HTTP/1.1
25458	09:01:23,638472493	192.168.1.23	172.19.0.2	HTTP	177	GET /.bash_history.bak HTTP/1.1

So the response is **html**

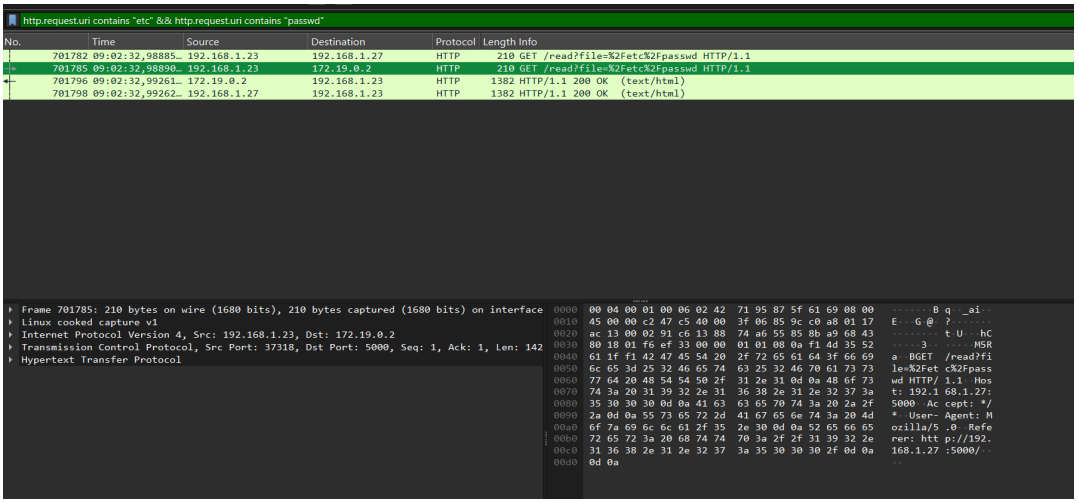
Solve Q7:

Wireshark Filter Used:

```
http.request.uri contains "etc" && http.request.uri contains "passwd"
```

This filter shows HTTP requests containing both "etc" and "passwd" in the URI, indicating a Local File Inclusion (LFI) attack.

Full Vulnerable Request:
Endpoint + Parameter: GET /read?file=%2Fetc%2Fpasswd HTTP/1.1



So the response is **file**

Solve Q8:

When you Enter the follow http stream of paquet number 701782 from the last screenshot and look at the `/etc/passwd` file contents returned in the HTTP response, the last entry shows:

```
zoro:x:1000:1000::/home/zoro:/bin/bash
```

Analysis:

User Details:

- Username: `zoro`
- UID: 1000 (typically the first regular user account)
- GID: 1000
- Home Directory: `/home/zoro`
- Shell: `/bin/bash` (full shell access)

```
GET /read?file=%2Fetc%2Fpasswd HTTP/1.1
Host: 192.168.1.27:5000
Accept: */*
User-Agent: Mozilla/5.0
Referer: http://192.168.1.27:5000/

HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.10.12
Date: Fri, 24 Oct 2025 09:02:32 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1314
Connection: close

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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
zoro:x:1000:1000::/home/zoro:/bin/bash
```

So the response is zoro

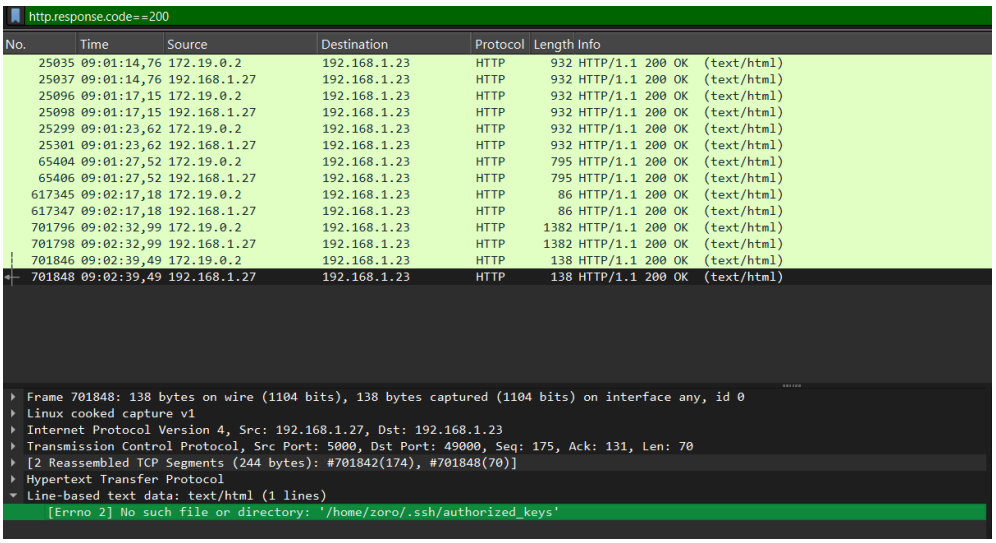
Solve Q9:

Wireshark Filter Used:

```
http.response.code==200
```

This filter shows successful HTTP responses to identify what files the attacker attempted to access.

SSH-Related File Accessed:
Full Path: /home/zoro/.ssh/authorized_keys



So the response is **/home/zoro/.ssh/authorized_keys**

Solve Q10:

When you inspect the PCAP, you can see the attacker retrieve a username during the directory brute-force. This is immediately followed by an SSH brute-force pattern.

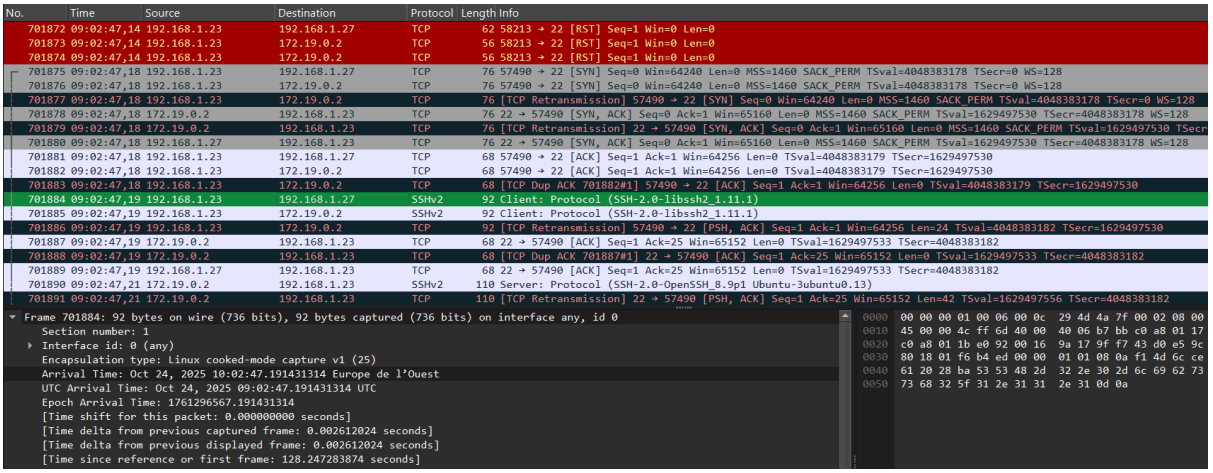
Connection Pattern:

- Multiple TCP connections from 192.168.1.23 to port 22 (SSH)
- TCP handshakes (SYN, SYN-ACK, ACK) followed by SSH protocol negotiation

Brute Force Indicators:

- Multiple rapid SSH connection attempts
- Same source IP (192.168.1.23) targeting SSH service
- Typical pattern of automated password guessing

First Brute Force Attempts: **09:02:47.19**



So the response is **09:02:47.19**