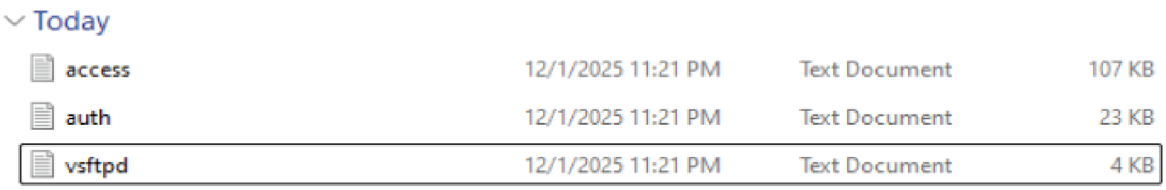
Juice Shop Investigation

Scenario: A shop has been breached by an attack. I have been provided log files to investigate the incident. As a SOC Analyst, I need to find out how the company has been breached and what data have they stolen.

Initial Review
At first glance, the evidence consisted of three text-based log files. My initial question was: *What activity appears abnormal?* I began by reviewing the access logs to identify reconnaissance patterns, suspicious user agents, and potential exploitation attempts.

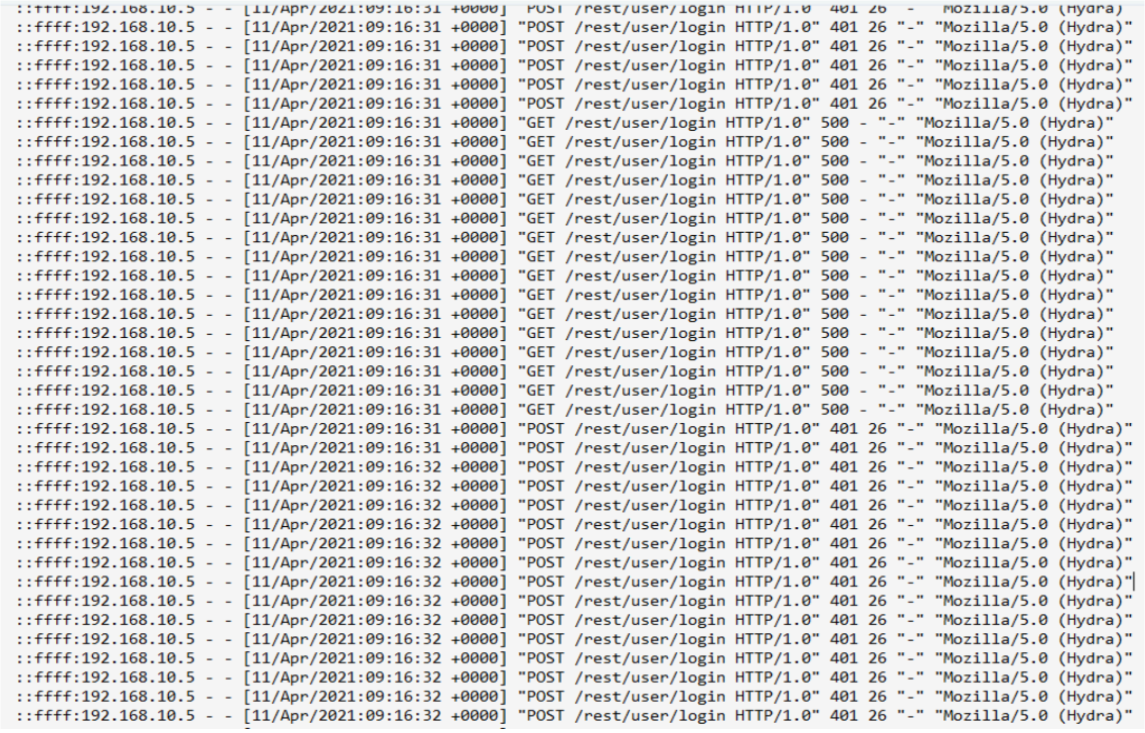


Today

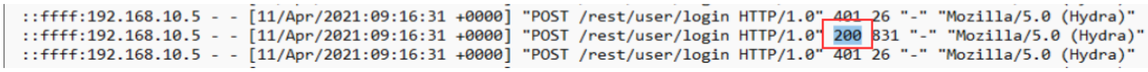
access	12/1/2025 11:21 PM	Text Document	107 KB
auth	12/1/2025 11:21 PM	Text Document	23 KB
vsftpd	12/1/2025 11:21 PM	Text Document	4 KB

During the initial scan of the access log, I immediately noticed requests associated with well-known offensive security tools: **Nmap**, **Hydra**, **sqlmap**, **curl**, and **feroxbuster**. Their presence strongly indicated active attack behavior and warranted deeper investigation.

Hydra traffic targeted the `/rest/user/login` endpoint. This revealed that the endpoint was exposed and accepting authentication attempts. While reviewing the login attempts, I identified one **successful login** with HTTP response code `200`, among many `401` failures, confirming that the attacker brute-forced a valid user account within the application. The logs did not reveal which specific account was compromised, but the attacker's success was confirmed based on the response size and status.

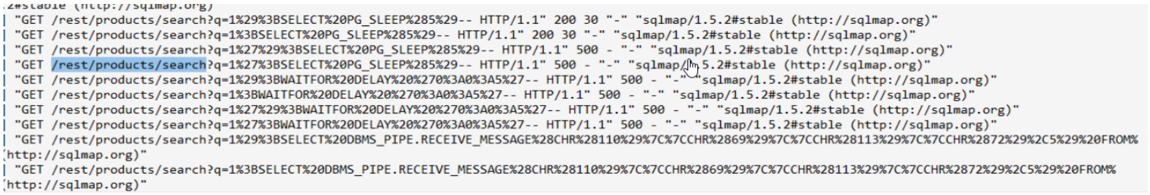


```
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:32 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
```

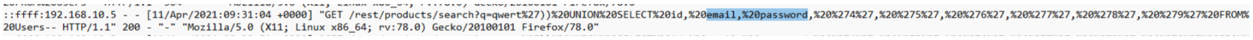


```
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 200 831 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
```

Next, I examined whether sqlmap identified exploitable vulnerabilities. The access logs show that sqlmap was used against `/rest/products/search`, specifically targeting the `q` parameter. Based on the types of payloads observed, sqlmap successfully detected SQL injection and proceeded to enumerate and extract information. Some common words I am looking that attackers will try to retrieve are “names, credit cards numbers, emails, password” and luckily I was able to confirm that the attacker retrieved **email and password pairs**, indicating exfiltration of sensitive user data.

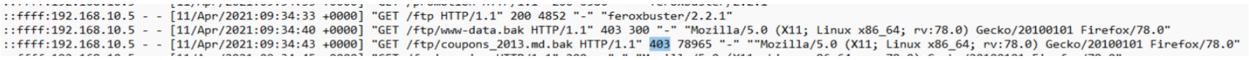


```
.2#stable (http://sqlmap.org)
| "GET /rest/products/search?q=1%29%3BSELECT%20PG_SLEEP%285%29-- HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%3BSELECT%20PG_SLEEP%285%29-- HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%27%29%3BSELECT%20PG_SLEEP%285%29-- HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%27%3BSELECT%20PG_SLEEP%285%29-- HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%29%3BWAITFOR%20DELAY%20%270%3A0%3A5%27-- HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%3BWAITFOR%20DELAY%20%270%3A0%3A5%27-- HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%27%29%3BWAITFOR%20DELAY%20%270%3A0%3A5%27-- HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%27%3BWAITFOR%20DELAY%20%270%3A0%3A5%27-- HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
| "GET /rest/products/search?q=1%29%3BSELECT%20DBMS_PIPE.RECEIVE_MESSAGE%28CHR%28110%29%7C%7CCHR%2869%29%7C%7CCHR%28113%29%7C%7CCHR%2872%29%2C5%29%20FROM%
(http://sqlmap.org)"
| "GET /rest/products/search?q=1%3BSELECT%20DBMS_PIPE.RECEIVE_MESSAGE%28CHR%28110%29%7C%7CCHR%2869%29%7C%7CCHR%28113%29%7C%7CCHR%2872%29%2C5%29%20FROM%
(http://sqlmap.org)"
```



```
::ffff:192.168.10.5 - - [11/Apr/2021:09:31:04 +0000] "GET /rest/products/search?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%
20Users-- HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Next, the attacker also used feroxbuster to perform forced browsing for hidden paths and discovered the `/ftp` directory. Their attempts to access files directly via HTTP resulted in `403 Forbidden` responses. This suggests that the directory was exposed but restricted.

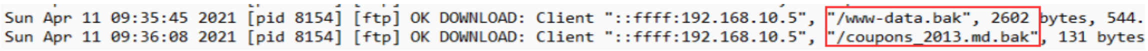


```
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /ftp HTTP/1.1" 200 4852 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:40 +0000] "GET /ftp/www-data.bak HTTP/1.1" 403 300 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:43 +0000] "GET /ftp/coupons_2013.md.bak HTTP/1.1" 403 78965 "-" ""Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

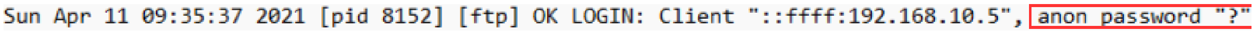
Correlating with the vsftpd logs, I observed that the attacker attempted an alternative method by logging in via FTP. The FTP service allowed **anonymous authentication**, which is a common misconfiguration. With this access, the attacker successfully downloaded two files:

- `/www-data.bak`
- `/coupons_2013.md.bak`

The downloads were confirmed in the vsftpd logs. This indicates that the attacker used the misconfigured FTP service to obtain potentially sensitive backup data



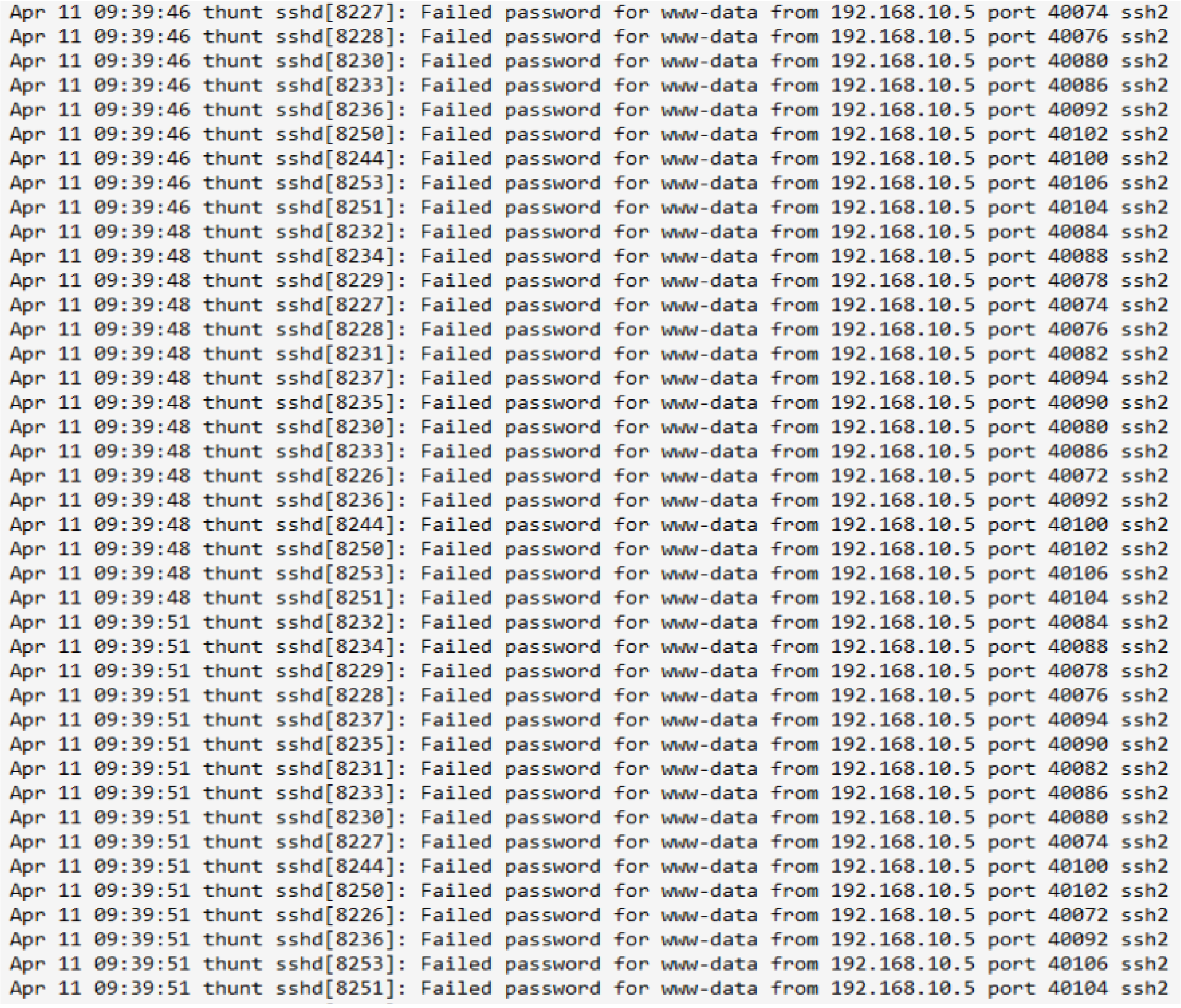
```
Sun Apr 11 09:35:45 2021 [pid 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/www-data.bak", 2602 bytes, 544.
Sun Apr 11 09:36:08 2021 [pid 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/coupons_2013.md.bak", 131 bytes
```



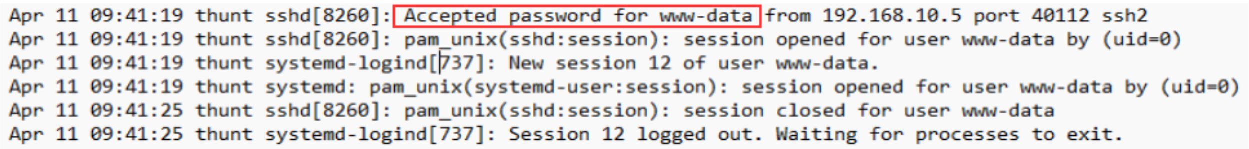
```
Sun Apr 11 09:35:37 2021 [pid 8152] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "?"
```

Finally, the authentication log revealed a large number of failed SSH login attempts targeting the `www-data` user, followed by a **successful login** originating from the attacker's IP. This brute-force pattern aligns with the attacker's previous behavior.

The most plausible explanation is that the attacker leveraged credentials obtained via SQL injection or from the downloaded `.bak` files to build a password list, which they then used in the SSH brute force attempt. Once authenticated, they initiated a shell session and attempted privilege escalation using `su` and `sudo`.



```
Apr 11 09:39:46 thunt sshd[8227]: Failed password for www-data from 192.168.10.5 port 40074 ssh2
Apr 11 09:39:46 thunt sshd[8228]: Failed password for www-data from 192.168.10.5 port 40076 ssh2
Apr 11 09:39:46 thunt sshd[8230]: Failed password for www-data from 192.168.10.5 port 40080 ssh2
Apr 11 09:39:46 thunt sshd[8233]: Failed password for www-data from 192.168.10.5 port 40086 ssh2
Apr 11 09:39:46 thunt sshd[8236]: Failed password for www-data from 192.168.10.5 port 40092 ssh2
Apr 11 09:39:46 thunt sshd[8250]: Failed password for www-data from 192.168.10.5 port 40102 ssh2
Apr 11 09:39:46 thunt sshd[8244]: Failed password for www-data from 192.168.10.5 port 40100 ssh2
Apr 11 09:39:46 thunt sshd[8253]: Failed password for www-data from 192.168.10.5 port 40106 ssh2
Apr 11 09:39:46 thunt sshd[8251]: Failed password for www-data from 192.168.10.5 port 40104 ssh2
Apr 11 09:39:48 thunt sshd[8232]: Failed password for www-data from 192.168.10.5 port 40084 ssh2
Apr 11 09:39:48 thunt sshd[8234]: Failed password for www-data from 192.168.10.5 port 40088 ssh2
Apr 11 09:39:48 thunt sshd[8229]: Failed password for www-data from 192.168.10.5 port 40078 ssh2
Apr 11 09:39:48 thunt sshd[8227]: Failed password for www-data from 192.168.10.5 port 40074 ssh2
Apr 11 09:39:48 thunt sshd[8228]: Failed password for www-data from 192.168.10.5 port 40076 ssh2
Apr 11 09:39:48 thunt sshd[8231]: Failed password for www-data from 192.168.10.5 port 40082 ssh2
Apr 11 09:39:48 thunt sshd[8237]: Failed password for www-data from 192.168.10.5 port 40094 ssh2
Apr 11 09:39:48 thunt sshd[8235]: Failed password for www-data from 192.168.10.5 port 40090 ssh2
Apr 11 09:39:48 thunt sshd[8230]: Failed password for www-data from 192.168.10.5 port 40080 ssh2
Apr 11 09:39:48 thunt sshd[8233]: Failed password for www-data from 192.168.10.5 port 40086 ssh2
Apr 11 09:39:48 thunt sshd[8226]: Failed password for www-data from 192.168.10.5 port 40072 ssh2
Apr 11 09:39:48 thunt sshd[8236]: Failed password for www-data from 192.168.10.5 port 40092 ssh2
Apr 11 09:39:48 thunt sshd[8244]: Failed password for www-data from 192.168.10.5 port 40100 ssh2
Apr 11 09:39:48 thunt sshd[8250]: Failed password for www-data from 192.168.10.5 port 40102 ssh2
Apr 11 09:39:48 thunt sshd[8253]: Failed password for www-data from 192.168.10.5 port 40106 ssh2
Apr 11 09:39:48 thunt sshd[8251]: Failed password for www-data from 192.168.10.5 port 40104 ssh2
Apr 11 09:39:51 thunt sshd[8232]: Failed password for www-data from 192.168.10.5 port 40084 ssh2
Apr 11 09:39:51 thunt sshd[8234]: Failed password for www-data from 192.168.10.5 port 40088 ssh2
Apr 11 09:39:51 thunt sshd[8229]: Failed password for www-data from 192.168.10.5 port 40078 ssh2
Apr 11 09:39:51 thunt sshd[8228]: Failed password for www-data from 192.168.10.5 port 40076 ssh2
Apr 11 09:39:51 thunt sshd[8237]: Failed password for www-data from 192.168.10.5 port 40094 ssh2
Apr 11 09:39:51 thunt sshd[8235]: Failed password for www-data from 192.168.10.5 port 40090 ssh2
Apr 11 09:39:51 thunt sshd[8231]: Failed password for www-data from 192.168.10.5 port 40082 ssh2
Apr 11 09:39:51 thunt sshd[8233]: Failed password for www-data from 192.168.10.5 port 40086 ssh2
Apr 11 09:39:51 thunt sshd[8230]: Failed password for www-data from 192.168.10.5 port 40080 ssh2
Apr 11 09:39:51 thunt sshd[8227]: Failed password for www-data from 192.168.10.5 port 40074 ssh2
Apr 11 09:39:51 thunt sshd[8244]: Failed password for www-data from 192.168.10.5 port 40100 ssh2
Apr 11 09:39:51 thunt sshd[8250]: Failed password for www-data from 192.168.10.5 port 40102 ssh2
Apr 11 09:39:51 thunt sshd[8226]: Failed password for www-data from 192.168.10.5 port 40072 ssh2
Apr 11 09:39:51 thunt sshd[8236]: Failed password for www-data from 192.168.10.5 port 40092 ssh2
Apr 11 09:39:51 thunt sshd[8253]: Failed password for www-data from 192.168.10.5 port 40106 ssh2
Apr 11 09:39:51 thunt sshd[8251]: Failed password for www-data from 192.168.10.5 port 40104 ssh2
```



```
Apr 11 09:41:19 thunt sshd[8260]: Accepted password for www-data from 192.168.10.5 port 40112 ssh2
Apr 11 09:41:19 thunt sshd[8260]: pam_unix(sshd:session): session opened for user www-data by (uid=0)
Apr 11 09:41:19 thunt systemd-logind[737]: New session 12 of user www-data.
Apr 11 09:41:19 thunt systemd: pam_unix(systemd-user:session): session opened for user www-data by (uid=0)
Apr 11 09:41:25 thunt sshd[8260]: pam_unix(sshd:session): session closed for user www-data
Apr 11 09:41:25 thunt systemd-logind[737]: Session 12 logged out. Waiting for processes to exit.
```

Summary of Attack Path

- Reconnaissance using Nmap to identify open services, including FTP
- Hydra brute force on `/rest/user/login`, resulting in one successful application login

- SQL injection exploitation on `/rest/products/search` using sqlmap, leading to extraction of email/password pairs
- Forced browsing with feroxbuster, discovering the `/ftp` directory
- Anonymous FTP login and download of sensitive files (`www-data.bak`, `coupons_2013.md.bak`)
- SSH brute force on `www-data`, ultimately successful
- Post-compromise actions including shell access and privilege escalation attempts