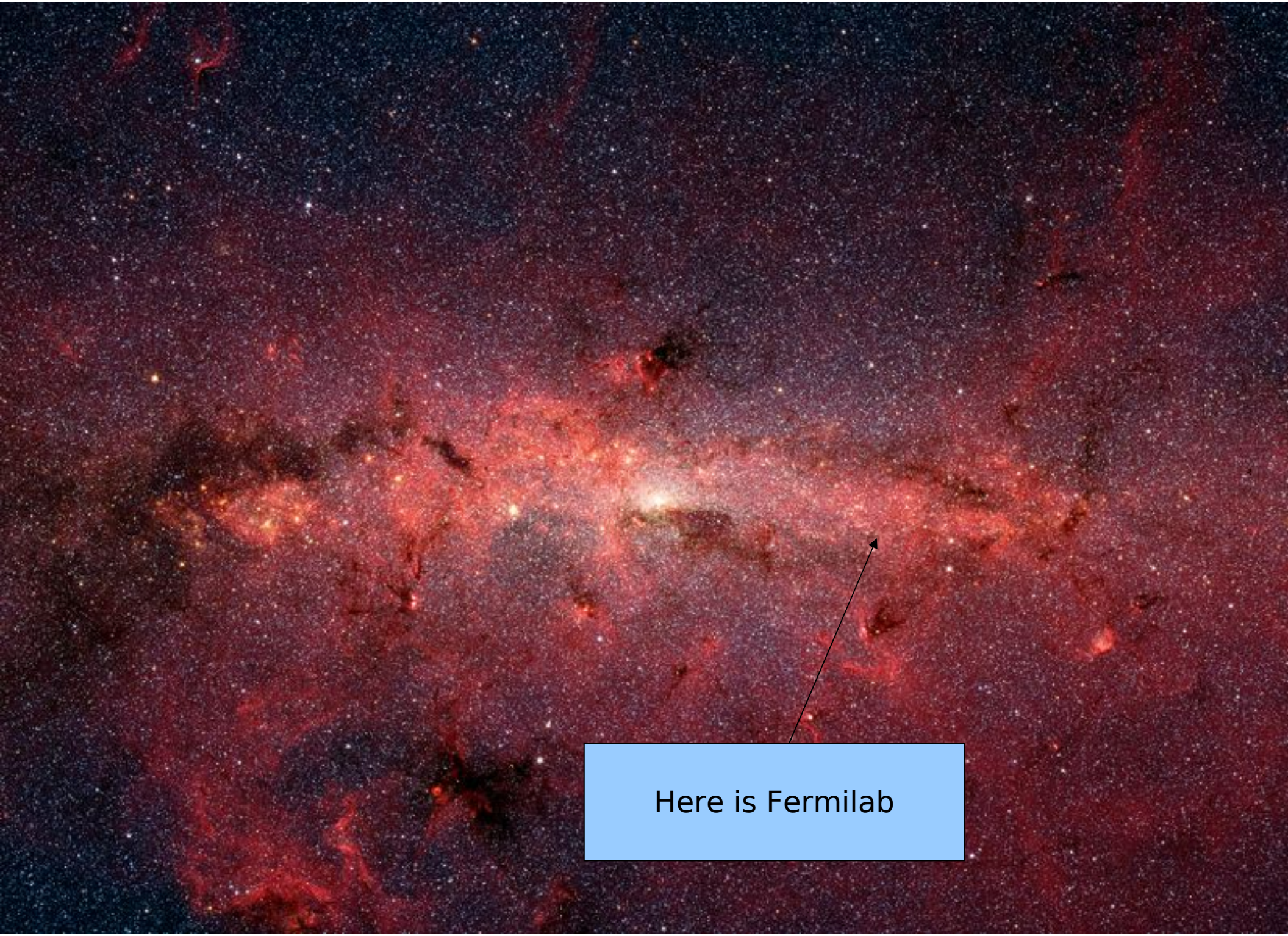
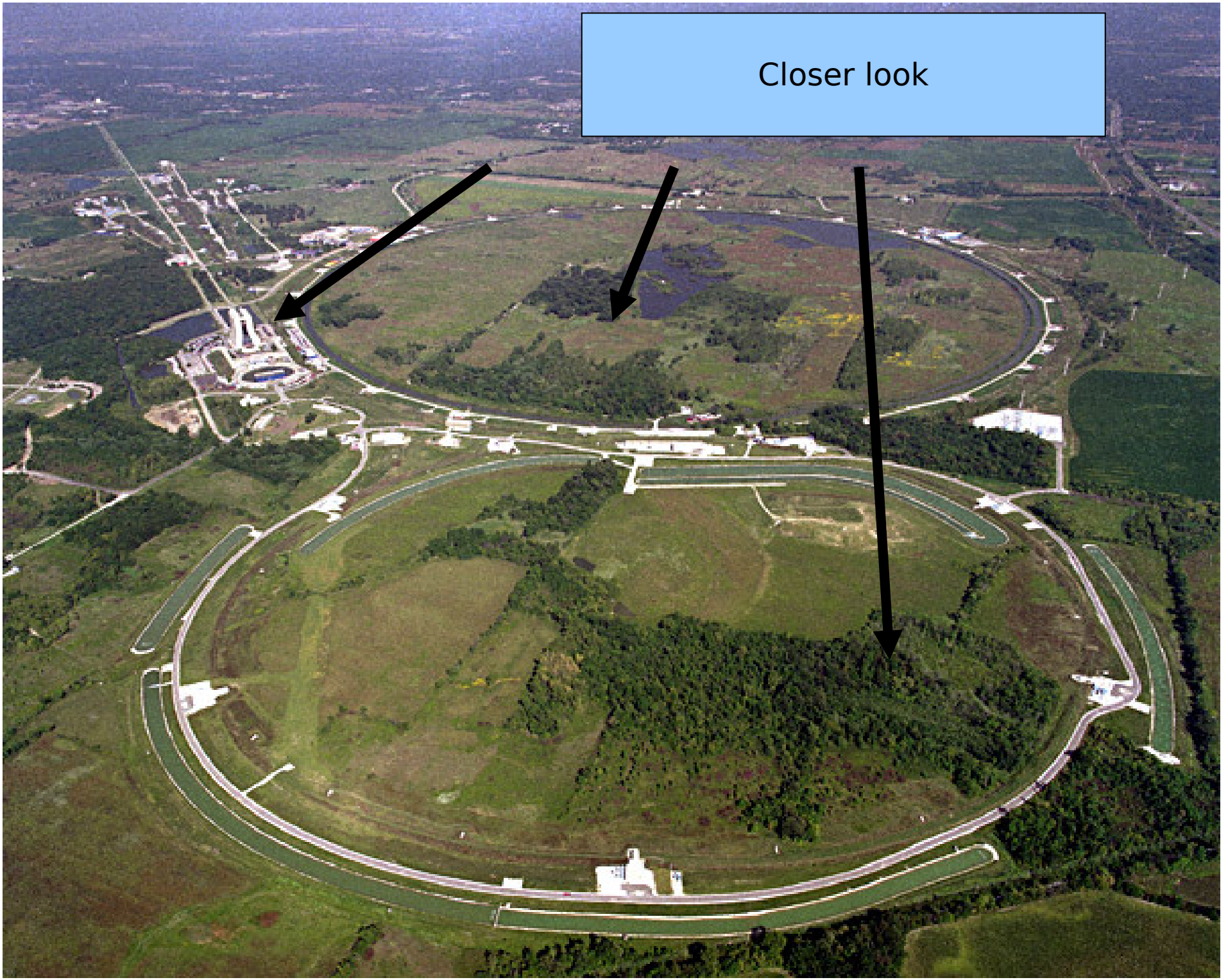
Computer Security @ FNAL

Frank Nagy

and

Tim Rupp


Here is Fermilab

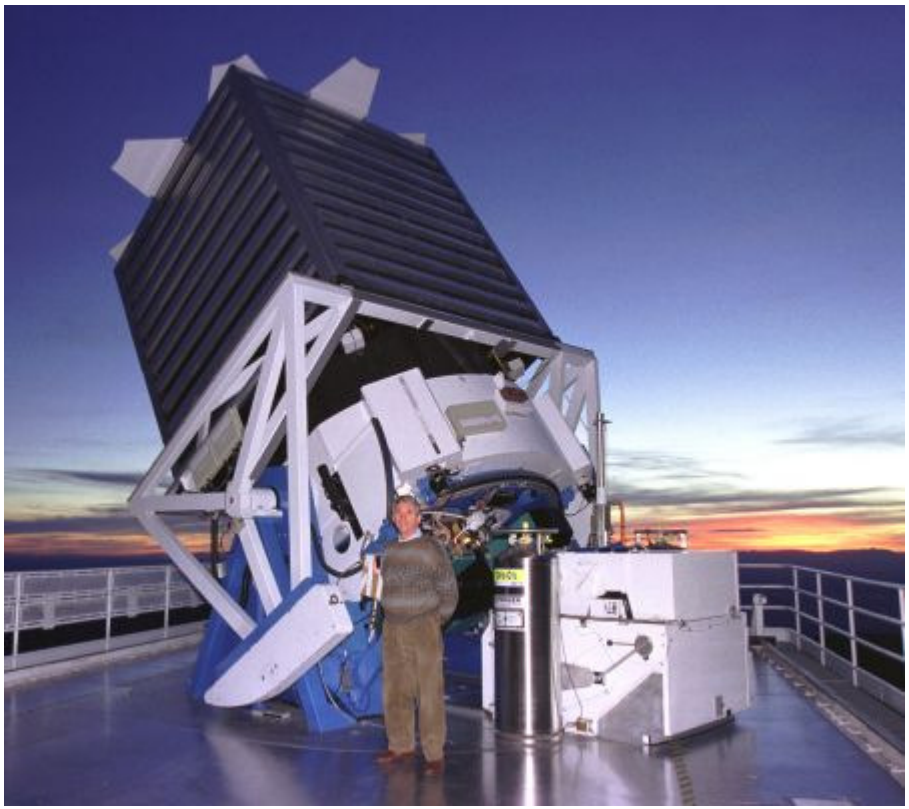

Closer look

Fermilab is

- A high energy physics lab
- Research in theoretical and experimental particle and astrophysics.
- Part of the Dept. of Energy
- Located in Batavia IL
- An “open science” lab
  - Collaboration with universities and labs around the world. Such as...

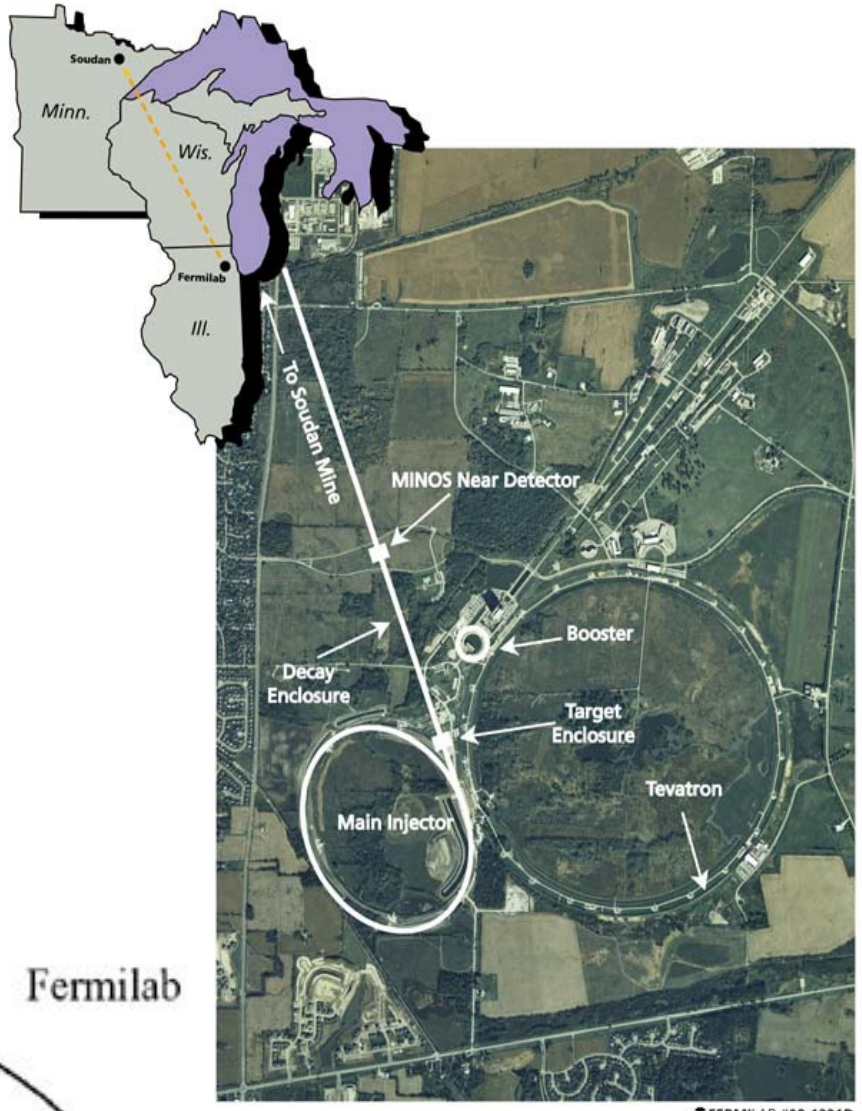
Open Science

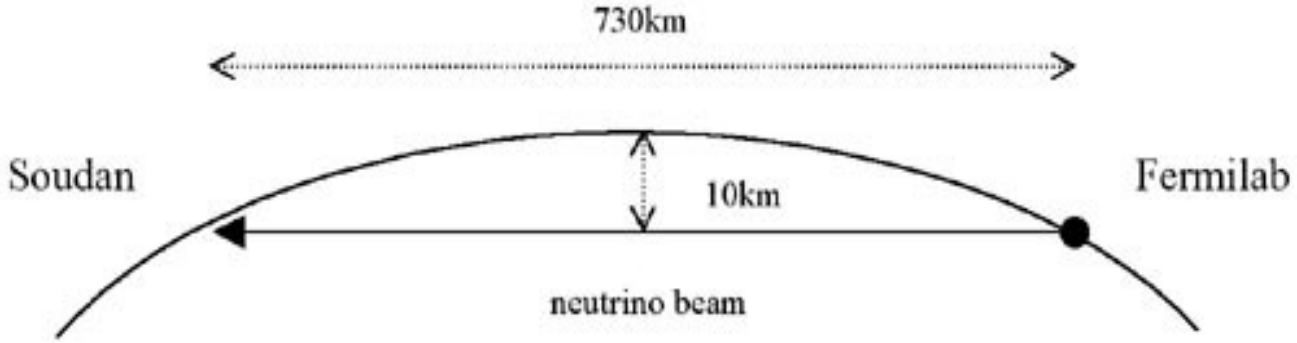
- SDSS telescope at Apache Point Observatory in Sunspot, New Mexico



More Science

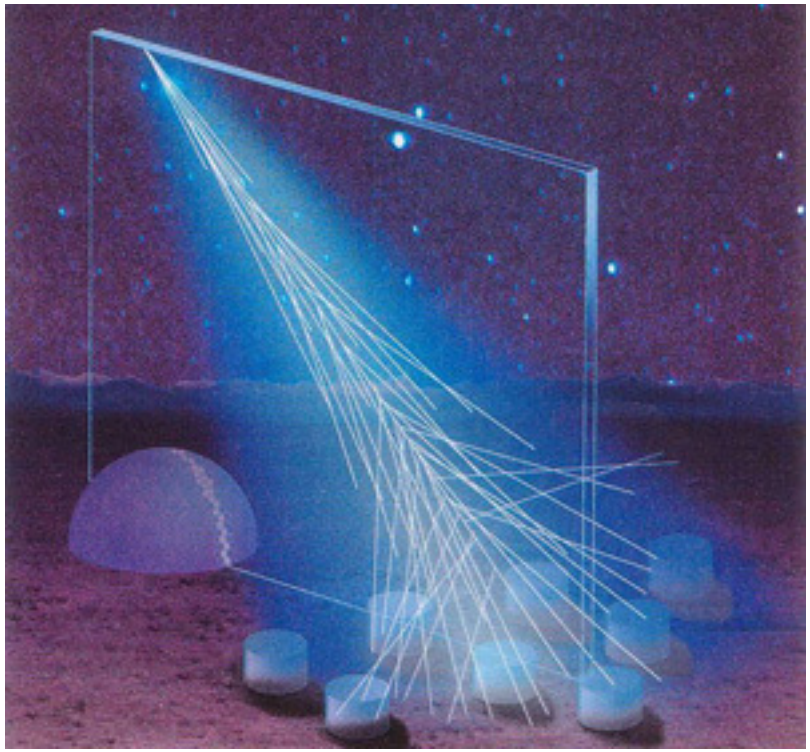
- Neutrino Detector in Soudan Minnesota





Some more open science

- Pierre Auger Cosmic Ray Detector in Argentina



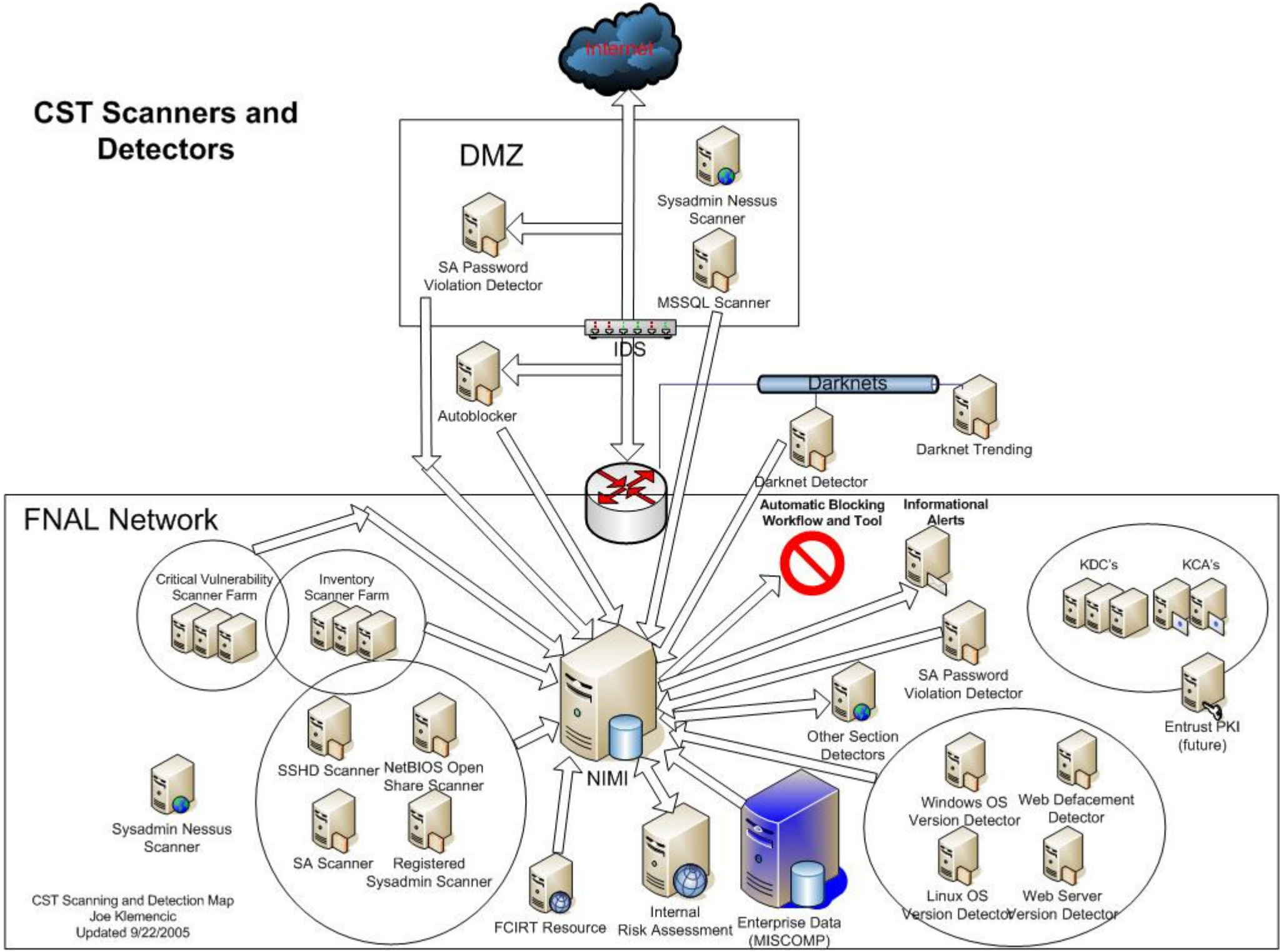
and much, much more

Back to computer security

Cogs in our System

- Policy, process and documentation
- Authentication
- Logging
- Scanning and Blocking
- Incidents and FCIRT
- Asset Tracking
- Community Awareness
- Outside help

CST Scanners and Detectors



Policies, process and docs

- Central location

security.fnal.gov

- Policies are the heart of the system
- Tools enforce the policies

Types of Policies

- Policy on computing
- CSPP (Cyber Security Program Plan)
  - Framework doc for all CompSec requirements at the lab
  - Baselines, major/minor apps, services
- Our policies are driven by
  - FISMA
  - NIST-800

Policy related tools

- CSA app
  - Risk assessments for all devices on network
- ST&E (System test and evaluation)
  - Used to satisfy auditors
  - Manual and automatic tests that verify policies we have in place
  - Logs who performs a test and their response to the evaluation

Policies

- Require that CST has a presence in almost every division.
- Be available to advise on new projects
- Involve lots of pen and paper

Tools

Have policy, will enforce

Authentication

- Kerberos and Active Directory
  - Unix realm and Win realm
  - Trust between the two
- X.509 certs tied to kerberos principal
  - Used for web auth
- DOEGrid certs
- Central LDAP authentication services
  - For those apps that can't do kerb or x509

Logging

- Central syslog-ng server
- Splunk
  - Fulltext search engine for our log files
- netflow database
  - Time partitioned Postgres database
  - Typically the first place we go to investigate incidents
  - 6 to 10 million flows an hour
  - Expected to increase as we go to 40 and 100 Gb/s by 2012

netflow

Netflow information for 131.225.82.104 from 02-01-2008 00:42:34 to 04-01-2008 07:44:16

```
Command=web:netflow.pl -a 131.225.82.104 -sd 02-01-2008 -st 00:42:34 -ed 04-01-2008 -et 07:44:16 -F /tmp/apache-359809969.flt
Start             End               Sif   SrcIPaddress    SrcP  DIf   DstIPaddress    DstP    P Fl Pkts       Octets
0201.01:08:33.031 0201.01:08:34.183 57    131.225.82.104  2100  58    89.43.242.34    3174  6   0  3          138
0201.01:08:33.030 0201.01:08:34.182 58    89.43.242.34    3174  57    131.225.82.104  2100  6   0  3          156
0201.03:28:57.463 0201.03:29:00.855 57    131.225.82.104  1024  58    72.36.164.228   80    6   0  2          92
0201.03:28:57.463 0201.03:29:00.855 58    72.36.164.228   80    57    131.225.82.104  1024  6   0  2          96
0201.06:30:33.811 0201.06:30:34.003 57    131.225.82.104  0     58    83.103.137.222  0     1   0  2          122
0201.06:30:33.812 0201.06:30:34.004 58    83.103.137.222  8     57    131.225.82.104  0     1   0  2          122
0201.08:29:44.977 0201.08:29:51.057 57    131.225.82.104  123   58    138.23.180.126  123   17  0  5          380
0201.08:29:45.172 0201.08:29:52.084 57    131.225.82.104  123   58    217.160.254.116 123   17  0  5          380
0201.08:29:45.172 0201.08:29:52.084 58    217.160.254.116 123   57    131.225.82.104  123   17  0  5          380
0201.08:29:45.044 0201.08:29:51.124 58    138.23.180.126  123   57    131.225.82.104  123   17  0  5          380
0201.08:29:45.363 0201.08:29:53.043 57    131.225.82.104  123   58    140.99.51.114   123   17  0  5          380
0201.08:29:45.427 0201.08:29:53.171 58    140.99.51.114   123   57    131.225.82.104  123   17  0  5          380
0201.08:30:56.208 0201.08:30:56.208 58    138.23.180.126  123   57    131.225.82.104  123   17  0  1          76
0201.08:30:56.148 0201.08:30:56.148 57    131.225.82.104  123   58    217.160.254.116 123   17  0  1          76
0201.08:30:56.148 0201.08:30:56.148 57    131.225.82.104  123   58    138.23.180.126  123   17  0  1          76
0201.08:30:56.147 0201.08:30:56.147 58    217.160.254.116 123   57    131.225.82.104  123   17  0  1          76
0201.08:30:58.195 0201.08:30:58.195 58    140.99.51.114   123   57    131.225.82.104  123   17  0  1          76
0201.08:30:58.131 0201.08:30:58.131 57    131.225.82.104  123   58    140.99.51.114   123   17  0  1          76
0201.08:31:59.248 0201.08:31:59.248 58    138.23.180.126  123   57    131.225.82.104  123   17  0  1          76
0201.08:32:02.194 0201.08:32:02.194 57    131.225.82.104  123   58    140.99.51.114   123   17  0  1          76
0201.08:32:02.194 0201.08:32:02.194 57    131.225.82.104  123   58    217.160.254.116 123   17  0  1          76
0201.08:32:02.194 0201.08:32:02.194 58    217.160.254.116 123   57    131.225.82.104  123   17  0  1          76
0201.08:32:02.258 0201.08:32:02.258 58    140.99.51.114   123   57    131.225.82.104  123   17  0  1          76
0201.08:31:59.186 0201.08:31:59.186 57    131.225.82.104  123   58    138.23.180.126  123   17  0  1          76
0201.08:33:08.238 0201.08:33:08.238 57    131.225.82.104  123   58    217.160.254.116 123   17  0  1          76
0201.08:33:08.306 0201.08:33:08.306 58    217.160.254.116 123   57    131.225.82.104  123   17  0  1          76
0201.08:33:05.295 0201.08:33:05.295 58    138.23.180.126  123   57    131.225.82.104  123   17  0  1          76
0201.08:33:05.231 0201.08:33:05.231 57    131.225.82.104  123   58    140.99.51.114   123   17  0  1          76
0201.08:33:05.231 0201.08:33:05.231 57    131.225.82.104  123   58    138.23.180.126  123   17  0  1          76
0201.08:33:05.362 0201.08:33:05.362 58    140.99.51.114   123   57    131.225.82.104  123   17  0  1          76
0201.08:34:12.303 0201.08:34:12.303 57    131.225.82.104  123   58    217.160.254.116 123   17  0  1          76
0201.08:34:12.370 0201.08:34:12.370 58    217.160.254.116 123   57    131.225.82.104  123   17  0  1          76
```

heatmaps from netflow

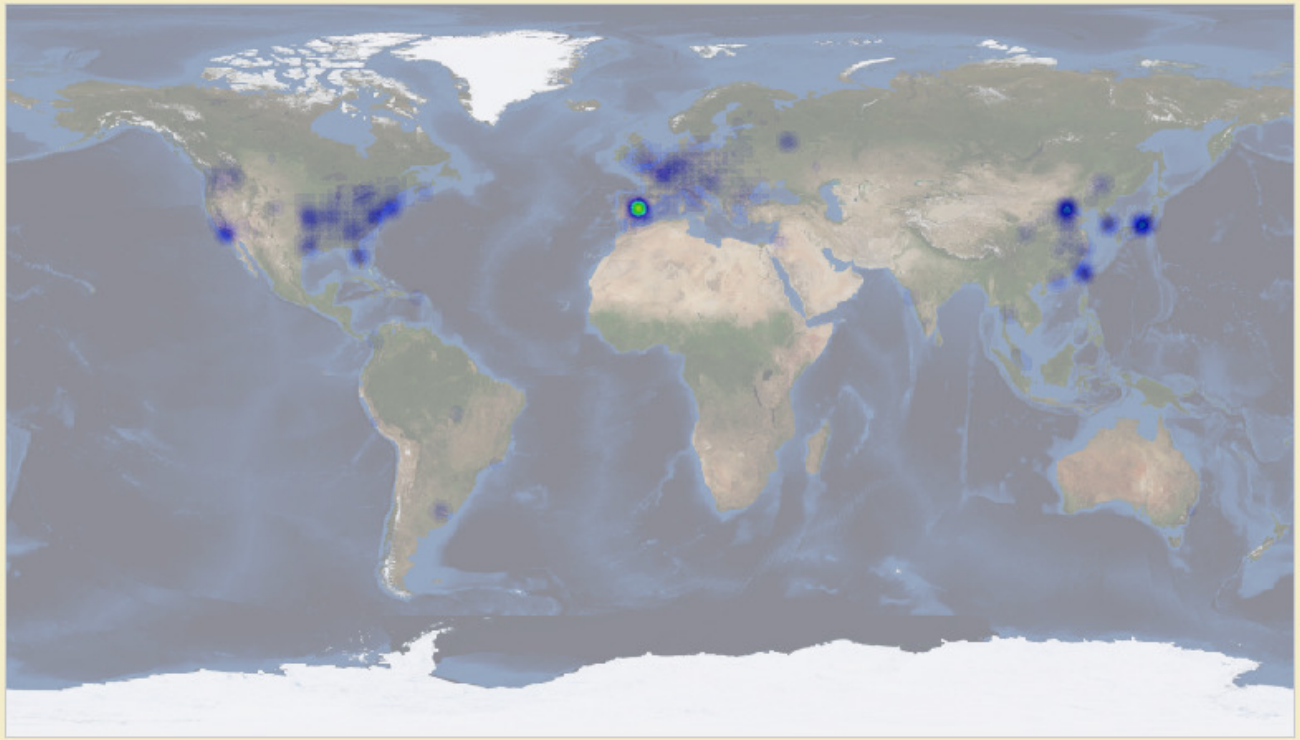
https://ovaltine.fnal.gov/heatmap/ — fnal csad

AB3 Events | What's going on where

Map of people talking to Fermilab : Last 24 hours

Top talkers

Talker	% of all talk
123.242.148.1	11.677 %
201.225.207.2	8.419 %
211.174.58.166	4.746 %
211.218.28.2	3.001 %
212.89.164.69	2.747 %
131.151.19.10	2.606 %
203.124.128.19	2.493 %
74.208.79.140	2.041 %
87.52.88.84	0.888 %
210.51.47.31	0.881 %
203.251.202.198	0.878 %
96.225.215.120	0.875 %
88.199.100.197	0.875 %



Top ports connected to

Service	% of all services
MSSQL	34.136 %
SSH	18.477 %
CIFS	6.847 %
NBT	6.798 %
ftp	5.095 %
NBT	4.749 %
MySQL	4.32 %
unknown: 32000	4.119 %
NBT	3.593 %
unknown: 1521	1.772 %
http	1.502 %
unknown: 21040	0.775 %
unknown: 1572	0.402 %

Top talker countries

Top talkers cloud

80.220.171.210 123.242.148.1 64.207.248.211 212.64.81.29 96.225.215.120 212.89.164.69 64.170.94.66
210.51.47.31 71.82.65.115 201.225.207.2 64.60.157.71 69.176.12.96 12.129.137.121 212.183.56.186 131.151.19.10
89.136.113.35 61.4.213.101 212.247.249.15 58.80.47.42 87.74.75.209 189.24.7.221 211.218.28.2 71.141.114.61 200.69.229.241
69.39.75.160 72.245.157.34 89.39.40.226 82.157.94.224 203.251.202.198 87.78.20.33 72.49.17.167 64.234.56.8 79.0.237.161
211.174.58.166 80.227.45.249 218.166.220.217 203.124.128.19 72.49.78.171 24.71.238.109 88.199.100.197 87.52.88.84
89.137.75.165 91.153.132.137 74.208.79.140 217.253.63.135 218.164.9.154 203.206.8.43 219.135.214.67 24.181.34.247
89.208.0.109

Top services connected to

Port	% of all ports
1433	34.136 %
22	18.477 %
445	6.847 %
139	6.798 %
21	5.095 %
137	4.749 %
3306	4.32 %
32000	4.119 %
135	3.593 %
1521	1.772 %
80	1.502 %
21040	0.775 %

Types of logs we've found useful

- Syslog
- Web GETs and POSTs
- Email headers
- DNS resolutions
- Firewall
- VPN

Scanning and Blocking

- Nessus scanner farm
- Special purpose scanners
  - MSSQL
  - Strong authentication
  - Critical vulnerabilities
- Autoblocking
  - Border, switchport, and DHCP
- Snort and Bro
- TIssue

TIssue

Issue Tracking Database (TIssue)

TIssue

- Home
- Action codes
- Source classes
- Source codes
- Severity codes
- Machines
- Issue codes
- Events
- User Front
- Exception Lists
- Block Methods
- Blocker Workflow
- Blocker Error List

Events Summary

By status Blocked: 165 Open: 29 Closed: 6469

By severity Warning (W): 196 Informational (I): 21 Critical (C): 1141

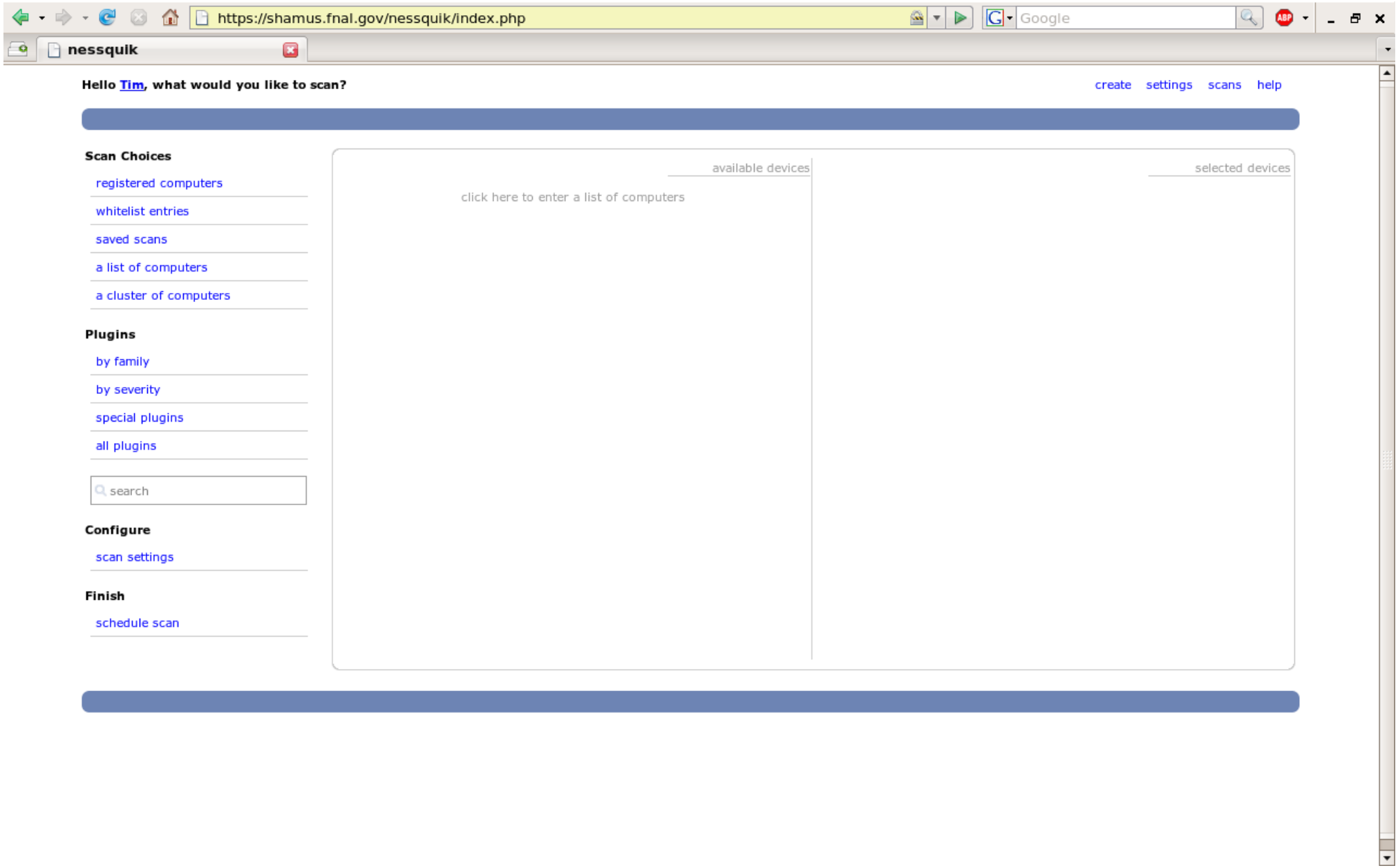
Most recent events

ID	Issue	Severity	Event Status	Block Status	IP	Machine ID	Found	Updated	Blocked
17076	Tel-unKerb	W	Open	U	[redacted]	FCDFDAS05	03/25/08 05:40:03	03/25/08 04:49:02	
17074	SSH-unKerb	W	Open	U	[redacted]	DUKPCDB	03/23/08 12:29:16	03/25/08 06:41:51	
17073	SSH-unKerb	W	Open	U	[redacted]	UNKNOWN	03/22/08 15:11:49	03/22/08 14:14:04	
17072	SSH-unKerb	W	Open	U	[redacted]	PC202235696227	03/22/08 13:59:22	03/23/08 01:04:18	
17071	MS06-040 (net chk)	C	Blocked	B	[redacted]	knu-shin	03/22/08 10:20:21	03/22/08 11:31:24	03/22/08
17069	SSH-unKerb	W	Open	B	[redacted]	MacBook	03/20/08 17:30:54	03/20/08 16:33:32	
17068	SSHD PasswordAuthentication	C	Blocked	B	[redacted]	MacBook	03/20/08 17:28:35	03/20/08 16:29:35	03/20/08
17062	Possible GDI+ compromise	C	Blocked	B	[redacted]	t40	03/20/08 08:55:29	03/20/08 07:59:38	03/20/08
17055	Open X Server	C	Blocked	B	[redacted]	Padilla-PC	03/16/08 17:30:12	03/19/08 10:28:26	03/19/08
17054	SSHD PasswordAuthentication	C	Blocked	B	[redacted]	DBA64	03/14/08 20:28:46	03/17/08 05:59:28	03/17/08
17045	SSHD PasswordAuthentication	C	Blocked	B	[redacted]	UNKNOWN	03/13/08 10:28:45	03/13/08 09:29:42	03/13/08
17040	Tel-unKerb	W	Open	U	[redacted]	NPI15E143	03/12/08 00:48:31	03/12/08 11:03:06	
17027	Open X Server	C	Blocked	B	[redacted]	AHIL	03/06/08 18:50:25	03/19/08 10:28:25	03/19/08
17025	r-cmds	W	Open	U	[redacted]	UNKNOWN	03/06/08 13:58:16	03/06/08 16:19:43	
17023	Tel-unKerb	W	Open	U	[redacted]	THPC04	03/05/08 15:52:45	03/19/08 04:31:53	
17008	SSHD PasswordAuthentication	C	Blocked	B	[redacted]	iPhone	03/03/08 13:48:32	03/03/08 15:00:01	03/03/08
17007	SSH-unKerb	W	Open	B	[redacted]	iPhone	03/03/08 12:08:53	03/03/08 15:04:31	
17003	SSHD PasswordAuthentication	C	Blocked	B	[redacted]	UNKNOWN	02/29/08 14:38:33	03/06/08 15:11:45	03/06/08
16995	SSHD PasswordAuthentication	C	Blocked	B	[redacted]	UNKNOWN	02/28/08 21:58:30	02/29/08 06:49:55	02/29/08
16993	Tel-unKerb	W	Open	U	[redacted]	DOEPLYCM	02/28/08 09:02:48	02/28/08 09:07:10	
16991	Tel-unKerb	W	Open	U	[redacted]	DOEPLYCM	02/27/08 17:23:49	02/27/08 17:33:11	
16990	MS06-040 (net chk)	C	Blocked	B	[redacted]	scaglietti	02/27/08 15:10:39	02/27/08 15:11:27	02/27/08
16988	Possible Spyware Installed	I	Open	U	[redacted]	PPD88814	02/27/08 08:11:57	02/27/08 08:13:26	
16982	Tel-unKerb	W	Open	U	[redacted]	reborg	02/24/08 19:36:49	02/24/08 19:38:21	
16981	Possible Spyware Installed	I	Open	U	[redacted]	TDPC611	02/24/08 09:22:15	02/24/08 09:23:09	

More scan & block

- ngreps
  - Basic auth scanner
  - Web GETs and POSTs
- Web proxies @ email center
- Self service tools
  - nessquik
  - *-me-now tools
- Captured subnet with temporary DHCP registration

nessquik


https://shamus.fnal.gov/nessquik/index.php
Google
nessquik
Hello Tim, what would you like to scan?
create
settings
scans
help
Scan Choices
registered computers
whitelist entries
saved scans
a list of computers
a cluster of computers
Plugins
by family
by severity
special plugins
all plugins
search
Configure
scan settings
Finish
schedule scan
available devices
click here to enter a list of computers
selected devices

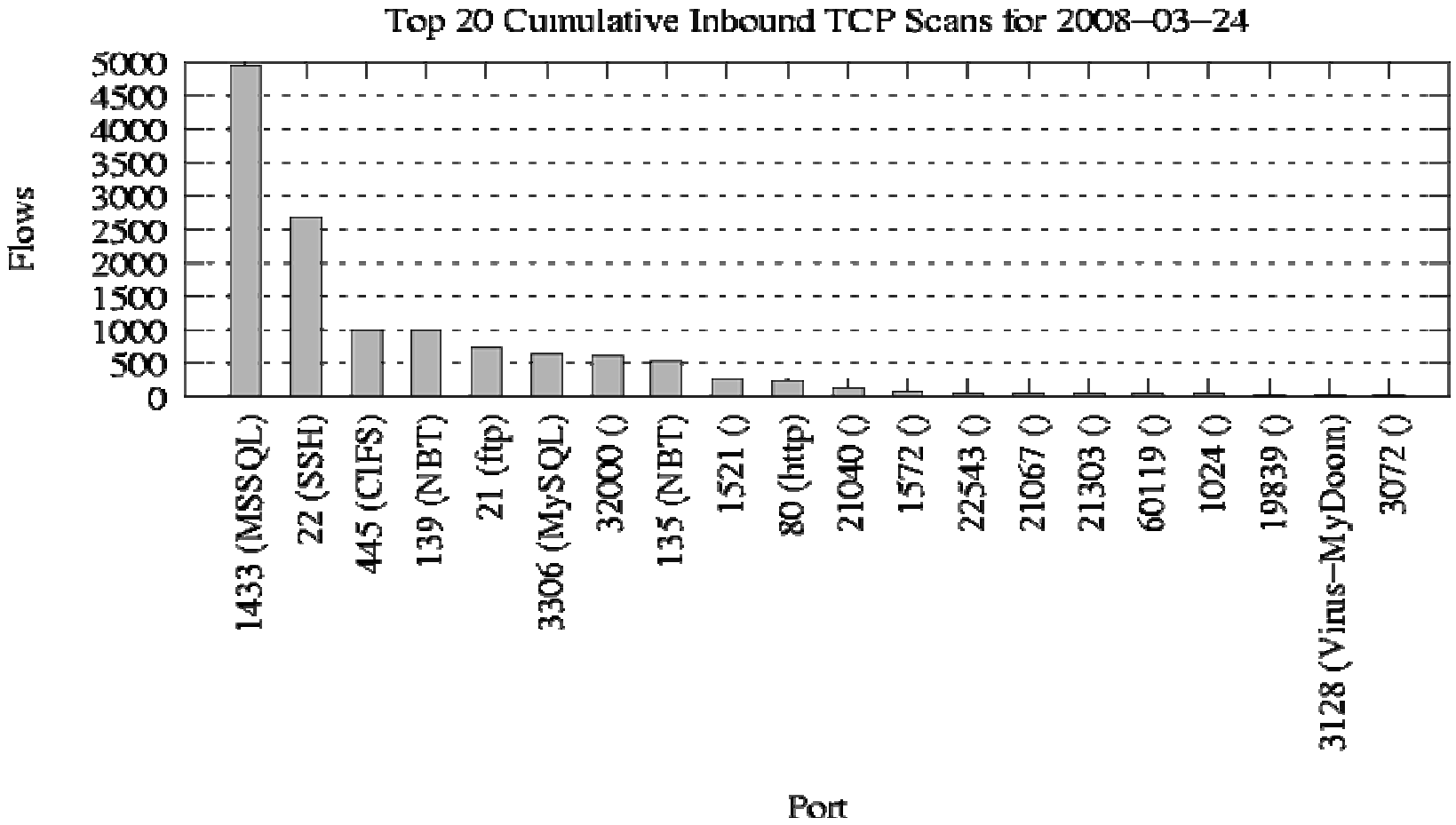
What's an ngrep?

- Tells who talked to what and when
- Browser used
- Sometimes basic auth strings (goes against computing policy)
- Badware domains can be picked out

T 2008/03/25 00:01:04.035956 111.222.111.222:37049 -> 89.149.169.88:80 [AP] GET /componentes/flash/newPlayer.swf HTTP/1.1..Host: www.marca.com..User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.12) Gecko/20080208 RedHat/1.5.0.12-0.10.el4 Firefox/1.5.0.12 pango-text..Accept:text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5..Accept-Language:en-us,en;q=0.5..Accept-Encoding: gzip,deflate..Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7..Keep-Alive: 300..Connection:keep-alive..Referer: http://www.marca.com/..Cookie: fontSize=0;MARCA_idusr=RzOfI8FugK0AABW2j9I-e82220f44e8e7eb9e8ff5691ba0f0000..Pragma: no-cache..Cache-Control: no-cache....

and more

- tarpits and darknets
  - valuable to find virus infected devices



Incidents and FCIRT

- Fermi Computer Incident Response Team
- GCSCs in each major division
- FIREs and SMOKEs
- Tell-me-now

TellMeNow

Primary owners of the subnet hosting 131.225.82.104:

DHCP Info for 131.225.82.104 for past month

Mac Address	IP Address	Nodename	Begin	Expiration		
00:12:3f:7b:bb:17	131.225.82.104	catbot	2008-02-01 00:42:34	2008-04-01 07:44:16		

Inventory data for 131.225.82.104 for month or last found

IP Address	Mac Address	Nodename	Timestamp	Proto	Port	Service	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 08:22:00	tcp	22	ssh	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 08:22:00	tcp	80	http	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 08:22:00	tcp	111	rpcbind	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 08:22:00	tcp	902	vmware-auth	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 08:22:00	tcp	5666	tcpwrapped	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 02:28:11	tcp	22	ssh	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 02:28:11	tcp	80	http	
131.225.82.104	00:12:3f:7b:bb:17	catbot.dhcp.fnal.gov	2008-03-25 02:28:11	tcp	111	rpcbind	

Asset Tracking

- Miscomp
- Sysadmin DB
- NIMI (network inventory)
  - With a lot-o-nmap going on
- Node Locater
- System management/inventory tools
  - SMS
  - Quest
  - OCS Inventory

Miscomp

Registered Node Search

New Search

Register new interfaces or Add/Modify MAC Address. Correct system administrator information in the System Administrators' Online Database

This IP address (131.225.88.79) is a Fermilab DHCP address and is currently assigned to MAC address (00-19-D2-AE-5B-75).

This machine's addresses (00-19-D2-AE-5B-75) is registered in MISCOMP as:

System Name	TONELICO
System Number	S17852
MAC Address	00-18-8B-C2-33-8A, 00-19-D2-AE-5B-75
Property Number	106260
SN	9GPBSC1
SI Number	
Class Name	DELL: XPS-M1210-T7600
Status	ISSUED TO USER
Member Of	
Purpose	
Location	FCC/3/360
Primary System Manager	13991N - Timothy Rupp
Authorized Administrator	
Your Fermi ID	[ ] Submit Make yourself the Primary System Manager of this system. End your Fermi ID with a "V" or "C" if you are an Visitor or Contractor
Node Name(s)	

Register new interfaces or Add/Modify MAC Address. Correct system administrator information in the System Administrators' Online Database

Sysadmin DB

MISCOMP SYSADMIN Online Maintenance

Listing for Timothy Rupp

Authorized Administrator For Clusters

System Name	System Number	FNAL Property Tag	Class	Purpose	Location	SI #	SN
CSTSERVERS	C01794			Mixed	FCC/2		
FERMISCANNERFARM	C01273			Security scanners	FCC/2/218		
KDC CLUSTER	C00422			KERBEROS SERVERS	FCC/2		

Authorized Administrator For Systems

Retire (remove from network & maintenance)	System Name	System Number	Node Name(s)	FNAL Property Tag	Class	Purpose	Location	SI #	SN
--		S04478		087636	DELL: PE6400-P3X-700		SITE-38/W2		5FWR201

Primary System Manager For Systems

Retire (remove from network & maintenance)	System Name	System Number	Node Name(s)	FNAL Property Tag	Class	Purpose	Location	SI #	SN
☐	ARCSIGHT	N53961	arcsight		CPU BOX		FCC/3/360		
☐	BABAR	S10984	babar	091441	ATIPA: D-ATHL-MP2000-2U-RM	cabsrv2,pbs	FCC/2/218		MI95532235
☐	BANANA	S25811		101501	HP: HX2490B		FCC/3/360		2CK6320NWC
☐	CATBOT	S17380		101124	DELL: DIM-9150-2200		FCC/3/360		8LSK9B1

Inventory open ports

```
scanner   7361  3319  0 09:18 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -sS -O2 131.225.82.115 131.225.82.116 131.225.82.119 131.225.82.122 131.225
root      7378  7361  0 09:18 ?        00:00:00 /usr/local/bin/nmap -sS -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m --min_parallelism 100 --max_
scanner   7379  3319  0 09:18 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -sS -O2 131.225.82.134 131.225.82.135 131.225.82.141 131.225.82.144 131.225
root      7392  7379  0 09:18 ?        00:00:00 /usr/local/bin/nmap -sS -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m --min_parallelism 100 --max_
scanner  10426  3319  0 09:20 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.133.144 131.225.133.124 131.225.133.131
root     10453 10426  1 09:20 ?        00:00:06 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  10491  3319  0 09:20 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -O2 131.225.135.105
root     10503 10491  0 09:20 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -O2 -oX - 131.225
scanner  10636  3319  0 09:20 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.80.53 131.225.80.69 131.225.80.224 131.225.8
root     10653 10636  0 09:20 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  10703  3319  0 09:20 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.232.152 131.225.232.18 131.225.232.155 131.2
root     10714 10703  1 09:20 ?        00:00:05 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  10766  3319  0 09:20 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.22.71 131.225.22.72 131.225.22.70 131.225.22
root     10780 10766  0 09:20 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  10914  3319  0 09:20 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.22.88 131.225.22.73 131.225.22.158
root     10923 10914  0 09:20 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  10971  3319  0 09:21 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.23.199 131.225.23.173 131.225.23.176 131.225
scanner  10972  3319  0 09:21 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.23.199 131.225.23.173 131.225.23.176 131.225
root     10984 10972  0 09:21 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
root     10988 10971  0 09:21 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  11024  3319  0 09:21 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.23.189 131.225.23.202 131.225.23.203 131.225
scanner  11025  3319  0 09:21 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.23.189 131.225.23.202 131.225.23.203 131.225
root     11040 11024  0 09:21 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
root     11041 11025  0 09:21 ?        00:00:00 /usr/local/bin/nmap -sS -p 1-65535 -P0 -T3 --osscan-limit --osscan-guess --host-timeout 15m -A -oX - 131.225.
scanner  11108  3319  0 09:21 ?        00:00:00 /bin/bash ./bin/run_nmap.sh --pro -d 1 -sS -p 1-65535 -A 131.225.42.103 131.225.42.58
```

and on and on and on....

Node Locater

Nodes connected to s-cd-fcc2(Fa5/19)

chuck-norris.dhcp	131.225.82.55	000c298b2910	Fa5/19	2008/02/19/10:01
catbot.dhcp	131.225.82.104	00123f7bbb17	Fa5/19	2008/02/19/10:01
fcc3e-hp3600dn	131.225.81.4	001438491809	Fa5/19	2008/02/19/09:01

Show all nodes on this switch

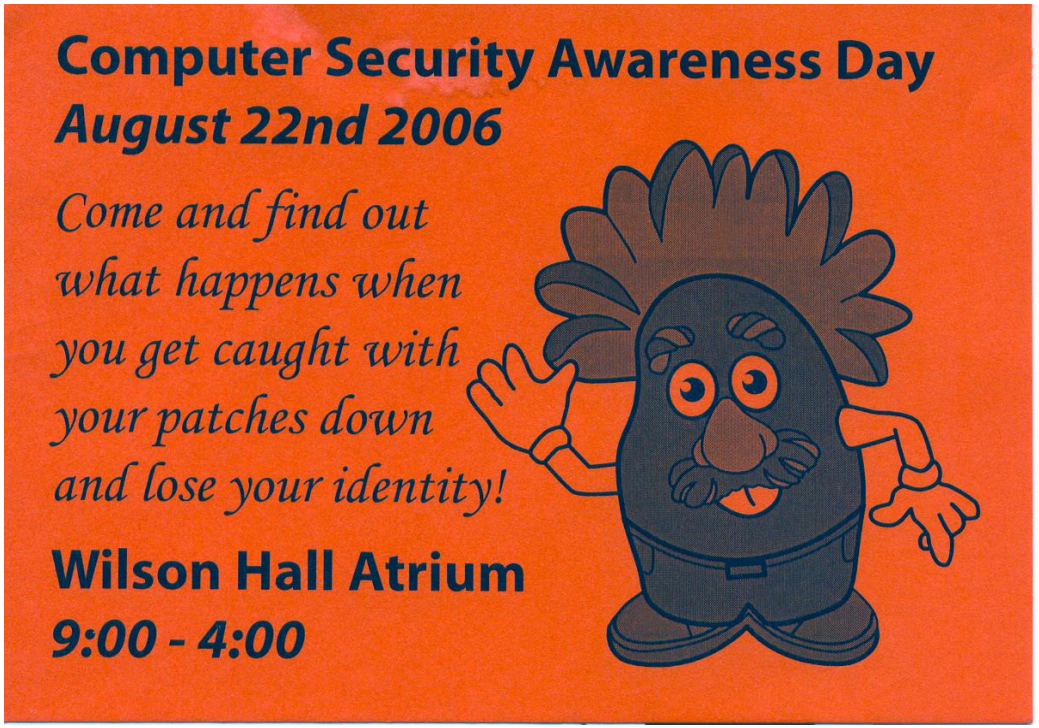
Search Again

Community Awareness

- Sysadmin round tables
  - Discuss security topics
  - Make admins aware of new vulnerabilities and exploits
- Security spots at other get-togethers
  - Linux users group
  - Mac users group
  - Windows policy group

More Awareness

- Computer Security Awareness Day
  - Yearly
  - Kiosks and demos



- Training
  - @ Orientation
  - Ongoing throughout your stay at FNAL

Outside help

- Federal Help
  - DOE
  - CI
  - CIAC
  - FBI
- Non-federal Help
  - Vendors we're friends with
  - Sister sites
  - Mailing lists, IRC, etc. The usual security hangouts

References

- http://security.fnal.gov
- NIST-800
  - http://csrc.nist.gov/publications/PubsSPs.html
- http://security.fnal.gov/awareness.html