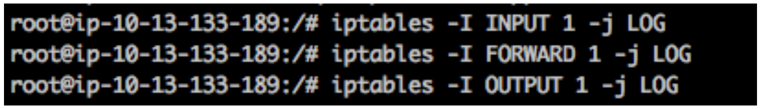
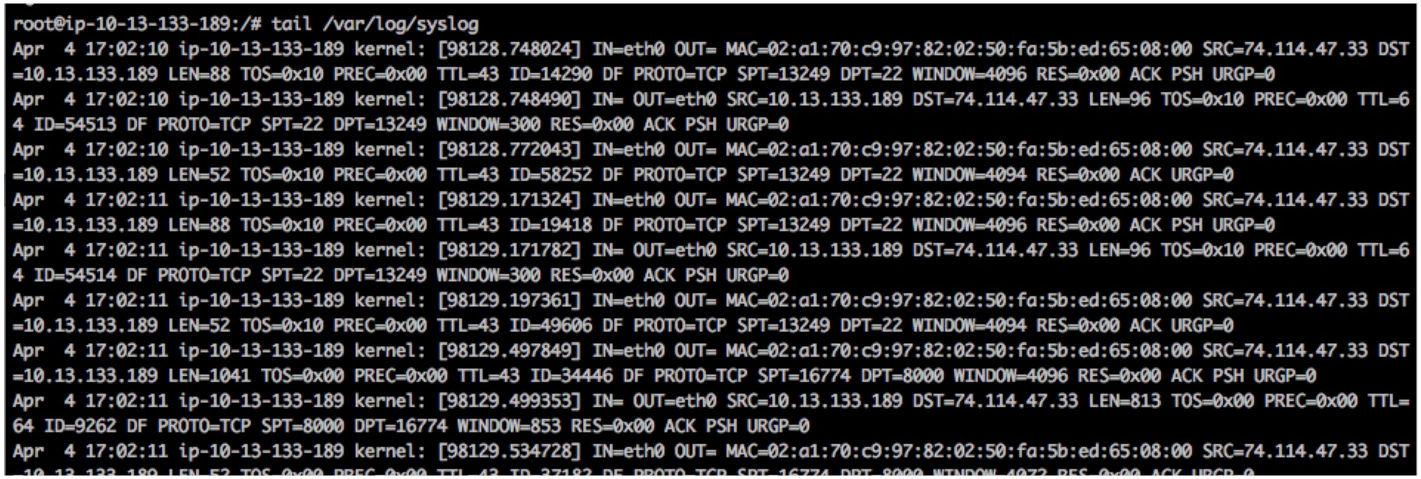
Lab 3: More Data

- Auth logs are interesting, but let’s add something else
- Start by making iptables log (allthethings)

```
iptables -I INPUT 1 -j LOG
iptables -I FORWARD 1 -j LOG
iptables -I OUTPUT 1 -j LOG
```



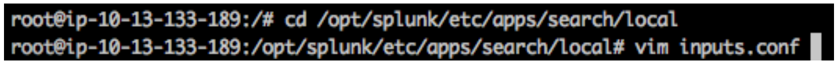
```
root@ip-10-13-133-189:/# iptables -I INPUT 1 -j LOG
root@ip-10-13-133-189:/# iptables -I FORWARD 1 -j LOG
root@ip-10-13-133-189:/# iptables -I OUTPUT 1 -j LOG
```



```
root@ip-10-13-133-189:/# tail /var/log/syslog
Apr  4 17:02:10 ip-10-13-133-189 kernel: [98128.748024] IN=eth0 OUT= MAC=02:a1:70:c9:97:82:02:50:fa:5b:ed:65:08:00 SRC=74.114.47.33 DST
=10.13.133.189 LEN=88 TOS=0x10 PREC=0x00 TTL=43 ID=14290 DF PROTO=TCP SPT=13249 DPT=22 WINDOW=4096 RES=0x00 ACK PSH URGP=0
Apr  4 17:02:10 ip-10-13-133-189 kernel: [98128.748490] IN= OUT=eth0 SRC=10.13.133.189 DST=74.114.47.33 LEN=96 TOS=0x10 PREC=0x00 TTL=6
4 ID=54513 DF PROTO=TCP SPT=22 DPT=13249 WINDOW=300 RES=0x00 ACK PSH URGP=0
Apr  4 17:02:10 ip-10-13-133-189 kernel: [98128.772043] IN=eth0 OUT= MAC=02:a1:70:c9:97:82:02:50:fa:5b:ed:65:08:00 SRC=74.114.47.33 DST
=10.13.133.189 LEN=52 TOS=0x10 PREC=0x00 TTL=43 ID=58252 DF PROTO=TCP SPT=13249 DPT=22 WINDOW=4094 RES=0x00 ACK URGP=0
Apr  4 17:02:11 ip-10-13-133-189 kernel: [98129.171324] IN=eth0 OUT= MAC=02:a1:70:c9:97:82:02:50:fa:5b:ed:65:08:00 SRC=74.114.47.33 DST
=10.13.133.189 LEN=88 TOS=0x10 PREC=0x00 TTL=43 ID=19418 DF PROTO=TCP SPT=13249 DPT=22 WINDOW=4096 RES=0x00 ACK PSH URGP=0
Apr  4 17:02:11 ip-10-13-133-189 kernel: [98129.171782] IN= OUT=eth0 SRC=10.13.133.189 DST=74.114.47.33 LEN=96 TOS=0x10 PREC=0x00 TTL=6
4 ID=54514 DF PROTO=TCP SPT=22 DPT=13249 WINDOW=300 RES=0x00 ACK PSH URGP=0
Apr  4 17:02:11 ip-10-13-133-189 kernel: [98129.197361] IN=eth0 OUT= MAC=02:a1:70:c9:97:82:02:50:fa:5b:ed:65:08:00 SRC=74.114.47.33 DST
=10.13.133.189 LEN=52 TOS=0x10 PREC=0x00 TTL=43 ID=49606 DF PROTO=TCP SPT=13249 DPT=22 WINDOW=4094 RES=0x00 ACK URGP=0
Apr  4 17:02:11 ip-10-13-133-189 kernel: [98129.497849] IN=eth0 OUT= MAC=02:a1:70:c9:97:82:02:50:fa:5b:ed:65:08:00 SRC=74.114.47.33 DST
=10.13.133.189 LEN=1041 TOS=0x00 PREC=0x00 TTL=43 ID=34446 DF PROTO=TCP SPT=16774 DPT=8000 WINDOW=4096 RES=0x00 ACK PSH URGP=0
Apr  4 17:02:11 ip-10-13-133-189 kernel: [98129.499353] IN= OUT=eth0 SRC=10.13.133.189 DST=74.114.47.33 LEN=813 TOS=0x00 PREC=0x00 TTL=
64 ID=9262 DF PROTO=TCP SPT=8000 DPT=16774 WINDOW=853 RES=0x00 ACK PSH URGP=0
Apr  4 17:02:11 ip-10-13-133-189 kernel: [98129.534728] IN=eth0 OUT= MAC=02:a1:70:c9:97:82:02:50:fa:5b:ed:65:08:00 SRC=74.114.47.33 DST
=10.13.133.189 LEN=52 TOS=0x00 PREC=0x00 TTL=43 ID=37182 DF PROTO=TCP SPT=16774 DPT=8000 WINDOW=4073 RES=0x00 ACK URGP=0
```

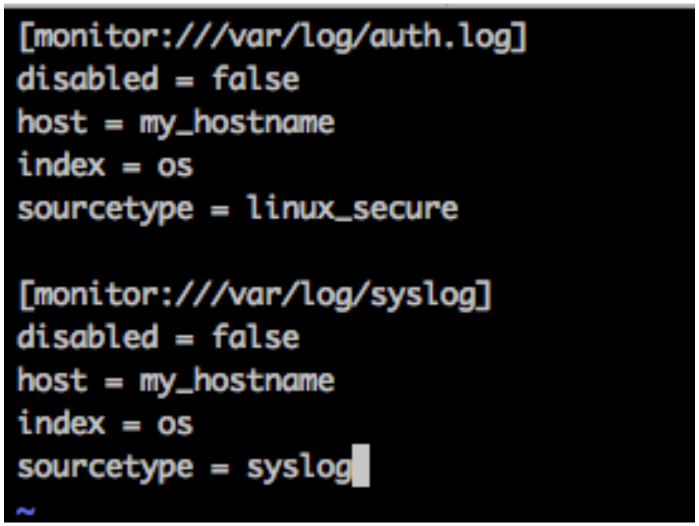
Time to Bring on Some More Data

- Let’s do this the hard(er) way



```
root@ip-10-13-133-189:/# cd /opt/splunk/etc/apps/search/local
root@ip-10-13-133-189:/opt/splunk/etc/apps/search/local# vim inputs.conf
```

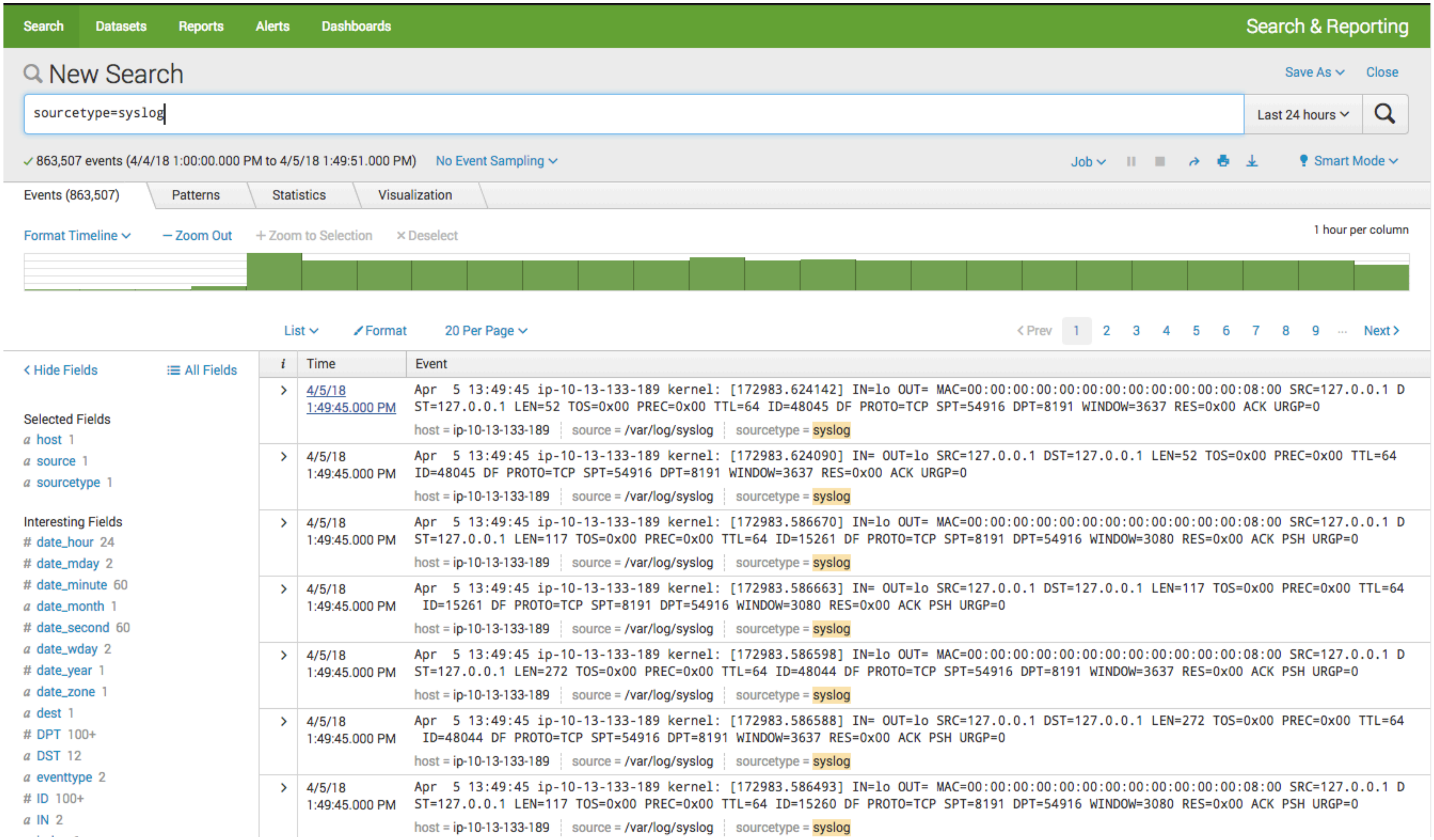
  - Open your inputs.conf from the previous exercise
  - Add an inputs stanza for the file containing iptables logs
  - Restart Splunk



```
[monitor:///var/log/auth.log]
disabled = false
host = my_hostname
index = os
sourcetype = linux_secure

[monitor:///var/log/syslog]
disabled = false
host = my_hostname
index = os
sourcetype = syslog
~
```

Now We Have iptables Logs:



New Search

```
sourcetype=syslog
```

Last 24 hours

✓ 863,507 events (4/4/18 1:00:00.000 PM to 4/5/18 1:49:51.000 PM) No Event Sampling

Smart Mode

Selected Fields
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- # date_hour 24
- # date_mday 2
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 2
- # date_year 1
- a date_zone 1
- a dest 1
- # DPT 100+
- a DST 12
- a eventtype 2
- # ID 100+
- a IN 2

i	Time	Event
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.624142] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48045 DF PROTO=TCP SPT=54916 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.624090] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48045 DF PROTO=TCP SPT=54916 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.586670] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=117 TOS=0x00 PREC=0x00 TTL=64 ID=15261 DF PROTO=TCP SPT=8191 DPT=54916 WINDOW=3080 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.586663] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=117 TOS=0x00 PREC=0x00 TTL=64 ID=15261 DF PROTO=TCP SPT=8191 DPT=54916 WINDOW=3080 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.586598] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=272 TOS=0x00 PREC=0x00 TTL=64 ID=48044 DF PROTO=TCP SPT=54916 DPT=8191 WINDOW=3637 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.586588] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=272 TOS=0x00 PREC=0x00 TTL=64 ID=48044 DF PROTO=TCP SPT=54916 DPT=8191 WINDOW=3637 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog
>	4/5/18 1:49:45.000 PM	Apr 5 13:49:45 ip-10-13-133-189 kernel: [172983.586493] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=117 TOS=0x00 PREC=0x00 TTL=64 ID=15260 DF PROTO=TCP SPT=8191 DPT=54916 WINDOW=3080 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = syslog