Security Network Infrastructure @uwaterloo.ca

Mike Patterson

WATERLOO
INFORMATION SYSTEMS & TECHNOLOGY
Information Security Services

09 March 2016

Outline

1. Who we are
2. What we do
3. How we do what we do
4. What we do after we do what we do

Who

Mark Gaulton
Security Operations Specialist

Terry Labach
Information Security Specialist

Sean Mason
IAM Specialist

Patrick Matlock
Information Security Specialist

Mike Patterson
Manager, IT Security Operations

Andy Redfearn
Information Systems Specialist

Jason Testart
Director, Information Security Services

Andrew Ward
IAM Specialist

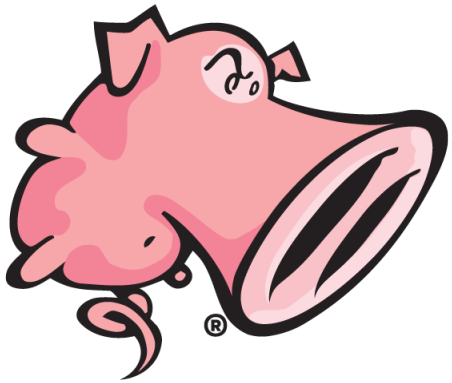
What

SOC work

1. IDS
2. Firewalls
3. Vulnerability management
4. LE and academic integrity requests
5. General scutwork

How

Network Monitoring



Snort

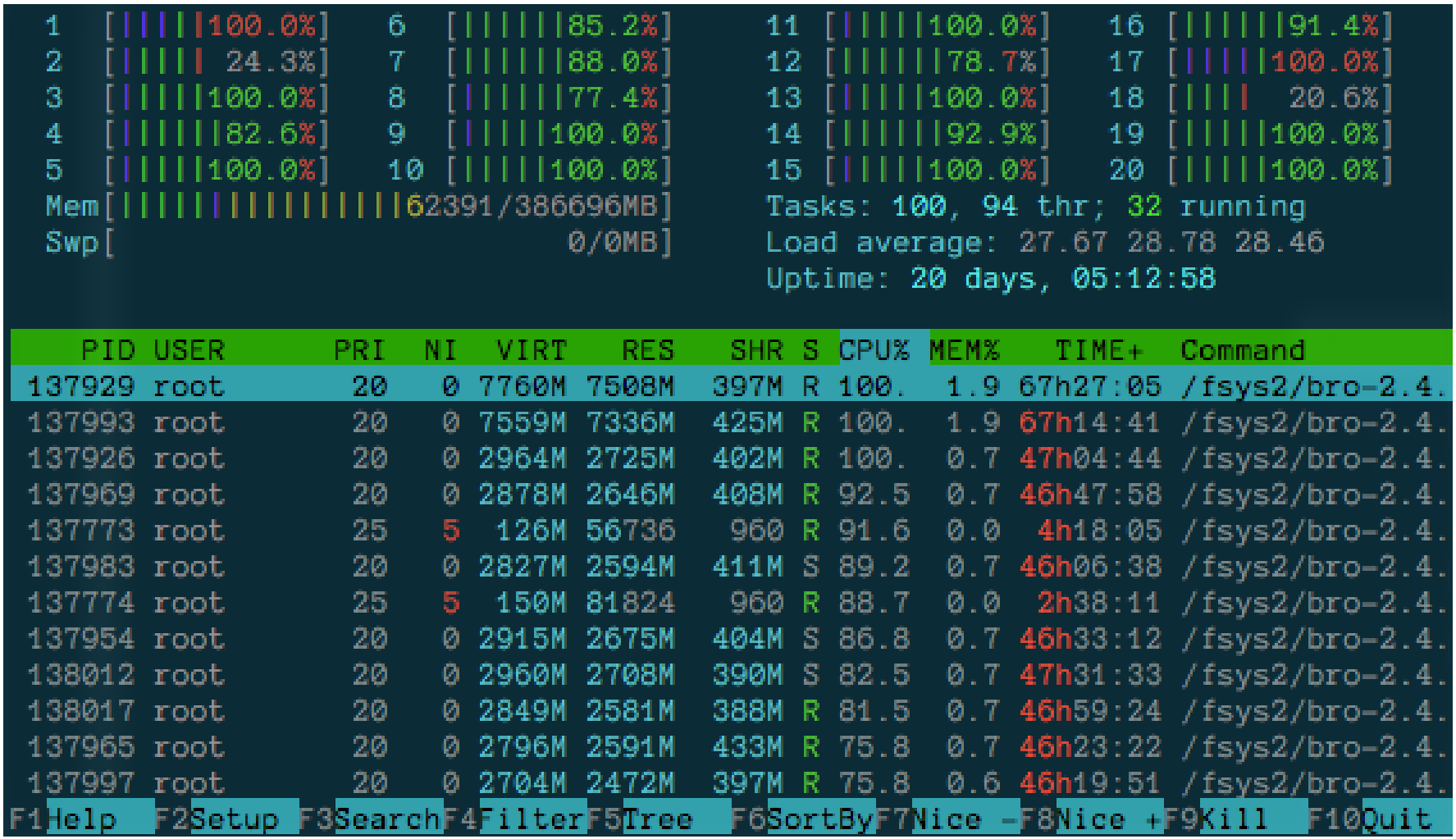
```
Sequence: 8:27952781
Timestamp: 2016-03-02 09:48:00 -0500
Signature: 2022482 Rev 1 (GID 1) | ET TROJAN JS/Nemucod
   requesting EXE payload 2016-02-01
Source: 129.97.xxx.yyy:55788
Destination: 91.196.50.241:80
Decoded payload (TCP):
----
GET /69.exe HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: soclosebutyetqq.com
Connection: Keep-Alive
```

Bro Usage

```
$ jq -c '[.ts, .uid, ."id.orig_p", ."id.resp_h", \
."id.resp_p", .method, .host, .uri, .response_body_len,\
 .status_code]' < dddd | grep 91.196.50.241

[1456930076.513924,"Cx6fTT1ckh1mXRvGXl",55788,
"91.196.50.241",80,"GET","soclosebutyetqq.com","/69.exe",
3844,200]
$
```

Bro Likes CPU



Firewalls


```
set security policies from-zone untrust to-zone Campus\
 policy TaurineWeirdSSH match source-address any
set security policies from-zone untrust to-zone Campus\
 policy TaurineWeirdSSH match destination-address\
 taurine.csclub.uwaterloo.ca
set security policies from-zone untrust to-zone Campus\
 policy TaurineWeirdSSH match application taurineSSH
set security policies from-zone untrust to-zone Campus\
 policy TaurineWeirdSSH then permit
```

Vulnerability Management: General


```
qualys=> select count(*) from vulns where last_detected
 > '2016-02-01';
 count
-------
 19527
(1 row)
```

Vulnerability Management: Specific

```
qualys=> \d wordpress
  Table "public.wordpress"
 Column  | Type | Modifiers
---------+------+-----------
 version | text |
 url     | text |
 first   | date |
 last    | date |
qualys=> select count(*) from xpfound where
 last > '2016-03-01';
 count
-------
   117
(1 row)
```

LE / Academic Integrity / Non-Academic Offenses

1. Stalking
2. Missing persons
3. Stolen laptops/mobiles
4. Somebody went to the bathroom with their phone
5. Somebody pulled their phone out *during* the exam
6. Somebody hired somebody else to *write* their exam

Scutwork

Entity: CEG TEK International
Subject: Copyright Infringement - Case C123987
ISP: University of Waterloo
Copyright Owner: Awesome Movies Inc
IP Address: 10.20.30.40
Source Port: 780013
Date of Infringement: right down to .xx seconds
Infringing Work : Battlefield Earth
Filename : At_Least_Somebody_Might_Watch_It.rar
Filesize : 4.3PB

Responses

1. Implement ACLs or firewall policies
2. Sinkhole DNS
3. Disable switch ports
4. Lock accounts
5. Report to AssDeans, LE
6. Information sharing communities

End

Thanks for coming out.

Attribution

Talk itself is CC-by-SA, except all logos are marks of their respective owners. These include:

- Snort, Pig logo are registered trade marks of Cisco
- Bro eye logo is a mark of The Bro Project
- Elastic logo is a trade mark of Elasticsearch BV
- QRadar logo is a mark of IBM
- Arista logo is a mark of Arista Networks
- Endace logo is a mark of Emulex Corporation
- Qualys logo is a mark of Qualys Inc