

CYBEROPS - Anatomy of Malware

- **Conduct a Search of Recent Malware**

1. McAfee Threat Center Threat Landscape Dashboard

DarkGate è un malware di tipo **loader** e **stealer**. I loader sono malware che dopo essersi avviato sul sistema da infettare, scaricano o avviano altri eseguibili malevoli.

Viene distribuito attraverso campagne di **mail phishing** tramite indirizzi mail rubati.

Oppure ancora tramite documenti **Office** spammati nelle chat di **Microsoft Teams** che se aperti avviano l'eseguibile malevolo.

Riesce a rubare le password, i cookies e la cronologia, agisce anche da **keylogger**, ruba i **token Discord**. Inoltre include funzionalità come **HVNC** o **Anydesk**, abilità di **privilege escalation** e anche di **cryptomining**.

2. Malwarebytes Labs Threat Center

Adware.OperatorMac è un **adware** che infetta sistemi OSX. Le versioni più recenti usano **mitmproxy** per effettuare il proxy di tutto il traffico http e https al fine di generare l'infezione.

3. Securityweek.com

Malware Delivered via Malicious Pidgin Plugin, Signal Fork: Gli sviluppatori di **Pidgin**, noto client di messaggistica, ha informato gli utenti che sta girando un malware sulla piattaforma per via di un plugin di terze parti infetto, nominato **ScreenShare-OTR**. Esso è un **keylogger** che effettua anche screenshots. In teoria il rischio non dovrebbe più sussistere dato che è stato ormai rimosso. Inoltre è stato appurato il fatto che avesse anche funzionalità di condivisione schermo tramite protocollo **OTR** e la sua installazione risultava possibile grazie ad un certificato valido fornito da una compagnia polacca. Esso poteva pure avviare una **PowerShell** per poter poi eseguire **DarkGate**. Le stesse funzionalità e rischi esistono pure nella versione Gnu/Linux. Poi, lo stesso malware è stato ritrovato in **Cradle**, un servizio di messaggistica anti forense, nonché **fork** di **Signal**. Il codice è lo stesso del plugin di **Pidgin** e lo scopo è sempre quello di scaricare **DarkGate**. Anche **Cradle Linux** è affetto dallo stesso codice malevolo.

4. Technewsworld.com

Log4j è una vulnerabilità software che permette alle applicazioni di tenere traccia della loro attività quando vengono eseguite. Molte applicazioni lo usano evitando di sviluppare ex novo una funzionalità simile semplificando così il codice. Visto che questo software ha una così grande diffusione, questa vulnerabilità è una vera minaccia informatica. È stato appurato che se si fa eseguire l'attività di **logging** a **Log4j** su un software malevolo esso lo esegue per portare a termine il compito. Così chiunque abbia progettato quel codice malevolo potrà prendere controllo sui server che eseguono **Log4j**. Inoltre, tramite una connessione di tipo **Javascript WebSocket** è possibile attivare l'esecuzione di codice da remoto. Qualsiasi server che esegue Log4j può attivare questa vulnerabilità in qualsiasi momento e il rischio di subire un exploit è elevatissimo, anche con una semplice connessione via browser sui server in ascolto. **WebSocket** è usato per il port scanning dei sistemi interni e ora rappresenta uno dei possibili **exploit** per la **remote code execution**. Dato che questa vulnerabilità è facilmente sfruttabile da remoto, gli esperti di sicurezza temono che l'unico modo di mitigare il rischio sia il **patching** dei sistemi, dato che nemmeno un sistema **WAF** è in grado di bloccare la minaccia.

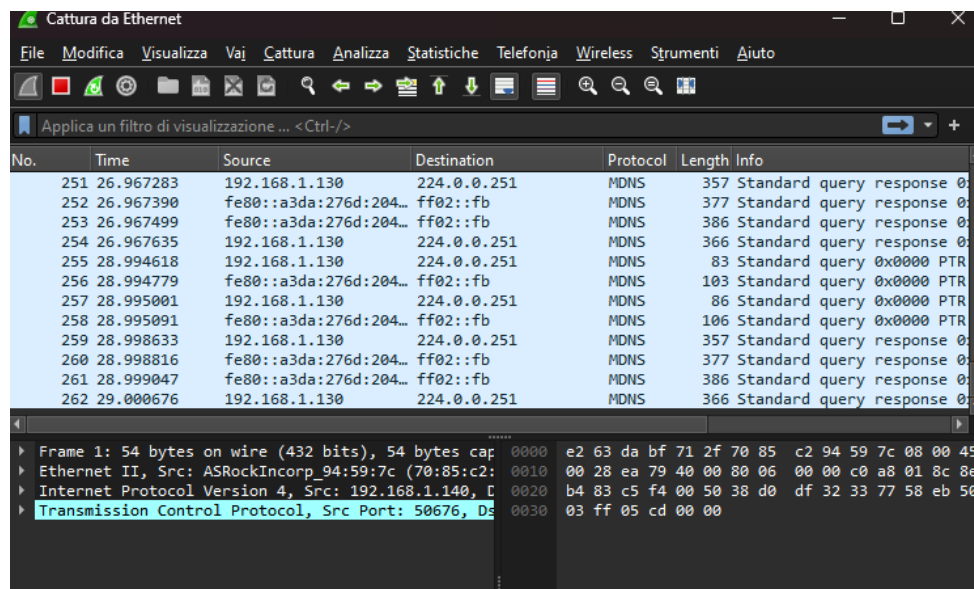
CYBEROPS - Exploring DNS Traffic

- **Part 1: Capture DNS Traffic**

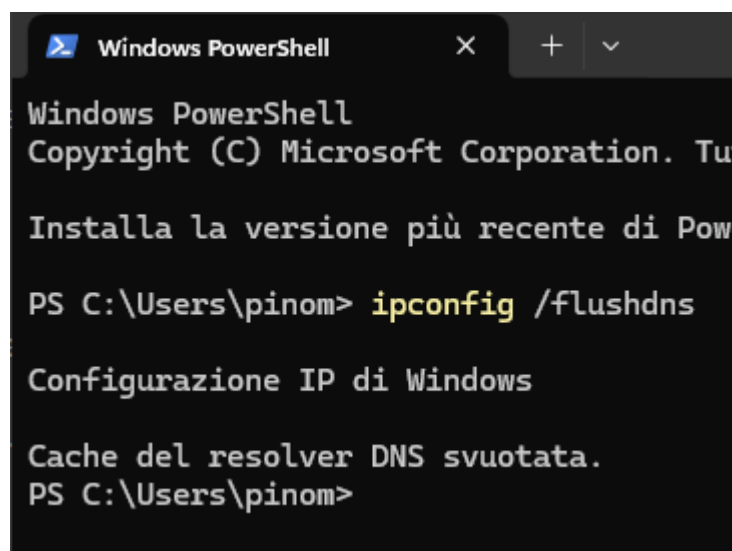
Step 1: Download and install Wireshark

Step 2: Capture DNS traffic

Avvio Wireshark e inizio a monitorare l'interfaccia Ethernet.



Avvio la shell e pulisco la cache DNS.



Dopo aver eseguito **nslookup** con l'indirizzo www.cisco.com, fermo la cattura con **Wireshark**.

```
PS C:\Users\pinom> nslookup
Server predefinito: fritz.box
Address: fd00::5e49:79ff:fe76:3fba

> www.cisco.com
Server: fritz.box
Address: fd00::5e49:79ff:fe76:3fba

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
*** Tempo scaduto per la richiesta a fritz.box
>
```

- **Part 2: Explore DNS Query Traffic**

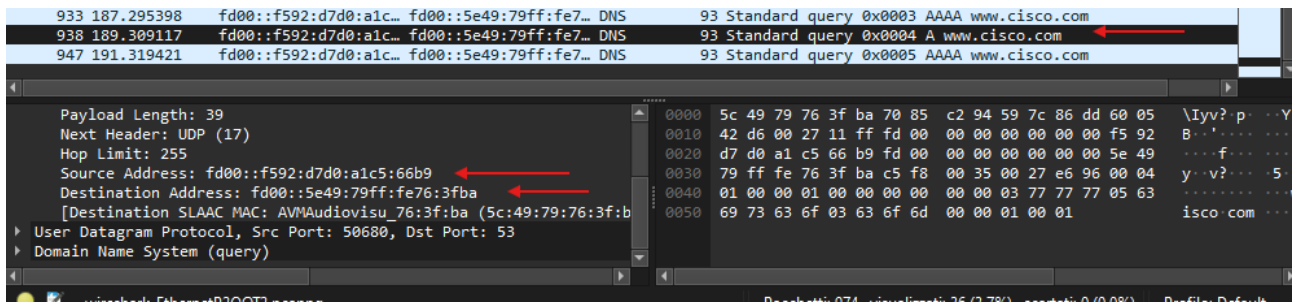
Impostando il filtro **udp.port==53**, e analizzando i pacchetti contenenti la descrizione “Standard query A www.cisco.com”, nel sottomenu “**Ethernet II**” si vede il **MAC address** del gateway e quello della scheda di rete del computer che fa la richiesta.

The image shows a Wireshark packet capture window with the filter **udp.port == 53**. The packet list shows a series of DNS queries and responses. The selected packet (932) is a "Standard query 0x0002 A www.cisco.com". The packet details pane shows the Ethernet II header with source MAC **ASRockIncorp_94:59:7c (70:85:c2:94:59:7c)** and destination MAC **AVMAudiovisu_76:3f:ba (5c:49:79:76:3f:ba)**. The packet bytes pane shows the raw data of the packet.

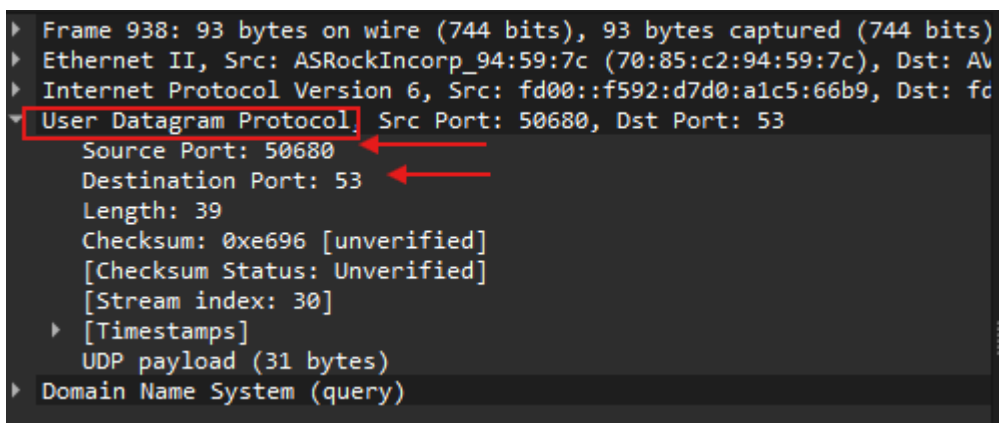
No.	Time	Source	Destination	Protocol	Length	Info
526	63.063586	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	103	Standard query 0xdff2 AAAA ctld1.windowsupdate.com
527	64.058158	192.168.1.140	192.168.1.1	DNS	83	Standard query 0xbf45 A ctld1.windowsupdate.com
528	64.058158	192.168.1.140	192.168.1.1	DNS	83	Standard query 0xdff2 AAAA ctld1.windowsupdate.com
529	64.130686	192.168.1.1	192.168.1.140	DNS	297	Standard query response 0xbf45 A ctld1.windowsupdate.com
530	65.063473	192.168.1.140	192.168.1.1	DNS	83	Standard query 0xdff2 AAAA ctld1.windowsupdate.com
531	65.064820	192.168.1.1	192.168.1.140	DNS	281	Standard query response 0xdff2 AAAA ctld1.windowsupdate.com
846	167.547378	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	96	Standard query 0x5078 A cdn.ghostery.com
855	168.544738	192.168.1.140	192.168.1.1	DNS	76	Standard query 0x5078 A cdn.ghostery.com
856	168.617339	192.168.1.1	192.168.1.140	DNS	128	Standard query response 0x5078 A cdn.ghostery.com CNAME g
857	168.618162	192.168.1.140	192.168.1.1	DNS	82	Standard query 0xa9f8 A ghostery-cdn.b-cdn.net
859	168.623841	192.168.1.1	192.168.1.140	DNS	98	Standard query response 0xa9f8 A ghostery-cdn.b-cdn.net A
888	175.025287	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	152	Standard query 0x0001 PTR a.b.f.3.6.7.e.f.f.f.9.7.9.4.e.5
889	175.026094	fd00::5e49:79ff:fe7...	fd00::f592:d7d0:a1c...	DNS	233	Standard query response 0x0001 PTR a.b.f.3.6.7.e.f.f.f.9
932	185.296417	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	93	Standard query 0x0002 A www.cisco.com
933	187.295398	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	93	Standard query 0x0003 AAAA www.cisco.com
938	189.309117	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	93	Standard query 0x0004 A www.cisco.com
947	191.319421	fd00::f592:d7d0:a1c...	fd00::5e49:79ff:fe7...	DNS	93	Standard query 0x0005 AAAA www.cisco.com

Frame 932: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Ethernet II, Src: ASRockIncorp_94:59:7c (70:85:c2:94:59:7c), Dst: AVMAudiovisu_76:3f:ba (5c:49:79:76:3f:ba)
Destination: AVMAudiovisu_76:3f:ba (5c:49:79:76:3f:ba)
Source: ASRockIncorp_94:59:7c (70:85:c2:94:59:7c)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fd00::f592:d7d0:a1c5:66b9, Dst: fd00::5e49:79ff:fe76:3fba
User Datagram Protocol, Src Port: 50678, Dst Port: 53
Domain Name System (query)

Sotto la voce “**Internet Protocol**” si possono vedere gli **IP** del computer (**source**) e del **gateway** (**destination**).



All'interno della voce “**User Datagram Protocol**” si vede la porta sorgente (**50680**) e la porta di destinazione (**53**) ovvero quella del **server DNS**.



Usando il comando “**ipconfig /all**” si vede che gli IP sorgente e di destinazione, ovvero del **server DNS**, coincidono con quelli su **Wireshark**.

```
PS C:\Users\pinom> ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : IBN5100
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No

Scheda Ethernet Ethernet:

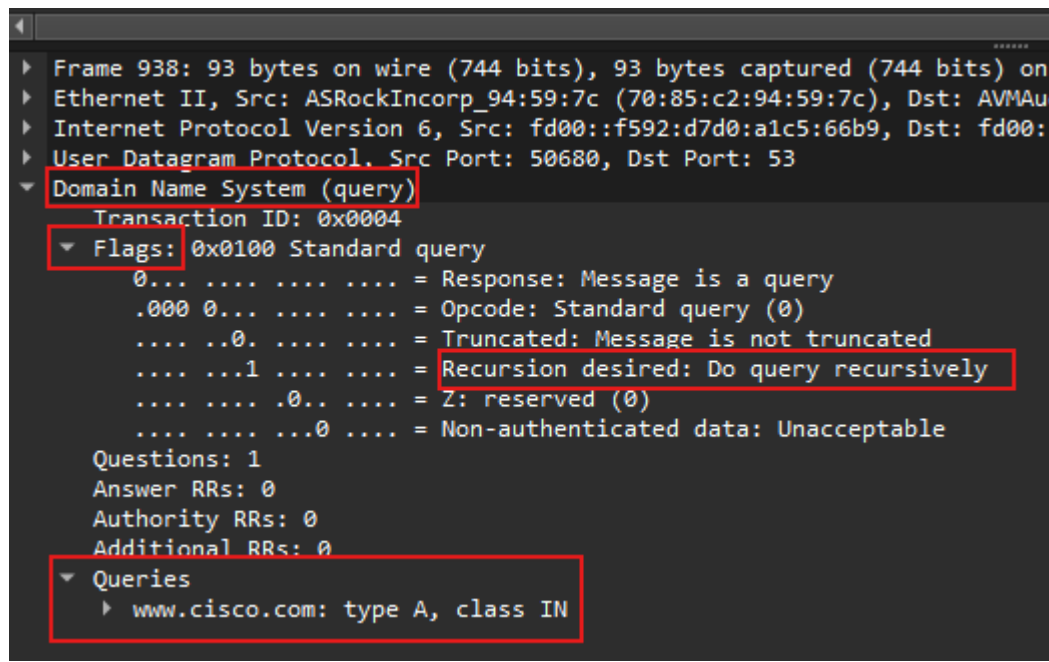
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Realtek Gaming 2.5GbE Family Controller
Indirizzo fisico. . . . . : 70-85-C2-94-59-7C
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IPv6 . . . . . : fd00::8d53:187:9c60:eb76(Preferenziale)
Indirizzo IPv6 temporaneo. . . . . : fd00::f592:d7d0:a1c5:66b9(Preferenziale)
Indirizzo IPv6 locale rispetto al collegamento . : fe80::5a47:adf1:c61a:bcfa%11(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.1.140(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Lease ottenuto. . . . . : mercoledì 4 settembre 2024 13:38:51
Scadenza lease . . . . . : mercoledì 4 settembre 2024 18:55:48
Gateway predefinito . . . . . : 192.168.1.1
Server DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 108037570
DUID Client DHCPv6 . . . . . : 00-01-00-01-2A-07-AF-A0-70-85-C2-94-59-7C
Server DNS . . . . . : fd00::5e49:79ff:fe76:3fba
                        192.168.1.1
NetBIOS su TCP/IP . . . . . : Attivato

Scheda Ethernet Ethernet 3:

Suffisso DNS specifico per connessione:
Descrizione . . . . . : VirtualBox Host-Only Ethernet Adapter
Indirizzo fisico. . . . . : 0A-00-27-00-00-07
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::a239:7ff8:e30d:bbaa%7(Preferenziale)
Indirizzo IPv4 configurazione automatica : 169.254.197.40(Preferenziale)
Subnet mask . . . . . : 255.255.0.0
Gateway predefinito . . . . . :
IAID DHCPv6 . . . . . : 436863015
DUID Client DHCPv6 . . . . . : 00-01-00-01-2A-07-AF-A0-70-85-C2-94-59-7C
NetBIOS su TCP/IP . . . . . : Attivato

PS C:\Users\pinom>
```

Il **flag** all'interno del pacchetto ci indica che è stata impostata una **query ricorsiva** per connettersi all'indirizzo "www.cisco.com".



```

▶ Frame 938: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on
▶ Ethernet II, Src: ASRockIncorp_94:59:7c (70:85:c2:94:59:7c), Dst: AVMAu
▶ Internet Protocol Version 6, Src: fd00::f592:d7d0:a1c5:66b9, Dst: fd00:
▶ User Datagram Protocol, Src Port: 50680, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0004
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0.. .... = Z: reserved (0)
    .... ....0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ www.cisco.com: type A, class IN

```

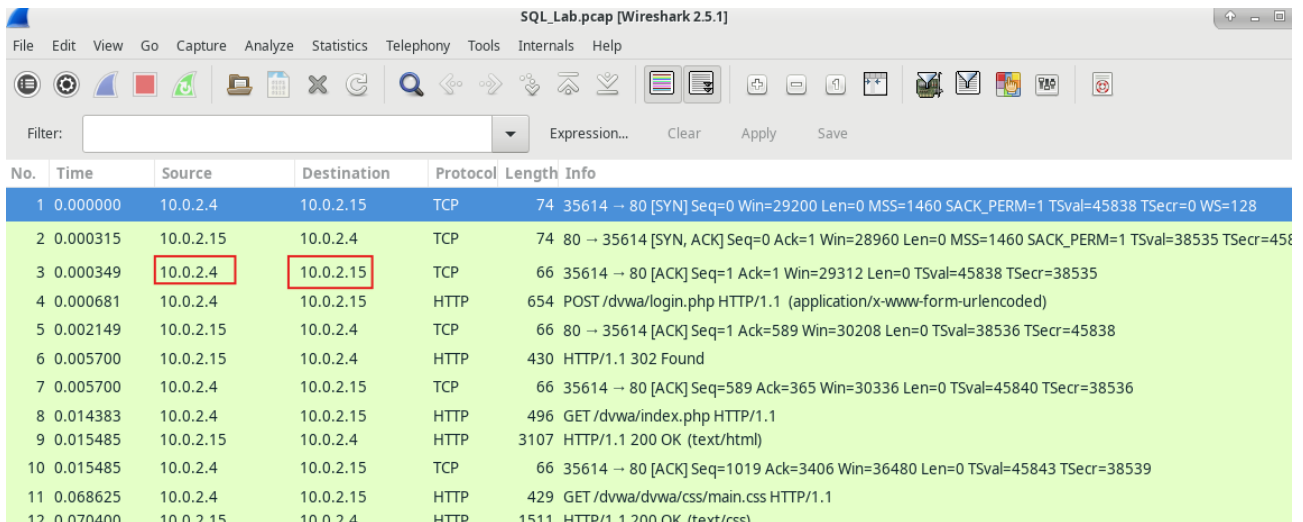
- **Part 3: Explore DNS Response Traffic**

Purtroppo per un errore di rete non ho potuto analizzare i pacchetti "Standard query response". Colpa della mia configurazione di rete.

CYBEROPS - Attacking a mySQL Database

- **Part 1: Open Wireshark and load the PCAP file**

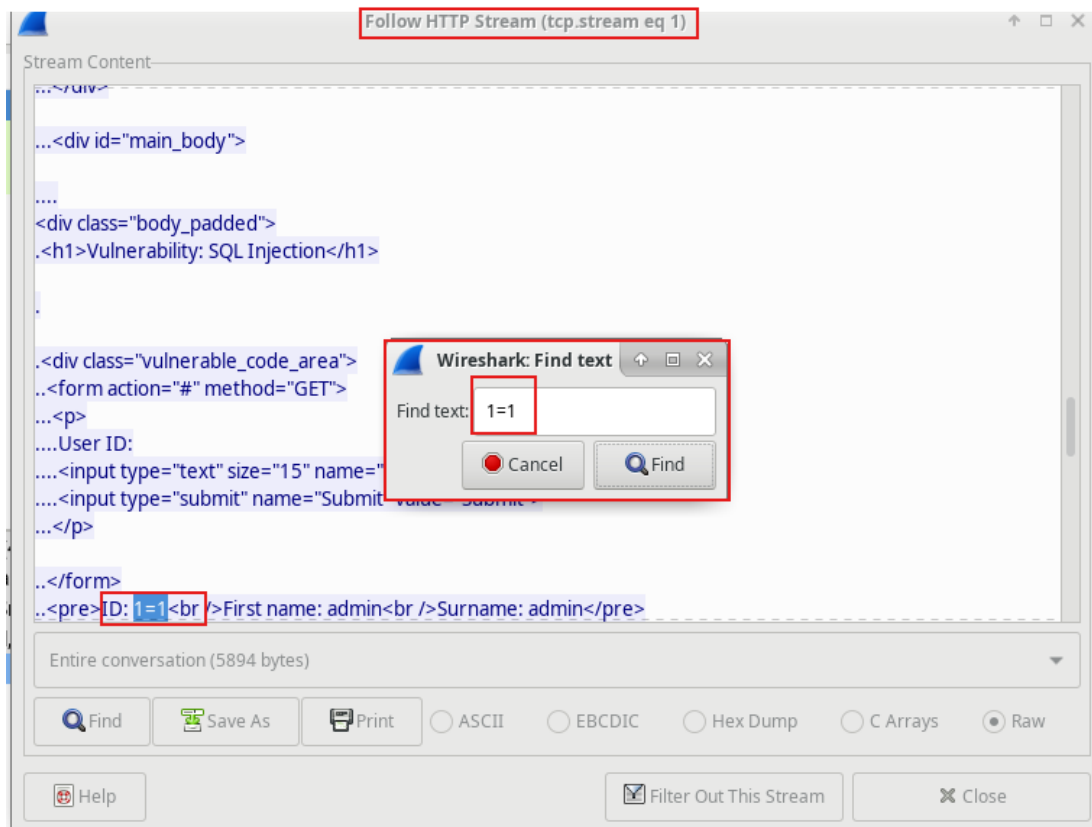
I due IP coinvolti nell'attacco.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38535 TSecr=45838
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)

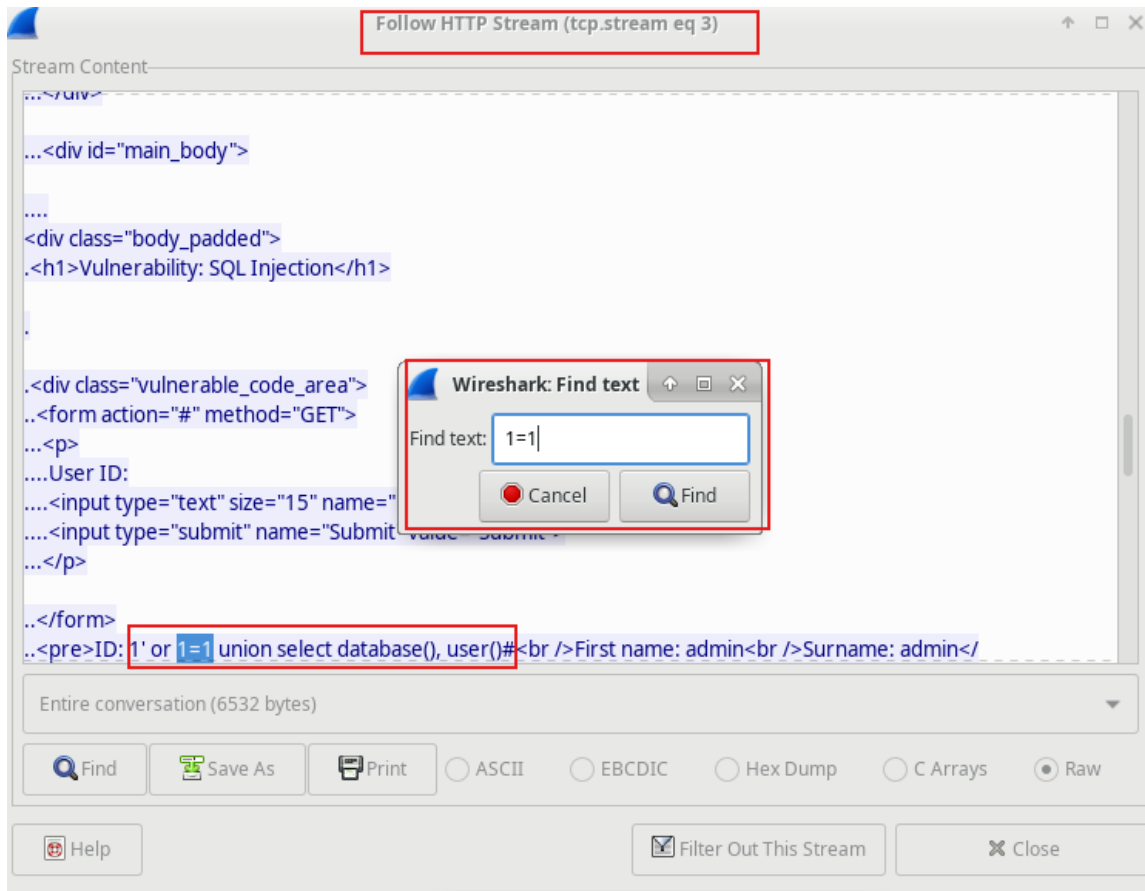
- **Part 2: View the SQL Injection Attack**

Qui si riesce a vedere la query che l'attaccante sta inviando al database SQL per verificare che sia vulnerabile alle **SQL Injection**. La query inserita ha sempre valore booleano **True**. Traffico in blu è dell'attaccante e quello in rosso del database SQL.



- **Part 3: The SQL Injection Attack continues...**

Ecco la successiva query che inserisce l'attaccante per violare il database SQL.

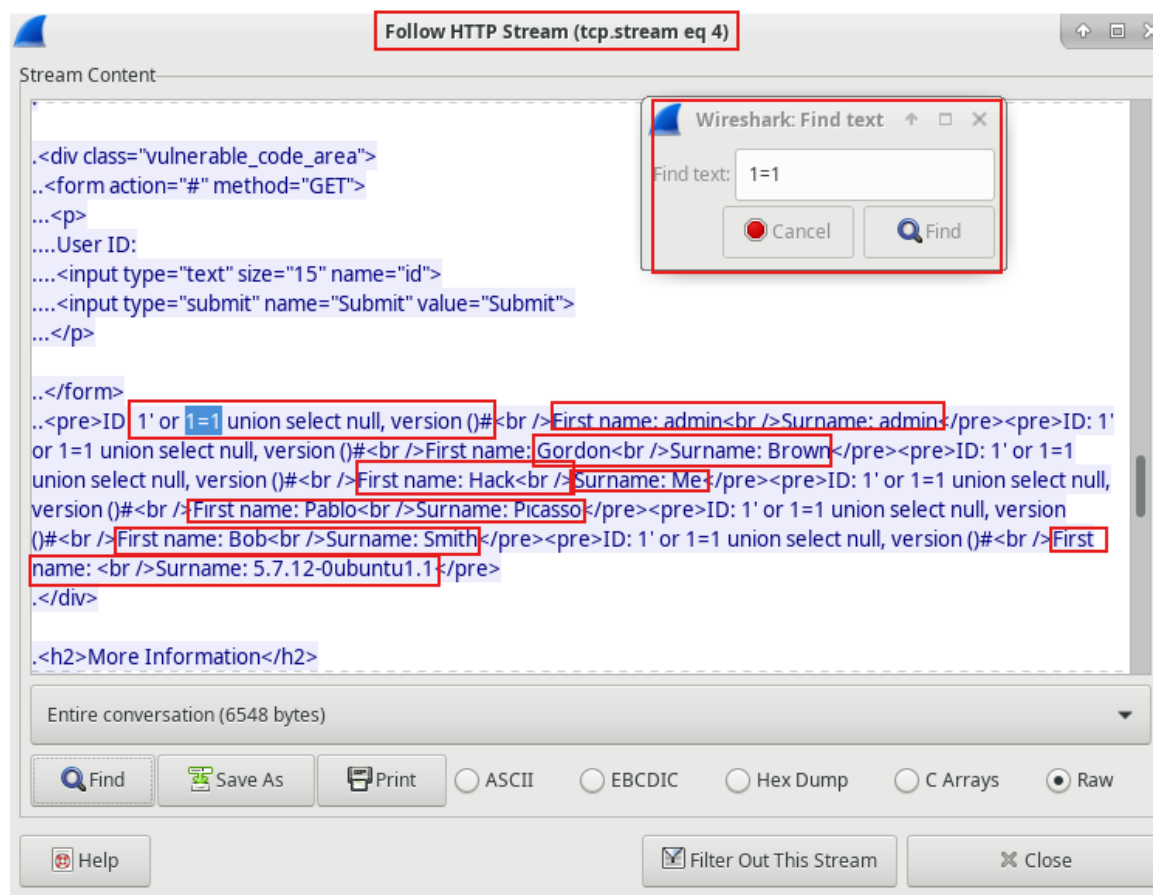


L'attacco sta avvenendo con successo dato che ora la pagina web del database sta eseguendo l'output dei nomi presenti al suo interno. Addirittura c'è il nome del database ovvero **"root@localhost"**.

```
..</form>
..<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre>
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>
```

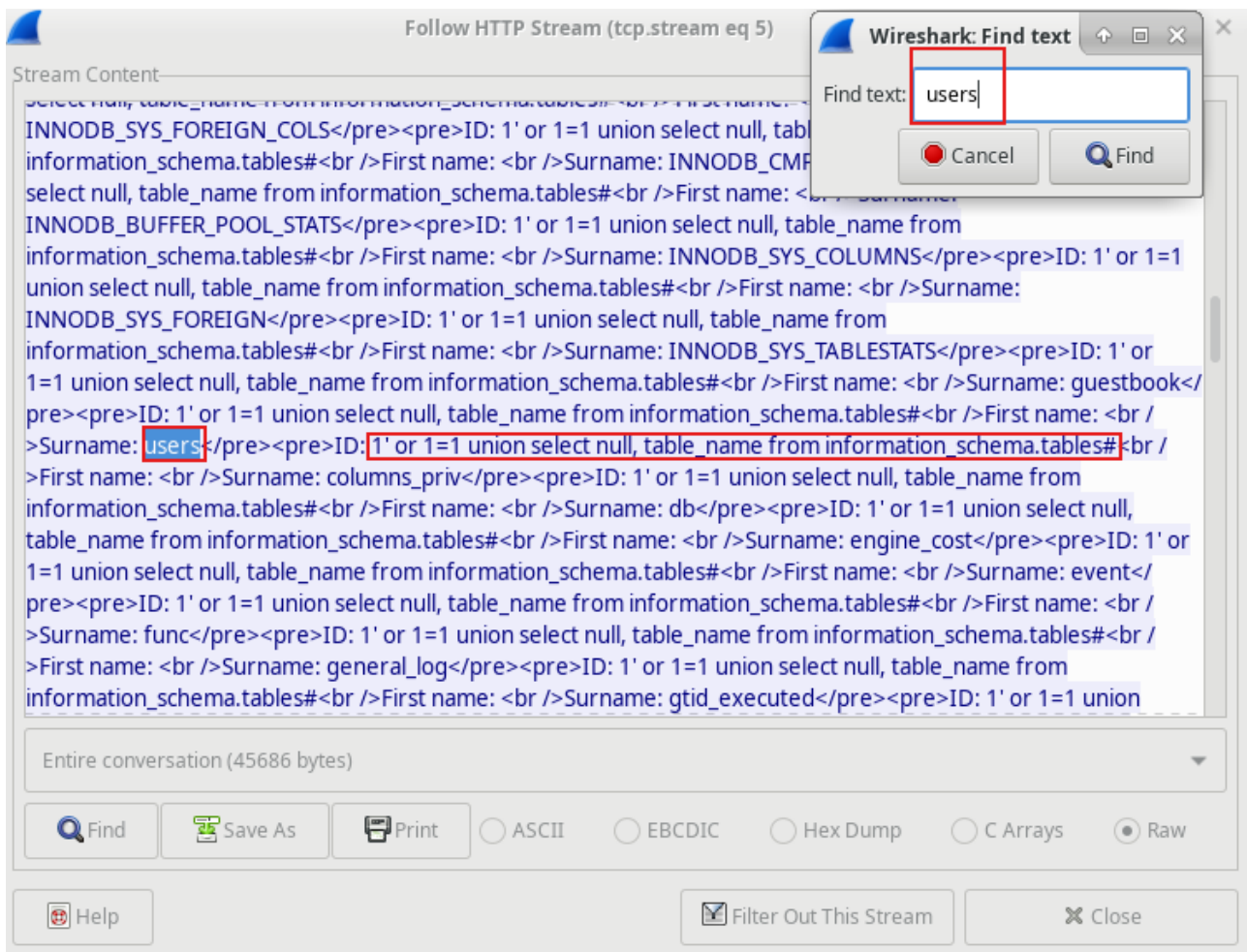

- **Part 4: The SQL Injection Attack provides system information.**

Andando alla riga 22, l'attaccante inserisce un'altra query per ottenere altre informazioni. Adesso ha ottenuto la versione del servizio che gira sul server ovvero la **5.7.12-0**.



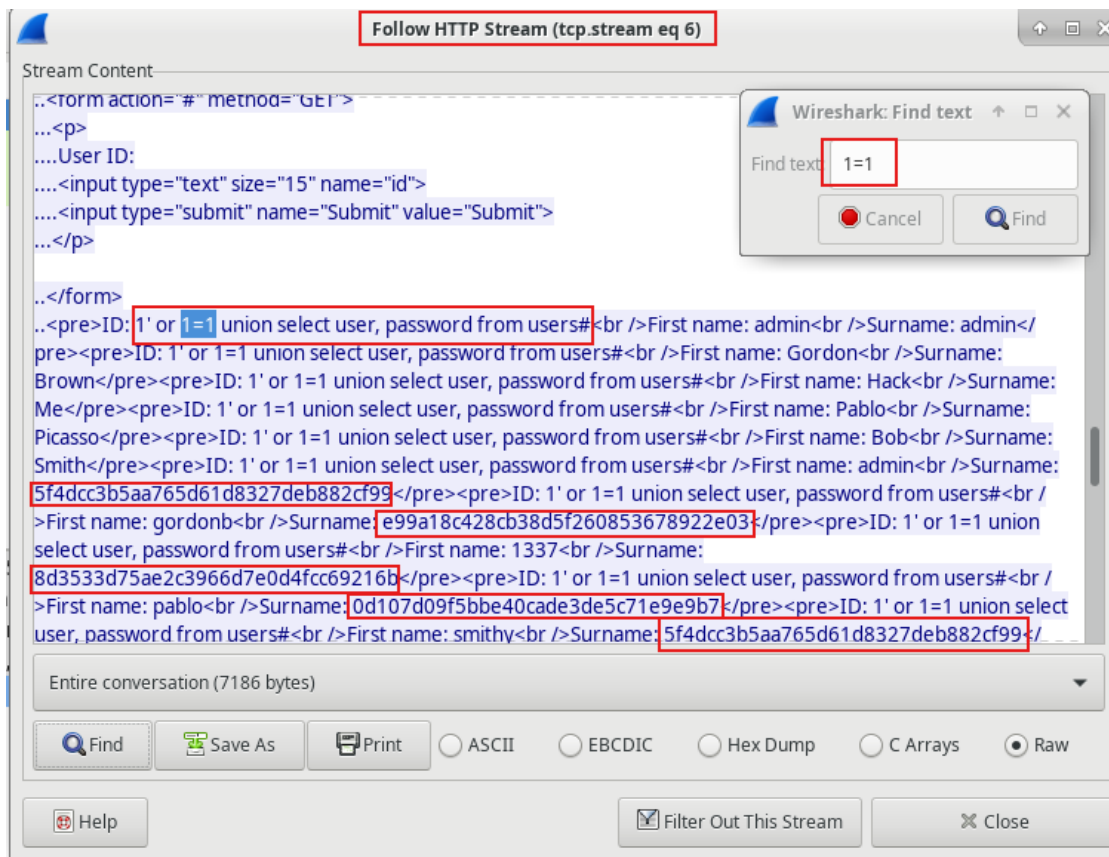
- **Part 5: The SQL Injection Attack and Table Information.**

Adesso l'attaccante, come si vede al contenuto html alla riga 25, inserisce una nuova query per estrapolare ancora più dati dalla pagina.



• Part 6: The SQL Injection Attack Concludes

Adesso, alla **riga 28**, analizzando il contenuto del flusso http, si vede che con una nuova query l'attaccante è riuscito ad ottenere gli **hash** delle password degli utenti del database.



Reflection Questions

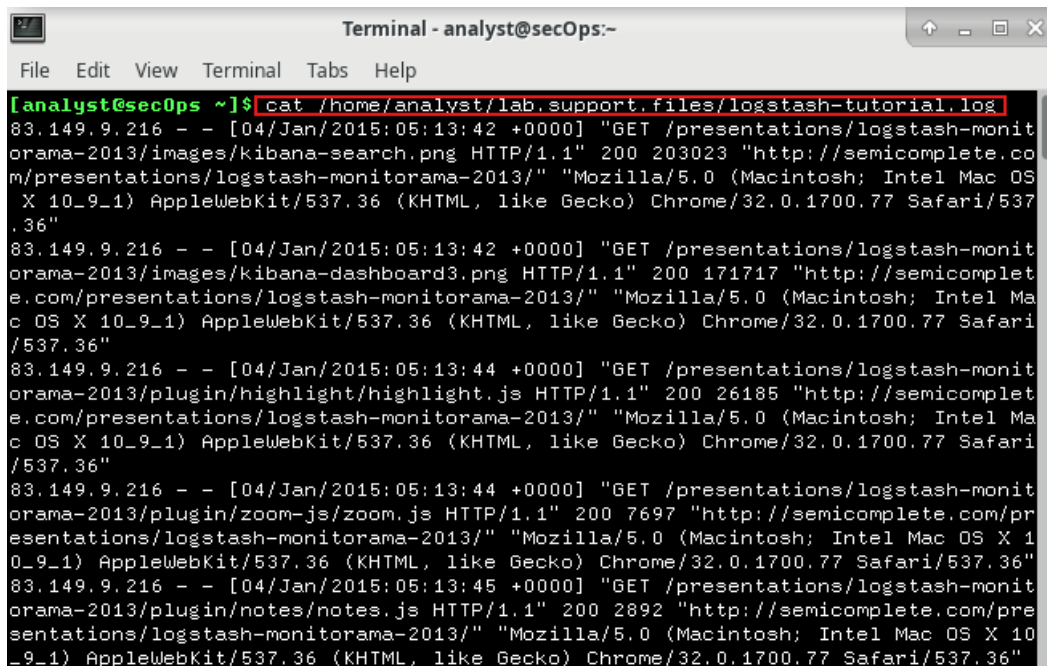
1. Il rischio di avere un database MySQL online è quello di subire numerosi attacchi dall'esterno per l'esfiltrazione dei dati al suo interno tramite le SQL Injection.
2. Per evitare ciò serve sanitizzare l'input dell'utente per eliminare ogni carattere speciale al suo interno ed utilizzare un Web Application Firewall a protezione dell'applicazione web.

CYBEROPS - Reading Server Logs

- **Part 1: Reading Log Files with Cat, More, Less, and Tail**

Step 1: Opening Log Files

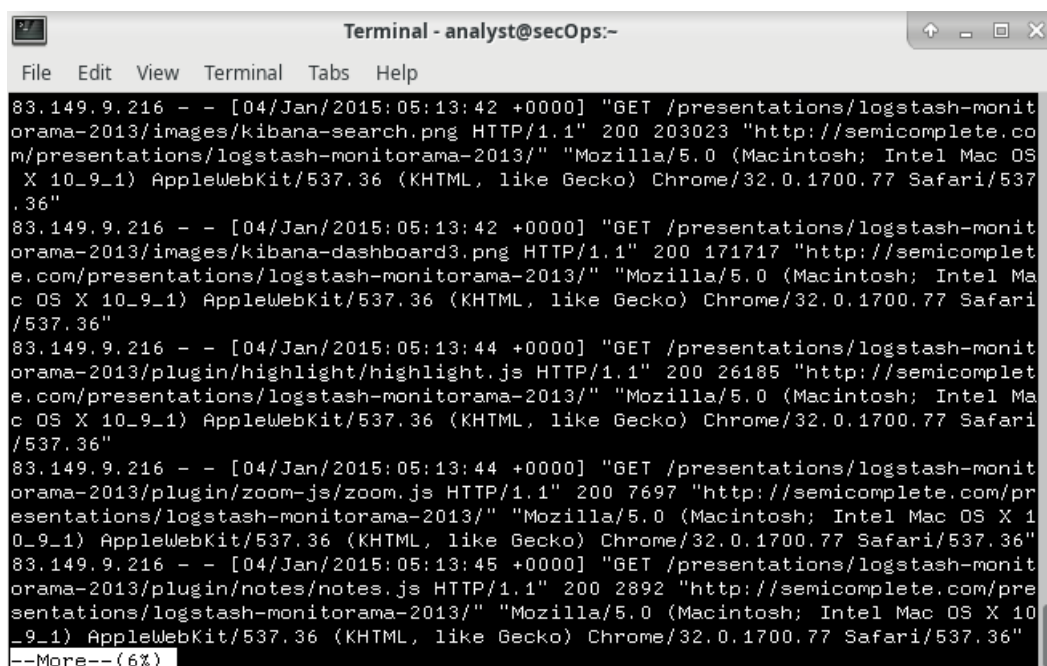
Lo svantaggi di usare **cat** per visualizzare il contenuto dei file di log è che sono molto lunghi e difficile consultarli comodamente. A volte non si riesce nemmeno a leggere la testa del file perché la lunghezza file supera quella del buffer della shell.



```
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"
```

more invece permette di scrollare il contenuto suddiviso in pagine con la barra dello spazio. Lo svantaggio è il non poter tornare indietro alla pagina precedente.

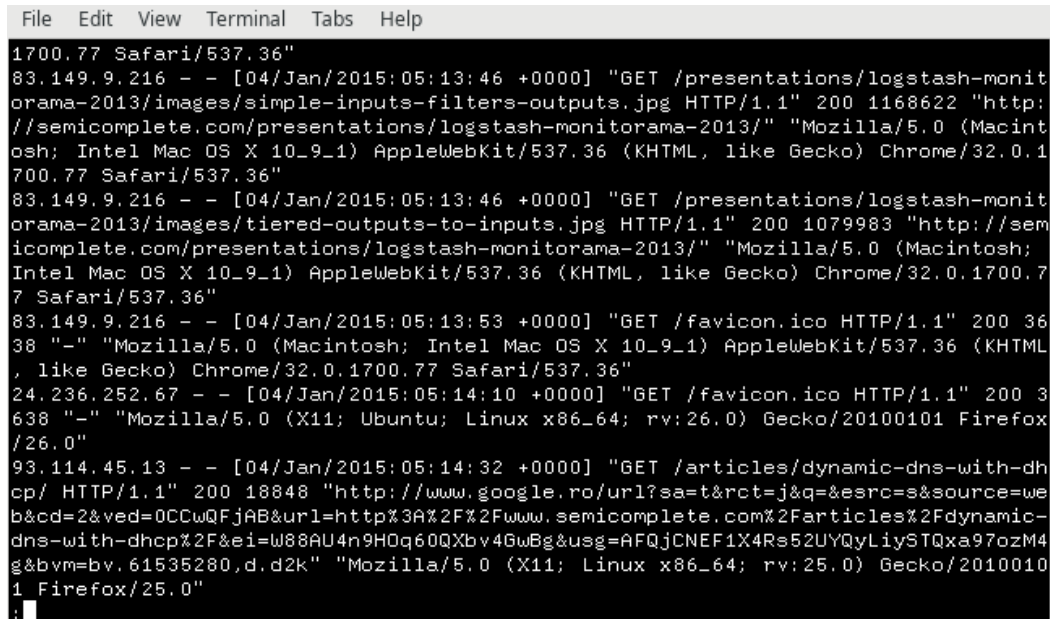


```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

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"
--More-- (6%)
```

Usando **less** si avanza di pagina sempre con la barra o per singola riga con INVIO e si torna indietro usando le freccette sulla tastiera. “q” per uscire.

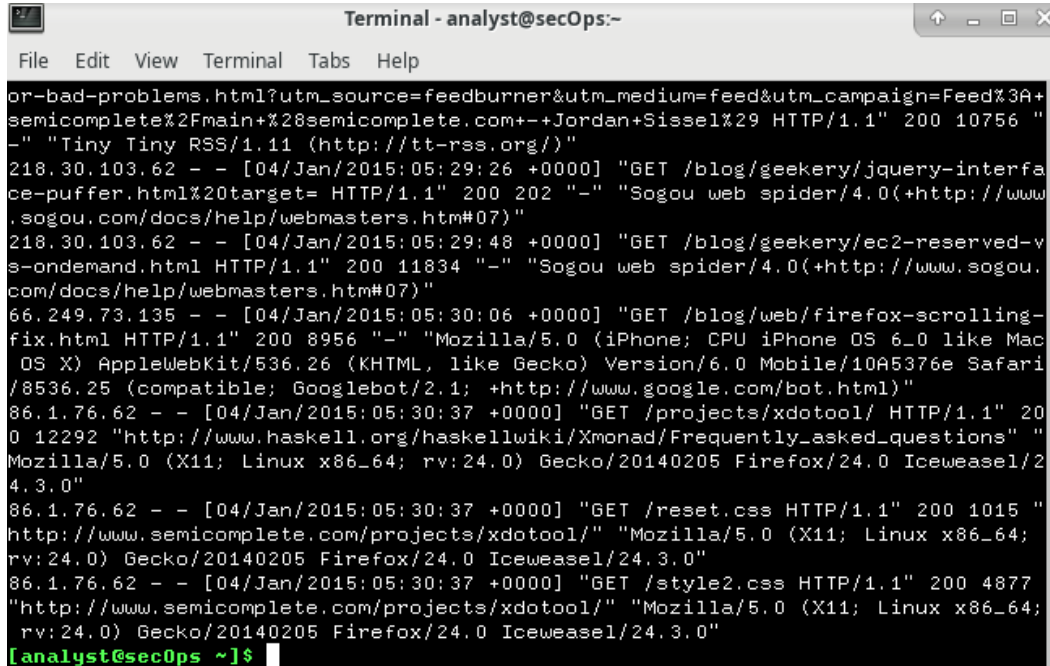
```
less /home/analyst/lab.support.files/logstash-tutorial.log
```



```
1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monit
orama-2013/images/simple-inputs-filters-outputs.jpg HTTP/1.1" 200 1168622 "http:
//semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macint
osh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1
700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monit
orama-2013/images/tiered-outputs-to-inputs.jpg HTTP/1.1" 200 1079983 "http://sem
icomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh;
Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.7
7 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:53 +0000] "GET /favicon.ico HTTP/1.1" 200 36
38 "-" "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"
24.236.252.67 - - [04/Jan/2015:05:14:10 +0000] "GET /favicon.ico HTTP/1.1" 200 3
638 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:26.0) Gecko/20100101 Firefox
/26.0"
93.114.45.13 - - [04/Jan/2015:05:14:32 +0000] "GET /articles/dynamic-dns-with-dh
cp/ HTTP/1.1" 200 18848 "http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=we
b&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fdynamic-
dns-with-dhcp%2F&ei=W88AU4n9H0q60QXbv4GwBg&usq=AFQjCNEF1X4Rs52UYQyLiySTQxa97ozM4
g&bvm=bv.61535280,d.d2k" "Mozilla/5.0 (X11; Linux x86_64; rv:25.0) Gecko/2010010
1 Firefox/25.0"
[analyst@secOps ~]$
```

Usando **tail** si visualizzano solo le ultime **10 righe** del file.

```
tail /home/analyst/lab.support.files/logstash-tutorial.log
```



```
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-interfa
ce-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-v
s-ondemand.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" 20
0 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 Icedove/2
4.3.0"
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 Icedove/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 Icedove/24.3.0"
[analyst@secOps ~]$
```

Step 2: Actively Following Logs

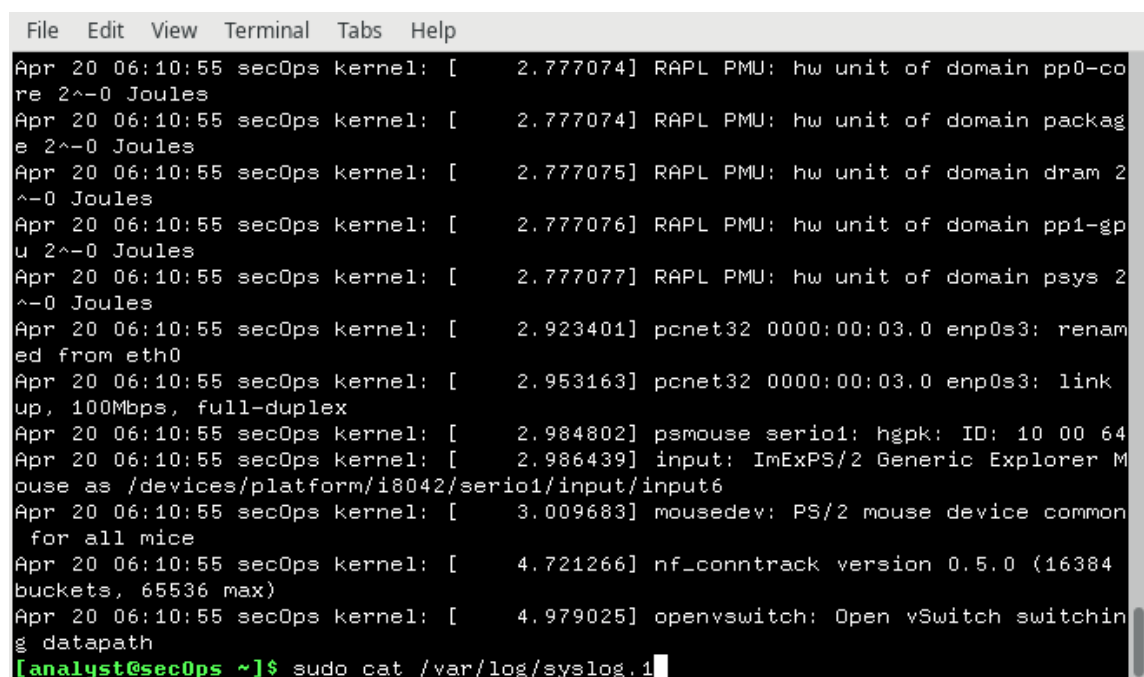
Si usa “**tail -f**” per visualizzare i log in real time mentre che viene aggiornato il loro contenuto.

```
[analyst@sec0ps ~]$ sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log
```

Usando questo comando il terminale resterà inutilizzabile perché impiegato per visualizzare il contenuto in tempo reale.

- **Part 2: Log Files and Syslog**

Per visionare i **log** in cartelle di sistema dentro la **root “/”**, ad esempio in **/var/log**, serve eseguire **cat** con privilegi di root.



```
File Edit View Terminal Tabs Help
Apr 20 06:10:55 sec0ps kernel: [ 2.777074] RAPL PMU: hw unit of domain pp0-core 2^~0 Joules
Apr 20 06:10:55 sec0ps kernel: [ 2.777074] RAPL PMU: hw unit of domain package 2^~0 Joules
Apr 20 06:10:55 sec0ps kernel: [ 2.777075] RAPL PMU: hw unit of domain dram 2^~0 Joules
Apr 20 06:10:55 sec0ps kernel: [ 2.777076] RAPL PMU: hw unit of domain pp1-gpu 2^~0 Joules
Apr 20 06:10:55 sec0ps kernel: [ 2.777077] RAPL PMU: hw unit of domain psys 2^~0 Joules
Apr 20 06:10:55 sec0ps kernel: [ 2.923401] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Apr 20 06:10:55 sec0ps kernel: [ 2.953163] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Apr 20 06:10:55 sec0ps kernel: [ 2.984802] psmouse serio1: hgpk: ID: 10 00 64
Apr 20 06:10:55 sec0ps kernel: [ 2.986439] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/input6
Apr 20 06:10:55 sec0ps kernel: [ 3.009683] mousedev: PS/2 mouse device common for all mice
Apr 20 06:10:55 sec0ps kernel: [ 4.721266] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Apr 20 06:10:55 sec0ps kernel: [ 4.979025] openvswitch: Open vSwitch switching datapath
[analyst@sec0ps ~]$ sudo cat /var/log/syslog.1
```

Il sistema conserva i vecchi log insieme a quelli più recenti per poter poi esser consultati in caso di necessità.

- **Part 3: Log Files and Journalctl**

Step 1: Running journalctl with no options

Tramite “journalctl” possiamo vedere tutti i logs di journald.

```
[analyst@secOps ~]$ journalctl
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 16:10:08 EDT, end at Wed 2024-09-04 12:28:50 EDT.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate man>
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and>
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ss>
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and>
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 16:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and>
Mar 20 16:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Reached target Sockets.
```

Step 2: Journalctl and a few options

Tramite il comando “sudo journalctl --utc” si possono leggere i timestamps in formato orario UTC.

```
[analyst@secOps ~]$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Wed 2024-09-04 17:34:16 UTC.
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-1>
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux roo>
Mar 20 19:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 19:28:45 secOps kernel:   Intel GenuineIntel
Mar 20 19:28:45 secOps kernel:   AMD AuthenticAMD
Mar 20 19:28:45 secOps kernel:   Centaur CentaurHauls
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 fl>
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE re>
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX re>
Mar 20 19:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]>
Mar 20 19:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context si>
Mar 20 19:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000000>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000009fc00-0x000000000000>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000003ff>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000003ffff000-0x000000000003ff>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fff>
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
Mar 20 19:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 19:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vi>
Mar 20 19:28:45 secOps kernel: Hypervisor detected: KVM
```


Si usa il comando “**sudo journalctl -b**” per leggere le entries dei log dell’ultimo boot di sistema.

```
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Wed 2024-09-04 13:36:09 EDT.
Sep 04 12:19:46 secOps kernel: Linux version 4.15.15-1-ARCH (builduser@heftig-4)
Sep 04 12:19:46 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=
Sep 04 12:19:46 secOps kernel: KERNEL supported cpus:
Sep 04 12:19:46 secOps kernel:   Intel GenuineIntel
Sep 04 12:19:46 secOps kernel:   AMD AuthenticAMD
Sep 04 12:19:46 secOps kernel:   Centaur CentaurHauls
Sep 04 12:19:46 secOps kernel: [Firmware Bug]: TSC doesn't count with P0 frequency
Sep 04 12:19:46 secOps kernel: x86/fpu: x87 FPU will use FXSAVE
Sep 04 12:19:46 secOps kernel: e820: BIOS-provided physical RAM map:
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000000009fc00-0x0000000000000000]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000000]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x000000000000100000-0x0000000000000dff]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x000000000000dff0000-0x0000000000000dff]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffff]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ff]
Sep 04 12:19:46 secOps kernel: NX (Execute Disable) protection: active
Sep 04 12:19:46 secOps kernel: random: fast init done
Sep 04 12:19:46 secOps kernel: SMBIOS 2.5 present.
Sep 04 12:19:46 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS Vi
Sep 04 12:19:46 secOps kernel: Hypervisor detected: KVM
Sep 04 12:19:46 secOps kernel: e820: update [mem 0x000000000-0x000000fff] usable
Sep 04 12:19:46 secOps kernel: e820: remove [mem 0x000a0000-0x000ffff] usable
Sep 04 12:19:46 secOps kernel: e820: last_pfn = 0x120000 max_arch_pfn = 0x40000
Sep 04 12:19:46 secOps kernel: MTRR default type: uncachable
Sep 04 12:19:46 secOps kernel: MTRR fixed ranges disabled:
Sep 04 12:19:46 secOps kernel:   00000-FFFFF uncachable
Sep 04 12:19:46 secOps kernel: MTRR variable ranges disabled:
```

Il comando “**sudo journalctl -u nginx.service --since today**” si usa per leggere il contenuto dei log del server **nginx** del giorno corrente.

```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Wed 2024-09-04 13:38:32 EDT.
-- No entries --
[analyst@secOps ~]$
```

Si usa lo switch “**-k**” come nel comando “**sudo journalctl -k**” per leggere solo i log del kernel.

```
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Wed 2024-09-04 13:40:47 EDT.
Sep 04 12:19:46 secOps kernel: Linux version 4.15.15-1-ARCH (builduser@heftig-4)
Sep 04 12:19:46 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=
Sep 04 12:19:46 secOps kernel: KERNEL supported cpus:
Sep 04 12:19:46 secOps kernel:   Intel GenuineIntel
Sep 04 12:19:46 secOps kernel:   AMD AuthenticAMD
Sep 04 12:19:46 secOps kernel:   Centaur CentaurHauls
Sep 04 12:19:46 secOps kernel: [Firmware Bug]: TSC doesn't count with P0 frequency
Sep 04 12:19:46 secOps kernel: x86/fpu: x87 FPU will use FXSAVE
Sep 04 12:19:46 secOps kernel: e820: BIOS-provided physical RAM map:
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000000000]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000000009fc00-0x0000000000000000]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000000]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x000000000000100000-0x0000000000000dff]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x000000000000dff0000-0x0000000000000dff]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffff]
Sep 04 12:19:46 secOps kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000011ff]
Sep 04 12:19:46 secOps kernel: NX (Execute Disable) protection: active
Sep 04 12:19:46 secOps kernel: random: fast init done
```


Mentre il comando “**sudo journalctl -f**” permette di seguire in real time la scrittura dei log di **journald**.

```
[analyst@sec0ps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Sep 04 13:38:32 sec0ps sudo[926]: pam_unix(sudo:session): session opened for use
r root by (uid=0)
Sep 04 13:38:35 sec0ps sudo[926]: pam_unix(sudo:session): session closed for use
r root
Sep 04 13:40:43 sec0ps sudo[935]: analyst : TTY=pts/1 ; PWD=/home/analyst ; USE
R=root ; COMMAND=/usr/bin/journalctl -k
Sep 04 13:40:43 sec0ps sudo[935]: pam_unix(sudo:session): session opened for use
r root by (uid=0)
Sep 04 13:40:43 sec0ps sudo[935]: pam_unix(sudo:session): session closed for use
r root
Sep 04 13:40:47 sec0ps sudo[938]: analyst : TTY=pts/1 ; PWD=/home/analyst ; USE
R=root ; COMMAND=/usr/bin/journalctl -k
Sep 04 13:40:47 sec0ps sudo[938]: pam_unix(sudo:session): session opened for use
r root by (uid=0)
Sep 04 13:40:49 sec0ps sudo[938]: pam_unix(sudo:session): session closed for use
r root
Sep 04 13:42:21 sec0ps sudo[945]: analyst : TTY=pts/1 ; PWD=/home/analyst ; USE
R=root ; COMMAND=/usr/bin/journalctl -f
Sep 04 13:42:21 sec0ps sudo[945]: pam_unix(sudo:session): session opened for use
r root by (uid=0)
```