SECURITY OPERATIONS CENTER

Incident Report

Internal Host Compromise — Web, FTP, and SSH Activity: Backup and User Credentials Exfiltration

Data source: index=lab05 | Analyst: David Belayev Gal | Primary activity date: 4/11/2021

SEVERITY: HIGH

Internal host 192.168.10.5 brute-forced both the web application's login endpoint and SSH, and exploited a SQL injection flaw on the web app. Anonymous local FTP access and backup-file exposure over FTP were also observed, alongside credential exfiltration via SQL injection.

Contents

Executive Summary

On 4/11/21, an internal host targeted two systems. These targets ran a web application connected to an SQL database, an FTP service, and SSH.

Initial Access & Execution

- The attacker first conducted reconnaissance on both targets.
- Next, they brute-forced the web application's login endpoint.
- They also brute-forced the web server user's SSH credentials.
- Then, they exploited an SQL injection vulnerability to execute commands on the underlying host.

Data Access & Exfiltration

- The attacker deployed a web shell to retrieve system account information (/etc/passwd, including password hashes).
- They exfiltrated application user credentials via SQL.
- They exfiltrated backup files using FTP.

This activity reflects a complete attack chain: scanning, credential access, and data exfiltration. The attacker relied primarily on public tools (Nmap, Hydra, sqlmap, feroxbuster, and curl).

Scope of Impact

Asset	Role	Impact
Web server	Public-facing web app	Login credentials brute-forced. Used to gain arbitrary command execution.
FTP service	File-transfer service	Anonymous local access confirmed. Used to exfiltrate system backup files.
SSH service	Remote shell access	www-data account compromised via credential brute-forcing.
Underlying OS	Host operating system	System account list and password hashes (/etc/passwd) extracted.

Timeline & Findings

Chronological Timeline

All events happened on 4/11/21

Time	Attack Phase	Event Description	Artifact
08:15:58 - 09:08:34	Initial Access	Successful anonymous FTP logins after initial failures	FTP
09:08:35	Reconnaissance	Web server scanning	Nmap
09:16:31	Credential Access	Brute-forced web app login	Hydra
09:20:32	Execution	Admin panel accessed; tested web-shell	Web-shell
09:29:15 - 09:32:51	Exfiltration	Injected SQL to exfiltrate password hashes and user credentials	Sqlmap, Curl
09:34:33	Reconnaissance	Discovered available web URIs	Feroxbuster
09:35:45	Exfiltration	Exfiltrated backup files	FTP
09:41:19	Credential Access	Gained account access via SSH brute-force	Syslog

Attacker's Likely Objective

Credential theft and exfiltration of system backup files.

Indicators of Compromise (IOC) Matrix

Proofs of Work for each IoC are provided in later sections of the report.

Type	Value	Context
Source IP	192.168.10.5	Primary attacker IP. Origin of reconnaissance, brute-force (web\SSH), SQL injection and directory enumeration.
Source IP (local)	127.0.0.1	Initial anonymous FTP access. Indicates potential pre-established foothold.
Referrer IP	192.168.10.4	Identified in HTTP Referrer headers. Potential origin or pivot point for lateral movement.
URI	/rest/user/login	Target of Hydra web login brute-force attack.
URI	/rest/user/whoami	Target of web-shell command execution testing. Potential staging for lateral movement.
URI	/rest/user/data-export	Accessed data export endpoint. Suspected exfiltration vector.
URI	/rest/products/search	SQL injection entry point.
URI	/rest/continue-code/*	Target of HTTP PUT request containing a suspected base64-encoded payload.
HTTP method	PROPFIND	Non-standard WebDAV method used for directory and resource fingerprinting.
File	/etc/passwd	System account file extracted via SQL injection command execution.
Auth event	SSH logins	Repeated authentication failures followed by a successful login.
User-Agent	Nmap	Network scanner user-agent used for service and configuration fingerprinting.
User-Agent	Hydra	Online brute-force tool user-agent targeting web login endpoints.
User-Agent	sqlmap	Automated SQL injection utility user-agent.
User-Agent	curl	Command-line HTTP client user-agent used for payload delivery and exfiltration.
FTP artifact	www-data.bak coupons_2013.md.bak	System backup archives exfiltrated via FTP

Environment Overview

Started at *04/11/2021, 08:13:32*

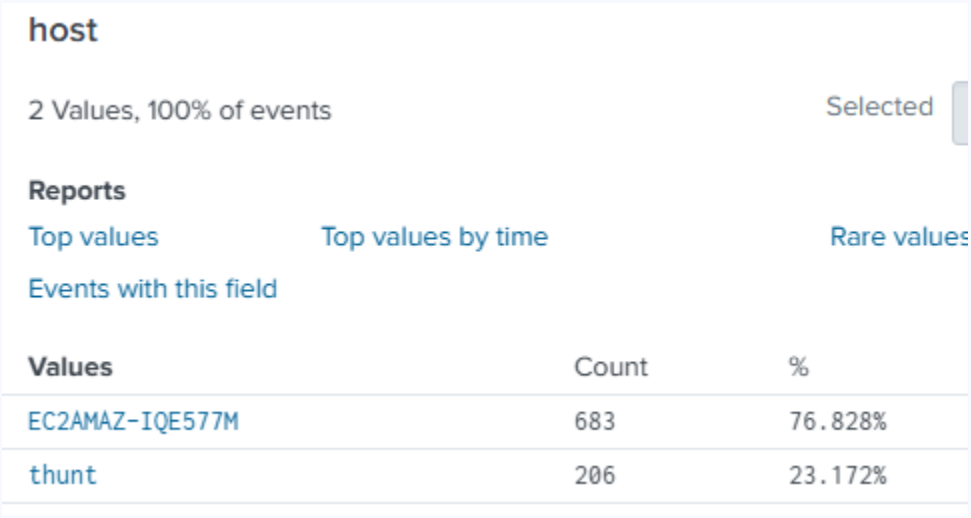
Finished at *04/11/2021, 09:43:37*

```
index="lab05"
| stats min(_time) as mintime, max(_time) as maxtime
| convert ctime(mintime), ctime(maxtime)
```

mintime	maxtime
04/11/2021 08:13:32	04/11/2021 09:34:52

Log source types are *Web, FTP and Auth (SSH)*

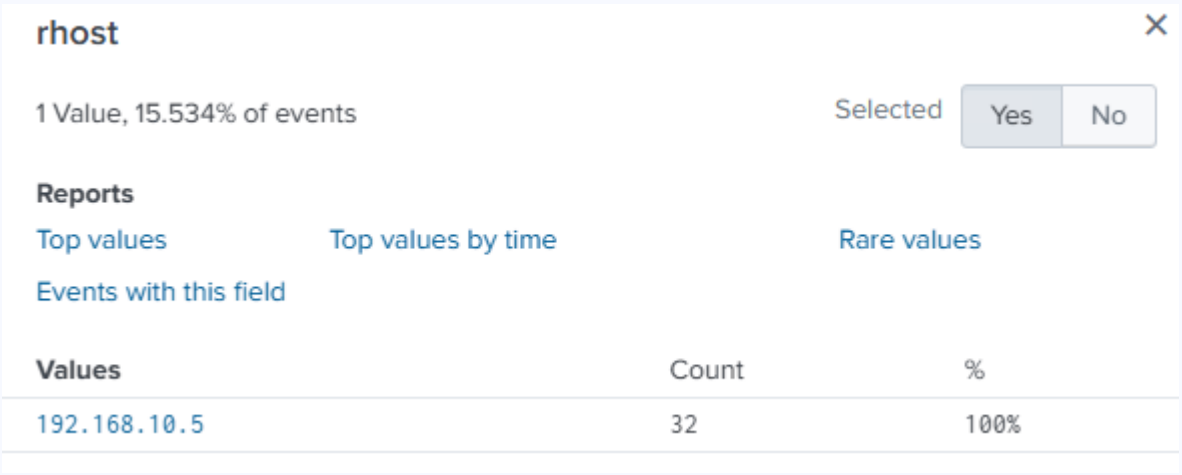
Hosts are *EC2AMAZ-IQ577M* and *thunt*



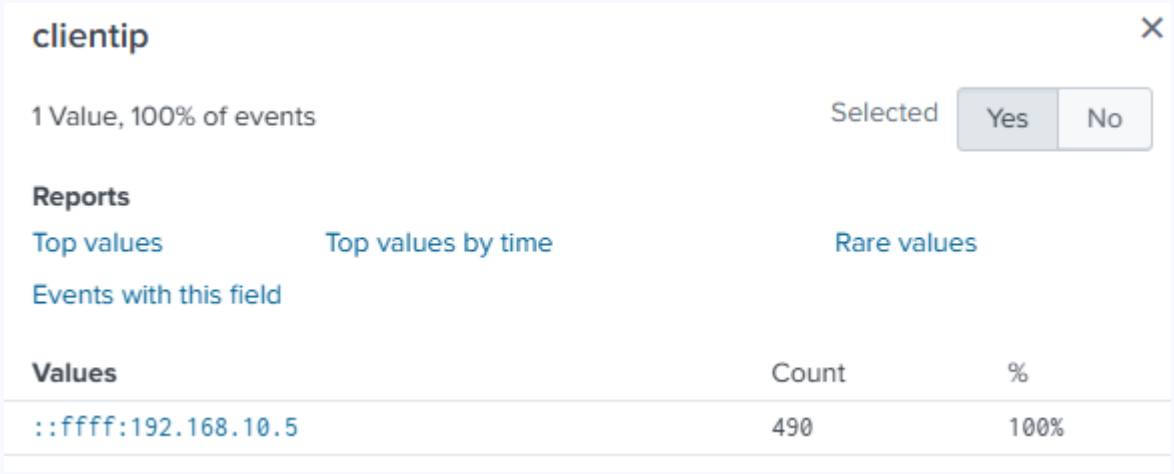
Attack Source:

- *Most traffic originated from 192.168.10.5.*

```
index="lab05" sourcetype="syslog" |
fields rhost
```



```
index="lab05" sourcetype="access_combined"
```



clientip

1 Value, 100% of events

Selected Yes No

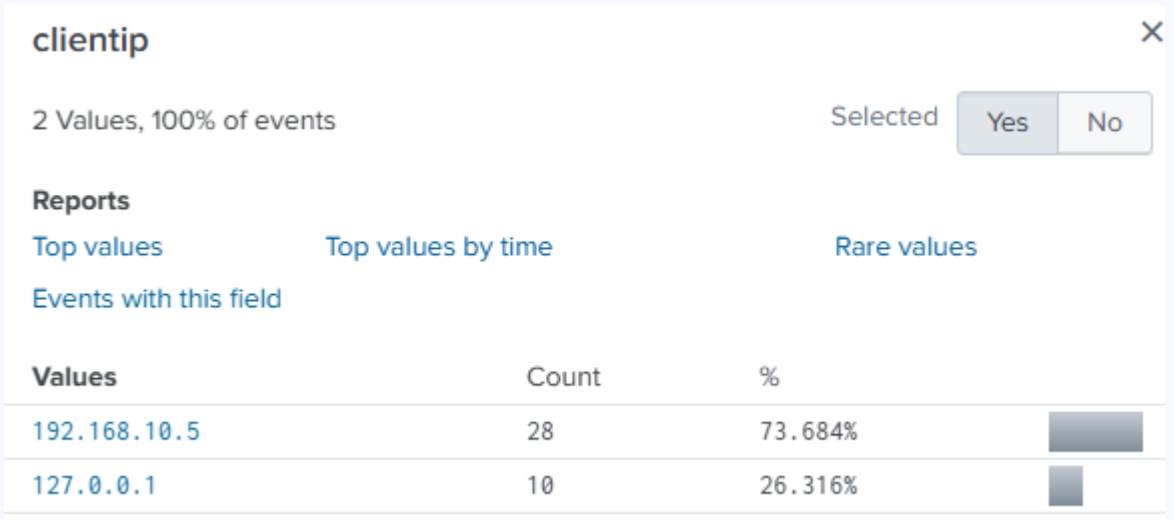
Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
::ffff:192.168.10.5	490	100%

```
index="lab05" sourcetype=vsftpd-too_small
| fields clientip
```



clientip

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
192.168.10.5	28	73.684%
127.0.0.1	10	26.316%

- *Only 10 events (FTP) include a different source IP, 127.0.0.1.*
- *Some web events include a referrer header with the value 192.168.10.4, indicating a potential compromise of additional hosts on the network.*

```
index="lab05" sourcetype="access_combined"
| dedup referer
| table referer
```

referer ⇕
-
http://192.168.10.4/

Web Activity

Initial Overview

The web server is hosted on EC2AMAZ-IQ577M. Of 645 total web requests, 300 targeted /rest/user/login alone. The vast majority of the /rest/user/login events carry an HTTP status of 500 or 401, indicating a potential brute-force \ directory mapping activity.

```
index="lab05" sourcetype="access_combined"
| fields uri_path
| stats count by uri_path
| sort - count
```

uri_path	count
/rest/user/login	300
/rest/products/search	91
/rest/user/whoami	68
/rest/admin/application-configuration	24

```
index="lab05" sourcetype="access_combined"
| stats count by status
| sort - count
| where count > 2
```

status	count
200	195
500	185
401	143
304	115

Other notable paths include:

```
index="lab05" sourcetype="access_combined"
| dedup uri
| table method useragent uri
```

URL	Screenshots
SQL Injection path: /rest/products/search?q=’	/rest/products/search?q=%27))%20UNION%20SELECT%20%271%27,%20%272%27,%20%273%27,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- /rest/products/search?q=%28SELECT%20%28CASE%20WHEN%20%285972%3D5972%29%20THEN%201%20ELSE%20%28SELECT%208493%20UNION%20SELECT%202338%29%20END%29%29 /rest/products/search?q=%28SELECT%20%28CASE%20WHEN%20%288195%3D8761%29%20THEN%201%20ELSE%20%28SELECT%208761%20UNION%20SELECT%203788%29%20END%29%29 /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 1&QKqcp74 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS") </script>',table_name FROM information_schema.tables WHERE 2>1- -/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')# qwert')) UNION SELECT id, email, password, '4', '5', '6', '7', '8', '9' FROM Users *Examples of URL-decoded queries (w\ CyberChef)*
/rest/user/whoami	/rest/user/whoami
/rest/user/data-export	/rest/user/data-export
PUT request with base64 parameter: /rest/continue-code/apply/6R8YrZYgwjv…	'6R8YrZYgwj1y2qMBPWQmEK8knv0pPT9iXp07Le4pOlRxXzbao3DV5J69NbXr *VirusTotal didn’t flag this as malicious and Base64 Decoding didn’t result in anything meaningful*
Backup files: /ftp/coupons_2013.md.bak /ftp/www-data.bak	/ftp /ftp/coupons_2013.md.bak /ftp/www-data.bak
Nmap-generated probe paths, including PROPFIND requests.	GET /Nmap/folder/check1618132114 GET /NmapUpperCheck1618132114 GET /nmaplowercheck1618132114 GET /.git/HEAD PROPFIND / POST /sdk
Badly encoded URL: /nice%20ports%2C/Tri%6Eity.txt%2ebak	/nice%20ports%2C/Tri%6Eity.txt%2ebak
Administrative panels: /rest/admin/application-*	/rest/admin/application-configuration /rest/admin/application-version

User-Agent Analysis

The User-Agent field confirms that this activity was tool-driven rather than manual browsing:

useragent
Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
feroxbuster/2.2.1
curl/7.74.0
sqlmap/1.5.2#stable (http://sqlmap.org)
Mozilla/5.0 (Hydra)
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
-

Nmap

Nmap traffic against the web server includes PROPFIND requests and configuration-probing scripts, consistent with automated service and directory fingerprinting ahead of the later brute-force and injection activity. This scanning establishes the reconnaissance phase of the attack chain and lines up with the earliest timestamps in the timeline.

```
index="lab05" sourcetype="access_combined"
| search useragent=*Nmap*
| dedup uri
| table uri
```

uri
/
/Nmap/folder/check1618132114
/NmapUpperCheck1618132114
/nmaplowercheck1618132114
/sdk
/.git/HEAD

Hydra

Hydra was used to brute-force the login endpoint. The web campaign started at 09:15:03 with a successful login from a browser. At 09:16:27 an automated brute-force Hydra session began, successfully breaking at 09:16:31. Four minutes later, a follow-up login occurred from the same source address using a standard browser User-Agent — consistent with an operator manually taking over the compromised session.

```
index="lab05" sourcetype="access_combined"
| search useragent=*Hydra*
| where status >= 200 AND status < 400
| table _time uri status
```

_time	uri	status	useragent
2021-04-11 09:15:03	/rest/user/login	200	Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
2021-04-11 09:16:31	/rest/user/login	200	Mozilla/5.0 (Hydra)
2021-04-11 09:20:43	/rest/user/login	200	Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

```
index="lab05" sourcetype="access_combined" earliest="04/11/2021:09:15:04" latest="04/11/2021:09:16:31"
| search uri=*rest/user/login*
| stats count by status useragent
```

status	useragent	count
401	Mozilla/5.0 (Hydra)	100
500	Mozilla/5.0 (Hydra)	112

Sqlmap

Traffic confirms automated SQL injection testing. The first malicious request was observed on 4/11/21 at 09:29:15 against /rest/products/search?q=. Decoding the request parameter shows the payload was not limited to testing for injection — it also exfiltrated table data and executed a shell command to retrieve the full list of system users and password hashes from /etc/passwd.

```
index="lab05" sourcetype="access_combined"
| search useragent=*sqlmap*
```

General query used to scan for malicious sqlmap activity.

```
index="lab05" sourcetype="access_combined"
| search useragent=*sqlmap* uri=*passwd*
| table _time uri
```

_time	uri
2021-04-11 09:29:15	/rest/products/search?q=1&QKqc=7074%20AND%201%3D1%20UNION%

```
1&QKqcp74 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")
</script>',table_name FROM information_schema.tables WHERE 2>1-
-/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#
```

Curl

Curl was used to exfiltrate web application user credentials following initial vulnerability validation with sqlmap. Once automated testing confirmed the SQL injection flaw, the attacker leveraged curl to issue direct HTTP requests and systematically extract database records.

```
index="lab05" sourcetype="access_combined"
| search useragent=*curl*
| table _time uri
```

_time	
2021-04-11 09:32:51	SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users

```
qwert')) UNION SELECT id, email, password, '4', '5', '6', '7',
'8', '9' FROM Users
```

Feroxbuster

Feroxbuster was used to enumerate additional content on the server. There are no logs showing that the attacker pursued these URIs other than ftp (403 - Unauthorized; Attacker exfiltrated data via ftp later directly connecting to the service).

```
index="lab05" sourcetype="access_combined"
| search useragent=*feroxbuster*
| table _time status uri
```

_time	status	uri
2021-04-11 09:34:33	200	/ftp
2021-04-11 09:34:33	200	/promotion
2021-04-11 09:34:33	200	/backup
2021-04-11 09:34:33	200	/admin
2021-04-11 09:34:33	200	/login
2021-04-11 09:34:33	200	/administartion
2021-04-11 09:34:33	500	/api
2021-04-11 09:34:33	200	/3e72ead66df04ca5bff7c9b741883cfbd30
2021-04-11 09:34:33	200	/a54372a1404141fe8842ae5c029a00e3

```
index="lab05" sourcetype="access_combined"
| search uri=*ftp*
| table _time status uri
| sort _time
```

_time	status	uri
2021-04-11 09:34:33	200	/ftp
2021-04-11 09:34:40	403	/ftp/www-data.bak
2021-04-11 09:34:43	403	/ftp/coupons_2013.md.bak

Authentication Activity

Rapid, repeated authentication failures on host ‘thunt’ indicate an automated brute-force campaign. The attack succeeded, resulting in an authenticated SSH session and account compromise.

```
index="lab05" sourcetype="syslog"
| search status IN ("Accepted", "Failed")
| stats min(_time) as mintime, max(_time) as maxtime, count by status
| convert ctime(mintime), ctime(maxtime)
| table status mintime maxtime count
```

status	mintime	maxtime	count
Accepted	04/11/2021 09:41:19	04/11/2021 09:41:32	2
Failed	04/11/2021 09:38:29	04/11/2021 09:39:51	98

FTP Activity

FTP (vsftpd) runs on EC2AMAZ-IQ577M. It was accessed from two distinct contexts:

- **127.0.0.1:** failed authentication attempts followed by a successful anonymous login at 08:15:58. This session starts the attack sequence as available in the index. This potentially indicates that the attacker already had a foothold in the system.

```
index="lab05" sourcetype="vsftpd-too_small"
| search clientip=*127.0.0.1* operation=*LOGIN*
| table _time operation message
| sort _time
```

_time	operation	message
2021-04-11 08:13:40	[anonymous] FAIL LOGIN	[anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
2021-04-11 08:15:14	[anonymous] FAIL LOGIN	[anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
2021-04-11 08:15:33	[anonymous] FAIL LOGIN	[anonymous] FAIL LOGIN: Client "::ffff:127.0.0.1"
2021-04-11 08:15:58	[ftp] OK LOGIN	[ftp] OK LOGIN: Client "::ffff:127.0.0.1", anon password "?"
2021-04-11 08:18:07	[ftp] OK LOGIN	[ftp] OK LOGIN: Client "::ffff:127.0.0.1", anon password "ls"

- **192.168.10.5:** FTP activity with a successful login established. Only after the web server activity ends does the attacker return to FTP to exfiltrate backup data files — /www-data.bak and /coupons_2013.md.bak.

```
index="lab05" sourcetype="vsftpd-too_small"
| search clientip=*192.168.10.5* operation=*OK*
| table _time message
| sort _time
```

_time	message
2021-04-11 08:29:34	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
2021-04-11 08:29:34	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
2021-04-11 08:29:35	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
2021-04-11 09:08:34	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
2021-04-11 09:08:34	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
2021-04-11 09:08:35	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
2021-04-11 09:35:37	[ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "?"
2021-04-11 09:35:45	[ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/www-data.bak", 2602 bytes, 544.81Kbyte/sec
2021-04-11 09:36:08	[ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/coupons_2013.md.bak", 131 bytes, 3.01Kbyte/sec

Incident Summary

What Happened?

On 4/11/21, between 08:13 and 09:41, an internal host scanned and compromised target servers hosting web (with SQL database), FTP and SSH services.

Following a reconnaissance campaign, the attacker brute-forced credentials for both the web application and SSH. They exploited a SQL injection vulnerability to execute host commands and extract system and web user credentials. Finally, the attacker downloaded two backup files over FTP.

IP Addresses Involved

- **192.168.10.5** — primary attacker address, internal (reconnaissance, brute force, SQL injection, enumeration, FTP, SSH auth attempts).
- **192.168.10.4** — referrer address associated with the attacker's traffic; possible lateral-movement pivot, unconfirmed.
- **127.0.0.1** — separate anonymous local FTP access; relationship to the main incident unconfirmed, suspected possible prior access.

Tools and Techniques

- Nmap
- Hydra
- Sqlmap
- Curl
- Feroxbuster
- Brute-force (SSH and web)
- Anonymous FTP access
- Web-shell

Unauthorized Access Gained

Brute-force campaigns against both /rest/user/login and SSH succeeded, and the SQL injection vulnerability was successfully exploited to execute commands and retrieve /etc/passwd contents, including password hashes. Backup files were downloaded via FTP. This constitutes confirmed unauthorized access on multiple services and a credential-exposure and data-exfiltration event.

Recommendations

- Enforce rate limiting on /rest/user/login to prevent brute-force attacks.
- Consider MFA logic for web users.
- Remediate the SQL injection vulnerability in /rest/products/search (and audit related endpoints) using parameterized queries.
- Ensure the application account does not have OS-level command execution privileges.
- Disable anonymous FTP access and unused HTTP methods such as PROPFIND.
- Remove or restrict access to backup files and other sensitive artifacts from web- and FTP-accessible directories.
- Rotate all credentials present in /etc/passwd on the affected host and force password resets for any exposed application accounts.
- Harden SSH access: enforce key-based authentication, disable password login if not required, and enforce account lockout / rate limiting.
- Deploy a WAF or equivalent detection for known attacker tool signatures (Nmap, Hydra, sqlmap, feroxbuster User-Agents) and alert on high-volume bursts to authentication endpoints.
- Investigate and confirm the relationship between the 192.168.10.4 referrer and the 127.0.0.1 anonymous FTP session to rule out lateral movement.