

LOOKING FOR A NEEDLE IS A STACK OF NEEDLES

Finding problems before they wake you up at night

16TH ANNUAL NEW YORK STATE CYBER SECURITY CONFERENCE

JUNE 2013

DAVID SANTERAMO

ABOUT ME

- Security Leader for Logic Technology (LTI) located in Schenectady.
- Former Navy Cryptographer
- 20 years networking and security experience in both public and private networks

Twitter - @dsantera

Email – dsantera@ltonline.com

Linkedin - www.linkedin.com/pub/david-santeramo/1/856/352/

A BRIEF TRIP INTO HISTORY

- Joe Rochefort
- Navy Cryptographer
- His team was able to decrypt only about 10% of Japanese secure communications.
- But watching traffic patterns (logs) he figured out a pattern
- Played a hunch



THE 2AM CALL



We have all been there. Sound asleep. Your phone starts to make that dreaded noise.

You receive a message, email or phone call saying that the web site is down

What is the first thing that you do to figure out what happened?

HOW MANY OF YOU HAVE A CRYSTAL BALL?

No one can predict or forecast when something will go wrong...

Or can you?

Most security organizations spend the vast majority of their time in firefighting mode.

Verizon report 47,000 reported breaches in 2012

Your organization will NEVER get ahead of the curve if it simply remains in a reactive posture.

Pre-emptive hack???

Remember, you have to be right all of the time. The person trying to breach your network only has to be right ONCE....

Security organizations need to use log analysis methodology in order to get an edge

GETTING ALL YOUR DATA IN ONE PLACE AND WORKING TOGETHER

- 1) Disk Disk and more Disk – in logging you can never have too much space
- 2) Access controls – You need to control access to your crystal ball.
- 3) Compliance needs – masking of data. How does logging play with your various logging needs.
- 4) Determining what needs to be logged?
 - 1) Authentication attempts/denies
 - 2) Changes
 - 3) Firewall rule activity? How much detail....

COVERT LOGGING

Logging when you don't want people to know you are logging

Where would you do this? DMZ, collocation facilities

Why?

- Keep the log server protected Last step of a good hack is to cover your tracks.
- Honeypots/Honeynets
- Could run into issues regarding compliance*

A PICTURE SAYS A 1000 WORDS

2013-05-01 17:26:58 67.248.133.5:2858 66.109.41.232:443 67.248.133.5:2858 10.1.1.28:443 HTTPS 263 sec. 3194
3053 Close - TCP RST

2013-05-01 17:26:54 74.70.107.197:53949 66.109.41.232:443 74.70.107.197:53949 10.1.1.28:443 HTTPS 7 sec. 1920
1030 Close - TCP RST

2013-05-01 17:26:48 66.87.117.4:44156 66.109.41.232:443 66.87.117.4:44156 10.1.1.28:443 HTTPS 18 sec. 3819
12988 Close - TCP FIN

2013-05-01 17:26:42 67.242.81.48:54536 66.109.41.232:443 67.242.81.48:54536 10.1.1.28:443 HTTPS 621 sec. 4299
3838 Close - TCP FIN

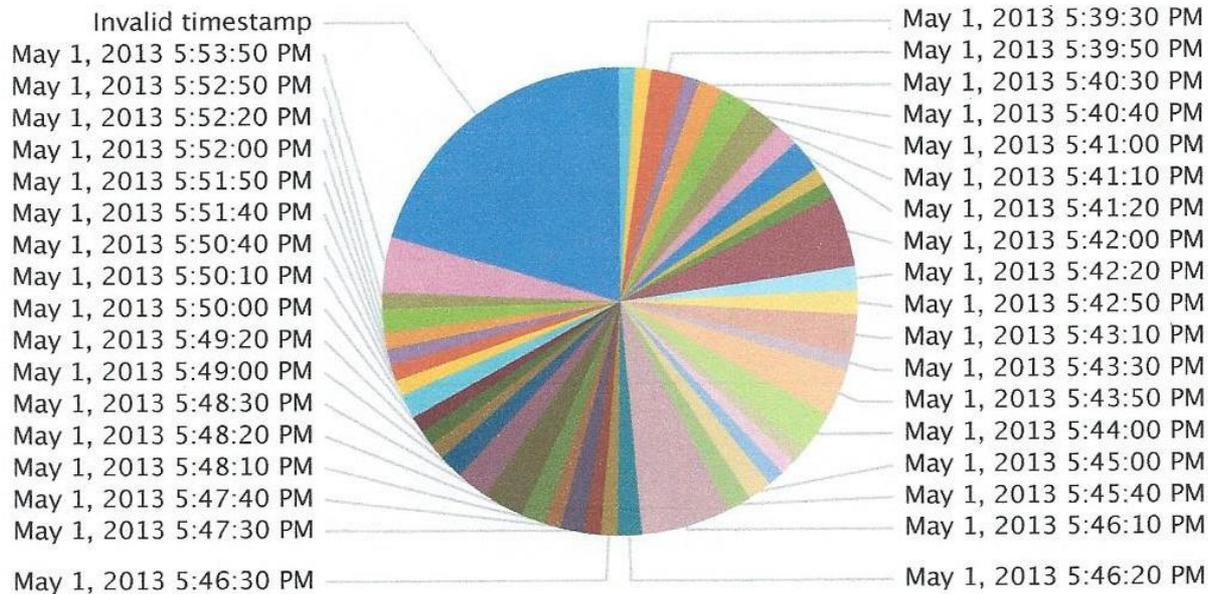
2013-05-01 17:26:36 208.87.203.23:5523 66.109.41.232:443 208.87.203.23:5523 10.1.1.28:443 HTTPS 29 sec. 12283
26475 Close - TCP FIN

2013-05-01 17:26:34 66.87.117.4:60418 66.109.41.232:443 66.87.117.4:60418 10.1.1.28:443 HTTPS 4 sec. 2201 1171
Close - TCP RST

2013-05-01 17:26:16 108.226.133.236:53774 66.109.41.232:443 108.226.133.236:53774 10.1.1.28:443 HTTPS 323
sec. 3458 3933 Close - TCP FIN

A PICTURE MAKES DATA MUCH EASIER TO READ

TCP FIN



LOG ANALYSIS TOOLS

The last thing that you want to do is be sorting through data in Excel

Trust me....

I have done the work this way

How do you pick the right one...

Next are some products that I have used to perform the necessary log correlation and data extraction.



FIREWALL LOG ANALYSIS WITHOUT A BUDGET

For all of you in IT that have no budget for tools.... There is hope.

What to do with the age old problem of figuring out how the hacker got in..

Logs usually have specific entries that allow for coorelation.

access-list OUTSIDE line 2 extended deny tcp host 192.168.208.63 host 192.168.150.77 range netbios-ssn 445 (**hitcnt=1842**) **0x5063b82f**

access-list OUTSIDE line 3 extended deny icmp host 192.168.208.63 host 192.168.150.77 (**hitcnt=6**) **0xd3f63b90**

SPLUNK

Summary | Search | Status | Dashboards & Views | Searches & Reports

Summary | Actions

search Last 30 days

All indexed data

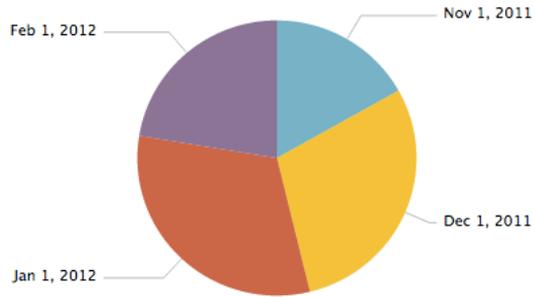
This lists all of the data you have loaded into your default indexes. [Add more data.](#)

Events indexed: 134,186,157
Earliest event: Mon Nov 14 11:51:51 2011
Latest event: Wed May 1 19:25:01 2013

Sources (2/3)

	source	Count	Last Update
1	udp:514	134,186,033	Wed May 1 19:25:01 2013
2	tcp:514	93	Mon Apr 2 10:17:16 2012
3	tcp:137	31	Mon Apr 2 10:15:40 2012

SPLUNK REPORTING



Table

Overlay: Enable Preview [Export](#)

10 per page

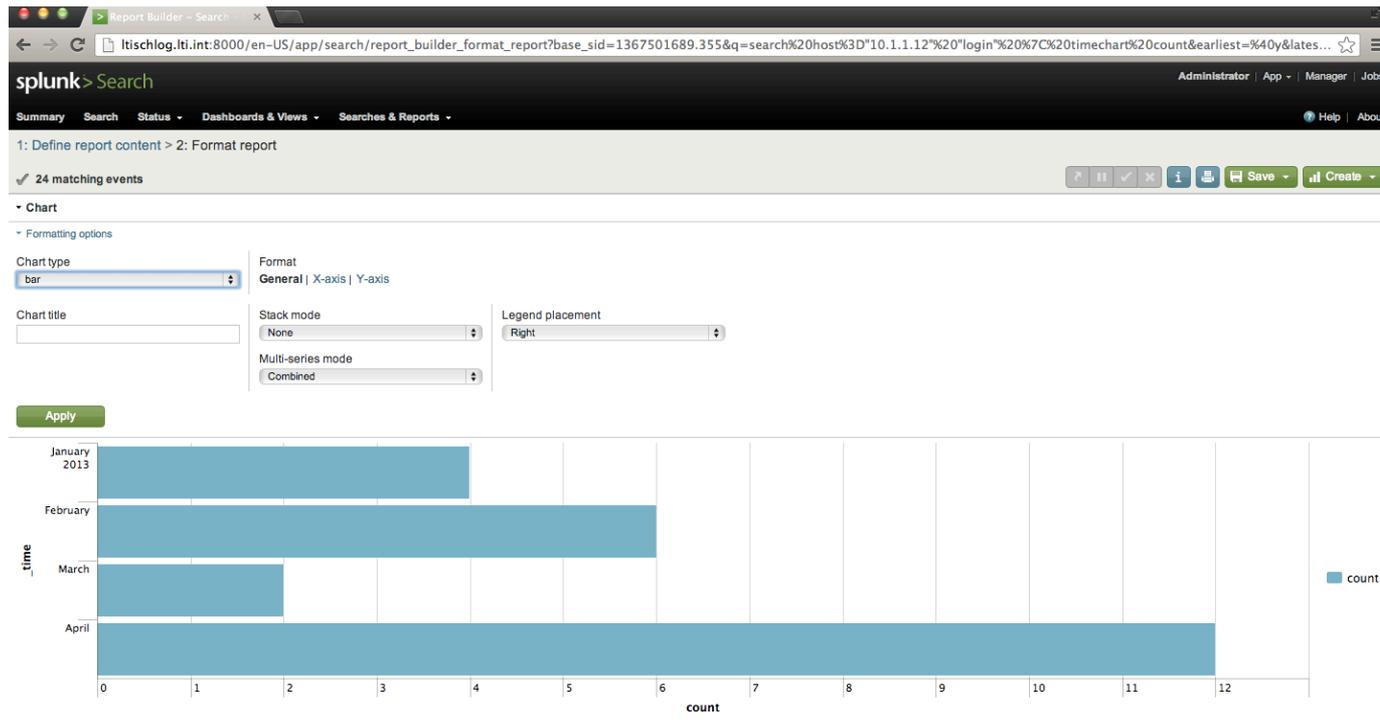
	_time ↓	count ↓
1	11/1/11 12:00:00.000 AM	197
2	12/1/11 12:00:00.000 AM	343
3	1/1/12 12:00:00.000 AM	367
4	2/1/12 12:00:00.000 AM	262

This is all from the free version



FURTHER USE OF DATA

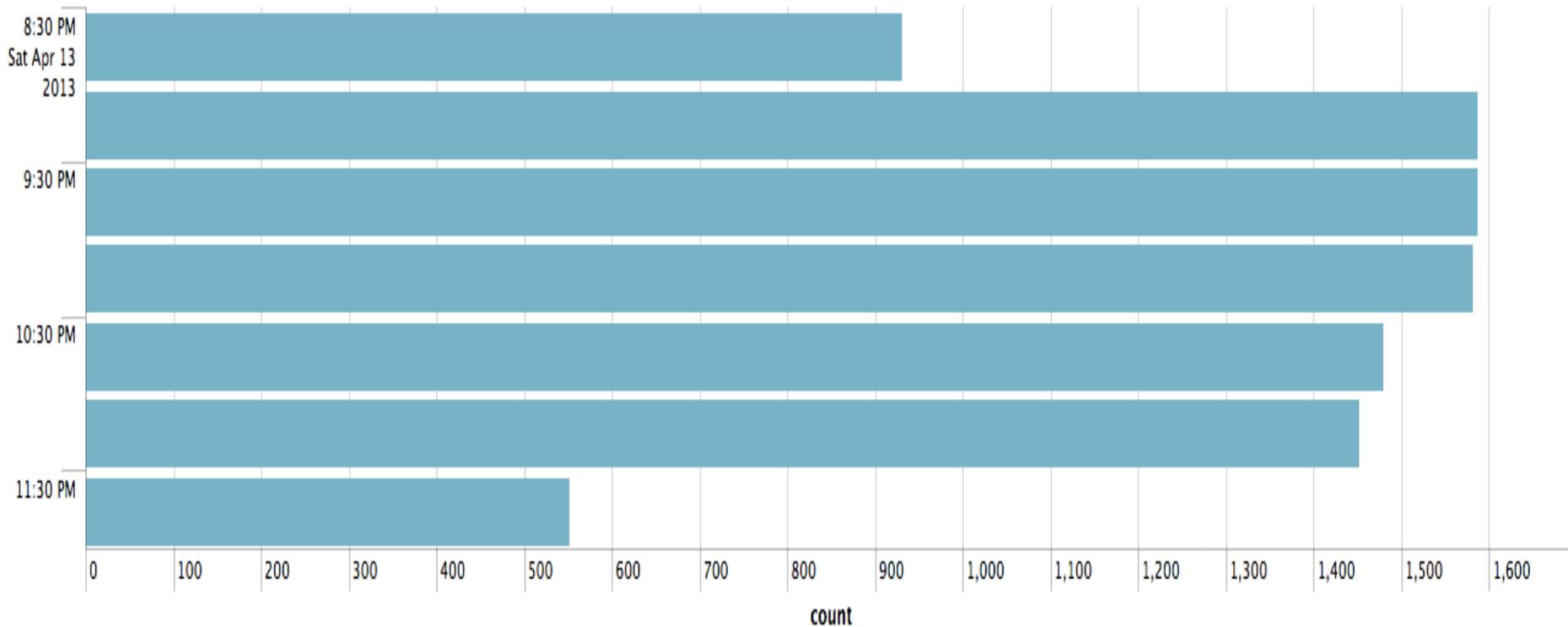
How many of you would like to trend the number of attempts from the Internet to log into a host



THE REAL POWER OF KNOWING YOUR DATA

Lets take a look at 218.108.0.91

Logs are showing repeated attempts to log into the same server on April 13th. 2013



SO WHO IS 218.108.0.91?

inetnum: 218.108.0.0 - 218.109.255.255
netname: WASU
descr: WASU TV & Communication Holding Co.,Ltd.
descr: 6/F, Jian Gong Building, NO.20 Wen San Road, Hangzhou,
descr: Zhejiang province, P.R.China 310012
country: CN
admin-c: XZ1291-AP
tech-c: TF142-AP
status: ALLOCATED PORTABLE
mnt-by: MAINT-CNNIC-AP
mnt-lower: MAINT-CNNIC-AP
mnt-routes: MAINT-CNNIC-AP
changed: hm-changed@apnic.net 20080123

For those not familiar with China....



Maps from google maps

AND THE LOGIN ATTEMPTS ARE CREATIVE

4/13/13

11:41:36.000 PM

Apr 13 23:41:36 10.1.1.14 sshd[11771]: Failed password for invalid user kevinmitnick from 218.108.0.91 port 54713 ssh2

Host=

They even tried to login using Kevin Mitnick as a username

IN SUMMARY

You have the data already in order to try to get ahead of the game.

Look at it...

The tools are out there. Even for those that have no budget.

Think of it this way

The more you learn about who is trying to get in the more you will sleep at night.

RESOURCES THAT MIGHT INTEREST YOU

Splunk - <http://www.splunk.com/>

Symantec - <http://www.symantec.com/>

Arcsight – <http://www.hp.com>

Tenable – www.tenable.com

AND SOME BOOKS TO READ ABOUT THE SUBJECT

Applied Security Visualization – Raffael Marty

Implementing Splunk: Big Data Reporting and Development for
Operational Intelligence - Vincent Bumgarner

Logging and Log management - Dr. Anton Chuvakin

QUESTIONS

