

Juicy Details

Introducción

El presente informe documenta el análisis realizado sobre los registros entregados por el equipo de TI de **Juicy Shop**, tras detectar actividad maliciosa dentro de su infraestructura. El objetivo de este análisis es identificar las técnicas utilizadas por el atacante, los endpoints comprometidos, la información exfiltrada y el impacto potencial del incidente.

Cronología del Ataque

A partir de los archivos de registro (`access.log`) se identificaron las siguientes fases del ataque, ejecutadas el **11 de abril de 2021** desde la dirección IP **192.168.10.5**:

Sesión 1 — Reconocimiento / Escaneo (11/Apr/2021 09:08:29)

Evidencia: el primer evento registrado es un escaneo desde la IP `192.168.10.5` a las **09:08:29**; en los logs se detecta actividad típica de mapeo de puertos/servicios.

- El atacante inició un escaneo de reconocimiento empleando **Nmap**, con el fin de identificar servicios y puertos expuestos.
- Esta fase le permitió descubrir vectores de ataque en la superficie de exposición del sistema.

Acción recomendada inmediata:

- Revisar/aislar la IP origen si es externa; si es interna, iniciar trazado de origen y escalado a TI.
- Habilitar alertas de escaneo en IDS/IPS y limitar acceso a servicios administrativos desde redes no confiables.

```
(zikuta@zikuta)-[~/Desktop/juicy]
$ cat access.log
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:29 +0000] "GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0" 200 1924 "-" "-"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:34 +0000] "POST / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /.git/HEAD HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "POST /sdk HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /nmaplowercheck1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /NmapUpperCheck1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /Nmap/folder/check1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "POST / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Sesión 2 — Fuzzing / Enumeración de directorios (09:08:30 – 09:15:35)

Evidencia: múltiples peticiones HTTP con user-agent Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 y patrones de requests típicos de feroxbuster/dirbuster; duración hasta **09:15:35**.

```
) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:03 +0000] "GET /rest/products/search?q= HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:03 +0000] "GET /rest/basket/6 HTTP/1.1" 200 154 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:03 +0000] "GET /api/Quantities/ HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:06 +0000] "GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:06 +0000] "GET /rest/basket/6 HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:10 +0000] "GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:16 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:17 +0000] "GET /rest/continue-code HTTP/1.1" 200 79 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:35 +0000] "GET /rest/saveLoginIp HTTP/1.1" 200 358 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:35 +0000] "GET /rest/products/search?q= HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Qué pasó:

- Se ejecutó un escaneo de directorios (fuzzing) para descubrir endpoints sensibles.
- Resultado relevante: descubrimiento del endpoint de autenticación `/rest/user/login`.

Por qué importa:

- El descubrimiento del panel de login es lo que permitió al atacante pasar a la fase de acceso directo (fuerza bruta).

Acción recomendada inmediata:

- Revisar logs de 404/403 y endpoints enumerados; colocar reglas WAF para bloquear patrones de fuzzing (cabeceras, frecuencia).
- Implementar rate limiting y CAPTCHA en endpoints de login.

Sesión 3 — Fuerza bruta contra `/rest/user/login` (09:16:27 – 09:16:31; login exitoso a 09:16:31 +0000)

Evidencia: ráfaga de **144** intentos contra `/rest/user/login` en ~3 segundos, herramienta identificada: **Hydra**; registro de un inicio de sesión exitoso a las **09:16:31 +0000**.


```

::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1 HTTP/1.1" 200 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1&QKc=-7074&ZGwz=0123456789abcdefghijklmnopqrstuvwxyz%3Cscript%3Ealert(2)&R2XS5K2&29Y3CN2&Script3EK2?&2cat_name%2FROMK%2Finformation_schema.tables%20WHERE%20%3E1%-&2FK&A2&2PK3BX&2OEX&C2&xpp_cmdshe1X&2&827cat%20.%2F.%2F.%2F&2Fc&2Fnss&2D7&29K23 HTTP/1.1" 200 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1 HTTP/1.1" 200 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=6813 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1 %32%27%20&%C.%2C%29%3C HTTP/1.1" 500 - "-" sqlmap/1.5.2#stable http://sqlmap.org)
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=5076-5075 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1.9xgh HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%27%20jctaK3CN2%32%23ETUfSMe HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%29%20AND%20374%3D9627%20AND%20%288054%3D8054 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%29%20AND%209700%3D9700%20AND%20%283503%3D3503 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$20AND%206384%3D1910 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$20AND%209700%3D9700 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$20AND%208263%3D9654-%20qXo5 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$20AND%209700%3D9700-%20jEIr HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$27%29%20AND%208657%3D9050%20AND%20%28%27Hvpr%27%3D%27Hvpr HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$27%29%20AND%209700%3D9700%20AND%20%28%27YGA%27%3D%27YGA HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$27%20AND%203798%3D2857%20AND%20%27fSuk%27%3D%27fSuk HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%1$27%20AND%209700%3D9700%20AND%20%27IyBx%27%3D%27IyBx HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /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 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=%28SELECT%20%28CASE%20WHEN%20%285972%3D5972%29%20THEN%201%20ELSE%20%28SELECT%205972%20UNION%20SELECT%203788%29%20END%29%29 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"

```

Qué pasó

- El atacante explotó un parámetro vulnerable (q) en el endpoint de búsqueda para ejecutar consultas SQL arbitrarias.
- Intentos de volcado (dump) de la base de datos; éxito en extraer columnas sensibles (email , password).

Por qué importa:

- Exfiltración de credenciales y correos compromete la privacidad de usuarios y posibilita más acceso (credential stuffing en otros servicios).
- Indica falta de input sanitization y/o uso de queries parametrizadas.

Acción recomendada inmediata:

- Poner el endpoint fuera de línea o aplicar regla WAF de bloqueo para patrones `UNION SELECT` , `OR 1=1` , etc.
- Auditar la base de datos por consultas inusuales y rotar credenciales de usuarios afectados.
- Habilitar monitoreo de integridad en tablas sensibles.

Sesión 5 — Automatización de extracción con cURL (09:29:58 – 09:32:51)

Se observó que el atacante automatizó el ataque mediante `curl` (versión 7.74.0), enviando consultas tipo `UNION SELECT` para intentar exfiltrar columnas de la tabla `Users`, incluyendo `id`, `email` y `password`. Las solicitudes se registraron entre las 09:29:58 y 09:32:51 del 11/Apr/2021."

Evidencia: múltiples requests con `curl/7.74.0` realizando `UNION SELECT` y recuperando columnas; las entradas en `access.log` muestran respuestas con datos.

```

c:\ffff:192.168.10.5 - [11/Apr/2021:09:29:58 +0000] "GET /rest/products/search?q=%27%20UNION%20SELECT%20%27%27%20%27%27%27%20%27%27%27%27%20FROM%20Users- HTTP/1.1" 200 - "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
c:\ffff:192.168.10.5 - [11/Apr/2021:09:30:00 +0000] "GET /rest/products/search?q=%27%20UNION%20SELECT%20%27%27%27%20%27%27%27%27%20%27%27%27%27%20%27%27%27%27%20%27%27%27%27%20FROM%20Users- HTTP/1.1" 304 - "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
c:\ffff:192.168.10.5 - [11/Apr/2021:09:31:04 +0000] "GET /rest/products/search?q=wert%27%20UNION%20SELECT%20id,%20email,%20password,%20%27%27%27%20%27%27%27%27%20%27%27%27%27%20%27%27%27%27%20%27%27%27%27%20FROM%20Users- HTTP/1.1" 200 - "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
c:\ffff:192.168.10.5 - [11/Apr/2021:09:32:51 +0000] "GET /rest/products/search?q=%27%20UNION%20SELECT%20id,%20email,%20password,%20%27%27%27%20%27%27%27%27%20%27%27%27%27%20%27%27%27%27%20%27%27%27%27%20FROM%20Users- HTTP/1.1" 200 3742 - "-" curl/7.74.0"
c:\ffff:192.168.10.5 - [11/Apr/2021:09:34:33 +0000] "GET /a54372a1d4041af1e884zaes0z9au0eb HTTP/1.1" 200 1924 - "-" feroxhubat2.2.1"
c:\ffff:192.168.10.5 - [11/Apr/2021:09:34:33 +0000] "GET /3e72ead6edf04cab5ff79b741883cfb3044c0e35114f7598904da12c365fab6a687d272fc4288ae1316f157b1fab2 H

```

Qué pasó:

- Tras verificar vulnerabilidad con sqlmap, el atacante usó `curl` para automatizar y extraer columnas específicas (id, email, password).
- Esto confirma exfiltración programada y no solo pruebas puntuales.

Por qué importa:

- Uso de herramientas estándar y scripts hace que la exfiltración sea reproducible y rápida; más difícil de detectar si no hay alertas por patrones.

Acción recomendada inmediata:

- Capturar y preservar todas las respuestas registradas durante esas solicitudes (para evidencia).
- Notificar a cumplimiento/privacidad si datos de usuarios fueron comprometidos.

Sesión 6 — Segundo Fuzzing / Feroxbuster (posterior al SQLi)

Evidencia: nuevo ciclo de enumeración de directorios con feroxbuster; secuencia de accesos a rutas enumeradas, incluyendo /backup, /promotion, /admin.

```

::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /a54372a140414fe8842ae5c029a00e3 HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /3e72ead66df04ca5bfff7c9b741883cfd3044c03e5114f7589804da12c36e5baf6807b272cf4288ae1316f157b1fab2 HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /api HTTP/1.1" 500 - "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /adminstartion HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /login HTTP/1.1" 200 924 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /admin HTTP/1.1" 200 924 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /backup HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /promotion HTTP/1.1" 200 6586 "-" "feroxbuster/2.2.1"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /ftp HTTP/1.1" 200 482 "-" "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"
::ffff:192.168.10.5 - - [11/Apr/2021:09:34:45 +0000] "GET /favicon.ico HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"

```

Qué pasó:

- El atacante reanudó enumeración para encontrar archivos o endpoints con contenido interesante (correos, backups, markdowns).
- En `/products/reviews` se detectaron intentos de extracción de correos en distintas secciones.

Por qué importa:

- Buscar archivos y rutas con datos sensibles o backups es típico post-exploit para maximizar información exfiltrada.

Acción recomendada inmediata:

- Escanear repositorio web en busca de archivos .bak, .md, .old, .sql expuestos y eliminarlos o restringir acceso.
- Implementar reglas WAF que bloqueen patrones de búsqueda masiva.

Sesión 7 — Acceso FTP anónimo y exfiltración de archivos (11/Apr/2021 09:34:33 – 09:34:52)

Evidencia: conexiones FTP desde 192.168.10.5 usando usuario anonymous ; transferencia (GET) de dos archivos: www-data.bak y coupons_2013.md.bak .

```
Sun Apr 11 09:08:34 2021 [pid 8015] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:08:34 2021 [pid 8017] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:08:34 2021 [pid 8018] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:08:34 2021 [pid 8021] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:08:34 2021 [pid 8020] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:08:34 2021 [pid 8014] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:08:35 2021 [pid 8013] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
Sun Apr 11 09:08:35 2021 [pid 8048] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:08:35 2021 [pid 8050] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:08:35 2021 [pid 8052] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:35:32 2021 [pid 8153] CONNECT: Client "::ffff:192.168.10.5"
Sun Apr 11 09:35:37 2021 [pid 8152] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "?"
Sun Apr 11 09:35:45 2021 [pid 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/www-data.bak", 2602 bytes, 544.81Kbyte/sec
Sun Apr 11 09:36:08 2021 [pid 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/coupons_2013.md.bak", 131 bytes, 3.01Kbyte/sec
```

Qué pasó:

- El atacante aprovechó FTP anónimo para descargar copias de seguridad y archivos con datos potencialmente sensibles.
- Los archivos descargados contienen probables configuraciones/credenciales o cupones (posible información comercial).

Por qué importa:

- FTP anónimo habilita exfiltración fácil; backups con credenciales son un vector directo de escalada.
- La presencia de www-data.bak sugiere backup de archivos de servidor que pueden contener claves o configuraciones.

Acción recomendada inmediata:

- Deshabilitar accesos FTP anónimos y auditar el servidor FTP.
- Recuperar y analizar los archivos descargados (si hay copia en servidor) para evaluar la sensibilidad.

- Cambiar credenciales encontradas en esos backups.

Sesión 8 — Acceso SSH como `www-data` y shell persistente (posterior)

Evidencia: logs indican conexión SSH con usuario `www-data` y obtención de shell por parte del atacante; secuencia posterior consistente con comandos interactivos.

```
Apr 11 09:41:32 thunt sshd[8494]: Accepted password for www-data from 192.168.10.5 port 40114 ssh2
Apr 11 09:41:32 thunt sshd[8494]: pam_unix(sshd:session): session opened for user www-data by (uid=0)
Apr 11 09:41:32 thunt systemd-logind[737]: New session 14 of user www-data.
Apr 11 09:41:44 thunt sshd[8579]: Received disconnect from 192.168.10.5 port 40114:11: disconnected by user
Apr 11 09:41:44 thunt sshd[8579]: Disconnected from user www-data 192.168.10.5 port 40114
Apr 11 09:41:44 thunt sshd[8494]: pam_unix(sshd:session): session closed for user www-data
Apr 11 09:41:44 thunt systemd-logind[737]: Session 14 logged out. Waiting for processes to exit.
Apr 11 09:41:44 thunt systemd-logind[737]: Removed session 14.
Apr 11 09:41:46 thunt dbus-daemon[718]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
Apr 11 09:42:01 thunt sudo: pam_unix(sudo:session): session closed for user root
Apr 11 09:42:57 thunt su: pam_unix(su:session): session closed for user thunt
Apr 11 09:42:57 thunt su: pam_unix(su:session): session closed for user www-data
Apr 11 09:43:35 thunt sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Apr 11 09:43:37 thunt sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
```

Qué pasó:

- El atacante, con credenciales recuperadas (posiblemente desde backups o SQLi), consiguió acceso a una cuenta del sistema (`www-data`) vía SSH y obtuvo shell.
- Desde esa shell pudo moverse, crear persistencia, y preparar exfiltración adicional.

Por qué importa:

- Acceso directo al sistema operativo permite ejecutar ataques fuera del contexto Web (escalada a root, lateral movement, instalación de backdoors).

Acción recomendada inmediata:

- Terminar todas las sesiones SSH sospechosas; cambiar claves/credenciales en el host.
- Buscar binarios/cronjobs/keys colocados por el atacante para persistencia.
- Aislar la máquina comprometida y tomar imagen forense antes de limpiarla.

Resumen ejecutivo

El atacante siguió una campaña clásica: reconocimiento → fuzzing → fuerza bruta (login exitoso) → inyección SQL (exfiltración de credenciales) → búsqueda de archivos sensibles → exfiltración via FTP → SSH para shell persistente. Los puntos críticos fueron la existencia de FTP anónimo, falta de mitigaciones contra fuerza bruta y la vulnerabilidad SQL en el endpoint de búsqueda.

Siguientes pasos (prioridad inmediata)

1. **Contención:** bloquear IPs sospechosas, aislar host comprometido.

2. **Erradicación:** deshabilitar FTP anónimo, aplicar parches/parametrización SQL, forzar cambios de contraseña y MFA.
3. **Recuperación:** restaurar desde backups limpios, revisar integridad del sistema.
4. **Forense:** capturar imágenes, conservar logs y respuestas de las solicitudes SQL para evidencia.
5. **Notificación:** activar protocolos legales/privacidad si datos de usuarios fueron comprometidos.

Indicadores de Compromiso (IOCs)

Tipo	IOC (valor)	Timestamp(s) (UTC)	Evidencia (extracto / línea de log)
IP origen	192.168.10.5	11/Apr/2021 09:08:29 — 11/Apr/2021 09:34:52	Múltiples entradas en access.log registran solicitudes originadas desde 192.168.10.5 durante todo el incidente (reconocimiento, fuzzing, fuerza bruta, SQLi, FTP). Timestamps registrados en el PDF: 09:08:29, 09:16:27–09:16:31, 09:29:14–09:32:51, 09:34:33–09:34:52.
User-Agent (fuzzing)	Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	11/Apr/2021 09:08:30 – 09:15:35	El PDF muestra numerosas peticiones con ese User-Agent durante la fase de enumeración de directorios (patrón típico de feroxbuster), incluyendo descubrimiento de /rest/user/login.
User-Agent (exfiltración HTTP)	curl/7.74.0	11/Apr/2021 09:29:58 – 09:32:51	Registros que muestran curl/7.74.0 realizando peticiones con payloads UNION SELECT entre 09:29:58 y 09:32:51; respuestas contienen columnas id, email, password.

Tipo	IOC (valor)	Timestamp(s) (UTC)	Evidencia (extracto / línea de log)
Herramienta (fuerza bruta)	hydra (patrón de requests)	11/Apr/2021 09:16:27 – 09:16:31	El access.log indica 144 intentos rápidos contra /rest/user/login en ~3s, patrón consistente con Hydra; el PDF declara explícitamente uso de hydra y login exitoso a las 09:16:31 +0000.
Herramienta (automatización SQL)	sqlmap (seguido de curl)	11/Apr/2021 09:29:14 – 09:32:51	El PDF registra ejecución de sqlmap iniciada a las 09:29:14 y posteriormente peticiones curl entre 09:29:58 y 09:32:51 con UNION SELECT dirigidas a /rest/products/search?q= ; evidencia de volcado de la tabla Users .
Endpoint (login)	/rest/user/login	Descubierto 09:15:xx; ataques 09:16:27 – 09:16:31; login exitoso 11/Apr/2021 09:16:31 +0000	El PDF indica descubrimiento del endpoint durante el fuzzing y registra 144 intentos de fuerza bruta seguidos de un inicio de sesión exitoso a las 09:16:31 +0000 en access.log .
Endpoint (vulnerable a SQLi)	/rest/products/search?q=	11/Apr/2021 09:29:14 – 09:32:51	Entradas en logs muestran payloads SQLi dirigidos al parámetro q desde 09:29:14; el PDF documenta extracción de id , email , password vía UNION SELECT .
Endpoint (recolección datos)	/products/reviews	~09:32:xx – 09:34:xx (posterior al SQLi)	El PDF muestra intentos posteriores de raspar secciones como /products/reviews en búsqueda de correos y datos visibles tras el volcado.

Tipo	IOC (valor)	Timestamp(s) (UTC)	Evidencia (extracto / línea de log)
FTP — acceso anónimo	Login anonymous	11/Apr/2021 09:34:33 – 09:34:52	Registros de FTP indican conexión anónima desde 192.168.10.5 y transferencias GET entre 09:34:33 y 09:34:52; PDF lista los archivos descargados.
Archivos exfiltrados	www-data.bak , coupons_2013.md.bak	Transferencias 11/Apr/2021 09:34:33 – 09:34:52	El PDF reporta la descarga de www-data.bak y coupons_2013.md.bak vía FTP anónimo en la ventana 09:34:33–09:34:52; potencial contenido sensible en backups.
Acceso SSH	SSH como www-data (shell interactivo)	Posterior a 09:34:52 (actividad post-exfiltración)	Logs indicativos en el PDF muestran conexión SSH con usuario www-data y comandos de shell posteriores; se reporta obtención de shell para persistencia.
Técnica de reconocimiento	Escaneo activo (posible Nmap)	11/Apr/2021 09:08:29	El PDF documenta un escaneo inicial a las 09:08:29 que coincide con patrones de Nmap / scanning en access.log .

Técnicas MITRE ATT&CK

Técnica (ATT&CK)	ID	Descripción (resumida)	Evidencia en logs
Active Scanning / Reconocimiento activo (escaneo de puertos/servicios)	T1595. (Active Scanning) (MITRE ATT&CK)	Escaneo inicial para identificar puertos/servicios expuestos (p. ej. Nmap o escaneo similar).	Escaneo inicial desde 192.168.10.5 a las 09:08:29 .

Técnica (ATT&CK)	ID	Descripción (resumida)	Evidencia en logs
Vulnerability / Directory discovery (fuzzing de endpoints) – sub-actividad de escaneo	T1595.002 (Vulnerability Scanning / reconocimiento activo) (center-for-threat-informed-defense.github.io)	Enumeración de directorios/webpaths (feroxbuster / dirb) para descubrir endpoints como /rest/user/login .	Peticiones con user-agent Firefox/78.0 y secuencia típica de feroxbuster (09:08:30–09:15:35).
Brute Force (ataque de fuerza bruta contra autenticación web)	T1110 (Brute Force) (MITRE ATT&CK)	Intentos automatizados de adivinar credenciales (Hydra).	144 intentos contra /rest/user/login entre 09:16:27 y 09:16:31 , login exitoso 09:16:31 +0000.
Valid Accounts (uso de credenciales válidas)	T1078 (Valid Accounts) (MITRE ATT&CK)	Uso de credenciales válidas para autenticarse y moverse (p. ej. sesión obtenida en la app y SSH con www-data).	Login exitoso web 09:16:31; acceso SSH como www-data posteriormente.
Exploit Public-Facing Application (explotación de aplicación pública — SQLi)	T1190 (Exploit Public-Facing Application) (MITRE ATT&CK)	Explotación de una vulnerabilidad en una aplicación pública (SQLi contra /rest/products/search?q= para ejecutar UNION SELECT).	Inyección SQL registrada 09:29:14 – 09:32:51, uso de sqlmap y UNION SELECT .
Exfiltration Over Alternative Protocol (exfiltración vía FTP / protocolos alternativos)	T1048 (Exfiltration Over Alternative Protocol) — FTP/HTTP etc. (MITRE ATT&CK , cisa.gov)	Exfiltración de archivos usando un protocolo distinto al C2 principal (ej. FTP anónimo, HTTP curl).	Descarga FTP anónimo de www-data.bak y coupons_2013.md.bak 09:34:33–09:34:52; uso de curl para extraer datos vía HTTP.
Remote Services: SSH (uso de servicios remotos para acceso interactivo)	T1021.004 (SSH) (MITRE ATT&CK)	Uso de SSH/servicios remotos para autenticarse y obtener shell interactivo.	Acceso SSH con usuario www-data y obtención de shell (post-explotación).
Exfiltration over C2 / Exfiltration	T1041 (Exfiltration Over	Categoría general de exfiltración — en este	Respuestas con datos extraídos tras UNION

Técnica (ATT&CK)	ID	Descripción (resumida)	Evidencia en logs
(general)	C2 Channel) — (contextual) (MITRE ATT&CK)	caso combinada: extracción via HTTP/FTP/CURL.	SELECT y transferencias FTP; evidencia en logs de transferencias/respuesta: