Blacklisting Badguys With IPTables

Gary Smith

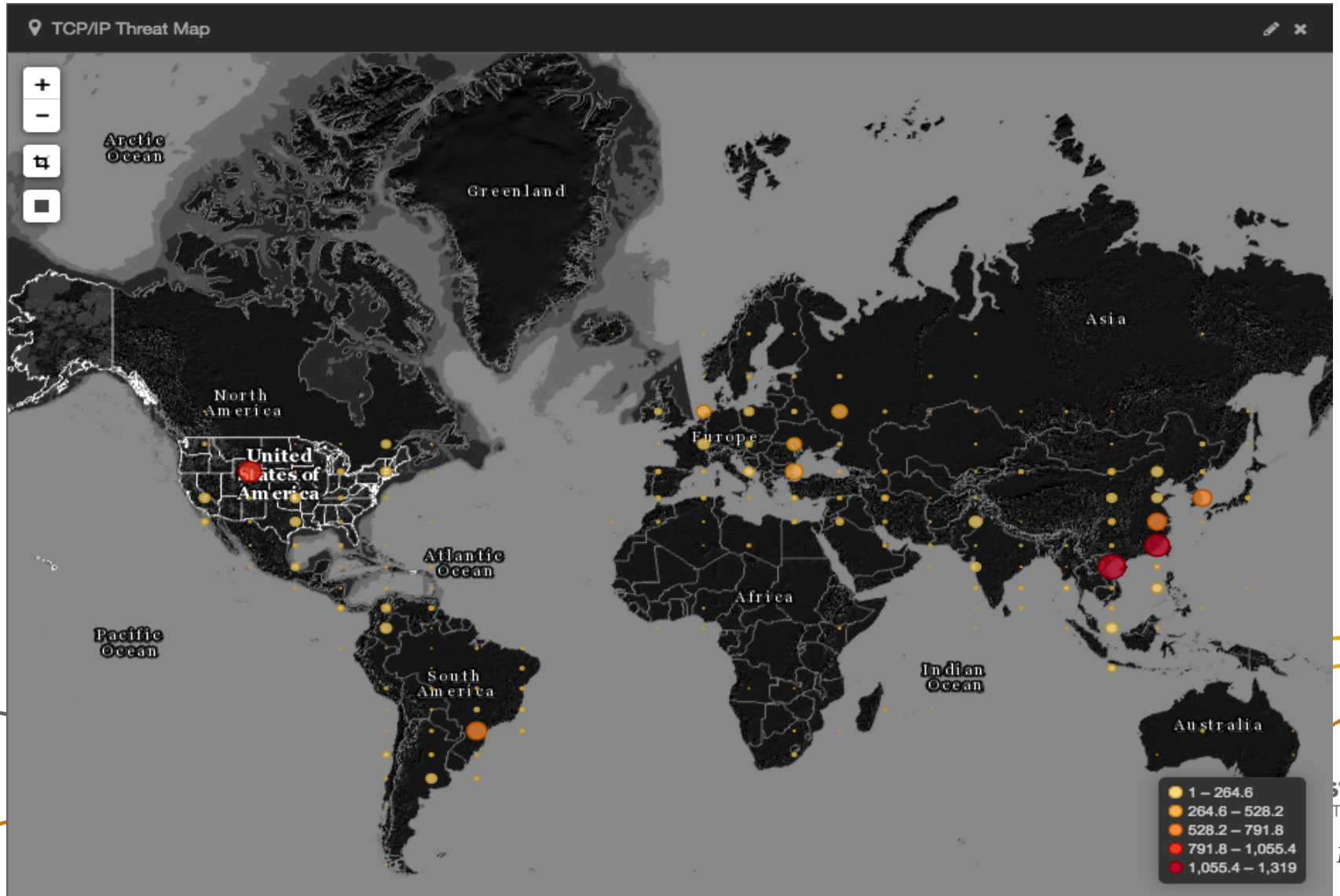
Cyber Security Analyst

Pacific Northwest National Laboratory

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

They Come From Everywhere



Lots of Threats Out There

Threat Name	Count	# Unique Sources
Microsoft SQL Server communication attempt	10128	3001
DoomJuice file upload attempt	7002	134
MS Terminal Server communication attempt	5198	2276
UPnP communication attempt	1134	338
VNC communication attempt	1098	409
Radmin Default install options attempt	977	335
Microsoft PPTP communication attempt	531	69
HP Web JetAdmin communication attempt	359	211
HP JetDirect LCD communication attempt	162	72
PCAnywhere communication attempt	124	59

Fwlogwatch Report

fwlogwatch summary
fwlogwatch@ [fwlogwatch@

Sent: Saturday, May 07, 2016 12:20 AM
To: Smith, Gary R

fwlogwatch summary

Generated Saturday May 07 03:20:01 EDT 2016 by root.
1419 (and 6002 older than 86400 seconds) of 19703 entries in the file "/var/log/messages" are packet logs, 729 have unique characteristics.
First packet log entry: May 06 03:20:53, last: May 07 03:18:56.
All entries were logged by the same host: "mscdtn".
All entries have the same target: ".".
Only entries with a count of at least 2 are shown.

#	start	end	interval	chain	interface	proto	source	hostname	port	service	destination	hostname	port	service	opts
34	May 06 04:00:28	May 07 02:55:29	00:22:55:01	Dropped by firewall INPUT	p6p1	tcp	125.46.58.43	hn.kd.ny.adsl [forward lookup failed]	6000	x11			1433	ms-sql-s	SYN
9	May 06 21:32:34	May 06 21:33:28	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	220.243.228.72	-	80	http			57325	-	---r--
9	May 06 21:33:14	May 06 21:34:36	00:00:01:22	Dropped by firewall INPUT	p6p1	tcp	74.125.200.102	sa-in-f102.1e100.net	80	http			40273	-	---r--
9	May 06 21:33:14	May 06 21:34:26	00:00:01:12	Dropped by firewall INPUT	p6p1	tcp	74.125.200.102	sa-in-f102.1e100.net	80	http			39405	-	---r--
9	May 06 21:33:14	May 06 21:34:23	00:00:01:09	Dropped by firewall INPUT	p6p1	tcp	74.125.200.102	sa-in-f102.1e100.net	80	http			37437	-	---r--
9	May 06 21:33:26	May 06 21:34:20	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	107.23.85.173	ec2-107-23-85-173.compute-1.amazonaws.com	80	http			37941	-	---r--
9	May 06 21:33:26	May 06 21:34:20	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	107.23.85.173	ec2-107-23-85-173.compute-1.amazonaws.com	80	http			60608	-	---r--
9	May 06 21:34:01	May 06 21:34:55	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	114.4.39.236	-	80	http			36994	-	---r--
9	May 06 21:34:02	May 06 21:34:56	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	52.74.165.151	ec2-52-74-165-151.ap-southeast-1.compute.amazonaws.com	80	http			51288	-	---r--
9	May 06 21:34:02	May 06 21:34:55	00:00:00:53	Dropped by firewall INPUT	p6p1	tcp	220.243.228.72	-	80	http			32993	-	---r--
9	May 06 21:34:03	May 06 21:34:57	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	54.193.40.98	ec2-54-193-40-98.us-west-1.compute.amazonaws.com	80	http			55930	-	---r--
9	May 06 21:35:12	May 06 21:36:06	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	52.22.237.171	ec2-52-22-237-171.compute-1.amazonaws.com	80	http			48533	-	---r--
9	May 06 21:35:12	May 06 21:36:06	00:00:00:54	Dropped by firewall INPUT	p6p1	tcp	52.22.237.171	ec2-52-22-237-171.compute-1.amazonaws.com	80	http			42217	-	---r--
9	May 06 21:36:42	May 06 21:37:49	00:00:01:07	Dropped by firewall INPUT	p6p1	tcp	31.13.79.251	xx-fbcdn-shv-01-sin1.fbcdn.net	443	https			50253	-	---r--

Blacklist Sources

- Project Honey Pot Directory of Dictionary Attacker IPs
- TOR Exit Nodes
- MaxMind GeoIP Anonymous Proxies
- BruteForceBlocker IP List
- Spamhaus Don't Route Or Peer List (DROP)
- C.I. Army Malicious IP List
- OpenBL.org 30 day List
- blocklist.de attackers
- StopForumSpam
- GreenSnow
- Firehol Level 1

It's Scripting Time!

- Create a script to pull the Badguys' IP Addresses from these sources.
- Remove the duplicate addresses.
- Sort them for readability.
- Format the addresses to look something like these IPTables commands:
  - -A INPUT -s 185.93.185.237/32 -j DROP
  - -A INPUT -s 204.2.134.164/24 -j DROP
  - -A INPUT -s 208.100.26.228/32 -j DROP
- And so on for 60,000 more rules… YIPES!

Houston, We Have A Problem!

- The problem is: **This doesn't scale.**
- Netfilter rules work like a fall-through trapdoor.
- In the end this means every single packet which is sent to your host needs to be checked whether it matches the patterns specified in every rule of yours.
- This requires a substantial computing overhead for every rule you are adding to your system.
- Being under attack, the performance of your server is poor already. However, by adding many rules to your firewall you are actually further increasing computing overhead for every request significantly.

Use the ipset, Luke

- ipset is a "match extension" for IPTables.
- To use it, you create and populate uniquely named "sets" using the ipset command-line tool, and then separately reference those sets in the match specification of one or more IPTables rules.
- A “set” is simply a list of addresses stored efficiently for fast lookup.

Example Use of ipset

- ipset create blacklist hash:net
- ipset add blacklist 185.93.185.237
- ipset add blacklist 204.2.134.0/24
- ipset add blacklist 208.100.26.228
- iptables -I INPUT 1 -m set --match-set blacklist src -j LOG --log-prefix "IP Blacklisted INPUT ”
- iptables -I INPUT 2 -m set --match-set blacklist src -j DROP

It’s scripting time, once again!

- Modify script to generate ipset commands instead of iptables commands to look similar to this:

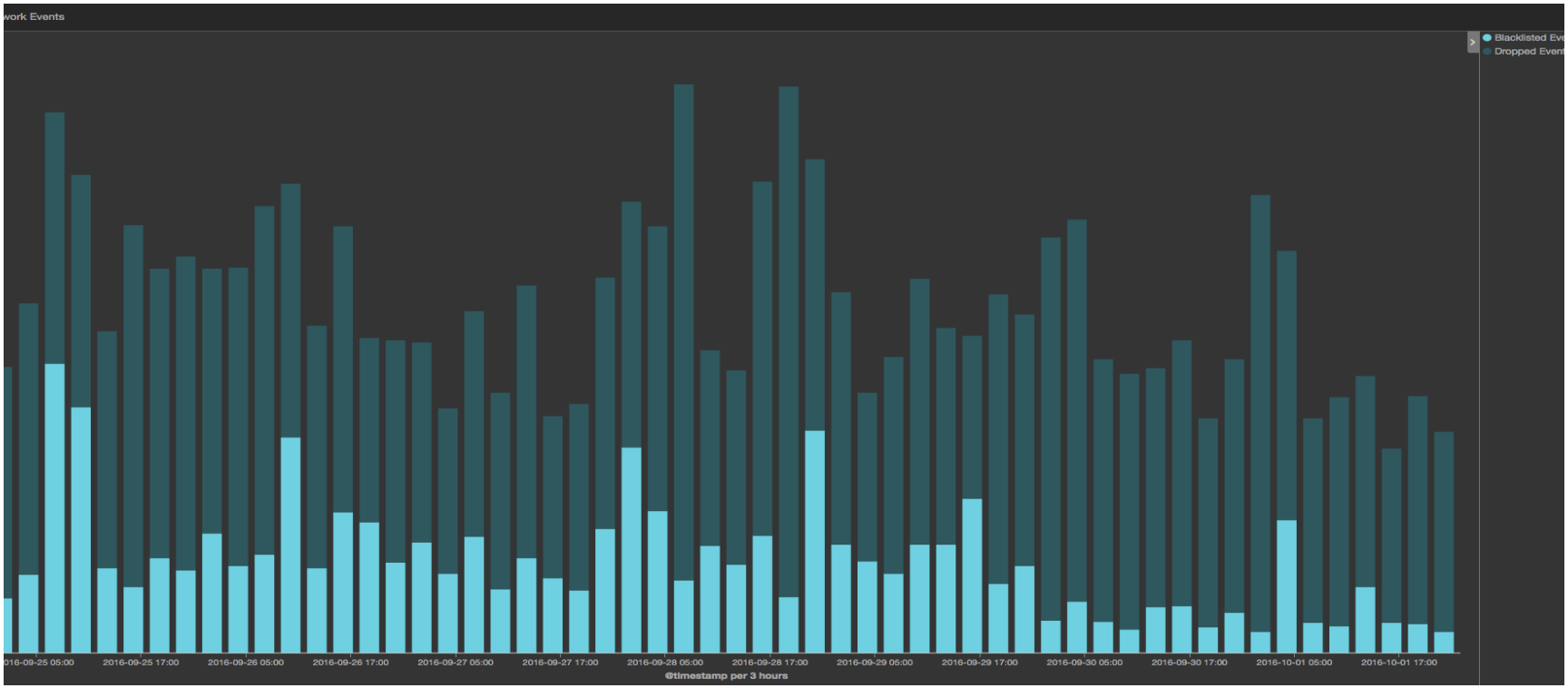
```
create blacklist -exist hash:net family inet hashsize 16384 maxelem 131072
add blacklist 1.0.197.74
add blacklist 1.10.16.0/20
add blacklist 1.1.1.1
add blacklist 1.1.249.4
add blacklist 1.116.0.0/14
add blacklist 1.129.96.131
add blacklist 1.136.22.224
```

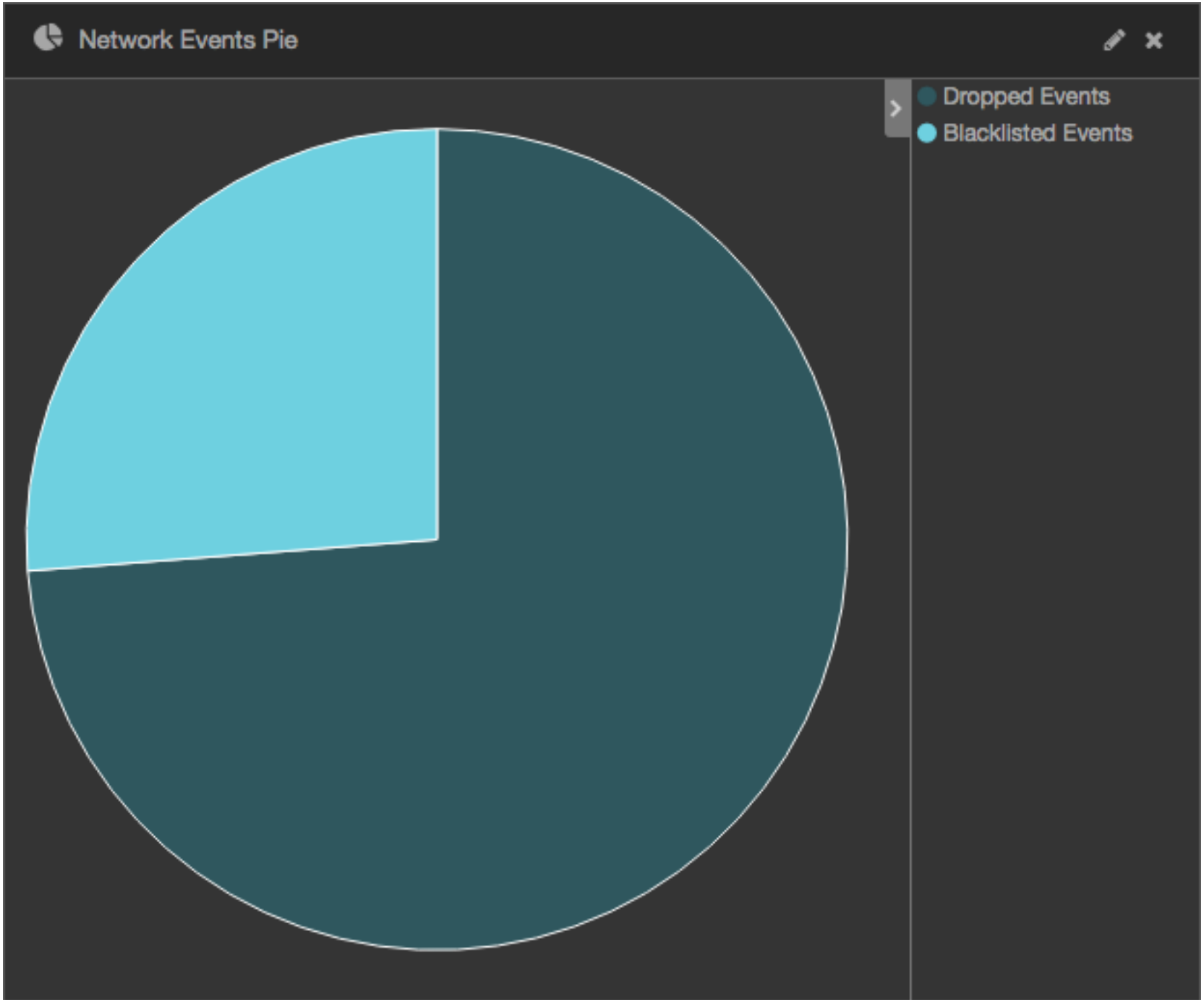
Iptables Config – Take 1

- Modify the beginning of /etc/sysconfig/iptables to look like this:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m set --match-set blacklist src -j LOG --log-prefix "IP Blacklisted INPUT "
-A INPUT -m set --match-set blacklist src -j DROP
```

Blacklisted versus Network Events




Network Events Pie
Dropped Events
Blacklisted Events

Adding A Custom Blacklist

- Remember the pretty html summary from fwlogwatch? It also has a text output option.
- Step 1: Run a fwlogwatch report with the text output option.
- Step 2: Extract the new offending IP addresses to a file.
- Step 3: It's scripting time once again => change the ipset command generating script to incorporate the custom blacklist.
- Step 4: Run the script.
- Step 5: Daily lather, rinse, repeat.

Dynamically Ban Hosts Attempting To Access Invalid Services

- ipset also provides a "target extension" to iptables that provides a mechanism for dynamically adding and removing set entries based on any iptables rule.
- Instead of having to add entries manually with the ipset command, you can have iptables add them for you on the fly.
- Now /etc/sysconfig/iptables looks like this:

/etc/sysconfig/iptables

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m multiport --dports 23,1433,2323,3306,3389,5060 -j SET --add-set blacklist src
-A INPUT -p udp -m multiport --dports 137,138,139,161,5060 -j SET --add-set blacklist src
-A INPUT -m set --match-set blacklist src -j LOG --log-prefix "IP Blacklisted INPUT "
-A INPUT -m set --match-set blacklist src -j DROP
```

Dynamically Adding Invalid Services With ipset

- ipset is not just for IP addresses.
- With ipset you can create a bitmap of ports/port ranges to store port numbers and such a set can store up to 65536 ports.
- Create a list of invalid services for TCP and UDP:

ipset create bl-tcp-ports bitmap:port range 0-65535

ipset create bl-udp-ports bitmap:port range 0-65535

Dynamically Adding Invalid Services With ipset

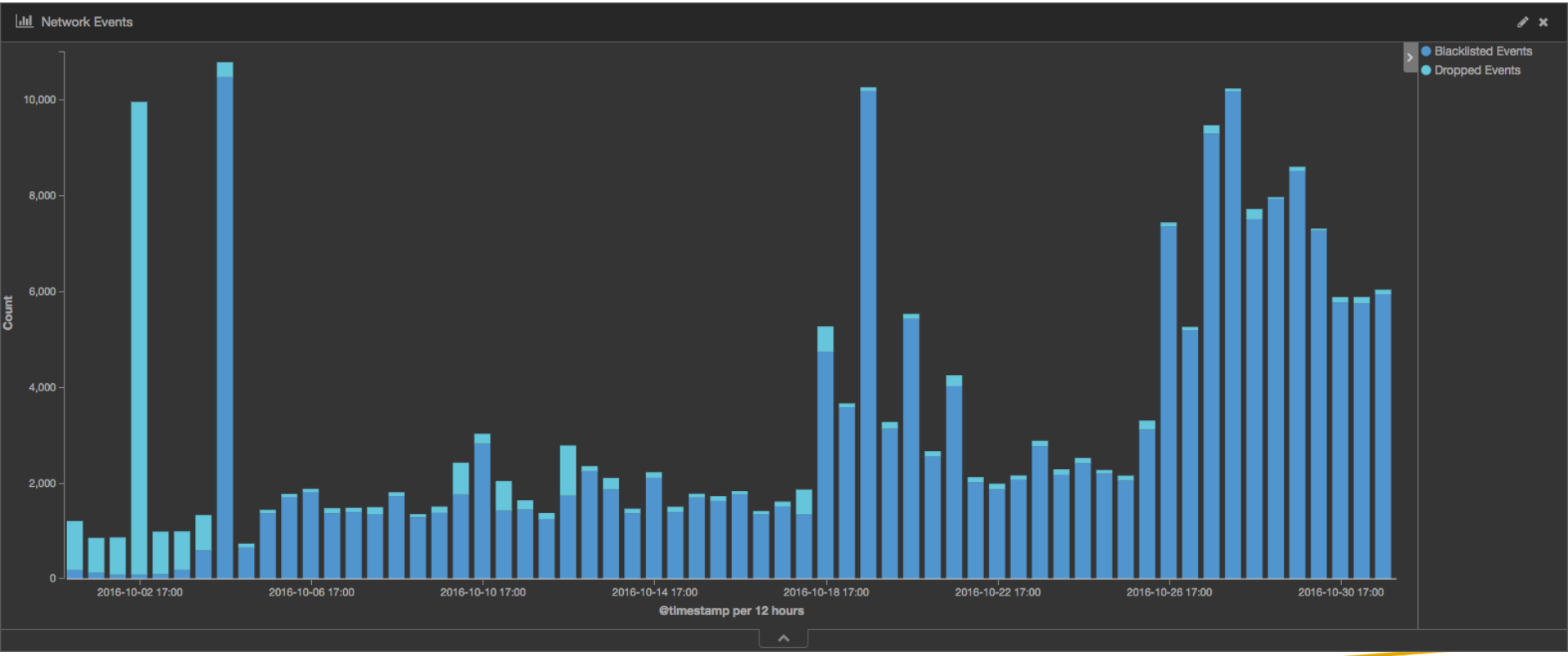
- Add the invalid ports into the ipset bitmaps:

```
ipset add bl-tcp-ports 23
ipset add bl-tcp-ports 1433
ipset add bl-tcp-ports 2323
ipset add bl-tcp-ports 3306
ipset add bl-tcp-ports 3389
ipset add bl-tcp-ports 5060
```

/etc/sysconfig/iptables – next revision

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp -m set --match-set bl-tcp-ports dst -j SET --add-set blacklist src
-A INPUT -p udp -m udp -m set --match-set bl-udp-ports dst -j SET --add-set blacklist src
-A INPUT -m set --match-set blacklist src -j LOG --log-prefix "IP Blacklisted INPUT "
-A INPUT -m set --match-set blacklist src -j DROP
```

Blacklisted Events vs. Dropped Events – After All The Improvements



Tweak Number 1 – Add A Whitelist

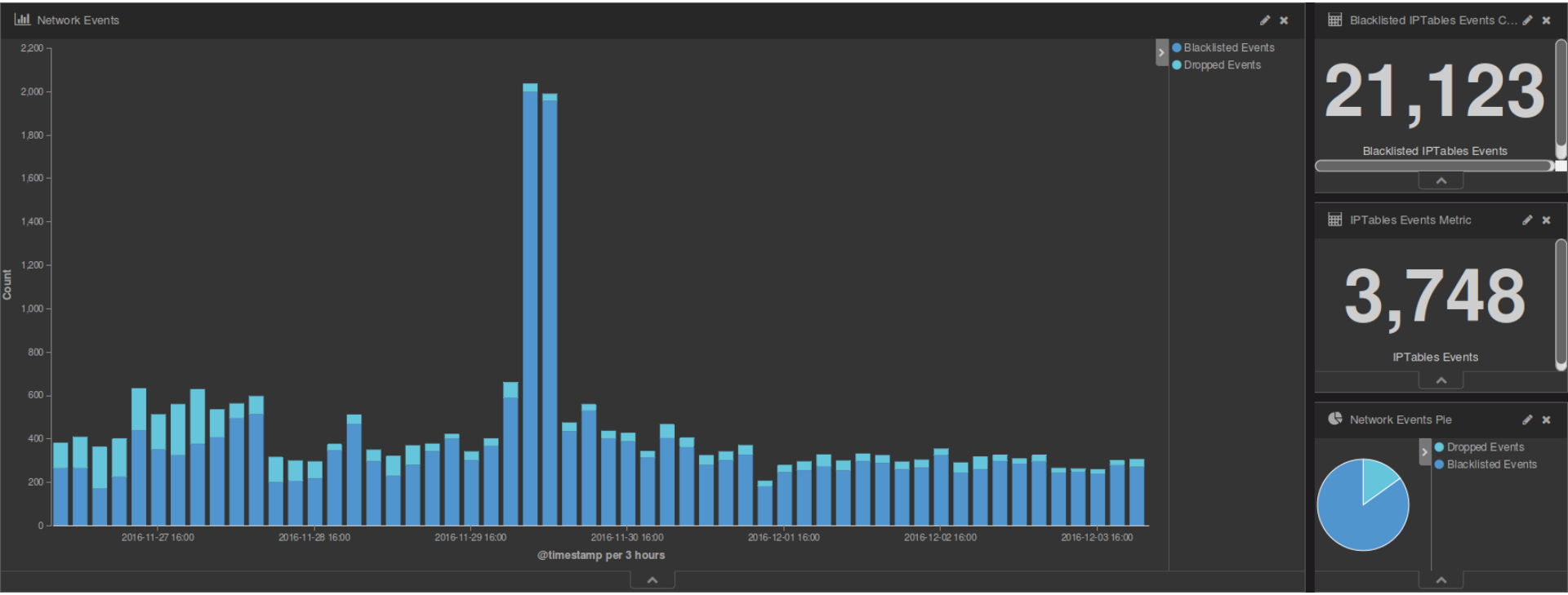
- Create a whitelist of IP addresses you want to allow access:
  - ipset create whitelist -exist hash:net family inet hashsize 16384 maxelem 131072
- Add hosts to the whitelist:
  - ipset add whitelist 192.168.101.102
- Modify /etc/sysconfig/iptables to use the whitelist:

/etc/sysconfig/iptables – With Whitelist

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m set --match-set whitelist src -j LOG --log-prefix "IP Whitelisted INPUT "
-A INPUT -m set --match-set whitelist src -j ACCEPT
-A INPUT -p tcp -m tcp -m set --match-set bl-tcp-ports dst -j SET --add-set blacklist src
-A INPUT -p udp -m udp -m set --match-set bl-udp-ports dst -j SET --add-set blacklist src
-A INPUT -m set --match-set blacklist src -j LOG --log-prefix "IP Blacklisted INPUT "
-A INPUT -m set --match-set blacklist src -j DROP
```

Tweak Number 2 – Blacklist with OUTPUT

- Add a line like this to /etc/sysconfig/iptables
  - -A OUTPUT -m set --match-set blacklist dst -j LOG --log-prefix "IP Blacklisted OUTPUT ”
- Why is there not a DROP statement after this LOG statement?


Network Events
Blacklisted Events
Dropped Events
2,200
2,000
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
Count
2016-11-27 16:00
2016-11-28 16:00
2016-11-29 16:00
2016-11-30 16:00
2016-12-01 16:00
2016-12-02 16:00
2016-12-03 16:00
@timestamp per 3 hours
Blacklisted IPTables Events C...
21,123
Blacklisted IPTables Events
IPTables Events Metric
3,748
IPTables Events
Network Events Pie
Dropped Events
Blacklisted Events

That's All Folks

- There are many, high quality, free IP address blacklists available on the Internet
- ipset adds many useful features and capabilities to the already very powerful netfilter/iptables suite.
- Any time you want to apply firewall rules to groups of hosts or addresses at once, you should be using ipset, especially for blacklisting (or whitelisting).
- IPTables and ipset make a great combination to keep the Badguys off the porch.
- Email me at gary.smith@pnnl.gov


BLACKLISTED!
imgflip.com