# Isolating Intrusions by Automatic Experiments

Stephan Neuhaus
Saarland University
Stephan.Neuhaus@acm.org

Joint work with Andreas Zeller <zeller@acm.org>
Talk given at *NDSS '06 San Diego*, February 2006

# An Intrusion

```
root:3oDVCkz6hgzCs:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
toor:DHYDevUsZyu2A:0:0:root:/:/bin/bash
```

# An Intrusion

```
root:3oDVCkz6hgzCs:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
toor:DHYDevUsZyu2A:0:0:root:/:/bin/bash
```

# An Intrusion

# Which Processes Were Responsible for the Intrusion?

# Analyzing Intrusions

# Analyzing Intrusions

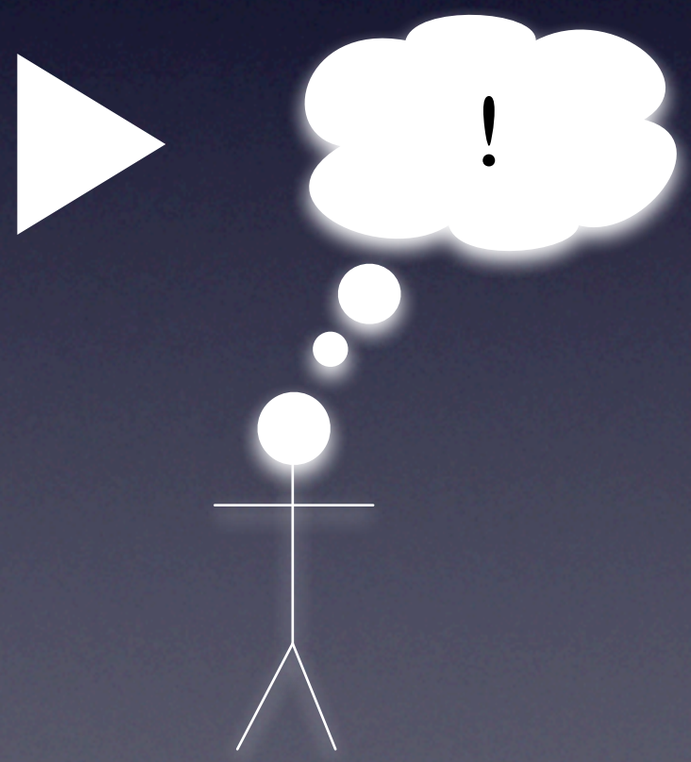
```
Oct 27 06:36:10 computer master[20273]: about to exec /usr/cyrus/bin/imapd
Oct 27 06:36:10 computer imap[20273]: executed
Oct 27 06:36:10 computer imapd[20273]: accepted connection
Oct 27 06:36:19 computer postfix/smtpd[20320]: connect from computer.domain.de[192.168.2.32]
Oct 27 06:36:19 computer postfix/smtpd[20320]: disconnect from computer.domain.de[192.168.2.32]
Oct 27 06:36:41 miller -- MARK --
Oct 27 06:37:10 computer master[2207]: process 20273 exited, status 0
Oct 27 06:38:01 comp10 /USR/SBIN/CRON[22308]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 comp8 /USR/SBIN/CRON[19072]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 computer /USR/SBIN/CRON[20538]: (mail) CMD (  if [ -x /usr/lib/exim/exim3 -a \
  -f /etc/exim/exim.conf ]; then /usr/lib/exim/exim3 -q ; fi)
Oct 27 06:38:49 comp3 -- MARK --
Oct 27 06:38:51 computer imapd[15316]: idle for too long, closing connection
Oct 27 06:38:52 computer imapd[15288]: idle for too long, closing connection
Oct 27 06:39:01 computer /USR/SBIN/CRON[20643]: (root) CMD (  [ -d /var/lib/php4 ] \
  && find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime) -print0 | xargs -r -0 rm)
Oct 27 06:39:51 computer master[2207]: process 15316 exited, status 0
Oct 27 06:39:52 computer master[2207]: process 15288 exited, status 0
Oct 27 06:39:52 comp9 syslogd 1.4.1#10: restart.
Oct 27 06:40:01 computer /USR/SBIN/CRON[20711]: (abcde) CMD (/home/abcde/bin/gofetch )
Oct 27 06:40:01 computer /USR/SBIN/CRON[20713]: (fghij) CMD (/home/fghij/.rss2email/r2e run)
Oct 27 06:40:29 bilal -- MARK --
Oct 27 06:40:56 comp5 syslogd 1.4.1#17: restart.
```

## Log Files, Traces, and other Forensic Evidence

# Analyzing Intrusions

```
Oct 27 06:36:10 computer master[20273]: about to exec /usr/cyrus/bin/imapd
Oct 27 06:36:10 computer imap[20273]: executed
Oct 27 06:36:10 computer imapd[20273]: accepted connection
Oct 27 06:36:19 computer postfix/smtpd[20320]: connect from computer.domain.de[192.168.2.32]
Oct 27 06:36:19 computer postfix/smtpd[20320]: disconnect from computer.domain.de[192.168.2.32]
Oct 27 06:36:41 miller -- MARK --
Oct 27 06:37:10 computer master[2207]: process 20273 exited, status 0
Oct 27 06:38:01 comp10 /USR/SBIN/CRON[22308]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 comp8 /USR/SBIN/CRON[19072]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 computer /USR/SBIN/CRON[20538]: (mail) CMD (  if [ -x /usr/lib/exim/exim3 -a \
  -f /etc/exim/exim.conf ]; then /usr/lib/exim/exim3 -q ; fi)
Oct 27 06:38:49 comp3 -- MARK --
Oct 27 06:38:51 computer imapd[15316]: idle for too long, closing connection
Oct 27 06:38:52 computer imapd[15288]: idle for too long, closing connection
Oct 27 06:39:01 computer /USR/SBIN/CRON[20643]: (root) CMD (  [ -d /var/lib/php4 ] \
  && find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime) -print0 | xargs -r -0 rm)
Oct 27 06:39:51 computer master[2207]: process 15316 exited, status 0
Oct 27 06:39:52 computer master[2207]: process 15288 exited, status 0
Oct 27 06:39:52 comp9 syslogd 1.4.1#10: restart.
Oct 27 06:40:01 computer /USR/SBIN/CRON[20711]: (abcde) CMD (/home/abcde/bin/gofetch )
Oct 27 06:40:01 computer /USR/SBIN/CRON[20713]: (fghij) CMD (/home/fghij/.rss2email/r2e run)
Oct 27 06:40:29 bilal -- MARK --
Oct 27 06:40:56 comp5 syslogd 1.4.1#17: restart.
```

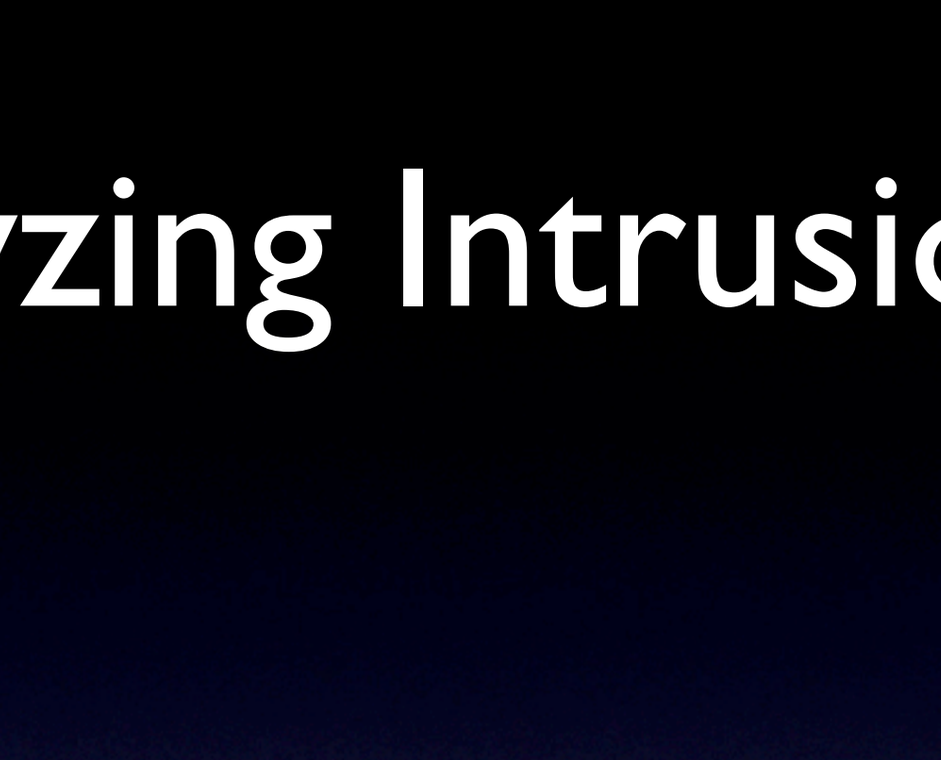
Log Files, Traces,
and other
Forensic Evidence

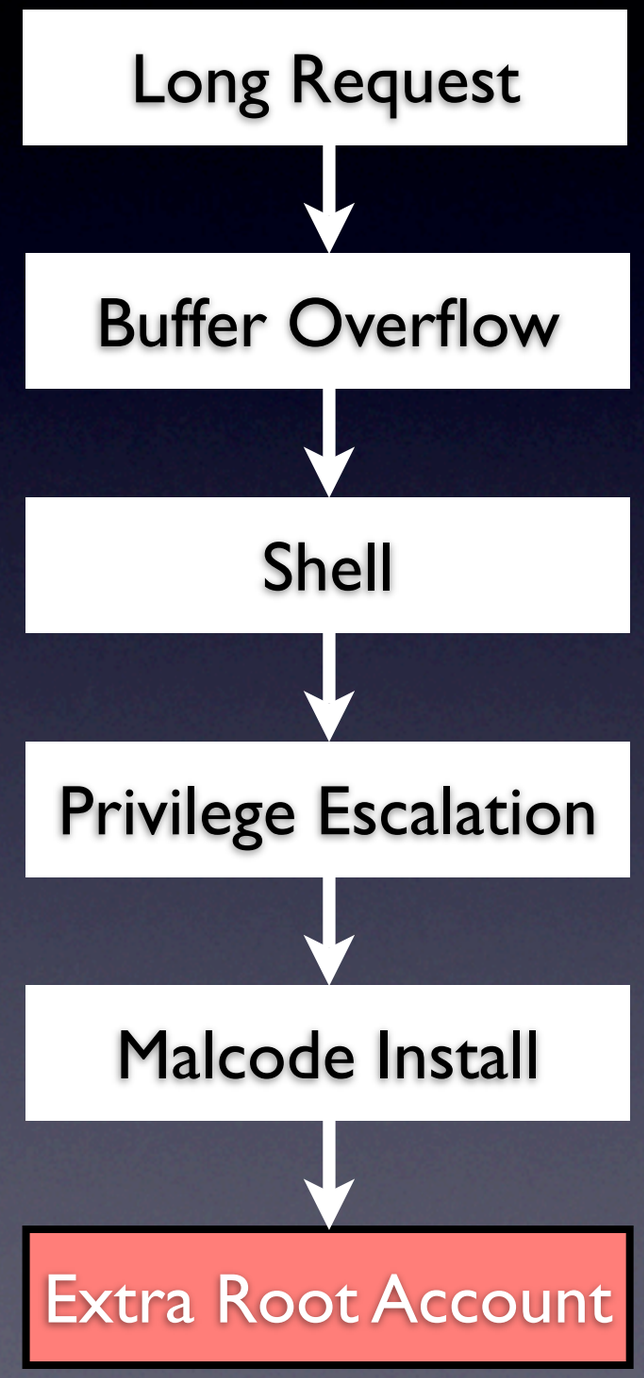


# Analyzing Intrusions

```
Oct 27 06:36:10 computer master[20273]: about to exec /usr/cyrus/bin/imapd
Oct 27 06:36:10 computer imap[20273]: executed
Oct 27 06:36:10 computer imapd[20273]: accepted connection
Oct 27 06:36:19 computer postfix/smtpd[20320]: connect from computer.domain.de[192.168.2.32]
Oct 27 06:36:19 computer postfix/smtpd[20320]: disconnect from computer.domain.de[192.168.2.32]
Oct 27 06:36:41 miller -- MARK --
Oct 27 06:37:10 computer master[2207]: process 20273 exited, status 0
Oct 27 06:38:01 comp10 /USR/SBIN/CRON[22308]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 comp8 /USR/SBIN/CRON[19072]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 computer /USR/SBIN/CRON[20538]: (mail) CMD (  if [ -x /usr/lib/exim/exim3 -a \
  -f /etc/exim/exim.conf ]; then /usr/lib/exim/exim3 -q ; fi)
Oct 27 06:38:49 comp3 -- MARK --
Oct 27 06:38:51 computer imapd[15316]: idle for too long, closing connection
Oct 27 06:38:52 computer imapd[15288]: idle for too long, closing connection
Oct 27 06:39:01 computer /USR/SBIN/CRON[20643]: (root) CMD (  [ -d /var/lib/php4 ] \
  && find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime) -print0 | xargs -r -0 rm)
Oct 27 06:39:51 computer master[2207]: process 15316 exited, status 0
Oct 27 06:39:52 computer master[2207]: process 15288 exited, status 0
Oct 27 06:39:52 comp9 syslogd 1.4.1#10: restart.
Oct 27 06:40:01 computer /USR/SBIN/CRON[20711]: (abcde) CMD (/home/abcde/bin/gofetch )
Oct 27 06:40:01 computer /USR/SBIN/CRON[20713]: (fghij) CMD (/home/fghij/.rss2email/r2e run)
Oct 27 06:40:29 bilal -- MARK --
Oct 27 06:40:56 comp5 syslogd 1.4.1#17: restart.
```

Log Files, Traces, and other Forensic Evidence

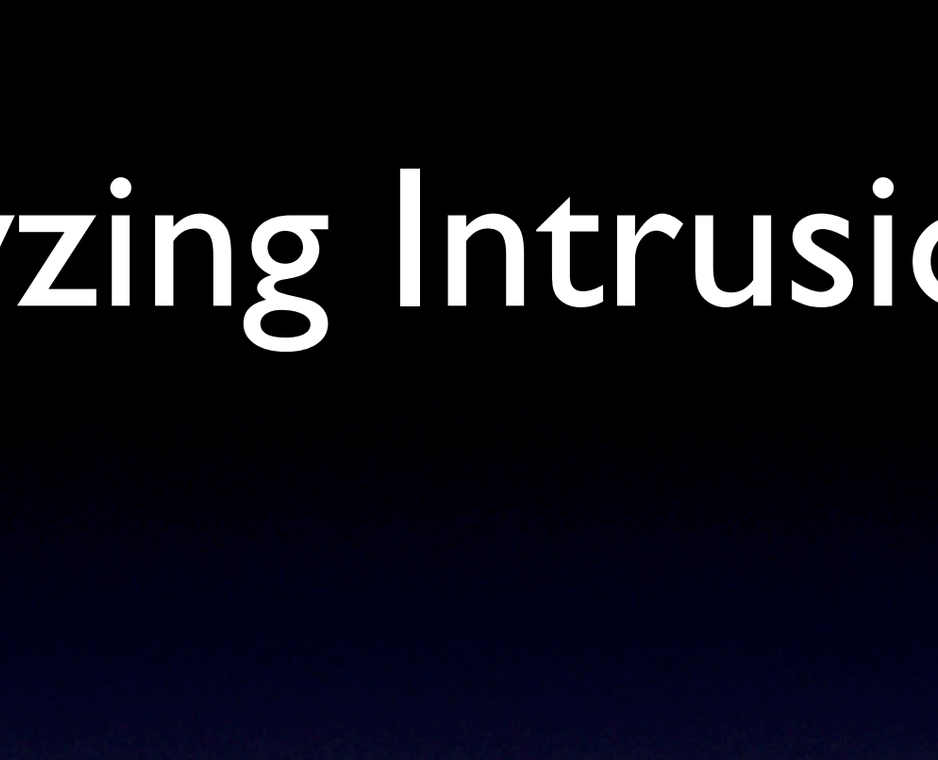


# Analyzing Intrusions

```
Oct 27 06:36:10 computer master[20273]: about to exec /usr/cyrus/bin/imapd
Oct 27 06:36:10 computer imap[20273]: executed
Oct 27 06:36:10 computer imapd[20273]: accepted connection
Oct 27 06:36:19 computer postfix/smtpd[20320]: connect from computer.domain.de[192.168.2.32]
Oct 27 06:36:19 computer postfix/smtpd[20320]: disconnect from computer.domain.de[192.168.2.32]
Oct 27 06:36:41 miller -- MARK --
Oct 27 06:37:10 computer master[2207]: process 20273 exited, status 0
Oct 27 06:38:01 comp10 /USR/SBIN/CRON[22308]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 comp8 /USR/SBIN/CRON[19072]: (mail) CMD (  if [ -x /usr/sbin/exim -a \
  -f /etc/exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Oct 27 06:38:01 computer /USR/SBIN/CRON[20538]: (mail) CMD (  if [ -x /usr/lib/exim/exim3 -a \
  -f /etc/exim/exim.conf ]; then /usr/lib/exim/exim3 -q ; fi)
Oct 27 06:38:49 comp3 -- MARK --
Oct 27 06:38:51 computer imapd[15316]: idle for too long, closing connection
Oct 27 06:38:52 computer imapd[15288]: idle for too long, closing connection
Oct 27 06:39:01 computer /USR/SBIN/CRON[20643]: (root) CMD (  [ -d /var/lib/php4 ] \
  && find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime) -print0 | xargs -r -0 rm)
Oct 27 06:39:51 computer master[2207]: process 15316 exited, status 0
Oct 27 06:39:52 computer master[2207]: process 15288 exited, status 0
Oct 27 06:39:52 comp9 syslogd 1.4.1#10: restart.
Oct 27 06:40:01 computer /USR/SBIN/CRON[20711]: (abcde) CMD (/home/abcde/bin/gofetch )
Oct 27 06:40:01 computer /USR/SBIN/CRON[20713]: (fghij) CMD (/home/fghij/.rss2email/r2e run)
Oct 27 06:40:29 bilal -- MARK --
Oct 27 06:40:56 comp5 syslogd 1.4.1#17: restart.
```

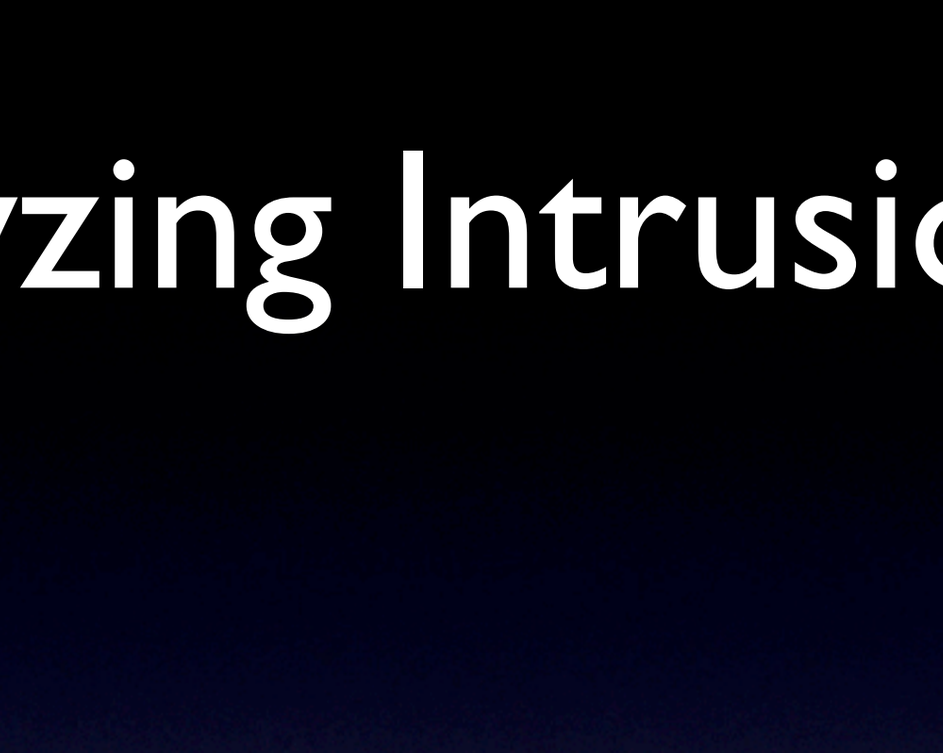
Log Files, Traces, and other Forensic Evidence




- Long Request
- Buffer Overflow
- Shell
- Privilege Escalation
- Malcode Install
- Extra Root Account

# Analyzing Intrusions

```
Jan 24 06:32:06 computer syslogd 1.4.1#17: restart (remote reception).
Jan 24 06:33:31 comp9 syslogd 1.4.1#17: restart.
Jan 24 06:34:26 comp2 kernel: IN=eth0 OUT=eth1 SRC=213.135.109.52 DST=192.168.2.11
LEN=28 TOS=0x00 PREC=0x00 TTL=112 ID=60915 PROTO=ICMP TYPE=8
 CODE=0 ID=512 SEQ=12687
Jan 24 06:35:01 lee /USR/SBIN/CRON[19868]: (root) CMD ([ -x /usr/lib/sysstat/sa1 ]
&& { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "true" ]
 && exec /usr/lib/sysstat/sa1; })
Jan 24 06:35:01 computer CRON[7559]: (root) CMD (   /root/ldap2files/ldap2files.sh)
Jan 24 06:35:01 computer /USR/SBIN/CRON[7561]: (root) CMD ([ -x /usr/lib/sysstat/
sa1 ] && { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "tru
e" ] && exec /usr/lib/sysstat/sa1; })
Jan 24 06:37:02 computer master[7618]: about to exec /usr/cyrus/bin/imapd
Jan 24 06:37:02 computer imap[7618]: executed
Jan 24 06:37:02 computer imapd[7618]: accepted connection
Jan 24 06:37:20 computer postfix/smtpd[7656]: connect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:20 computer postfix/smtpd[7656]: disconnect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:54 computer master[7672]: about to exec /usr/cyrus/bin/ctl_cyrusdb
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: checkpointing cyrus databases
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving database file: /var/imap/
mailboxes.db
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: done checkpointing cyrus databases
Jan 24 06:37:54 computer master[1135]: process 7672 exited, status 0
Jan 24 06:38:01 comp8 CRON[14063]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:01 comp10 CRON[6650]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:02 computer master[1135]: process 7618 exited, status 0
Jan 24 06:38:07 comp2 CRON[4688]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:39:01 computer /USR/SBIN/CRON[7685]: (root) CMD (  [ -d /var/lib/php4 ] &&
find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:39:01 comp9 CRON[27917]: (root) CMD (  [ -d /var/lib/php4 ] && find /var/
lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:40:02 computer CRON[7726]: (user1) CMD (/home/user1/bin/gofetch )
Jan 24 06:40:02 comp3 CRON[4864]: (root) CMD (hdparm /dev/hdc | mail -s "$(date +)
Jan 24 06:40:03 comp4 -- MARK --
Jan 24 06:40:24 comp5 syslogd 1.4.1#17: restart.
Jan 24 06:43:11 comp6 -- MARK --
Jan 24 06:44:02 comp3 syslogd 1.4.1#17: restart.
Jan 24 06:44:11 comp7 -- MARK --
Jan 24 06:44:21 computer postfix/smtpd[7795]: connect from mail-gw[192.168.254.200]
Jan 24 06:44:21 computer postfix/smtpd[7795]: C6B291BE1D: client=mail-gw
[192.168.254.200]
Jan 24 06:44:21 computer postfix/cleanup[7797]: C6B291BE1D: message-id=<43D5BC8A.
7020206@rftp.com>
Jan 24 06:44:21 computer postfix/qmgr[29705]: C6B291BE1D: from=<caml-list-
bounces@yquem.inria.fr>, size=6641, nrcpt=1 (queue active)
Jan 24 06:44:21 computer lmtpd[7007]: accepted connection
Jan 24 06:44:21 computer lmtpd[7007]: lmtp connection preauth'd as postman
Jan 24 06:44:21 computer master[7808]: about to exec /usr/cyrus/bin/lmtpd
Jan 24 06:44:22 computer lmtpunix[7808]: executed
Jan 24 06:44:22 computer postfix/local[7798]: C6B291BE1D:
to=<user4@computer.domain.de>, relay=local, delay=0, status=sent (delivered to
comman
d: /usr/bin/procmail -a "$EXTENSION")
Jan 24 06:44:22 computer postfix/qmgr[29705]: C6B291BE1D: removed
Jan 24 06:44:22 computer postfix/smtpd[7795]: disconnect from mail-gw
```




Long Request

Buffer Overflow

Shell

Privilege Escalation

Malcode Install

Extra Root Account

# Analyzing Intrusions

```
Jan 24 06:32:06 computer syslogd 1.4.1#17: restart (remote reception).
Jan 24 06:33:31 comp9 syslogd 1.4.1#17: restart.
Jan 24 06:34:26 comp2 kernel: IN=eth0 OUT=eth1 SRC=213.135.109.52 DST=192.168.2.11
LEN=28 TOS=0x00 PREC=0x00 TTL=112 ID=60915 PROTO=ICMP TYPE=8
 CODE=0 ID=512 SEQ=12687
Jan 24 06:35:01 lee /USR/SBIN/CRON[19868]: (root) CMD ([ -x /usr/lib/sysstat/sa1 ]
&& { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "true" ]
 && exec /usr/lib/sysstat/sa1; })
Jan 24 06:35:01 computer CRON[7559]: (root) CMD (   /root/ldap2files/ldap2files.sh)
Jan 24 06:35:01 computer /USR/SBIN/CRON[7561]: (root) CMD ([ -x /usr/lib/sysstat/
sa1 ] && { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "tru
e" ] && exec /usr/lib/sysstat/sa1; })
Jan 24 06:37:02 computer master[7618]: about to exec /usr/cyrus/bin/imapd
Jan 24 06:37:02 computer imap[7618]: executed
Jan 24 06:37:02 computer imapd[7618]: accepted connection
Jan 24 06:37:20 computer postfix/smtpd[7656]: connect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:20 computer postfix/smtpd[7656]: disconnect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:54 computer master[7672]: about to exec /usr/cyrus/bin/ctl_cyrusdb
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: checkpointing cyrus databases
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving database file: /var/imap/
mailboxes.db
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: done checkpointing cyrus databases
Jan 24 06:37:54 computer master[1135]: process 7672 exited, status 0
Jan 24 06:38:01 comp8 CRON[14063]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:01 comp10 CRON[6650]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:02 computer master[1135]: process 7618 exited, status 0
Jan 24 06:38:07 comp2 CRON[4688]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:39:01 computer /USR/SBIN/CRON[7685]: (root) CMD (  [ -d /var/lib/php4 ] &&
find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:39:01 comp9 CRON[27917]: (root) CMD (  [ -d /var/lib/php4 ] && find /var/
lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:40:02 computer CRON[7726]: (user1) CMD (/home/user1/bin/gofetch )
Jan 24 06:40:02 comp3 CRON[4864]: (root) CMD (hdparm /dev/hdc | mail -s "$(date +)
Jan 24 06:40:03 comp4 -- MARK --
Jan 24 06:40:24 comp5 syslogd 1.4.1#17: restart.
Jan 24 06:43:11 comp6 -- MARK --
Jan 24 06:44:02 comp3 syslogd 1.4.1#17: restart.
Jan 24 06:44:11 comp7 -- MARK --
Jan 24 06:44:21 computer postfix/smtpd[7795]: connect from mail-gw[192.168.254.200]
Jan 24 06:44:21 computer postfix/smtpd[7795]: C6B291BE1D: client=mail-gw
[192.168.254.200]
Jan 24 06:44:21 computer postfix/cleanup[7797]: C6B291BE1D: message-id=<43D5BC8A.
7020206@rftp.com>
Jan 24 06:44:21 computer postfix/qmgr[29705]: C6B291BE1D: from=<caml-list-
bounces@yquem.inria.fr>, size=6641, nrcpt=1 (queue active)
Jan 24 06:44:21 computer lmtpd[7007]: accepted connection
Jan 24 06:44:21 computer lmtpd[7007]: lmtp connection preauth'd as postman
Jan 24 06:44:21 computer master[7808]: about to exec /usr/cyrus/bin/lmtpd
Jan 24 06:44:22 computer lmtpunix[7808]: executed
Jan 24 06:44:22 computer postfix/local[7798]: C6B291BE1D:
to=<user4@computer.domain.de>, relay=local, delay=0, status=sent (delivered to
comman
d: /usr/bin/procmail -a "$EXTENSION")
Jan 24 06:44:22 computer postfix/qmgr[29705]: C6B291BE1D: removed
Jan 24 06:44:22 computer postfix/smtpd[7795]: disconnect from mail-gw
```


Long Request

Buffer Overflow

Shell

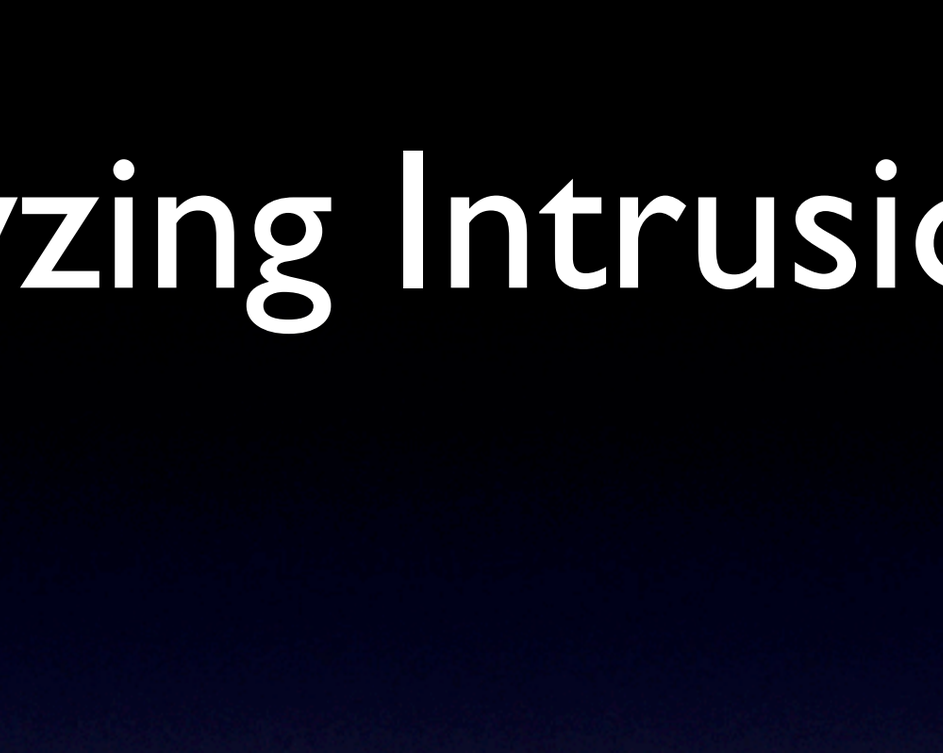
Privilege Escalation

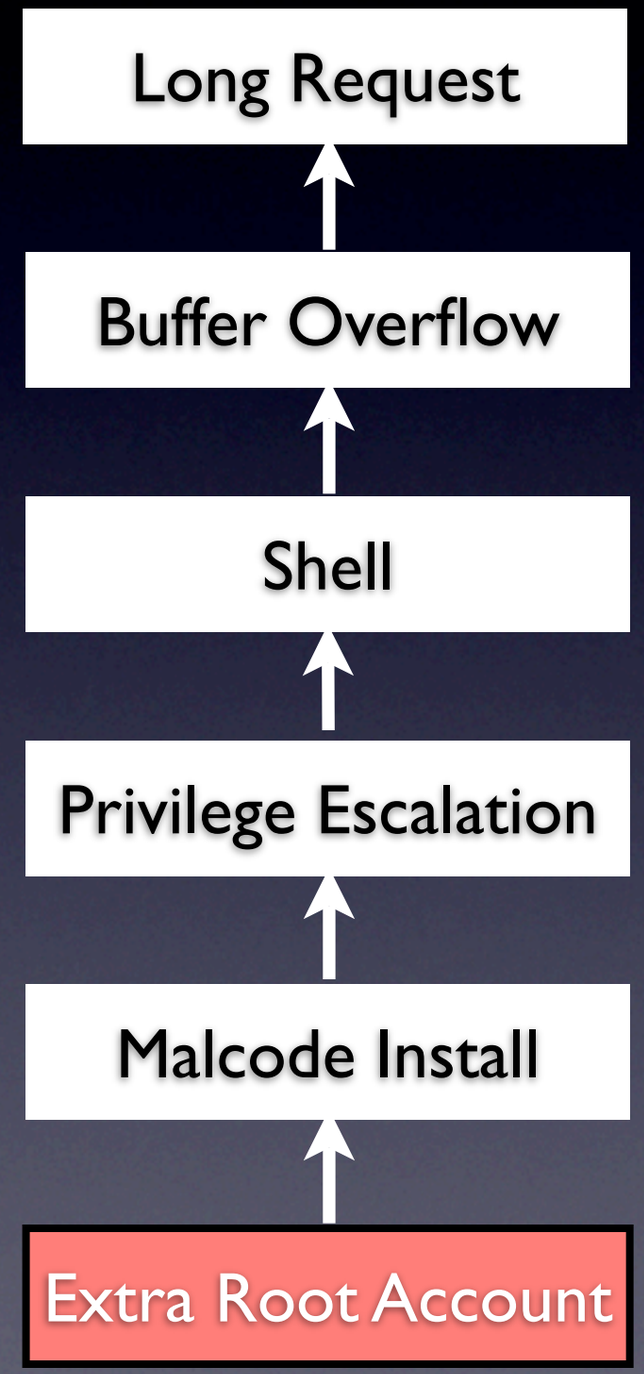
Malcode Install

Extra Root Account

# Analyzing Intrusions

```
Jan 24 06:32:06 computer syslogd 1.4.1#17: restart (remote reception).
Jan 24 06:33:31 comp9 syslogd 1.4.1#17: restart.
Jan 24 06:34:26 comp2 kernel: IN=eth0 OUT=eth1 SRC=213.135.109.52 DST=192.168.2.11
LEN=28 TOS=0x00 PREC=0x00 TTL=112 ID=60915 PROTO=ICMP TYPE=8
 CODE=0 ID=512 SEQ=12687
Jan 24 06:35:01 lee /USR/SBIN/CRON[19868]: (root) CMD ([ -x /usr/lib/sysstat/sa1 ]
&& { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "true" ]
 && exec /usr/lib/sysstat/sa1; })
Jan 24 06:35:01 computer CRON[7559]: (root) CMD (   /root/ldap2files/ldap2files.sh)
Jan 24 06:35:01 computer /USR/SBIN/CRON[7561]: (root) CMD ([ -x /usr/lib/sysstat/
sa1 ] && { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "tru
e" ] && exec /usr/lib/sysstat/sa1; })
Jan 24 06:37:02 computer master[7618]: about to exec /usr/cyrus/bin/imapd
Jan 24 06:37:02 computer imap[7618]: executed
Jan 24 06:37:02 computer imapd[7618]: accepted connection
Jan 24 06:37:20 computer postfix/smtpd[7656]: connect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:20 computer postfix/smtpd[7656]: disconnect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:54 computer master[7672]: about to exec /usr/cyrus/bin/ctl_cyrusdb
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: checkpointing cyrus databases
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving database file: /var/imap/
mailboxes.db
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: done checkpointing cyrus databases
Jan 24 06:37:54 computer master[1135]: process 7672 exited, status 0
Jan 24 06:38:01 comp8 CRON[14063]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:01 comp10 CRON[6650]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:02 computer master[1135]: process 7618 exited, status 0
Jan 24 06:38:07 comp2 CRON[4688]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:39:01 computer /USR/SBIN/CRON[7685]: (root) CMD (  [ -d /var/lib/php4 ] &&
find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:39:01 comp9 CRON[27917]: (root) CMD (  [ -d /var/lib/php4 ] && find /var/
lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:40:02 computer CRON[7726]: (user1) CMD (/home/user1/bin/gofetch )
Jan 24 06:40:02 comp3 CRON[4864]: (root) CMD (hdparm /dev/hdc | mail -s "$(date +)
Jan 24 06:40:03 comp4 -- MARK --
Jan 24 06:40:24 comp5 syslogd 1.4.1#17: restart.
Jan 24 06:43:11 comp6 -- MARK --
Jan 24 06:44:02 comp3 syslogd 1.4.1#17: restart.
Jan 24 06:44:11 comp7 -- MARK --
Jan 24 06:44:21 computer postfix/smtpd[7795]: connect from mail-gw[192.168.254.200]
Jan 24 06:44:21 computer postfix/smtpd[7795]: C6B291BE1D: client=mail-gw
[192.168.254.200]
Jan 24 06:44:21 computer postfix/cleanup[7797]: C6B291BE1D: message-id=<43D5BC8A.
7020206@rftp.com>
Jan 24 06:44:21 computer postfix/qmgr[29705]: C6B291BE1D: from=<caml-list-
bounces@yquem.inria.fr>, size=6641, nrcpt=1 (queue active)
Jan 24 06:44:21 computer lmtpd[7007]: accepted connection
Jan 24 06:44:21 computer lmtpd[7007]: lmtp connection preauth'd as postman
Jan 24 06:44:21 computer master[7808]: about to exec /usr/cyrus/bin/lmtpd
Jan 24 06:44:22 computer lmtpunix[7808]: executed
Jan 24 06:44:22 computer postfix/local[7798]: C6B291BE1D:
to=<user4@computer.domain.de>, relay=local, delay=0, status=sent (delivered to
comman
d: /usr/bin/procmail -a "$EXTENSION")
Jan 24 06:44:22 computer postfix/qmgr[29705]: C6B291BE1D: removed
Jan 24 06:44:22 computer postfix/smtpd[7795]: disconnect from mail-gw
```



# Analyzing Intrusions

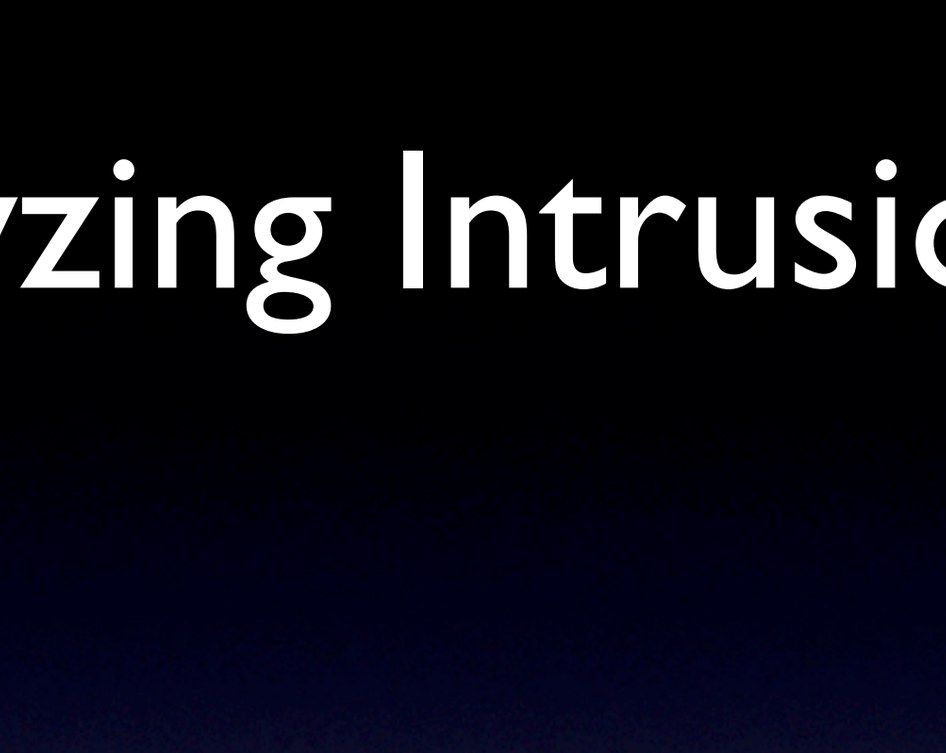
```
Jan 24 06:32:06 computer syslogd 1.4.1#17: restart (remote reception).
Jan 24 06:33:31 comp9 syslogd 1.4.1#17: restart.
Jan 24 06:34:26 comp2 kernel: IN=eth0 OUT=eth1 SRC=213.135.109.52 DST=192.168.2.11
LEN=28 TOS=0x00 PREC=0x00 TTL=112 ID=60915 PROTO=ICMP TYPE=8
 CODE=0 ID=512 SEQ=12687
Jan 24 06:35:01 lee /USR/SBIN/CRON[19868]: (root) CMD ([ -x /usr/lib/sysstat/sa1 ]
&& { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "true" ]
 && exec /usr/lib/sysstat/sa1; })
Jan 24 06:35:01 computer CRON[7559]: (root) CMD (   /root/ldap2files/ldap2files.sh)
Jan 24 06:35:01 computer /USR/SBIN/CRON[7561]: (root) CMD ([ -x /usr/lib/sysstat/
sa1 ] && { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "tru
e" ] && exec /usr/lib/sysstat/sa1; })
Jan 24 06:37:02 computer master[7618]: about to exec /usr/cyrus/bin/imapd
Jan 24 06:37:02 computer imap[7618]: executed
Jan 24 06:37:02 computer imapd[7618]: accepted connection
Jan 24 06:37:20 computer postfix/smtpd[7656]: connect from somputer.nsa.gov
[192.168.2.32]
Jan 24 06:37:20 computer postfix/smtpd[7656]: disconnect from somputer.nsa.gov
[192.168.2.32]
Jan 24 06:37:54 computer [7672]: about to exec /usr/cyrus/bin/ctl_cyrusdb
Jan 24 06:37:54 computer [7672]: checkpointing cyrus databases
Jan 24 06:37:54 computer [7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer [7672]: archiving database file: /var/imap/
mailboxes.db
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer [7672]: done checkpointing cyrus databases
Jan 24 06:37:54 computer [7672]: process 7672 exited, status 0
Jan 24 06:38:01 comp8 CRON[14063]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
```

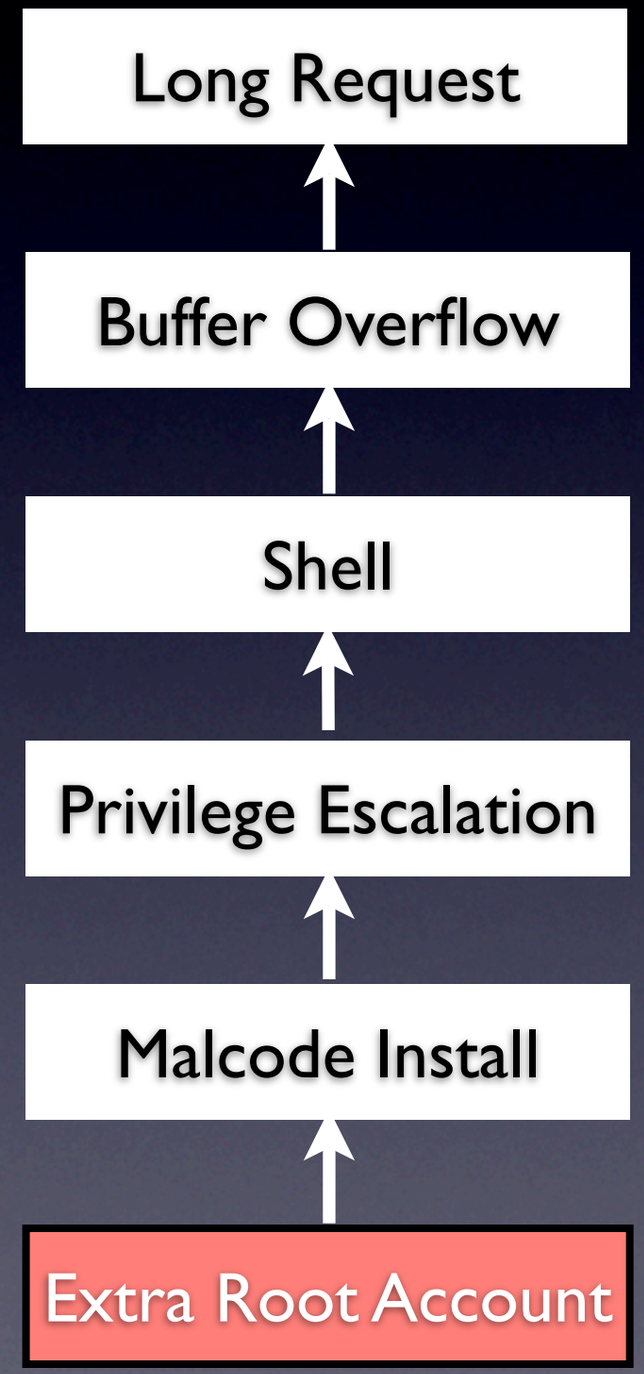
myprocess

myprocess

myprocess

```
Jan 24 06:40:02 computer CRON[7726]: (user1) CMD (/home/user1/bin/gofetch )
Jan 24 06:40:02 comp3 CRON[4864]: (root) CMD (hdparm /dev/hdc | mail -s "$(date +)
Jan 24 06:40:03 comp4 -- MARK --
Jan 24 06:40:24 comp5 syslogd 1.4.1#17: restart.
Jan 24 06:43:11 comp6 -- MARK --
Jan 24 06:44:02 comp3 syslogd 1.4.1#17: restart.
Jan 24 06:44:11 comp7 -- MARK --
Jan 24 06:44:21 computer postfix/smtpd[7795]: connect from somputer.nsa.gov
Jan 24 06:44:21 computer postfix/smtpd[7795]: C6B291BE1D:
[192.168.254.200]
Jan 24 06:44:21 computer postfix/cleanup[7797]: C6B291BE1D: message-id=<43D5BC8A.
7020206@rftp.com>
Jan 24 06:44:21 computer postfix/qmgr[29705]: C6B291BE1D: from=<caml-list-
bounces@yquem.inria.fr>, size=6641, nrcpt=1 (queue active)
Jan 24 06:44:21 computer lmtpd[7007]: accepted connection
Jan 24 06:44:21 computer lmtpd[7007]: lmtp connection preauth'd as postman
Jan 24 06:44:21 computer master[7808]: about to exec /usr/cyrus/bin/lmtpd
Jan 24 06:44:22 computer lmtpunix[7808]: executed
Jan 24 06:44:22 computer postfix/local[7798]: C6B291BE1D:
to=<user4@computer.domain.de>, relay=local, delay=0, status=sent (delivered to
comman
d: /usr/bin/procmail -a "$EXTENSION")
Jan 24 06:44:22 computer postfix/qmgr[29705]: C6B291BE1D: removed
Jan 24 06:44:22 computer postfix/smtpd[7795]: disconnect from mail-gw
```

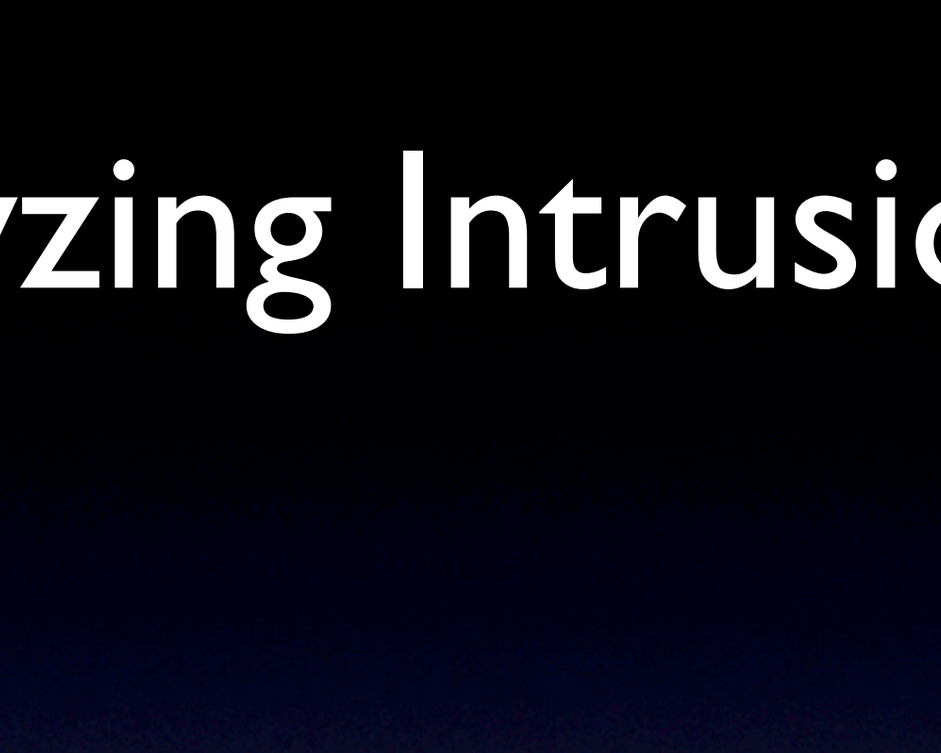


# Analyzing Intrusions

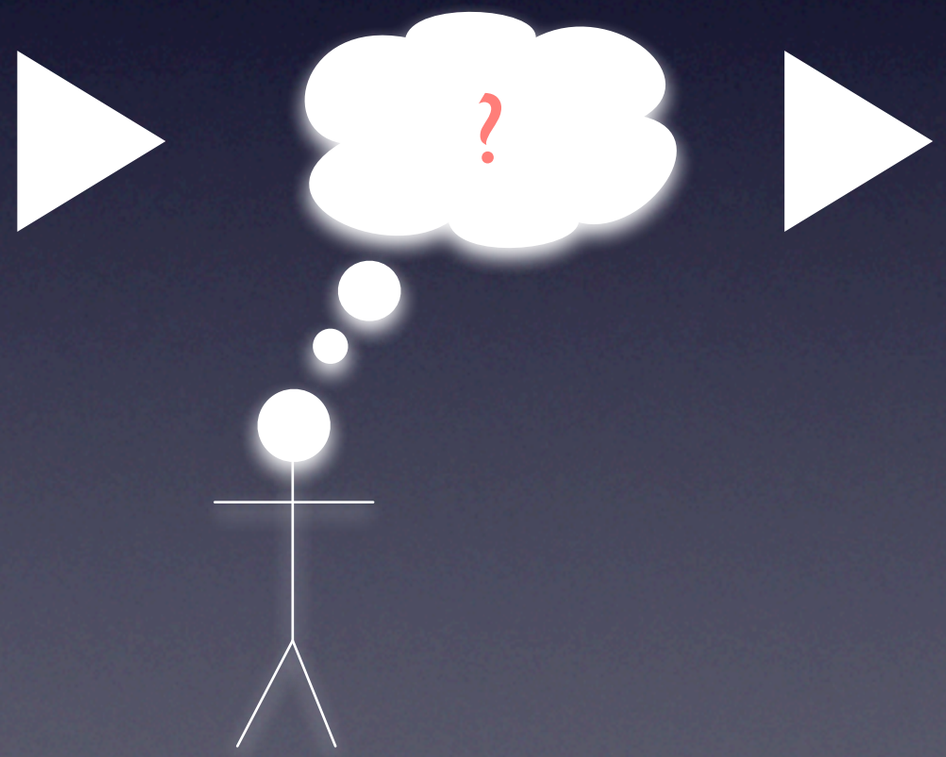
```
Jan 24 06:32:06 computer syslogd 1.4.1#17: restart (remote reception).
Jan 24 06:33:31 comp9 syslogd 1.4.1#17: restart.
Jan 24 06:34:26 comp2 kernel: IN=eth0 OUT=eth1 SRC=213.135.109.52 DST=192.168.2.11
LEN=28 TOS=0x00 PREC=0x00 TTL=112 ID=60915 PROTO=ICMP TYPE=8
 CODE=0 ID=512 SEQ=12687
Jan 24 06:35:01 lee /USR/SBIN/CRON[19868]: (root) CMD ([ -x /usr/lib/sysstat/sa1 ]
&& { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "true" ]
 && exec /usr/lib/sysstat/sa1; })
Jan 24 06:35:01 computer CRON[7559]: (root) CMD (   /root/ldap2files/ldap2files.sh)
Jan 24 06:35:01 computer /USR/SBIN/CRON[7561]: (root) CMD ([ -x /usr/lib/sysstat/
sa1 ] && { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "tru
e" ] && exec /usr/lib/sysstat/sa1; })
Jan 24 06:37:02 computer master[7618]: about to exec /usr/cyrus/bin/imapd
Jan 24 06:37:02 computer imap[7618]: executed
Jan 24 06:37:02 computer imapd[7618]: accepted connection
Jan 24 06:37:20 computer postfix/smtpd[7656]: connect from somputer.nsa.gov
[192.168.2.32]
Jan 24 06:37:20 computer postfix/smtpd[7656]: disconnect from somputer.nsa.gov
[192.168.2.32]
Jan 24 06:37:54 computer [7672]: about to exec /usr/cyrus/bin/ctl_cyrusdb
Jan 24 06:37:54 computer myprocess [7672]: checkpointing cyrus databases
Jan 24 06:37:54 computer [7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer myprocess [7672]: archiving database file: /var/imap/
mailboxes.db
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer myprocess [7672]: done checkpointing cyrus databases
Jan 24 06:37:54 computer [7672]: process 7672 exited, status 0
Jan 24 06:38:01 comp8 CRON[14063]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
```

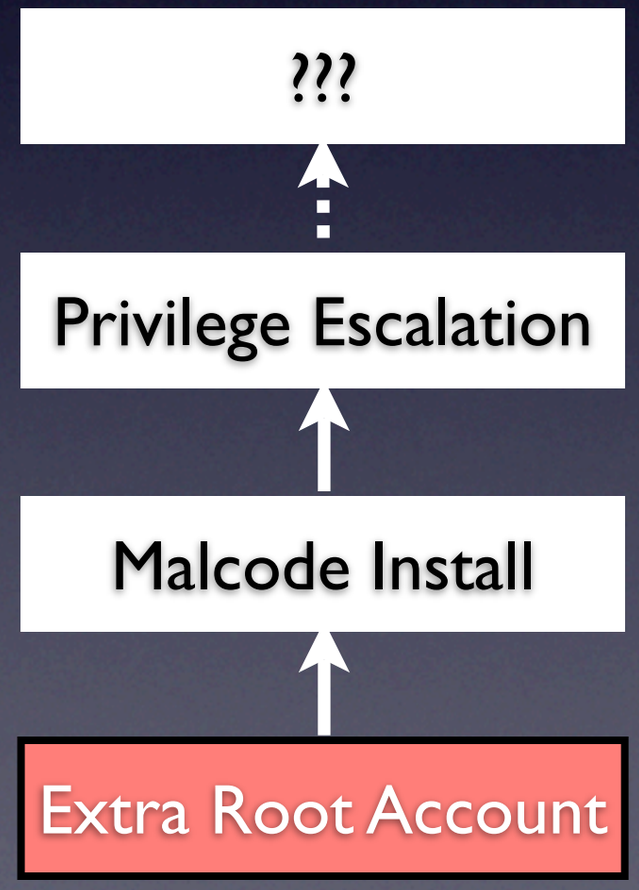
```
Jan 24 06:40:02 computer CRON[7726]: (user1) CMD (/home/user1/bin/gofetch )
Jan 24 06:40:02 comp3 CRON[4864]: (root) CMD (hdparm /dev/hdc | mail -s "$(date +)
Jan 24 06:40:03 comp4 -- MARK --
Jan 24 06:40:24 comp5 syslogd 1.4.1#17: restart.
Jan 24 06:43:11 comp6 -- MARK --
Jan 24 06:44:02 comp3 syslogd 1.4.1#17: restart.
Jan 24 06:44:11 comp7 -- MARK --
Jan 24 06:44:21 computer postfix/smtpd[7795]: connect from somputer.nsa.gov
Jan 24 06:44:21 computer postfix/smtpd[7795]: C6B291BE1D:
[192.168.254.200]
Jan 24 06:44:21 computer postfix/cleanup[7797]: C6B291BE1D: message-id=<43D5BC8A.
7020206@rftp.com>
Jan 24 06:44:21 computer postfix/qmgr[29705]: C6B291BE1D: from=<caml-list-
bounces@yquem.inria.fr>, size=6641, nrcpt=1 (queue active)
Jan 24 06:44:21 computer lmtpd[7007]: accepted connection
Jan 24 06:44:21 computer lmtpd[7007]: lmtp connection preauth'd as postman
Jan 24 06:44:21 computer master[7808]: about to exec /usr/cyrus/bin/lmtpd
Jan 24 06:44:22 computer lmtpunix[7808]: executed
Jan 24 06:44:22 computer postfix/local[7798]: C6B291BE1D:
to=<user4@computer.domain.de>, relay=local, delay=0, status=sent (delivered to
comman
d: /usr/bin/procmail -a "$EXTENSION")
Jan 24 06:44:22 computer postfix/qmgr[29705]: C6B291BE1D: removed
Jan 24 06:44:22 computer postfix/smtpd[7795]: disconnect from mail-gw
```




# Analyzing Intrusions

```
Jan 24 06:32:06 computer syslogd 1.4.1#17: restart (remote reception).
Jan 24 06:33:31 comp9 syslogd 1.4.1#17: restart.
Jan 24 06:34:26 comp2 kernel: IN=eth0 OUT=eth1 SRC=213.135.109.52 DST=192.168.2.11
LEN=28 TOS=0x00 PREC=0x00 TTL=112 ID=60915 PROTO=ICMP TYPE=8
 CODE=0 ID=512 SEQ=12687
Jan 24 06:35:01 lee /USR/SBIN/CRON[19868]: (root) CMD ([ -x /usr/lib/sysstat/sa1 ]
&& { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "true" ]
 && exec /usr/lib/sysstat/sa1; })
Jan 24 06:35:01 computer CRON[7559]: (root) CMD (   /root/ldap2files/ldap2files.sh)
Jan 24 06:35:01 computer /USR/SBIN/CRON[7561]: (root) CMD ([ -x /usr/lib/sysstat/
sa1 ] && { [ -r "$DEFAULT" ] && . "$DEFAULT" ; [ "$ENABLED" = "tru
e" ] && exec /usr/lib/sysstat/sa1; })
Jan 24 06:37:02 computer master[7618]: about to exec /usr/cyrus/bin/imapd
Jan 24 06:37:02 computer imap[7618]: executed
Jan 24 06:37:02 computer imapd[7618]: accepted connection
Jan 24 06:37:20 computer postfix/smtpd[7656]: connect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:20 computer postfix/smtpd[7656]: disconnect from computer.domain.de
[192.168.2.32]
Jan 24 06:37:54 computer master[7672]: about to exec /usr/cyrus/bin/ctl_cyrusdb
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: checkpointing cyrus databases
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving database file: /var/imap/
mailboxes.db
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: archiving log file: /var/imap/db/log.
0000000026
Jan 24 06:37:54 computer ctl_cyrusdb[7672]: done checkpointing cyrus databases
Jan 24 06:37:54 computer master[1135]: process 7672 exited, status 0
Jan 24 06:38:01 comp8 CRON[14063]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:01 comp10 CRON[6650]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:38:02 computer master[1135]: process 7618 exited, status 0
Jan 24 06:38:07 comp2 CRON[4688]: (mail) CMD (  if [ -x /usr/sbin/exim -a -f /etc/
exim/exim.conf ]; then /usr/sbin/exim -q ; fi)
Jan 24 06:39:01 computer /USR/SBIN/CRON[7685]: (root) CMD (  [ -d /var/lib/php4 ] &&
find /var/lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:39:01 comp9 CRON[27917]: (root) CMD (  [ -d /var/lib/php4 ] && find /var/
lib/php4/ -type f -cmin +$(/usr/lib/php4/maxlifetime
) -print0 | xargs -r -0 rm)
Jan 24 06:40:02 computer CRON[7726]: (user1) CMD (/home/user1/bin/gofetch )
Jan 24 06:40:02 comp3 CRON[4864]: (root) CMD (hdparm /dev/hdc | mail -s "$(date +)
Jan 24 06:40:03 comp4 -- MARK --
Jan 24 06:40:24 comp5 syslogd 1.4.1#17: restart.
Jan 24 06:43:11 comp6 -- MARK --
Jan 24 06:44:02 comp3 syslogd 1.4.1#17: restart.
Jan 24 06:44:11 comp7 -- MARK --
Jan 24 06:44:21 computer postfix/smtpd[7795]: connect from mail-gw[192.168.254.200]
Jan 24 06:44:21 computer postfix/smtpd[7795]: C6B291BE1D: client=mail-gw
[192.168.254.200]
Jan 24 06:44:21 computer postfix/cleanup[7797]: C6B291BE1D: message-id=<43D5BC8A.
7020206@rftp.com>
Jan 24 06:44:21 computer postfix/qmgr[29705]: C6B291BE1D: from=<caml-list-
bounces@yquem.inria.fr>, size=6641, nrcpt=1 (queue active)
Jan 24 06:44:21 computer lmtpd[7007]: accepted connection
Jan 24 06:44:21 computer lmtpd[7007]: lmtp connection preauth'd as postman
Jan 24 06:44:21 computer master[7808]: about to exec /usr/cyrus/bin/lmtpd
Jan 24 06:44:22 computer lmtpunix[7808]: executed
Jan 24 06:44:22 computer postfix/local[7798]: C6B291BE1D:
to=<user4@computer.domain.de>, relay=local, delay=0, status=sent (delivered to
comman
d: /usr/bin/procmail -a "$EXTENSION")
Jan 24 06:44:22 computer postfix/qmgr[29705]: C6B291BE1D: removed
Jan 24 06:44:22 computer postfix/smtpd[7795]: disconnect from mail-gw
```

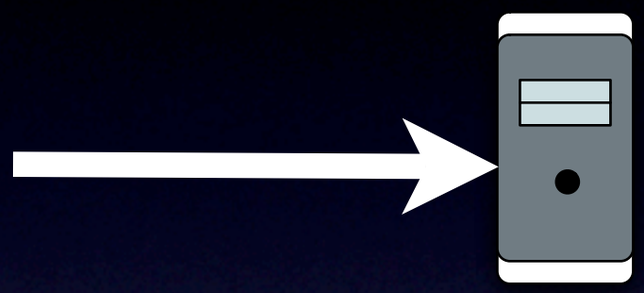


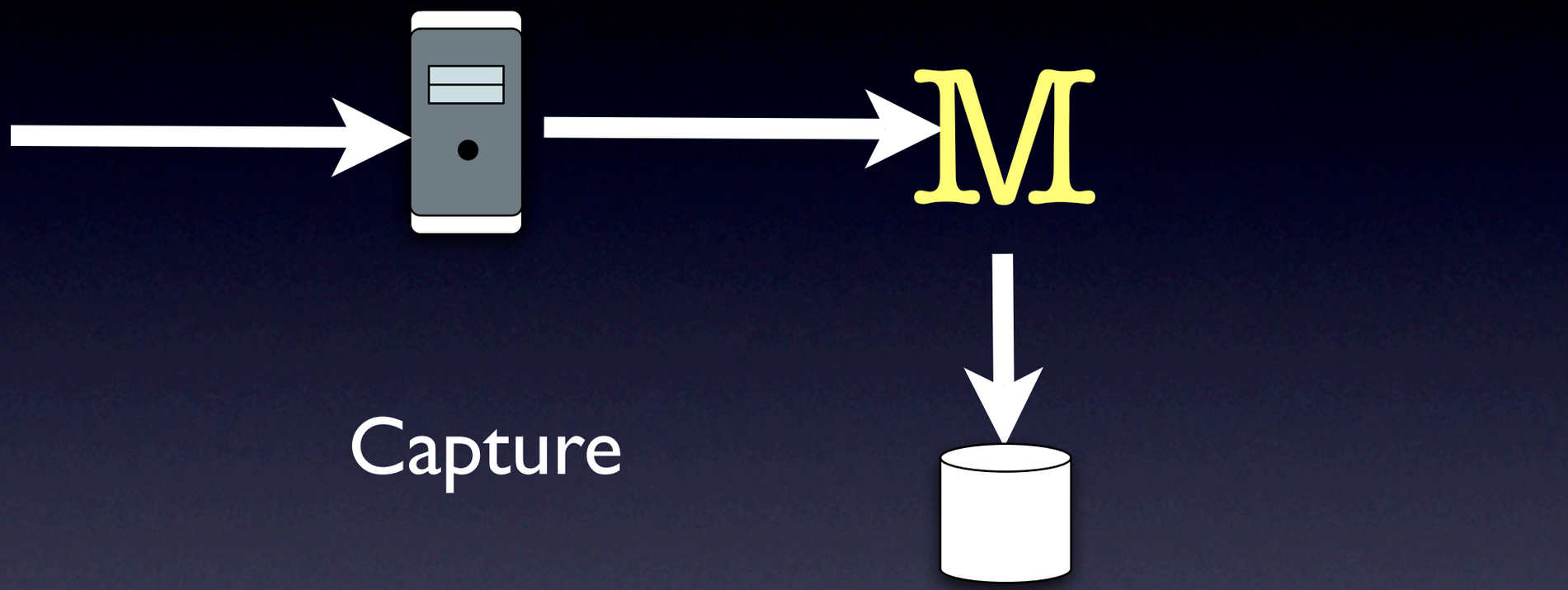
# Malfor Architecture

# Malfor Architecture

# Malfor Architecture

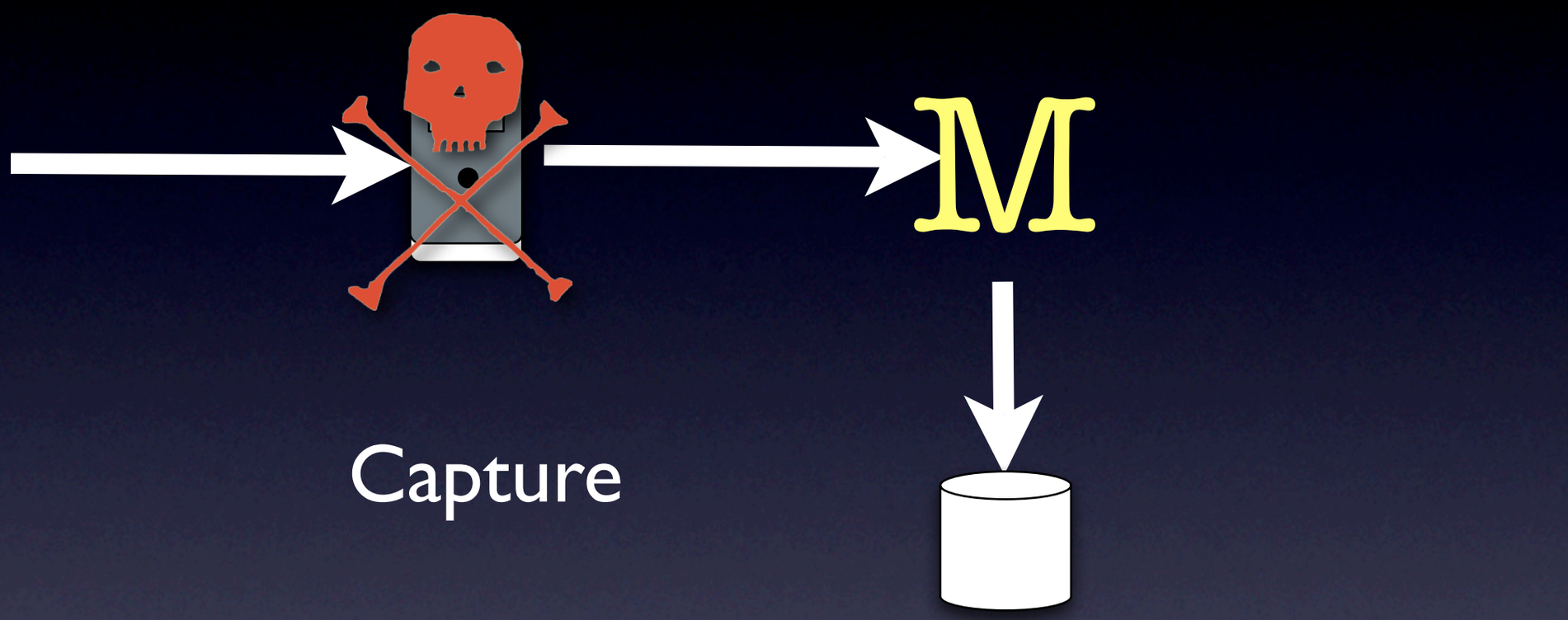


# Malfor Architecture



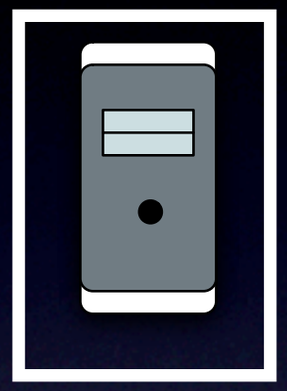

Processes ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

# Malfor Architecture



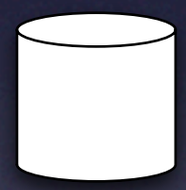

Processes ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■

# Malfor Architecture



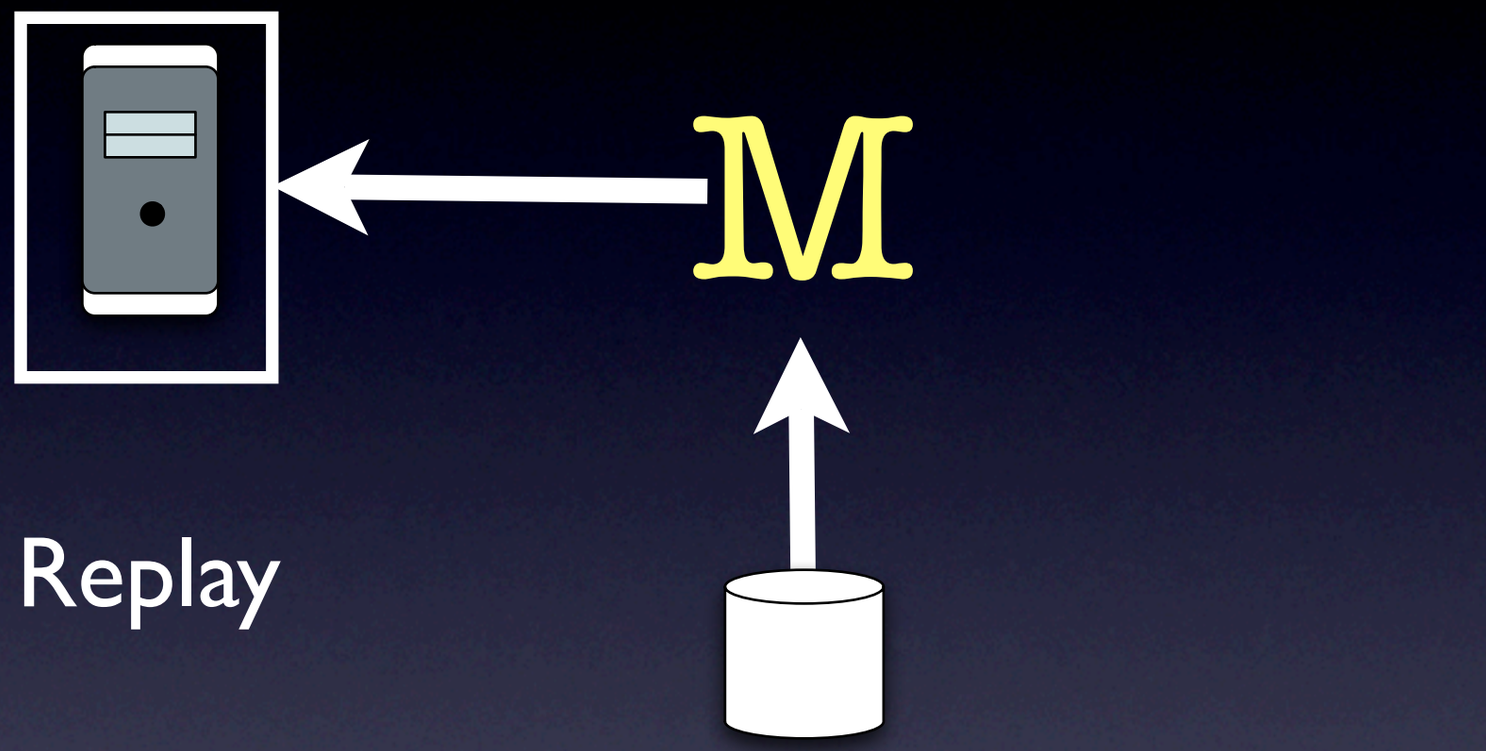
M

Replay



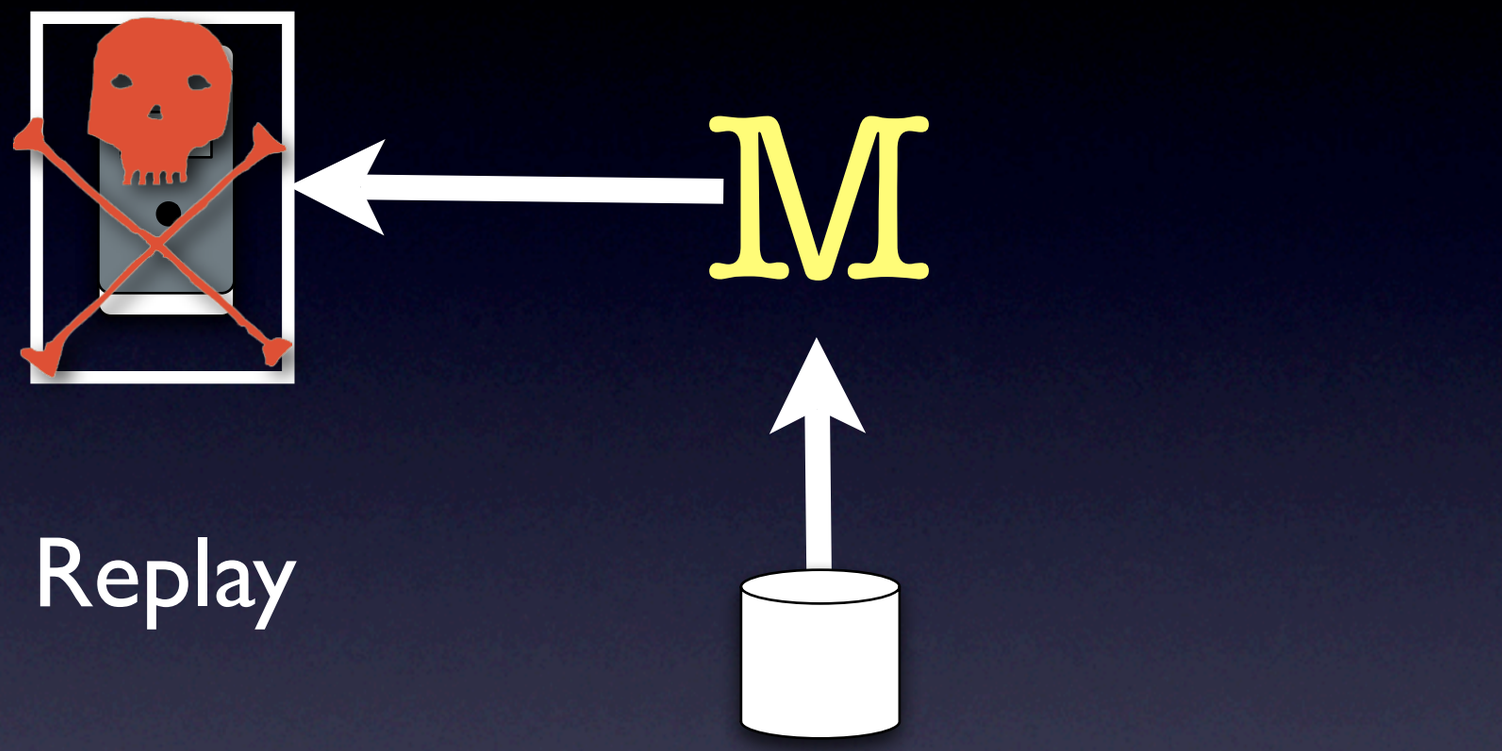
Processes

# Malfor Architecture



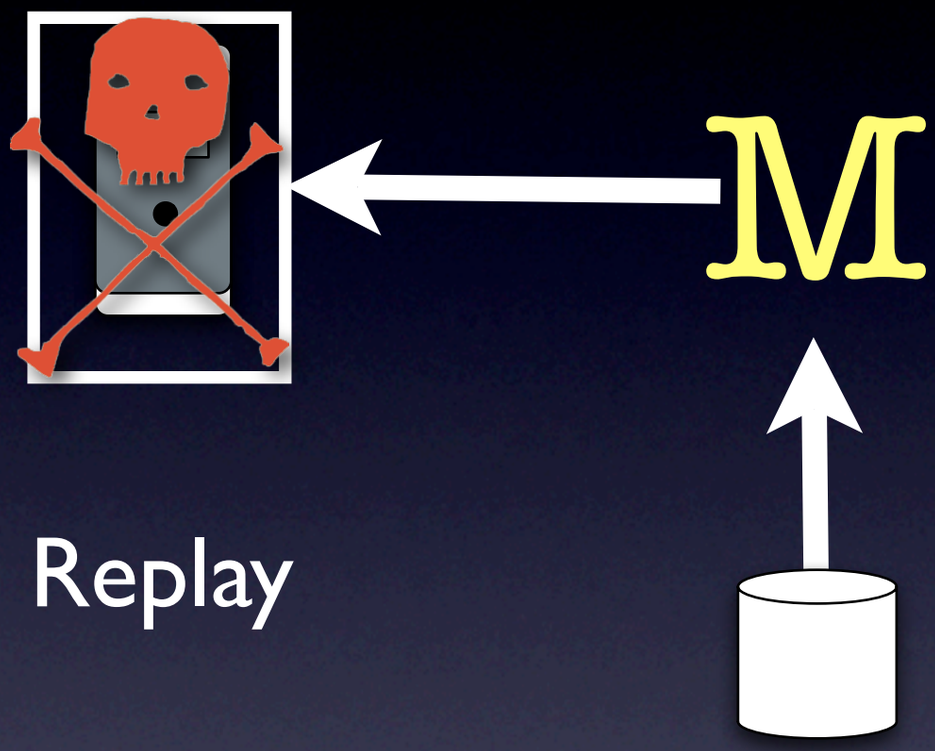

Processes

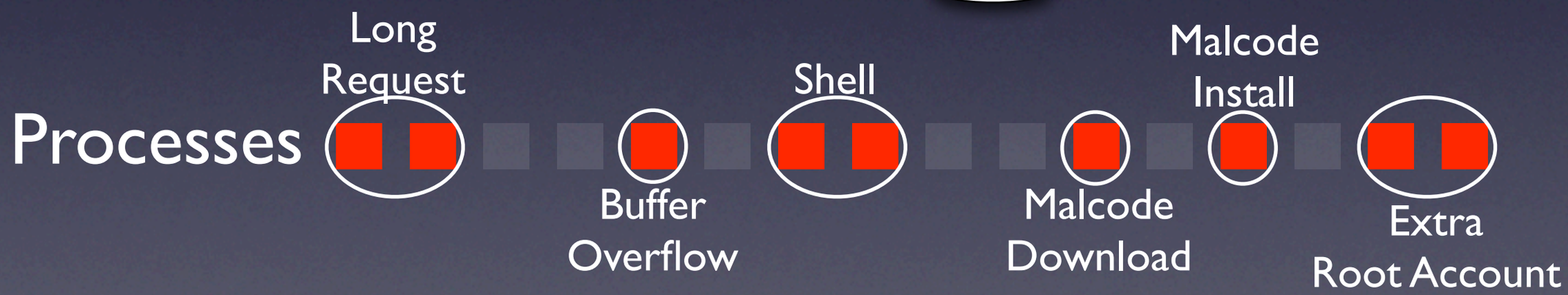
# Malfor Architecture




Processes

# Malfor Architecture



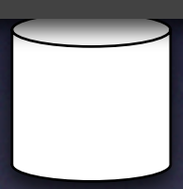



# Malfor Architecture

M

Partly Automated Diagnosis

Replay



Processes

Long Request

Buffer Overflow

Shell

Malcode Download

Malcode Install

Extra Root Account

# Requirements

# Requirements

- Capture/Replay *infrastructure*

# Requirements

- Capture/Replay *infrastructure*
- Must allow *suppression* of processes

# Requirements

- Capture/Replay *infrastructure*
- Must allow *suppression* of processes
- Must have ability to *replay or execute* I/O

# Requirements

- Capture/Replay *infrastructure*
  - Must allow *suppression* of processes
  - Must have ability to *replay or execute* I/O
- Method to *minimize set of processes*

# Delta Debugging

# Delta Debugging

- *Reduces* set of failure-inducing circumstances

# Delta Debugging

- *Reduces* set of failure-inducing circumstances
- Resulting set has *only relevant circumstances*

Zeller and Hildebrandt, FSE 2002

# Delta Debugging

- *Reduces* set of failure-inducing circumstances
- Resulting set has *only relevant circumstances*

  Zeller and Hildebrandt, FSE 2002

- *Practical method*, finds defects in gcc

  Cleve and Zeller, ICSE 2005

# Delta Debugging

- *Reduces* set of failure-inducing circumstances
- Resulting set has *only relevant circumstances*

  Zeller and Hildebrandt, FSE 2002

- *Practical method*, finds defects in gcc

  Cleve and Zeller, ICSE 2005

- Works by *repeating experiments on subsets*

# Delta Debugging

- *Reduces* set of failure-inducing circumstances
- Resulting set has *only relevant circumstances*

  Zeller and Hildebrandt, FSE 2002

- *Practical method*, finds defects in gcc

  Cleve and Zeller, ICSE 2005

- Works by *repeating experiments on subsets*
  - If test fails (✘): *reduce set*

# Delta Debugging

- *Reduces* set of failure-inducing circumstances
- Resulting set has *only relevant circumstances*

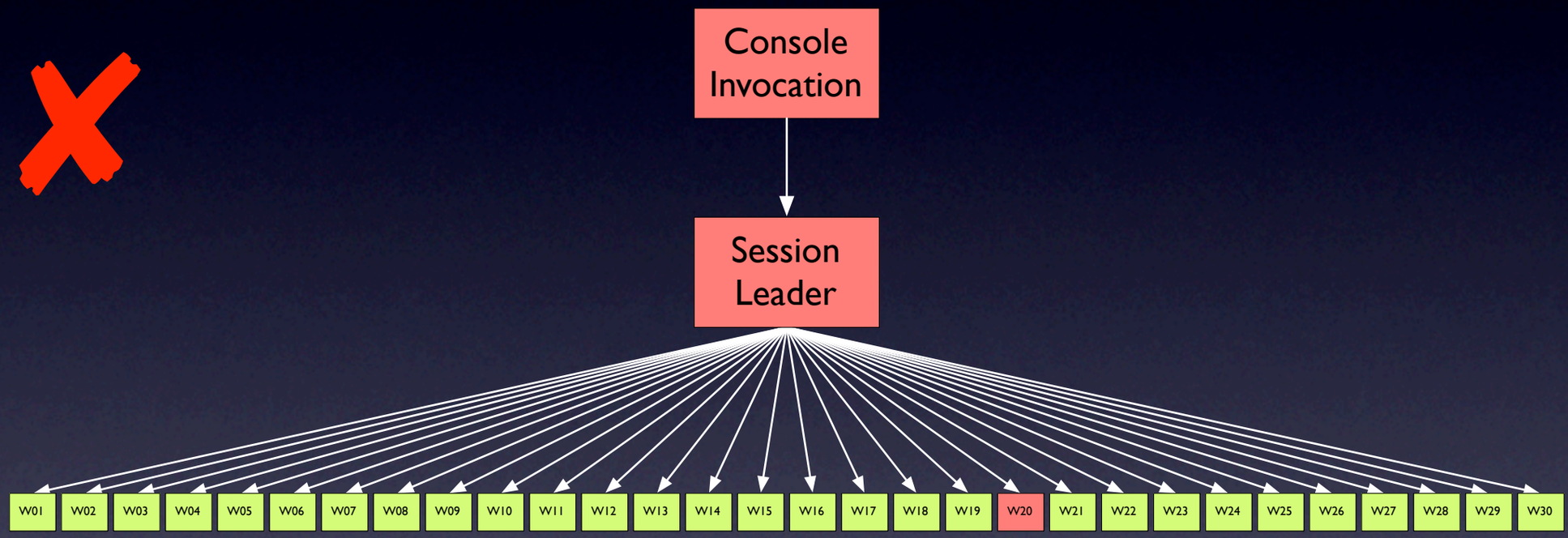
  Zeller and Hildebrandt, FSE 2002

- *Practical method*, finds defects in gcc

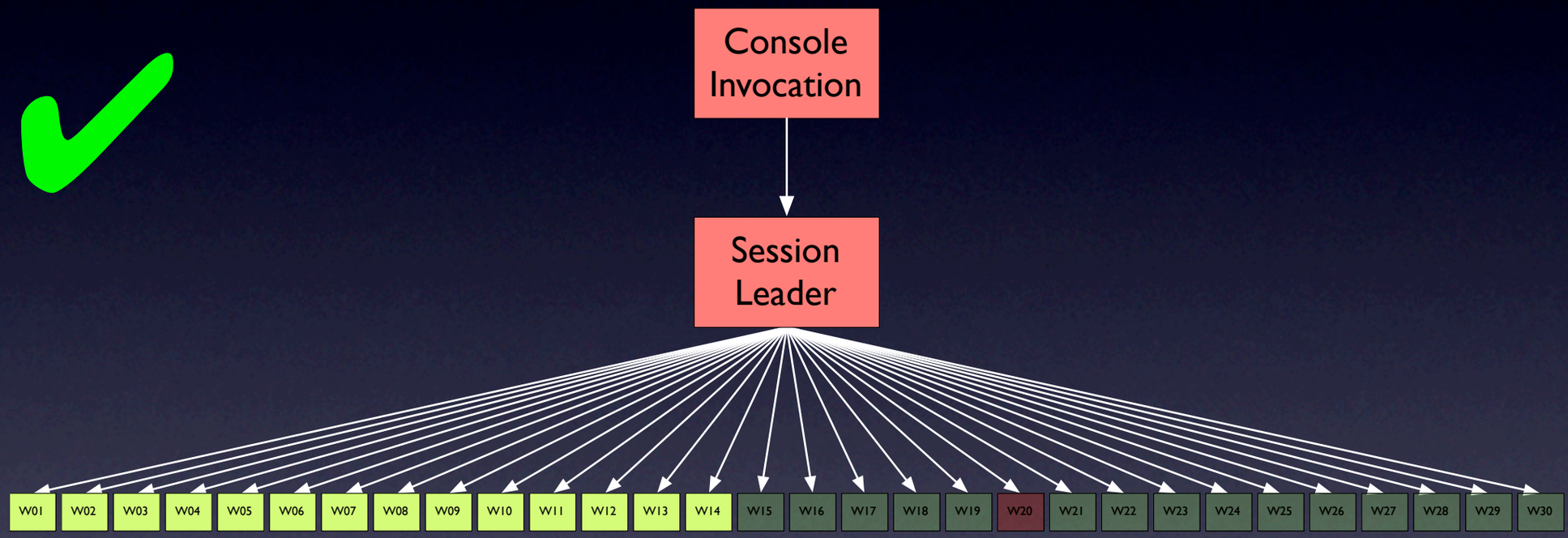
  Cleve and Zeller, ICSE 2005

- Works by *repeating experiments on subsets*
  - If test fails (✘): *reduce set*
  - If test passes (✔): *try different subset*

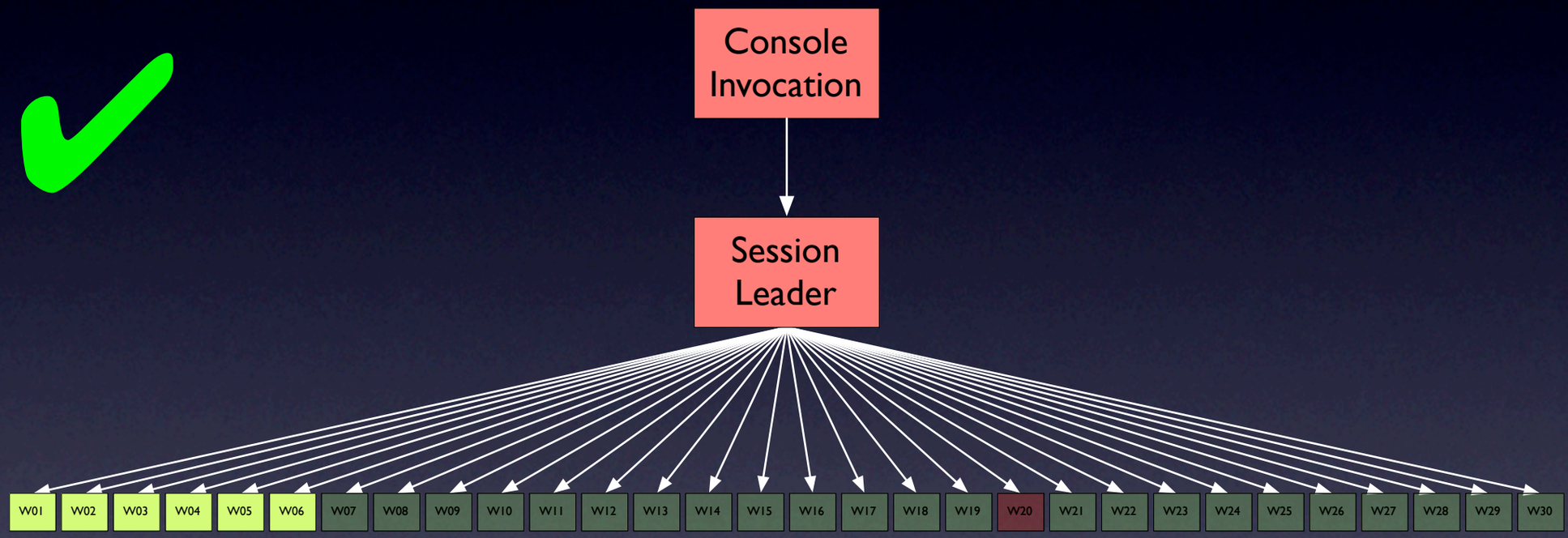
# Minimizing Process Sets



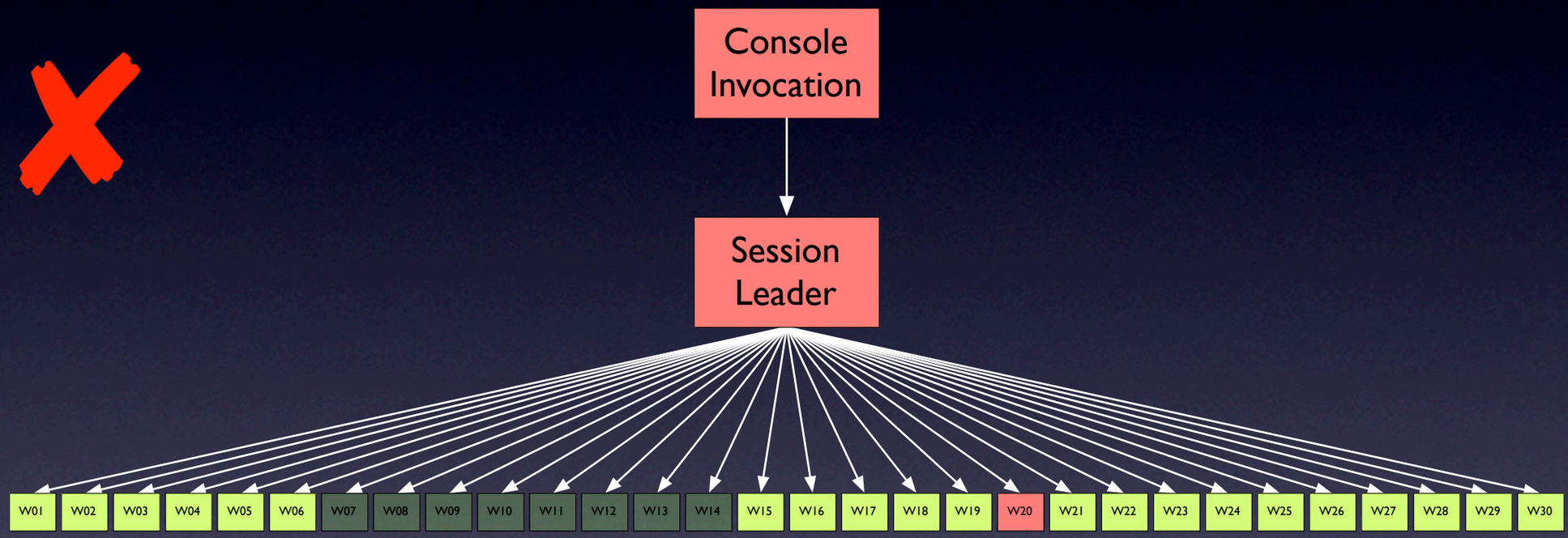
# Minimizing Process Sets



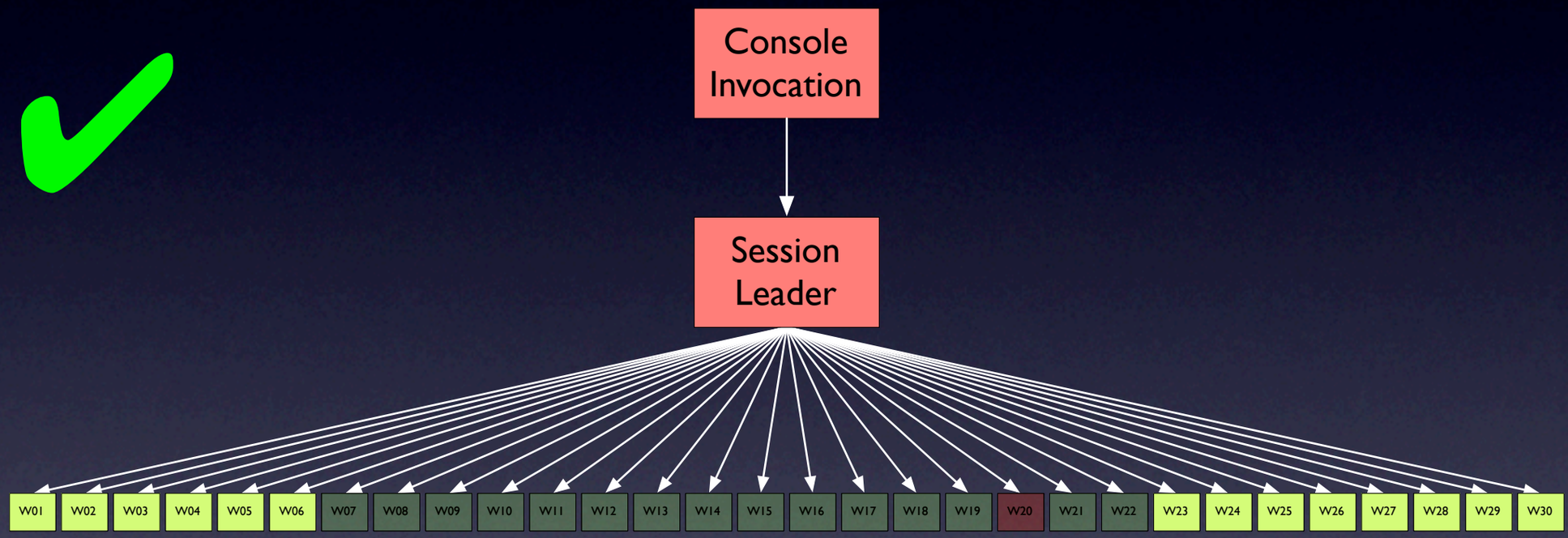
# Minimizing Process Sets



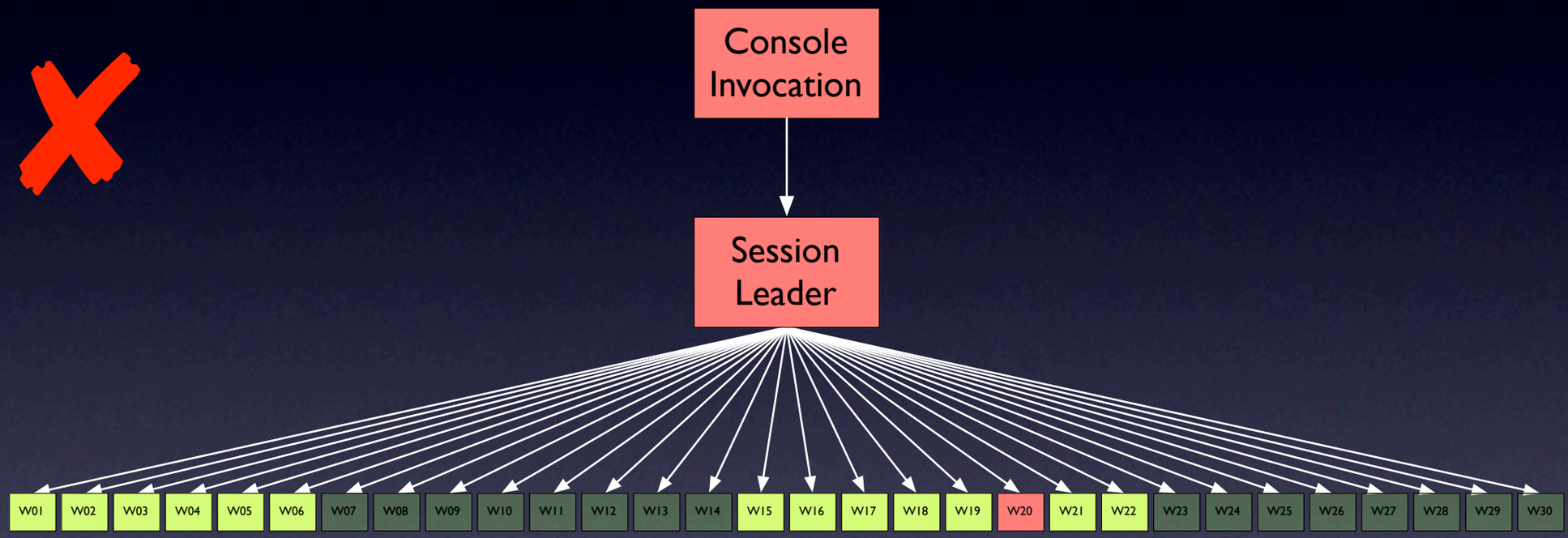
# Minimizing Process Sets



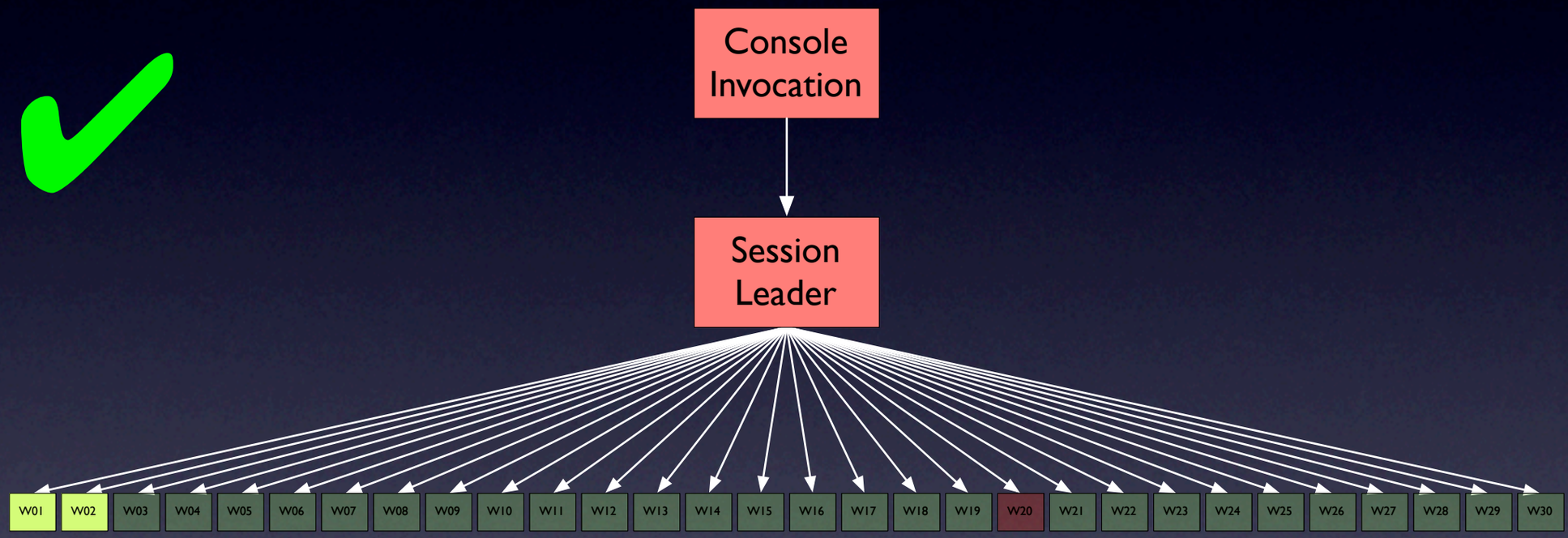
# Minimizing Process Sets



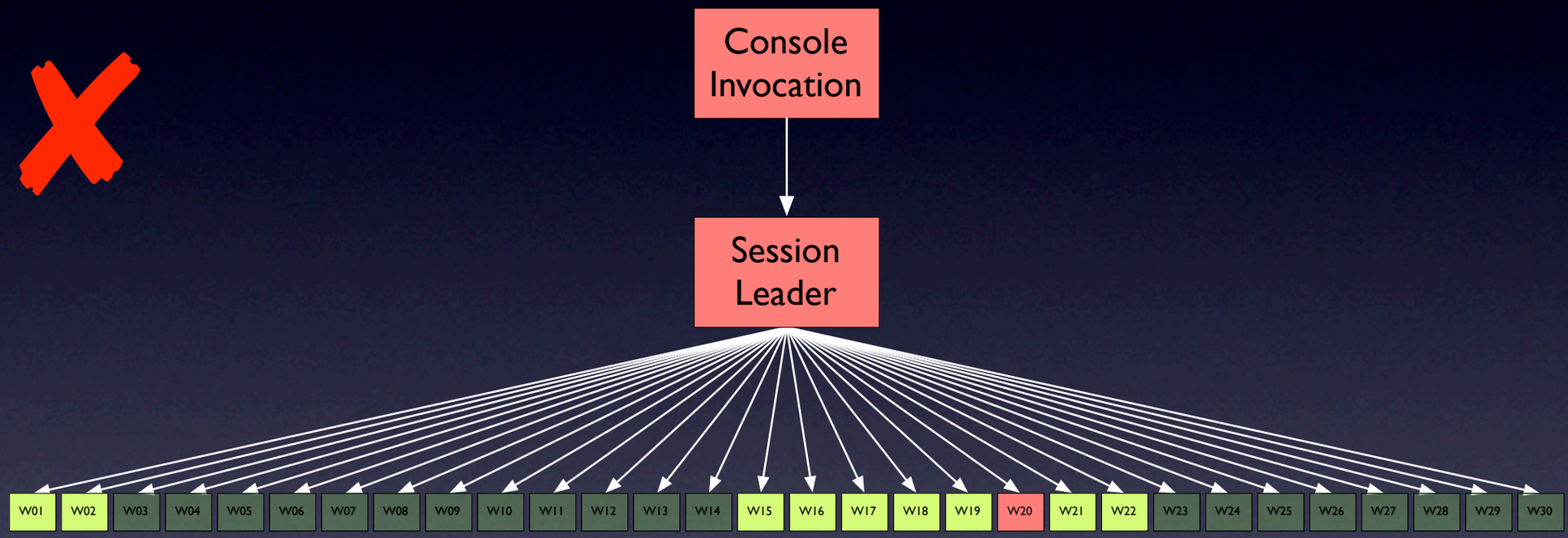
# Minimizing Process Sets



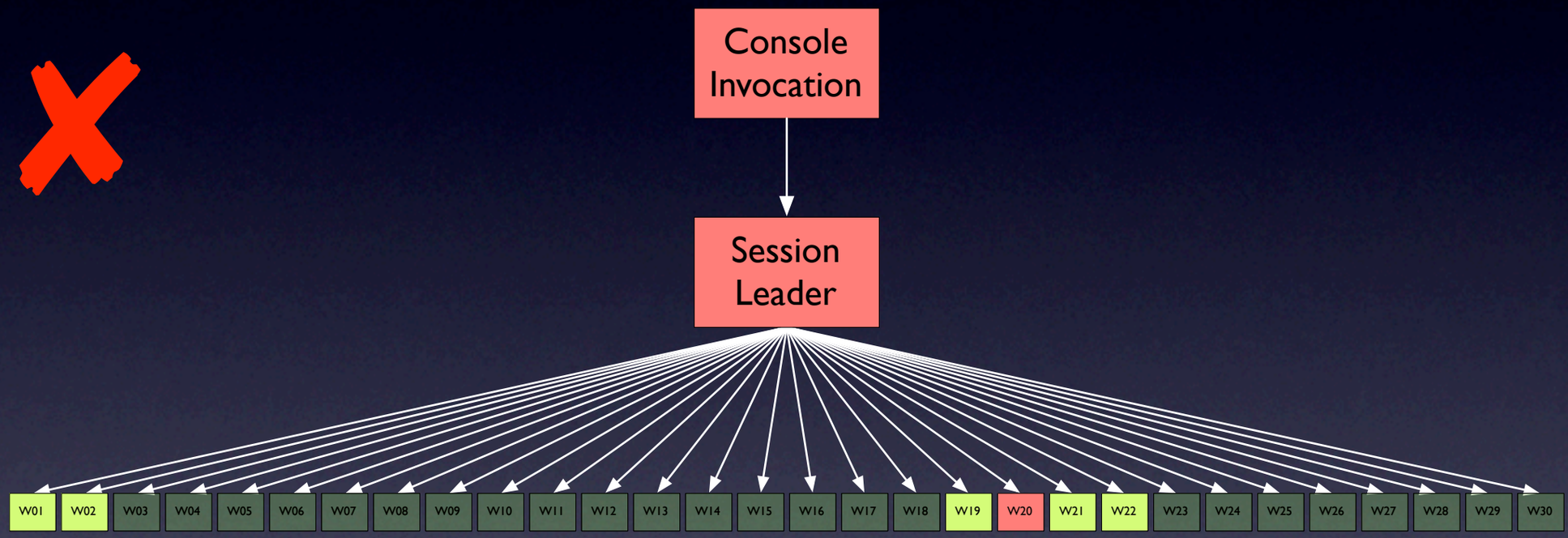
# Minimizing Process Sets



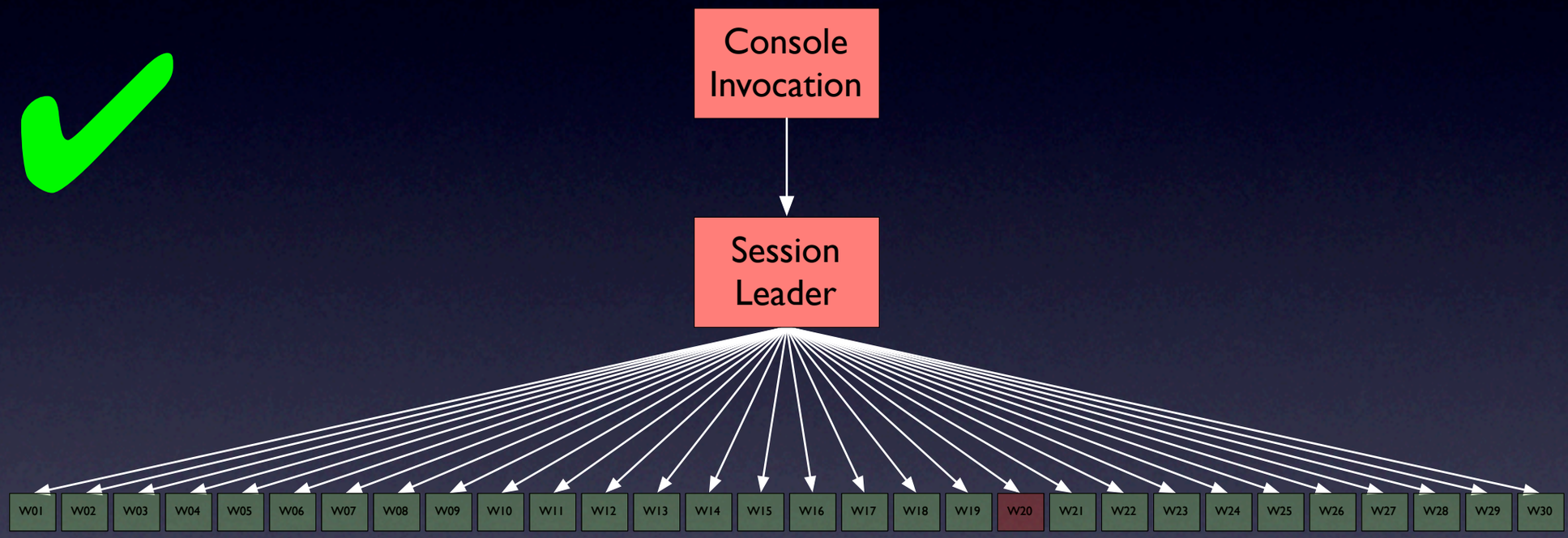
# Minimizing Process Sets



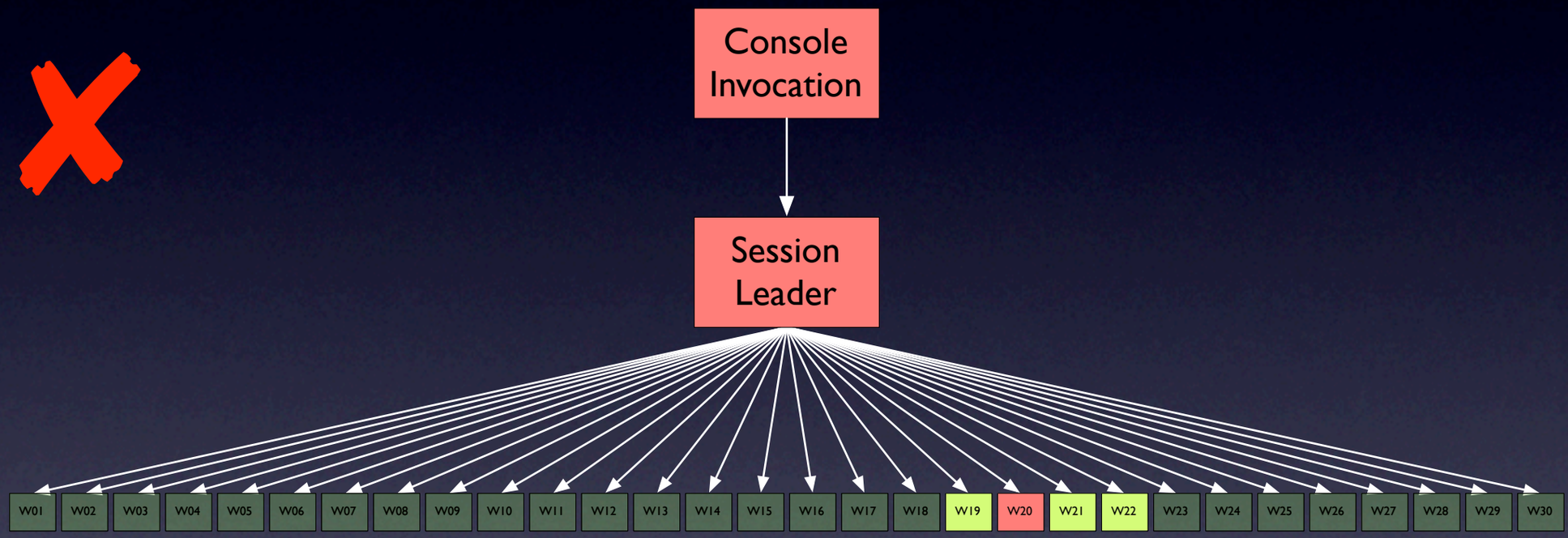
# Minimizing Process Sets



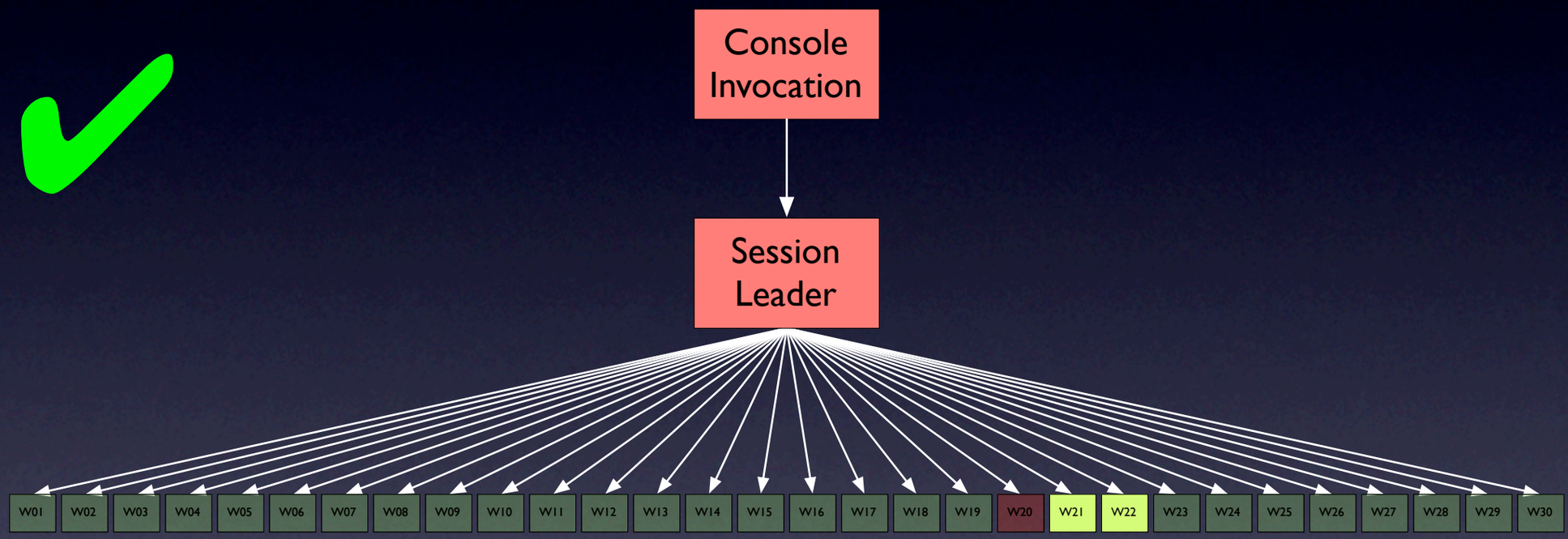
# Minimizing Process Sets



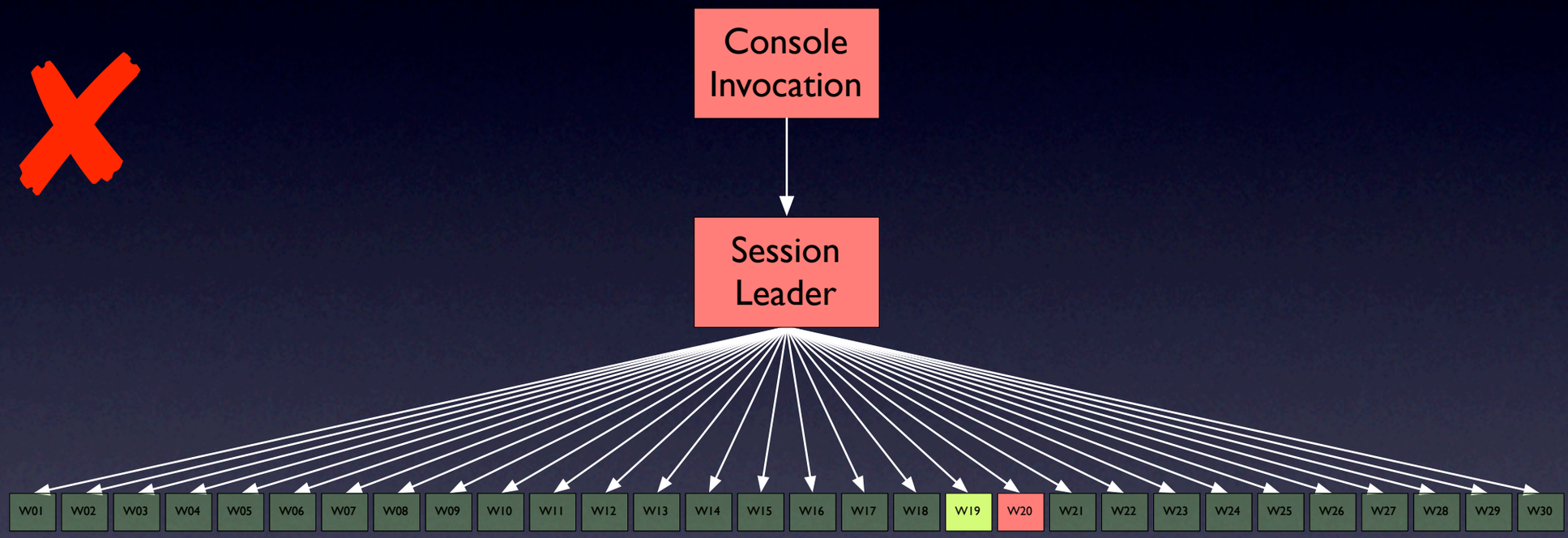
# Minimizing Process Sets



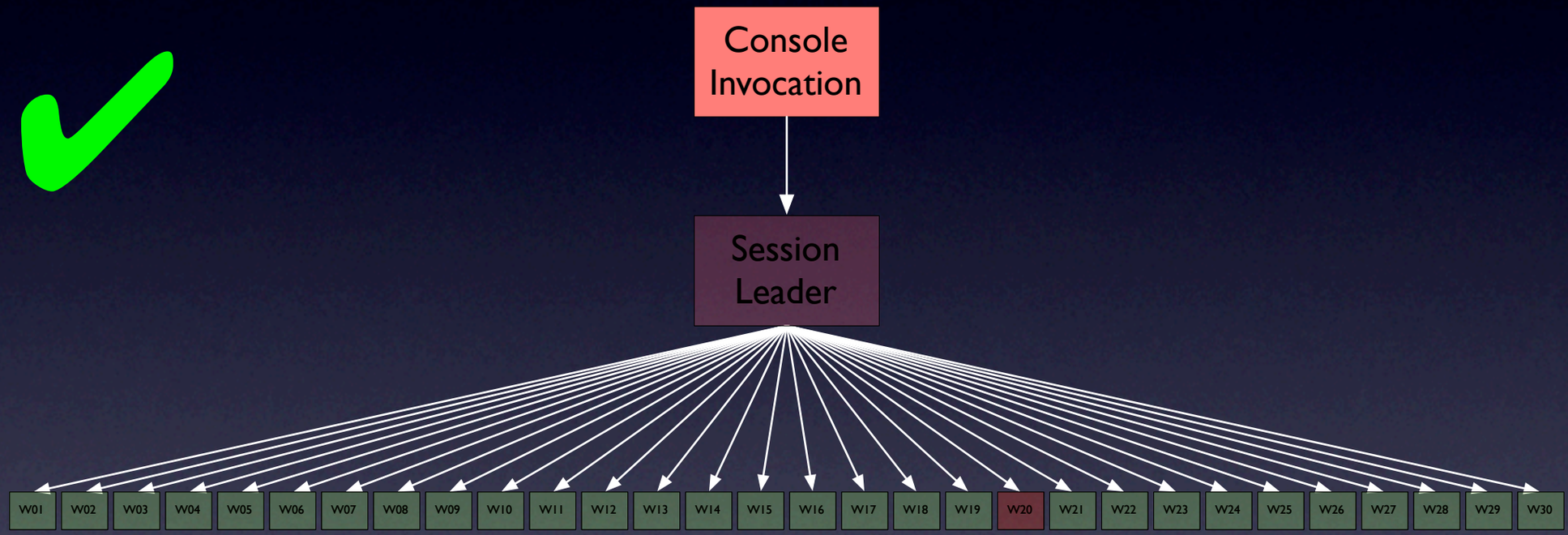
# Minimizing Process Sets



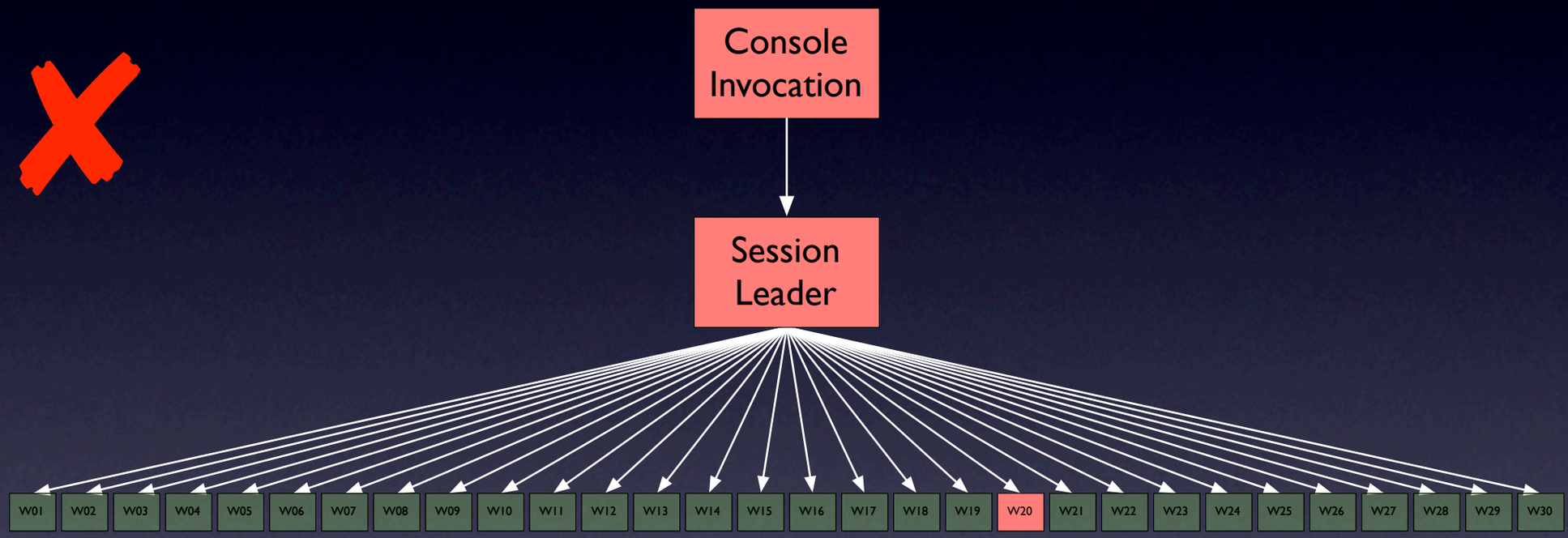
# Minimizing Process Sets



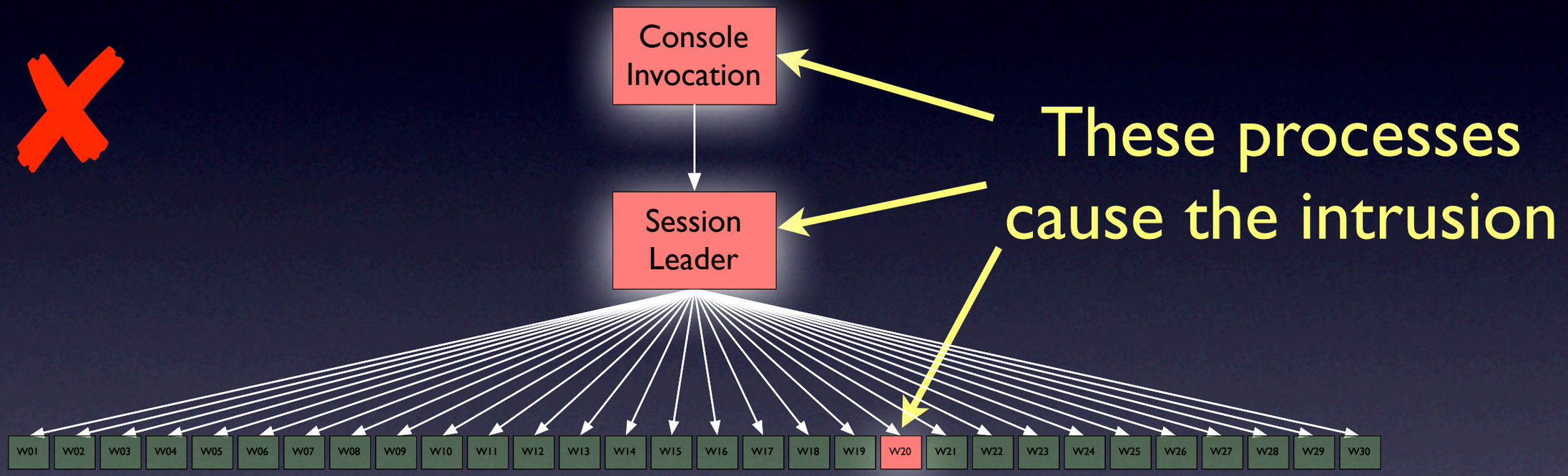
# Minimizing Process Sets



# Minimizing Process Sets



# Minimizing Process Sets



# After Minimization...

# After Minimization...

- Resulting process set is *small*

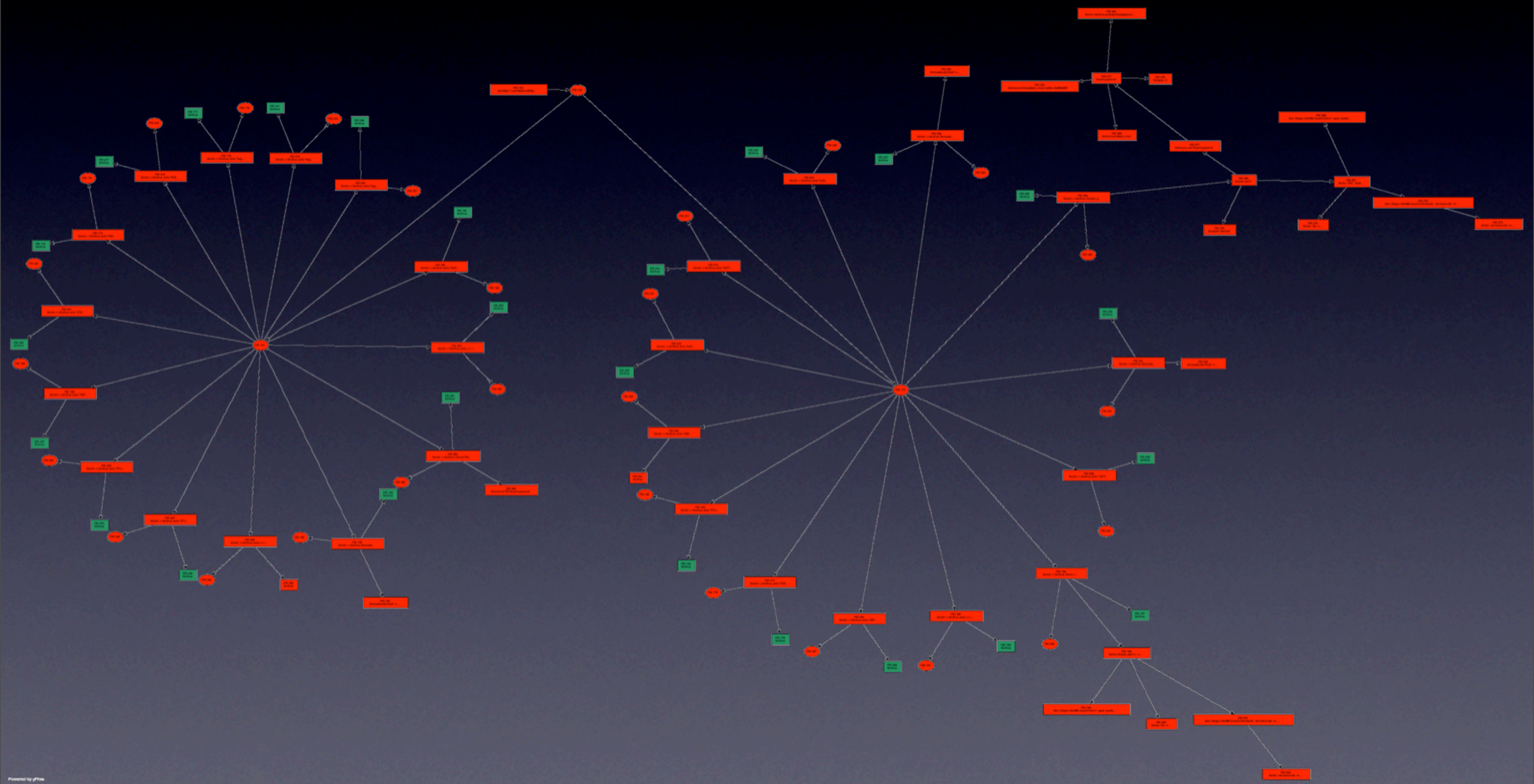
# After Minimization...

- Resulting process set is *small*
- *Experimentally shown* to be relevant

# After Minimization...

- Resulting process set is *small*
- *Experimentally shown* to be relevant
- Shows *complete chain of events*

# Backtracker Attack



# Features of Attack

# Features of Attack

- Get root

# Features of Attack

- Get root
- Load kernel module

# Features of Attack

- Get root
- Load kernel module
- Kernel Module modifies password file

# Features of Attack

- Get root
- Load kernel module
- Kernel Module modifies password file

➡ *No system call that modifies the password file*

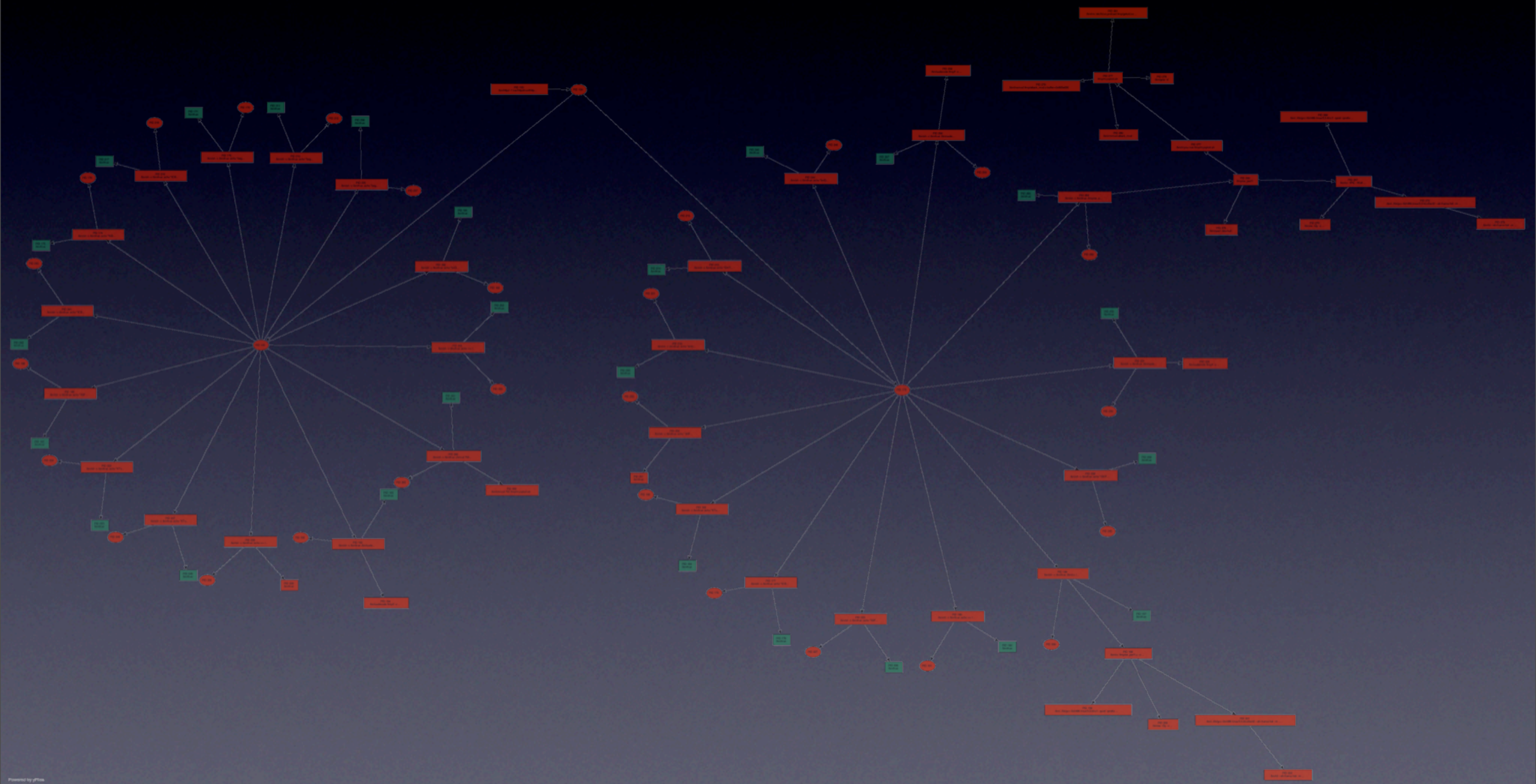
# Features of Attack

- Get root
- Load kernel module
- Kernel Module modifies password file

➡ *No system call that modifies the password file*

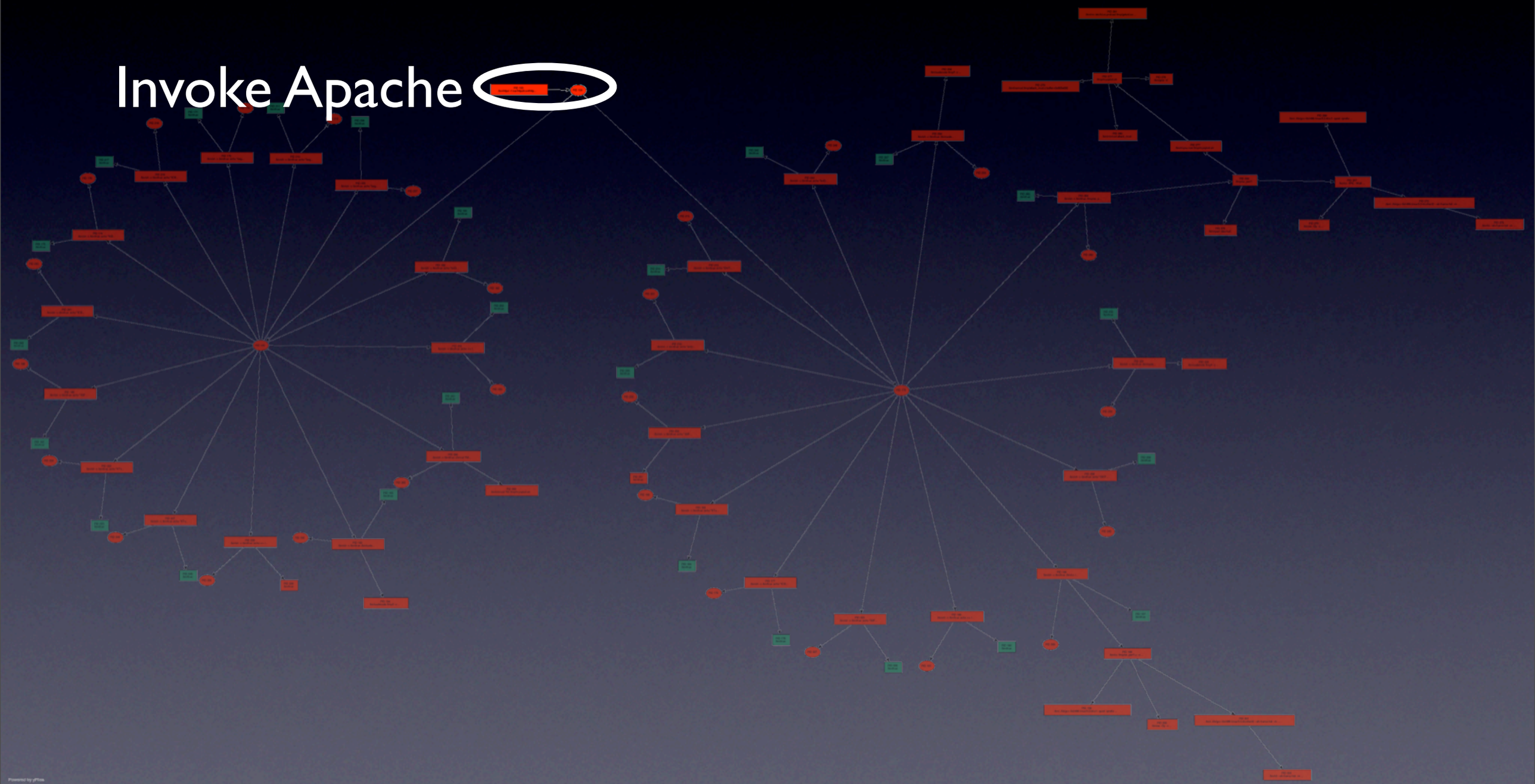
➡ *No analysis of system calls will analyze attack*

# Backtracker Attack



# Backtracker Attack

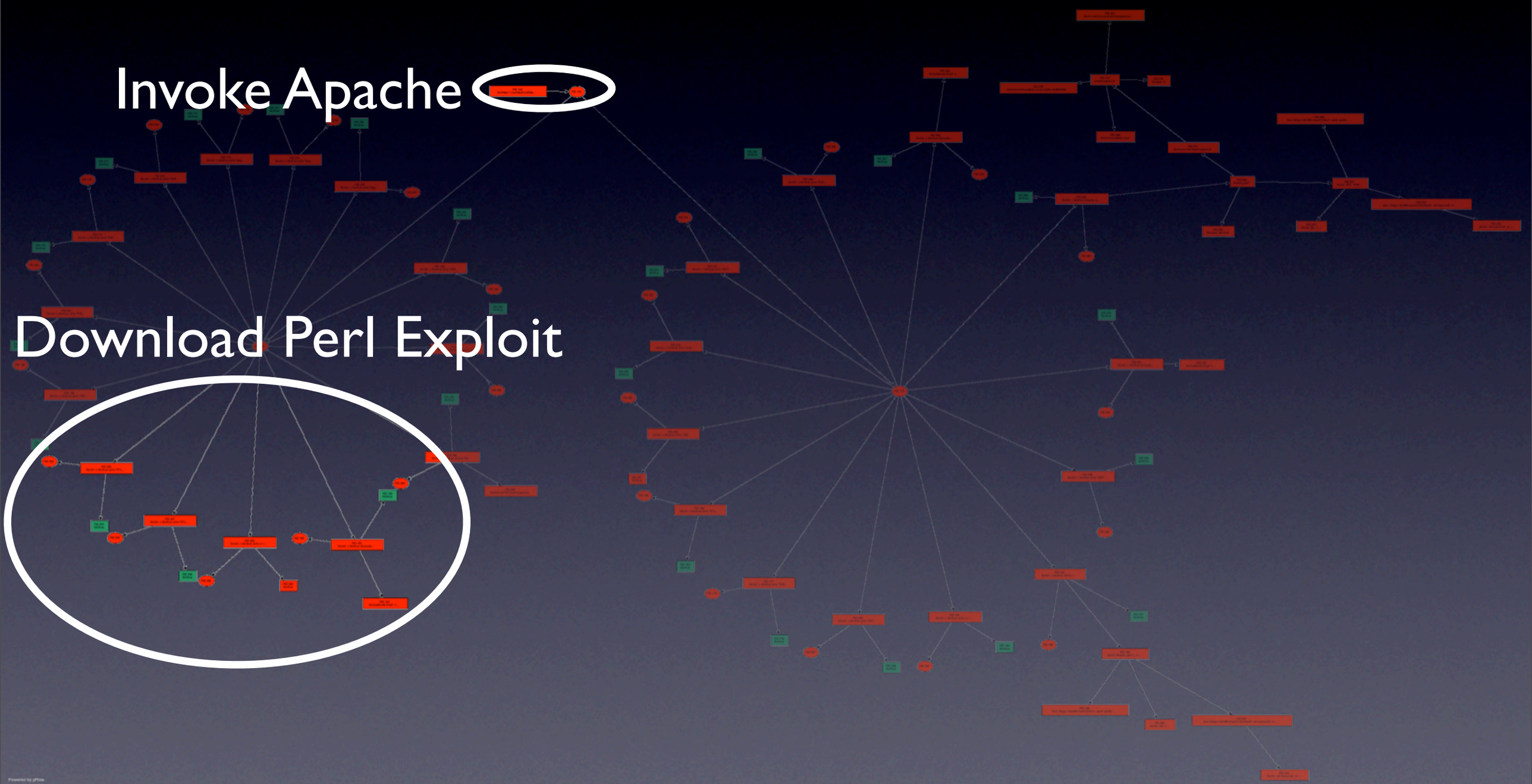
Invoke Apache



# Backtracker Attack

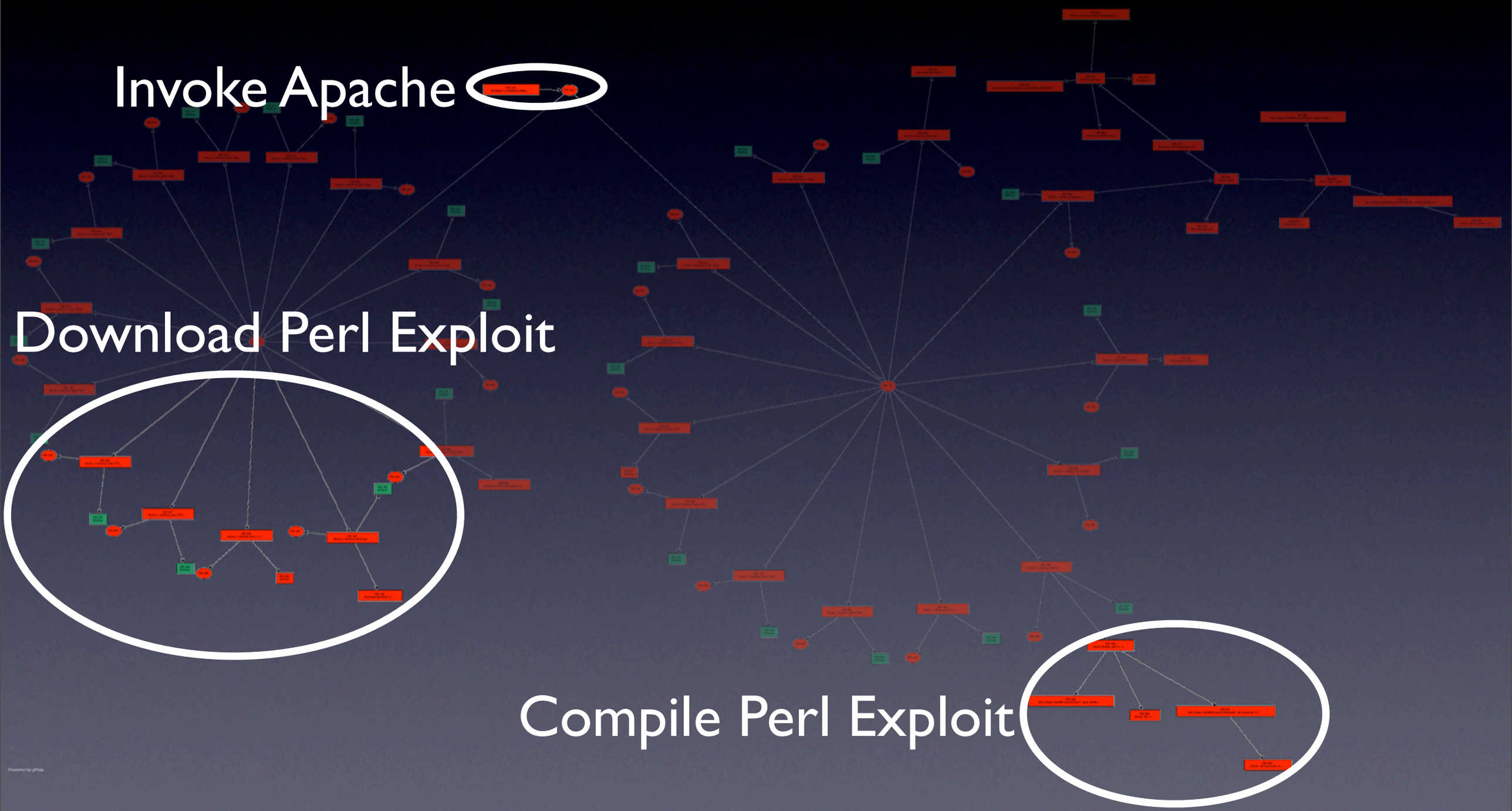
Invoke Apache

Download Perl Exploit



# Backtracker Attack

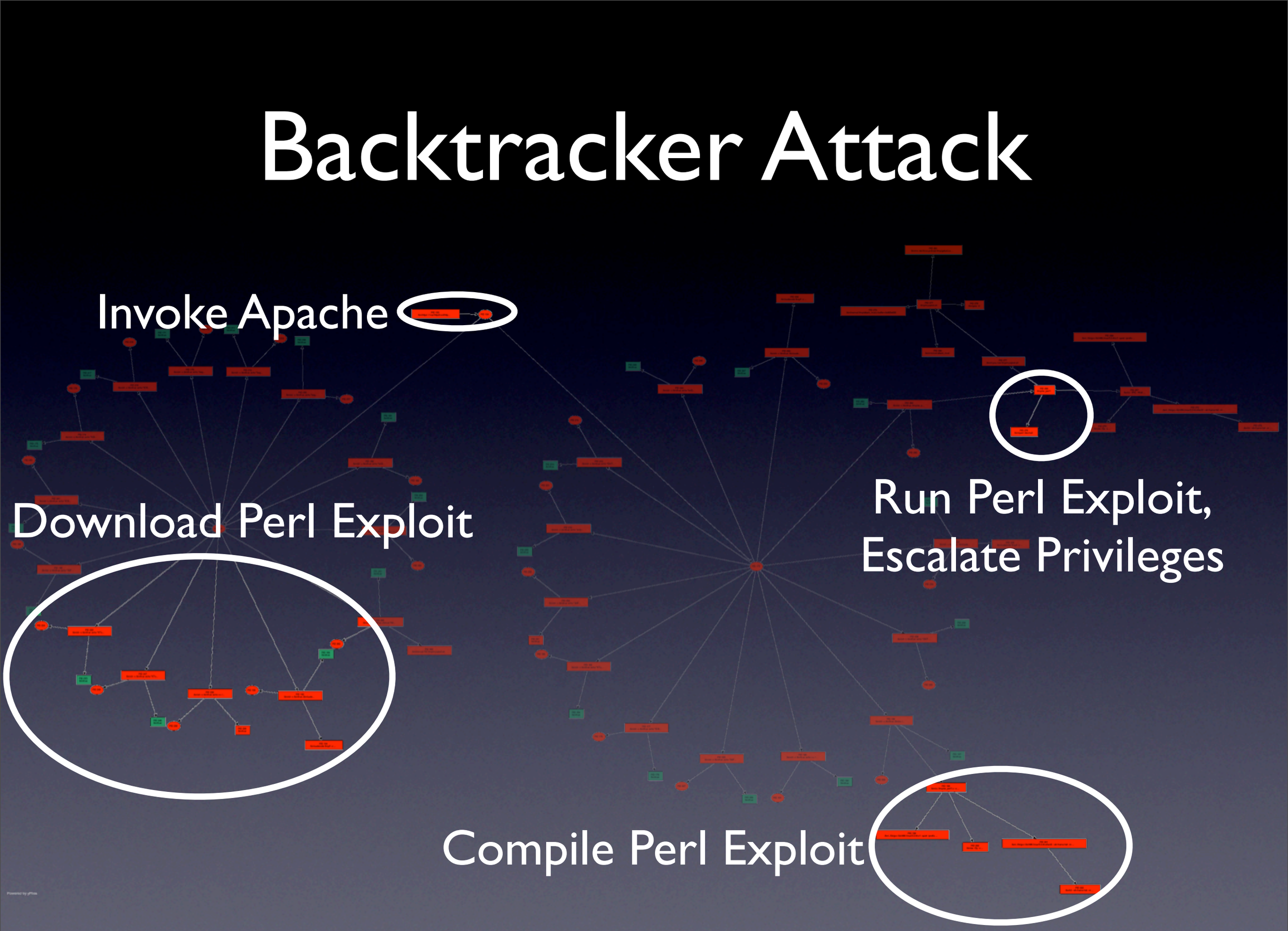
Invoke Apache



Download Perl Exploit

Compile Perl Exploit

# Backtracker Attack



# Backtracker Attack

Invoke Apache

Load Kernel Module,
Install Backdoor

Download Perl Exploit

Run Perl Exploit,
Escalate Privileges

Compile Perl Exploit

# Advantages of Approach

- Leverages *executability* of software
- Produces (re-)*executable test case*
- Carries incontrovertible *proof of validity*
- Can be *demonstrated*, e.g., in court

# Future Work

# Future Work

- Find *attack signatures* automatically (perhaps)

# Future Work

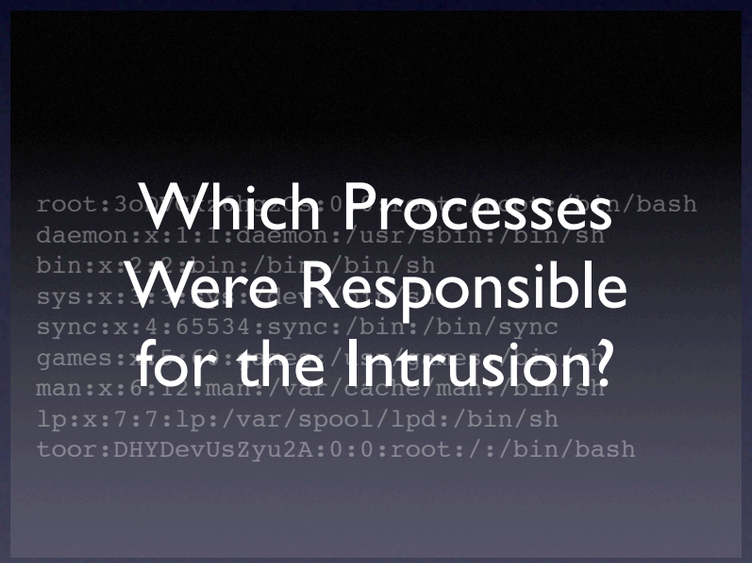
- Find *attack signatures* automatically (perhaps)
- Expand Malfor to *distributed systems*

# Future Work

- Find *attack signatures* automatically (perhaps)
- Expand Malfor to *distributed systems*
- Expand Malfor to general *cause-effect relationships*

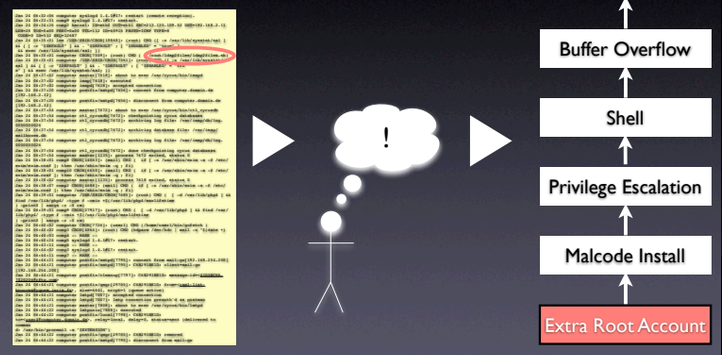
# Conclusion

# Conclusion



# Conclusion

## Analyzing Intrusions

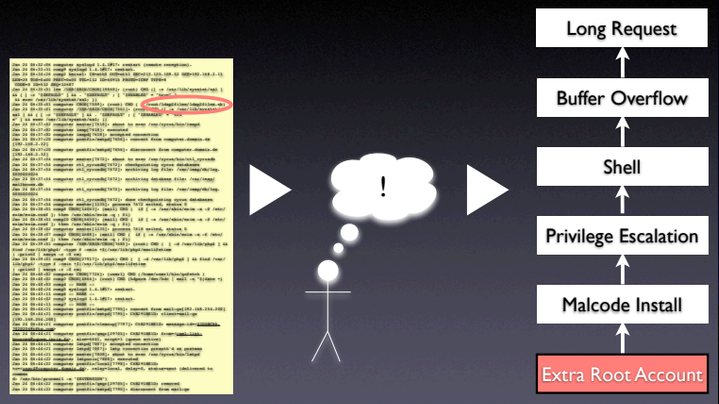




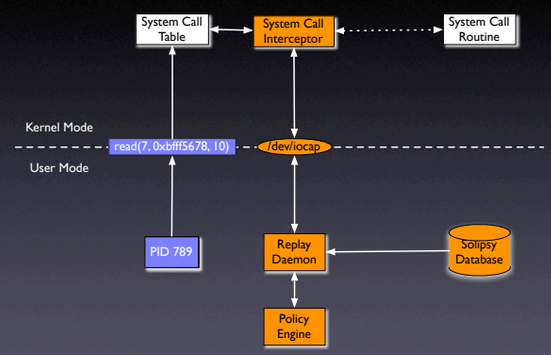
## Which Processes Were Responsible for the Intrusion?

# Conclusion

## Analyzing Intrusions




## Capture/Replay



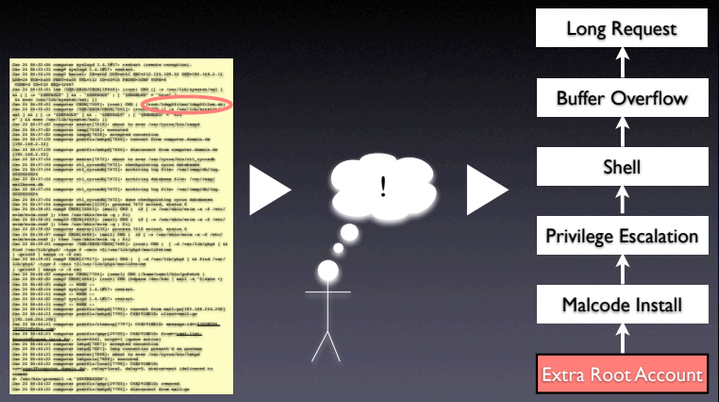

Replay Phase

## Which Processes Were Responsible for the Intrusion?

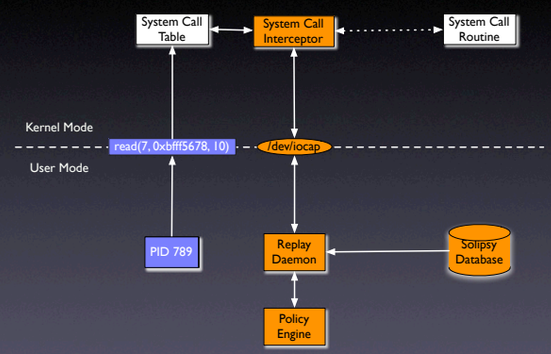
```
root:3oWGazpvTbzGc:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
toor:DHYDevUsZyu2A:0:0:root:/:/bin/bash
```

# Conclusion

## Analyzing Intrusions



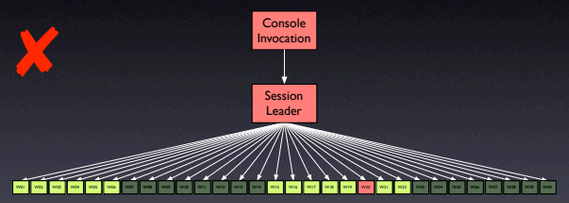

## Capture/Replay




Replay Phase

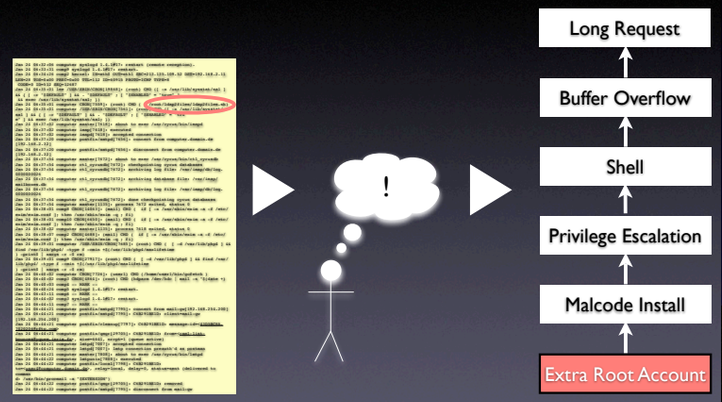
## Which Processes Were Responsible for the Intrusion?

## Minimizing Process Sets

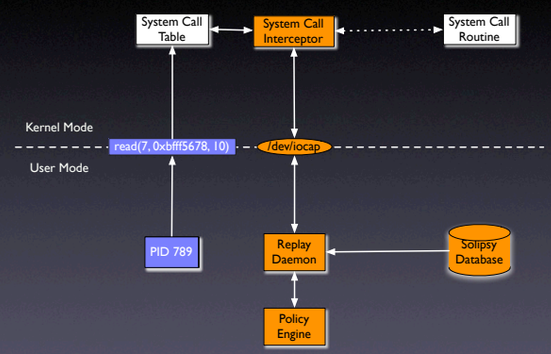


# Conclusion

## Analyzing Intrusions



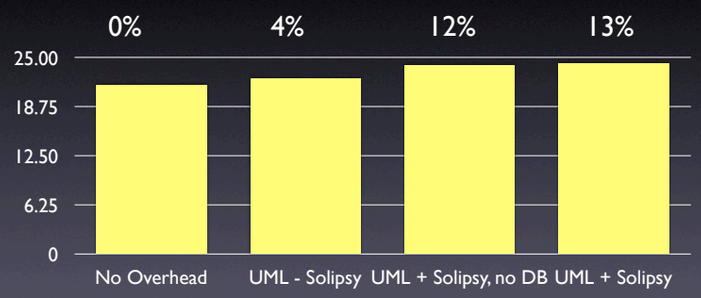

## Capture/Replay



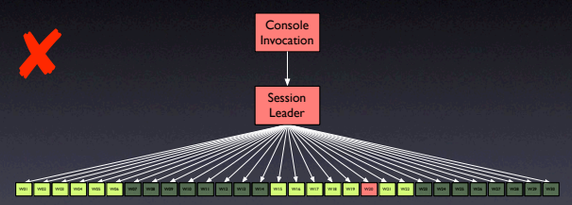

Replay Phase

## Which Processes Were Responsible for the Intrusion?

## Solipsy Overhead vs. Dedicated Machine

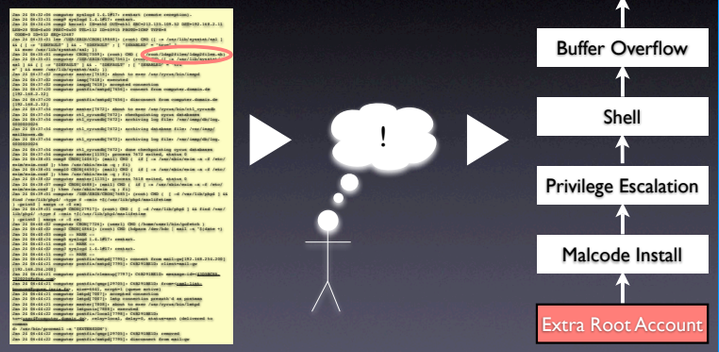



## Minimizing Process Sets

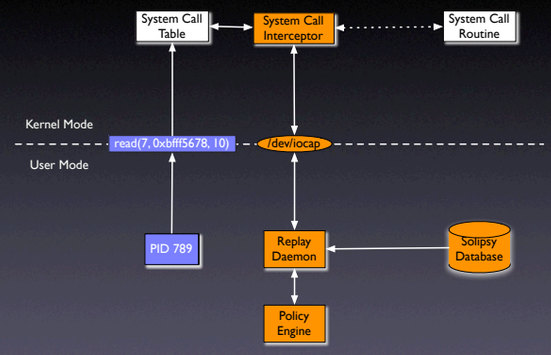


# Conclusion

## Analyzing Intrusions



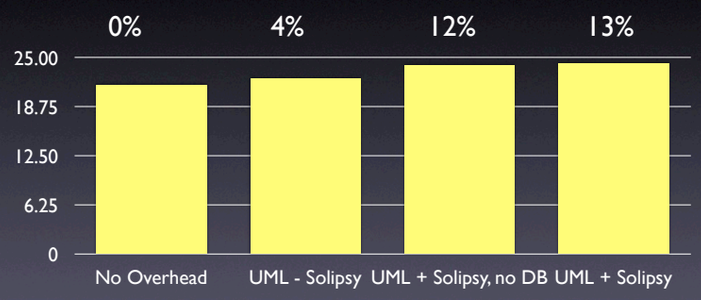

## Capture/Replay




Replay Phase

# Malfor

## Solipsy Overhead vs. Dedicated Machine




## Minimizing Process Sets