System Administration & Security

COMP 175 | Fall 2021 | University of the Pacific | Jeff Shafer

Monitoring

(System & Security)

Monitoring

"System" Monitoring

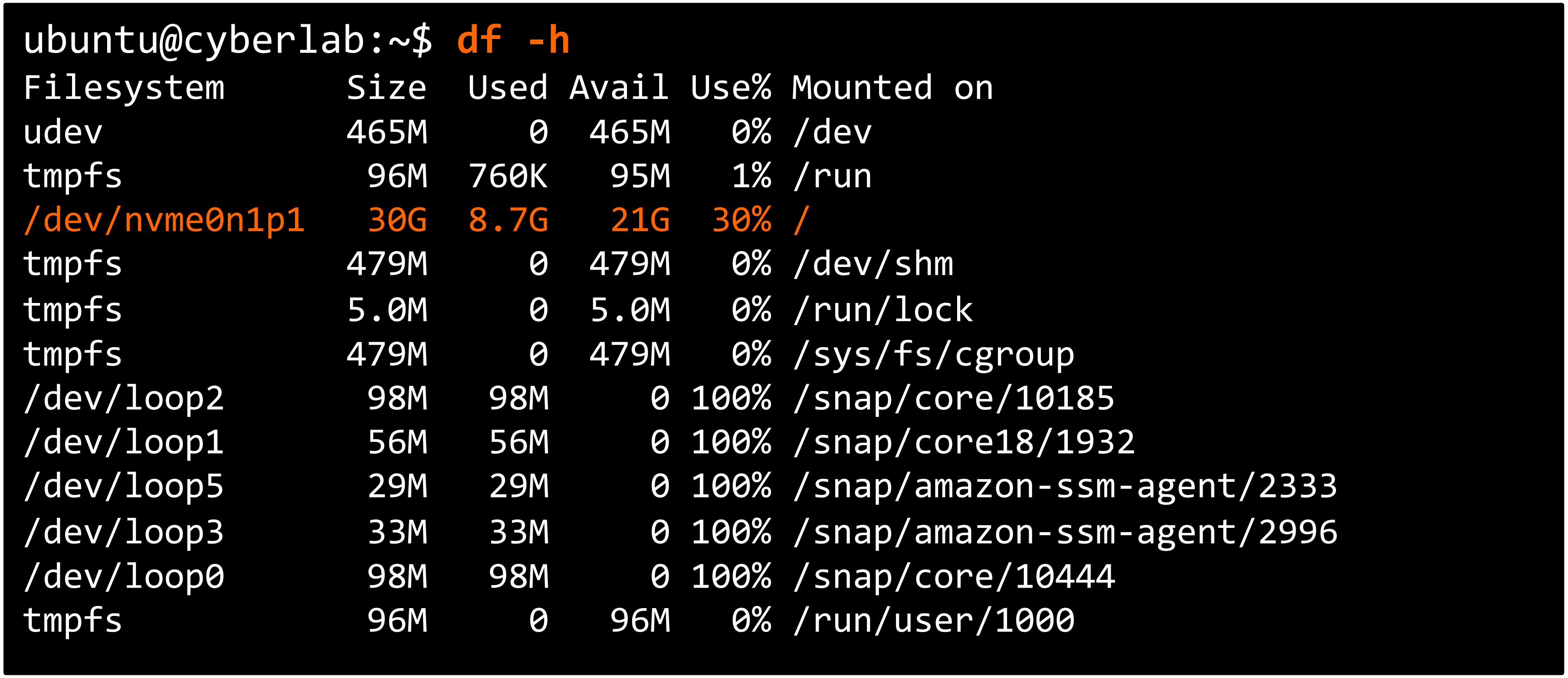
- Host monitoring
  - Disk full?
  - CPU maxed out?
  - Memory maxed out?
  - Memory ECC errors?
  - Disk errors?
- Network monitoring
- Application monitoring
  - Web service
  - Database service
  - Firewall service

Security Monitoring

- Security scanners
- Honeypots

Disk Utilization

- How much disk space is used on each partition?



```
ubuntu@cyberlab:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            465M     0  465M   0% /dev
tmpfs            96M  760K   95M   1% /run
/dev/nvme0n1p1   30G  8.7G   21G  30% /
tmpfs           479M     0  479M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           479M     0  479M   0% /sys/fs/cgroup
/dev/loop2       98M   98M     0 100% /snap/core/10185
/dev/loop1       56M   56M     0 100% /snap/core18/1932
/dev/loop5       29M   29M     0 100% /snap/amazon-ssm-agent/2333
/dev/loop3       33M   33M     0 100% /snap/amazon-ssm-agent/2996
/dev/loop0       98M   98M     0 100% /snap/core/10444
tmpfs            96M     0   96M   0% /run/user/1000
```

RAM Utilization

- How much RAM is used / available?

```
ubuntu@cyberlab:~$ free -m
        total     used     free   shared  buff/cache   available
Mem:      957      262       94       73         600         457
Swap:       0        0        0
```

- **total** – Total installed memory
- **used** – Used memory (calculated as total - free - buffers - cache)
- **free** – Unused memory
- **shared** – Memory used (mostly) by tmpfs
- **buff/cache** – Sum of buffers and cache
  - **buffers** – Memory used by kernel buffers
  - **cache** – Memory used by the page cache
- **available** – Estimate of how much memory is available for starting new applications **without swapping**

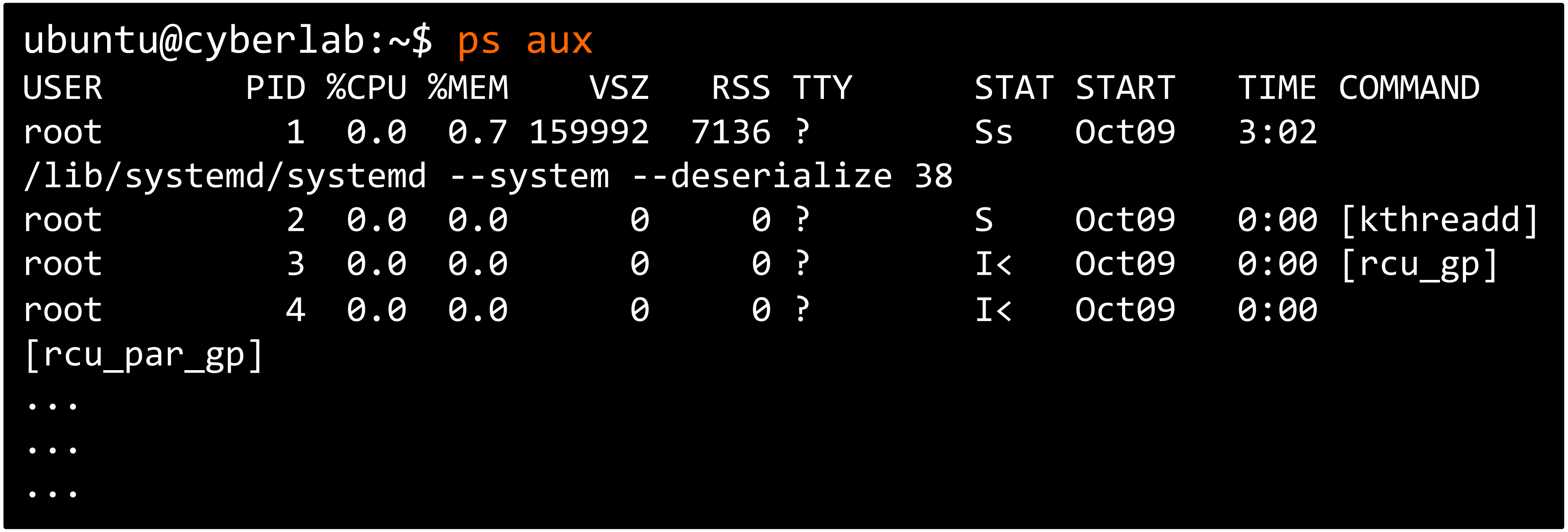
Active Processes

- What processes are running as *my user*?

```
ubuntu@cyberlab:~$ ps
  PID TTY          TIME CMD
22162 pts/0    00:00:00 bash
22282 pts/0    00:00:00 ps
```

Active Processes

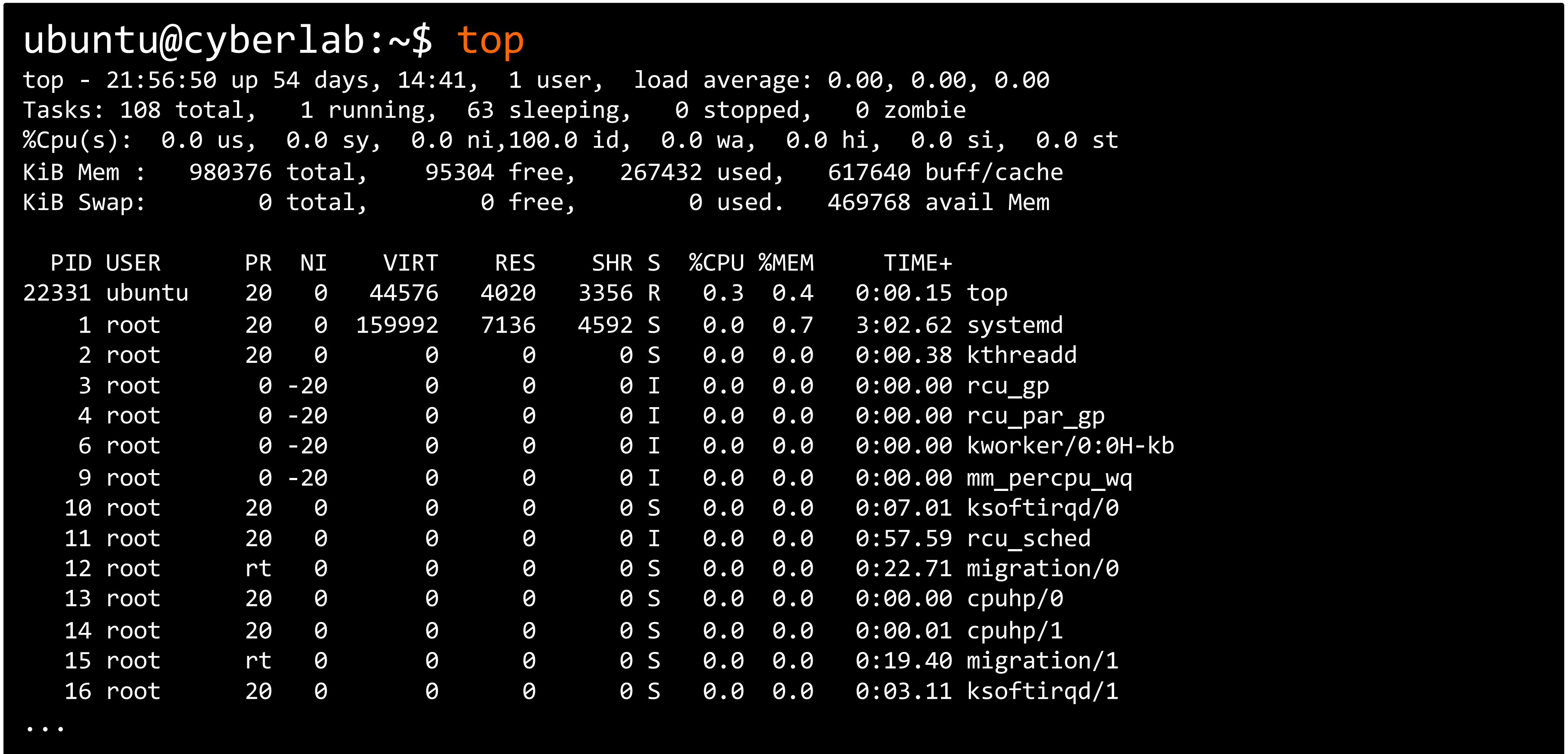
- What processes are running as *any user*? (plus extended output)



```
ubuntu@cyberlab:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.7 159992  7136 ?        Ss   Oct09   3:02
/lib/systemd/systemd --system --deserialize 38
root         2  0.0  0.0      0     0 ?        S    Oct09   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I<   Oct09   0:00 [rcu_gp]
root         4  0.0  0.0      0     0 ?        I<   Oct09   0:00
[rcu_par_gp]
...
...
...
```

Active Processes

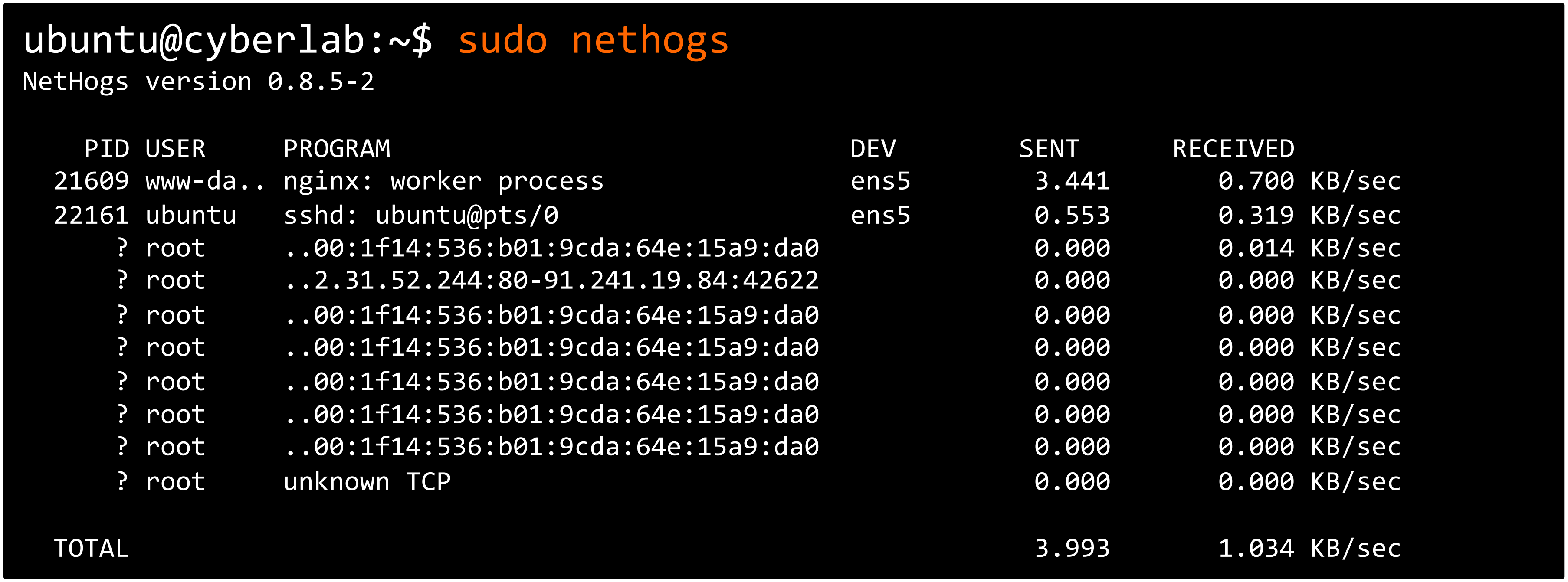
- What process is taking all the CPU right now?



```
ubuntu@cyberlab:~$ top
top - 21:56:50 up 54 days, 14:41,  1 user,  load average: 0.00, 0.00, 0.00
Tasks: 108 total,   1 running,  63 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :   980376 total,    95304 free,   267432 used,   617640 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   469768 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+
22331 ubuntu    20   0   44576   4020   3356 R   0.3  0.4   0:00.15 top
    1 root      20   0  159992   7136   4592 S   0.0  0.7   3:02.62 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.38 kthreadd
    3 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 rcu_par_gp
    6 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/0:0H-kb
    9 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 mm_percpu_wq
   10 root      20   0       0      0      0 S   0.0  0.0   0:07.01 ksoftirqd/0
   11 root      20   0       0      0      0 I   0.0  0.0   0:57.59 rcu_sched
   12 root      rt   0       0      0      0 S   0.0  0.0   0:22.71 migration/0
   13 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/0
   14 root      20   0       0      0      0 S   0.0  0.0   0:00.01 cpuhp/1
   15 root      rt   0       0      0      0 S   0.0  0.0   0:19.40 migration/1
   16 root      20   0       0      0      0 S   0.0  0.0   0:03.11 ksoftirqd/1
...
```

Network Utilization

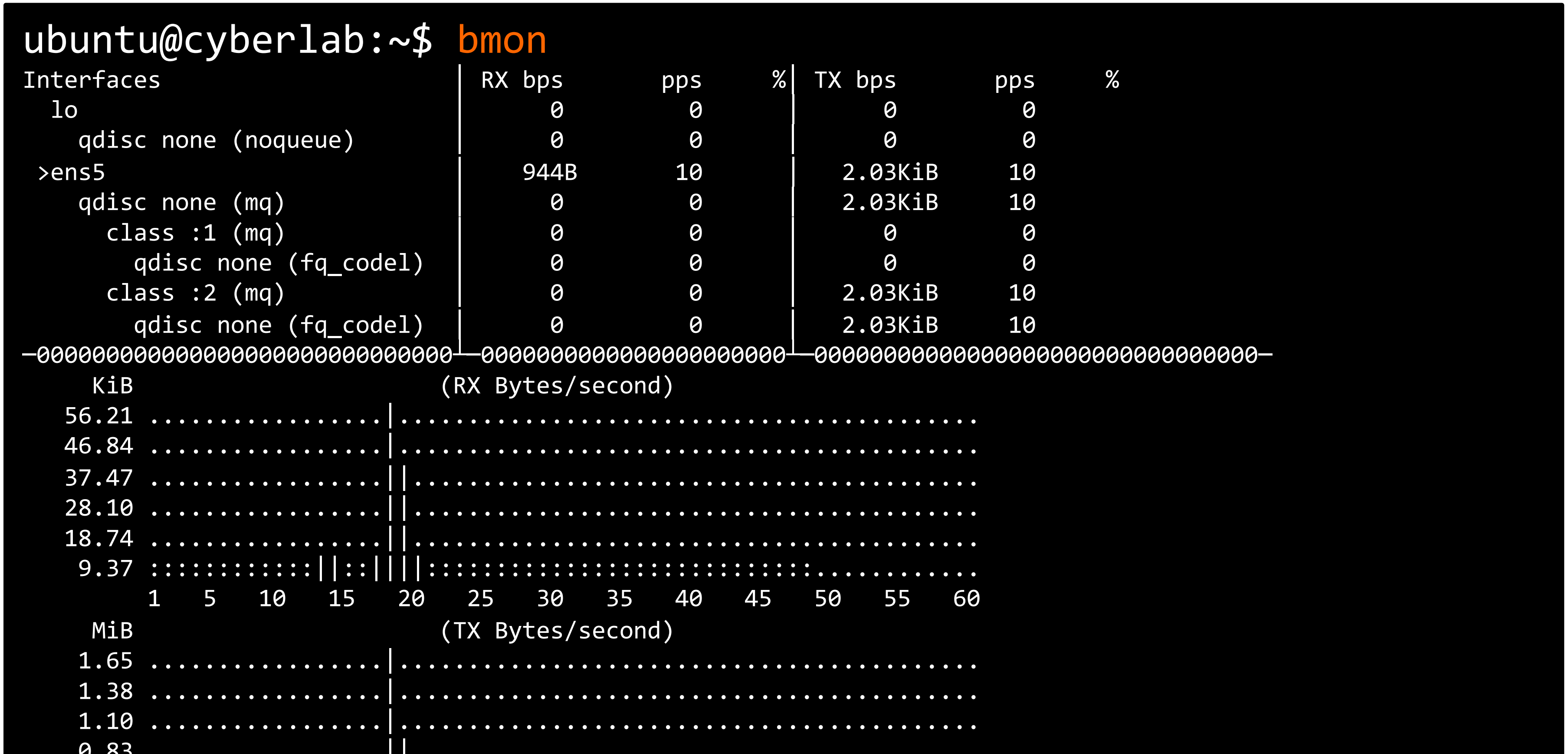
- What process is taking all the network bandwidth right now?



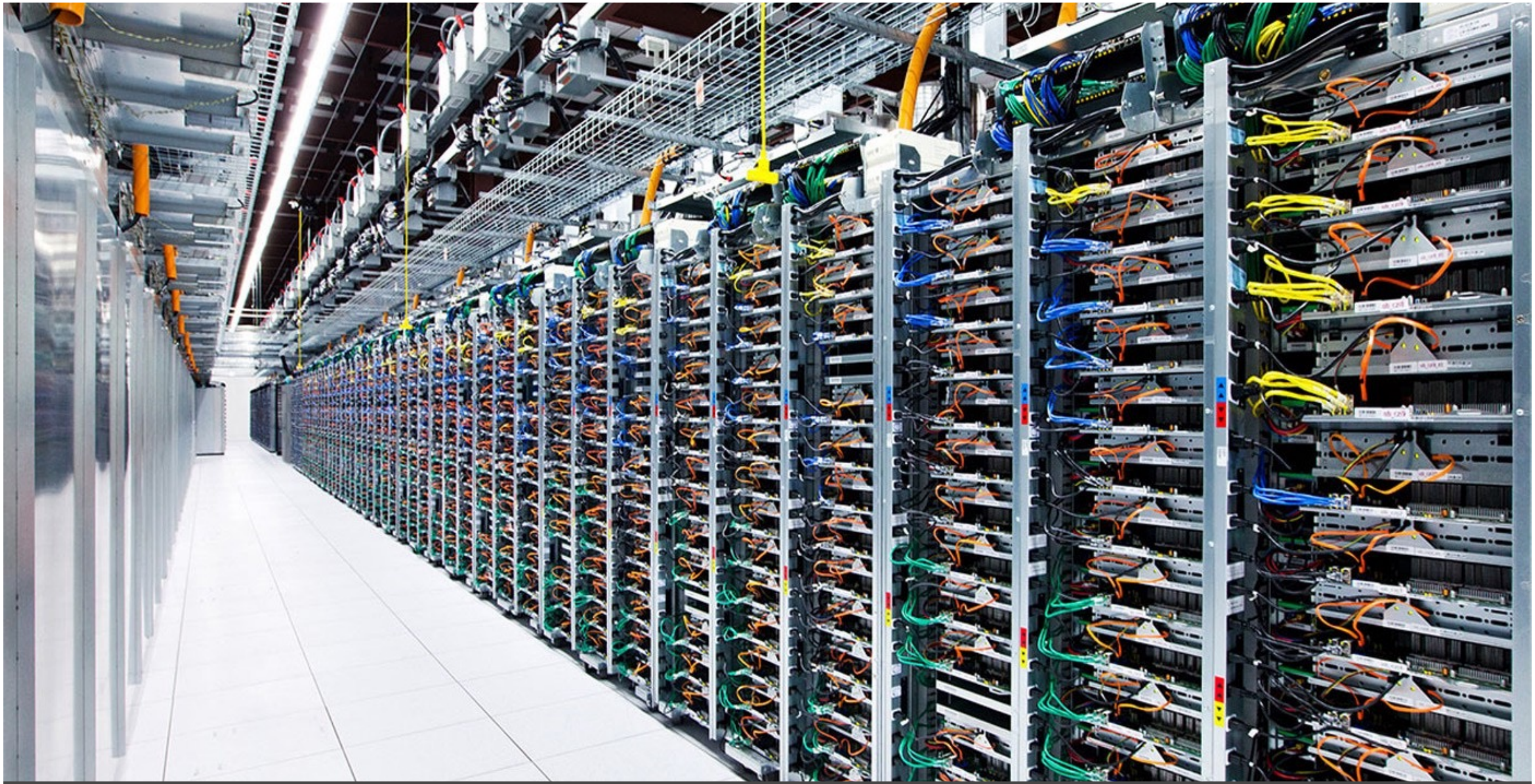
```
ubuntu@cyberlab:~$ sudo nethogs
NetHogs version 0.8.5-2

    PID USER     PROGRAM                              DEV        SENT      RECEIVED
  21609 www-da.. nginx: worker process                ens5        3.441       0.700 KB/sec
  22161 ubuntu   sshd: ubuntu@pts/0                   ens5        0.553       0.319 KB/sec
      ? root     ..00:1f14:536:b01:9cda:64e:15a9:da0              0.000       0.014 KB/sec
      ? root     ..2.31.52.244:80-91.241.19.84:42622              0.000       0.000 KB/sec
      ? root     ..00:1f14:536:b01:9cda:64e:15a9:da0              0.000       0.000 KB/sec
      ? root     ..00:1f14:536:b01:9cda:64e:15a9:da0              0.000       0.000 KB/sec
      ? root     ..00:1f14:536:b01:9cda:64e:15a9:da0              0.000       0.000 KB/sec
      ? root     ..00:1f14:536:b01:9cda:64e:15a9:da0              0.000       0.000 KB/sec
      ? root     ..00:1f14:536:b01:9cda:64e:15a9:da0              0.000       0.000 KB/sec
      ? root     unknown TCP                                      0.000       0.000 KB/sec

  TOTAL                                                           3.993       1.034 KB/sec
```

Network Utilization

- How busy is the network now?

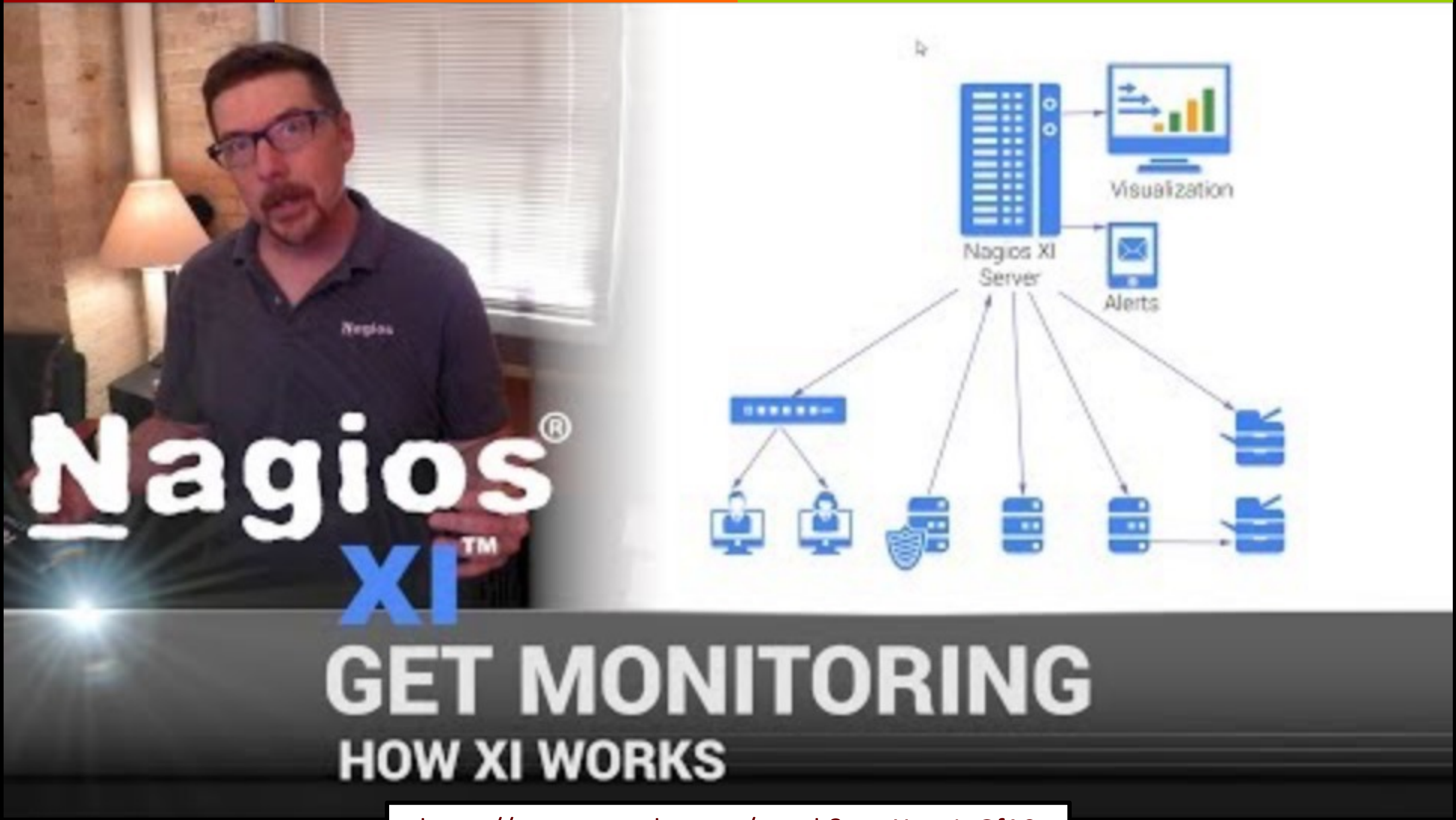


```
ubuntu@cyberlab:~$ bmon
Interfaces                     | RX bps       pps     %| TX bps       pps     %
  lo                           |      0         0      |      0         0
    qdisc none (noqueue)       |      0         0      |      0         0
 >ens5                         |    944B       10      |   2.03KiB     10
    qdisc none (mq)            |      0         0      |   2.03KiB     10
      class :1 (mq)            |      0         0      |      0         0
        qdisc none (fq_codel)  |      0         0      |      0         0
      class :2 (mq)            |      0         0      |   2.03KiB     10
        qdisc none (fq_codel)  |      0         0      |   2.03KiB     10
─000000000000000000000000000000└─0000000000000000000000└─00000000000000000000000000000000─
     KiB                      (RX Bytes/second)
   56.21 .................|..........................................
   46.84 .................|..........................................
   37.47 .................||.........................................
   28.10 .................||.........................................
   18.74 .................||.........................................
    9.37 ::::::::::::||::||||::::::::::::::::::::::::::::............
         1   5   10   15   20   25   30   35   40   45   50   55   60
     MiB                      (TX Bytes/second)
    1.65 .................|..........................................
    1.38 .................|..........................................
    1.10 .................|..........................................
    0.83                  ||
```



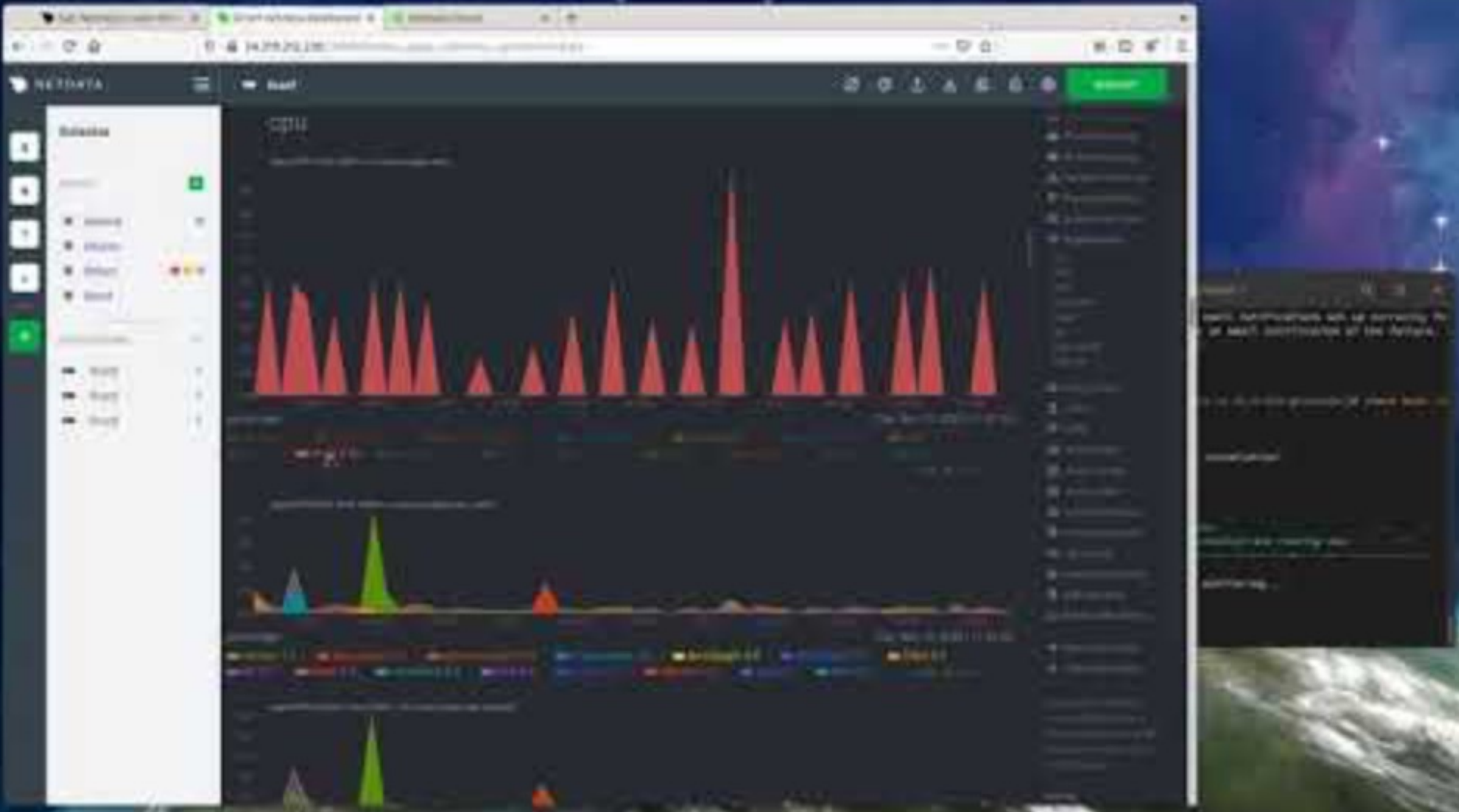
Monitoring *Many* Servers

Nagios (Introduction)



https://www.youtube.com/watch?v=wXpcpLrGfA0

Netdata



https://www.youtube.com/watch?v=CShH3nAOGkU

Vulnerability Scanners

Vulnerability Scanners

Commercial

- **Nessus**
- Industry standard / must-have if you can bill this expense to your company or client
- Nessus Professional
  - Annual subscription - **$3390**
- Nessus Essentials
  - Free home/education version (limited to 16 IPs)

https://www.tenable.com/products/nessus

Free

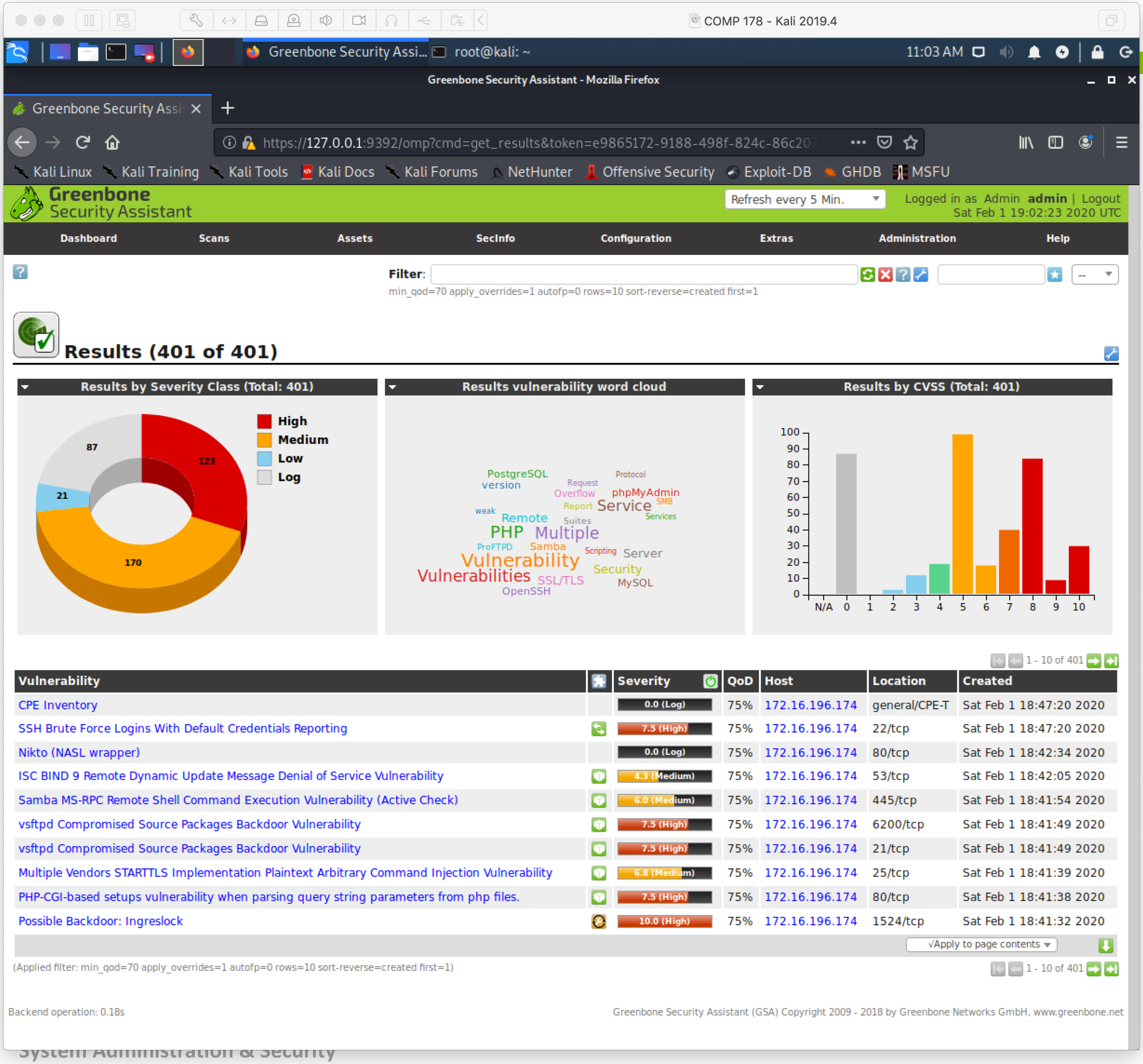
- **OpenVAS**
  - Open **V**ulnerability **A**ssessment **S**canner
- Open source fork of Nessus from 2005 *before* it went commercial
- Regular updates to Network Vulnerability Tests (NVTs)
  - 86000+ as-of Jan 2021

https://openvas.org/

Vulnerability Scanners

- Many other vulnerability scanners
  - **Rapid7 Nexpose** ($)
    - https://www.rapid7.com/products/nexpose/
  - **Core Impact** ($)
    - https://www.coresecurity.com/core-impact
  - **Tripwire IP360** ($)
    - https://www.tripwire.com/products/tripwire-ip360/
  - **…**
- Design question: Do you want your scanner "on premise" or "in the cloud"
  - Vendors happy to take your $$ either way!

OpenVAS



COMP 178 - Kali 2019.4

Greenbone Security Assi... root@kali: ~ 11:03 AM

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi ×

https://127.0.0.1:9392/omp?cmd=get_results&token=e9865172-9188-498f-824c-86c20

Kali Linux · Kali Training · Kali Tools · Kali Docs · Kali Forums · NetHunter · Offensive Security · Exploit-DB · GHDB · MSFU

Greenbone Security Assistant

Refresh every 5 Min. · Logged in as Admin **admin** | Logout · Sat Feb 1 19:02:23 2020 UTC

Dashboard · Scans · Assets · SecInfo · Configuration · Extras · Administration · Help

Filter:

min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1

Results (401 of 401)

1 - 10 of 401

Vulnerability		Severity	QoD	Host	Location	Created
CPE Inventory		0.0 (Log)	75%	172.16.196.174	general/CPE-T	Sat Feb 1 18:47:20 2020
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	75%	172.16.196.174	22/tcp	Sat Feb 1 18:47:20 2020
Nikto (NASL wrapper)		0.0 (Log)	75%	172.16.196.174	80/tcp	Sat Feb 1 18:42:34 2020
ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability		4.3 (Medium)	75%	172.16.196.174	53/tcp	Sat Feb 1 18:42:05 2020
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)		6.0 (Medium)	75%	172.16.196.174	445/tcp	Sat Feb 1 18:41:54 2020
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	75%	172.16.196.174	6200/tcp	Sat Feb 1 18:41:49 2020
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	75%	172.16.196.174	21/tcp	Sat Feb 1 18:41:49 2020
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	75%	172.16.196.174	25/tcp	Sat Feb 1 18:41:39 2020
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	75%	172.16.196.174	80/tcp	Sat Feb 1 18:41:38 2020
Possible Backdoor: Ingreslock		10.0 (High)	75%	172.16.196.174	1524/tcp	Sat Feb 1 18:41:32 2020

√Apply to page contents

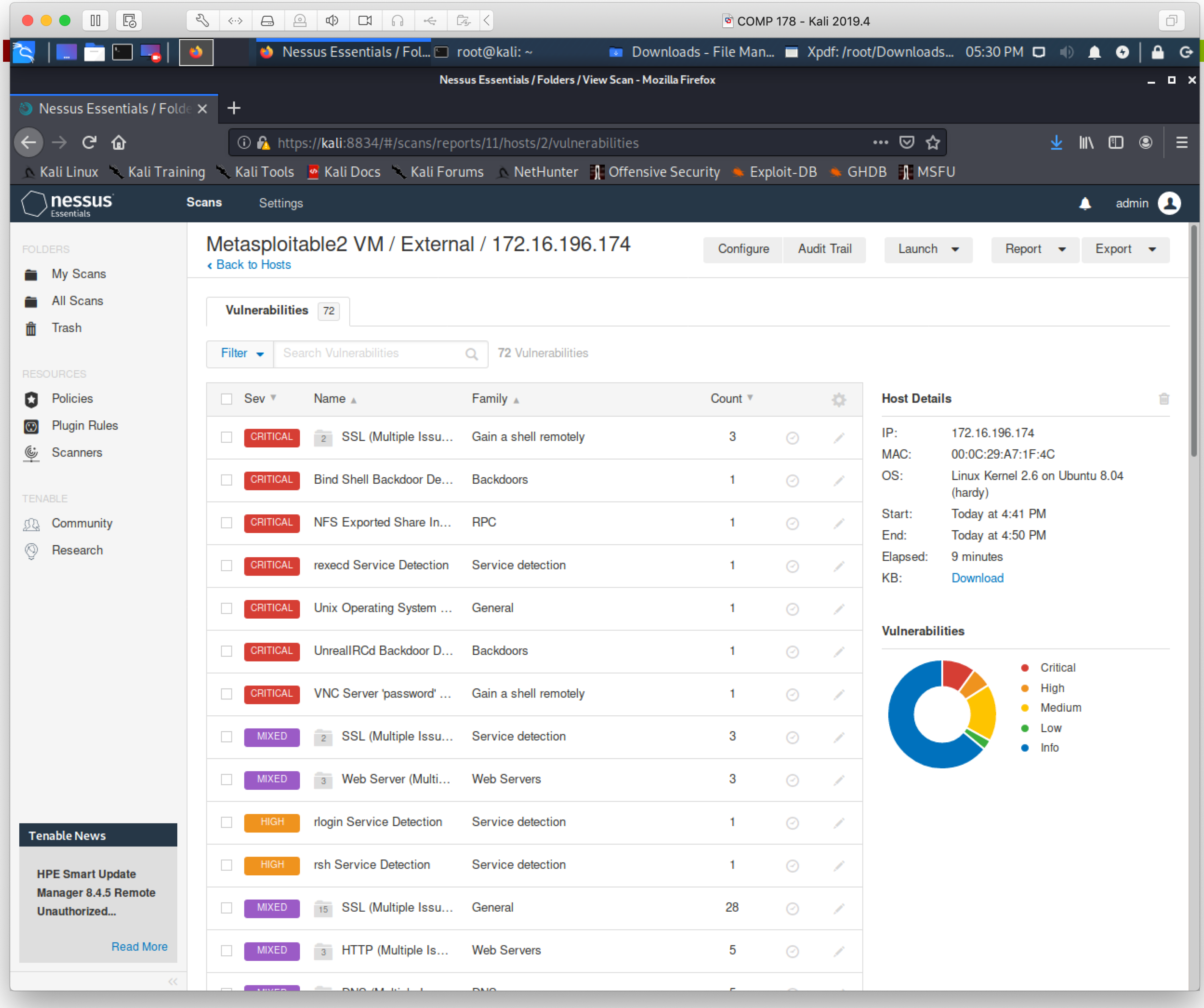
(Applied filter: min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1)

1 - 10 of 401

Backend operation: 0.18s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Nessus



COMP 178 - Kali 2019.4

Nessus Essentials / Folders / View Scan - Mozilla Firefox

https://kali:8834/#/scans/reports/11/hosts/2/vulnerabilities

Metasploitable2 VM / External / 172.16.196.174

Vulnerabilities 72

72 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	2 SSL (Multiple Issu…	Gain a shell remotely	3
CRITICAL	Bind Shell Backdoor De…	Backdoors	1
CRITICAL	NFS Exported Share In…	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System …	General	1
CRITICAL	UnrealIRCd Backdoor D…	Backdoors	1
CRITICAL	VNC Server 'password' …	Gain a shell remotely	1
MIXED	2 SSL (Multiple Issu…	Service detection	3
MIXED	3 Web Server (Multi…	Web Servers	3
HIGH	rlogin Service Detection	Service detection	1
HIGH	rsh Service Detection	Service detection	1
MIXED	15 SSL (Multiple Issu…	General	28
MIXED	3 HTTP (Multiple Is…	Web Servers	5

Host Details

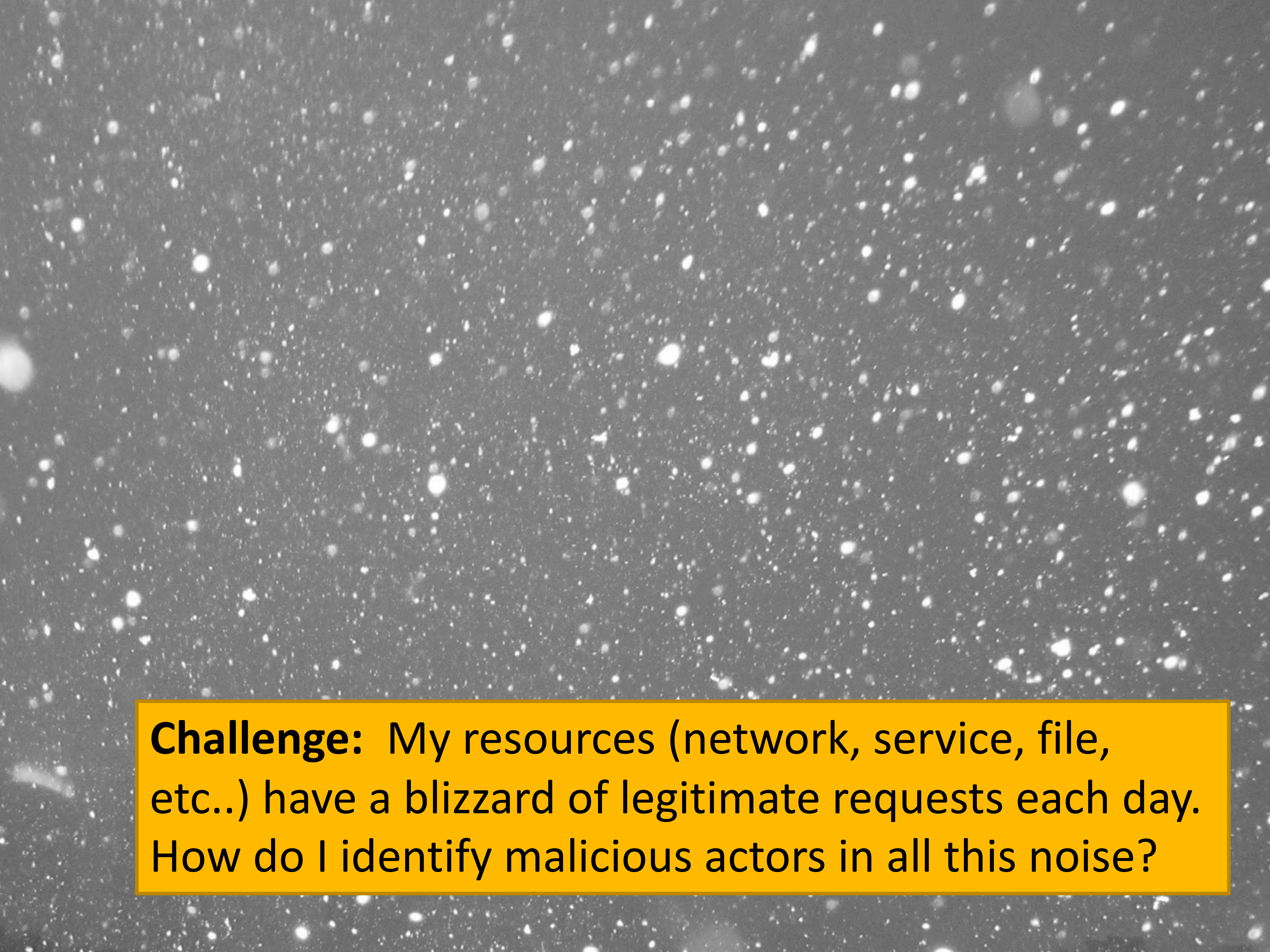
IP:	172.16.196.174
MAC:	00:0C:29:A7:1F:4C
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 4:41 PM
End:	Today at 4:50 PM
Elapsed:	9 minutes
KB:	Download

Vulnerabilities

Tenable News

HPE Smart Update Manager 8.4.5 Remote Unauthorized...

Read More



Challenge: My resources (network, service, file, etc..) have a blizzard of legitimate requests each day. How do I identify malicious actors in all this noise?

Honeypots

- A resource that has *no value to legitimate users* but is attractive to attackers
  - Greatly simplifies alerting, as activity on resource is almost always malicious
- **Alert** – Provide early warning of attack (rather than FBI notification 6+ months later)
- **Lure –** Make the attackers waste lots of time here
- **Monitor** – What are the attackers trying to do?
  - Commands entered?
  - Malware uploaded?

Honeypot Use Cases

- **Production systems**
  - *Goal: Protect our current systems*
  - Alert to ongoing attacks that are missed by pattern-based IDS
  - Deterrence (potentially?) if attackers realize they are being monitored
  - Useful for all businesses

Honeypot Use Cases

- **Research**
  - *Goal: Study attackers*
  - Learn about attacker skill level, tools, motives, origin, …
  - Useful for academics, governments, security researchers, …

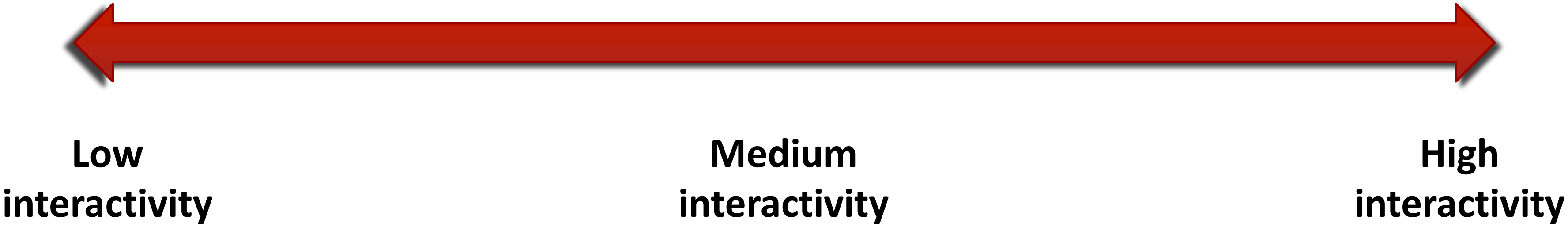
TrendMicro "Factory Honeypot"

https://www.youtube.com/watch?v=0bnjKwmmjzs

Honeypot Interactivity

What kind of interaction can the attacker have with the honeypot?

(in comparison to a *real* vulnerable system)



Low interactivity

Medium interactivity

High interactivity

Low Interaction Honeypot

- Minimal functionality
  - Example: Listen on all TCP ports, accept all connections, and receive data for up to 20 seconds. Send minimal or no replies.
- Pros: Minimal danger to other systems, simple implementation
- Cons: Minimal information learned
  - Source IP, source port, payload sent (if any)

Medium Interaction Honeypot

- System emulates vulnerabilities only
  - Partial simulation of a real system
  - Attacker can’t do much after exploiting vulnerability
- Pros: Reduced danger to other systems
- Cons: Some information learned
  - Attacker is present (source IP)
  - Attacker used specific vulnerability to gain entry
  - What would attacker have done once inside?

High Interaction Honeypot

- Attacker can interact with system at all levels
  - Probe, attack, and compromise
  - Pivot through system for additional attacks
- Equivalent to a real system with hidden monitoring infrastructure
  - Key logging, network logging, file logging, …
  - Data control – Limit where the attacker can go *after* entering honeypot

- Pros: High level of information learned
  - Where are the attackers coming from?
  - What is their skill level?
  - What tools are they using?
- Cons: Risk in letting attacker own our system?
  - Attack the rest of our network?
  - Attack systems outside our organization?
  - Store/distribute illegal content?

Honeypots

- Wide range of possible implementations
  - Dedicated machine
  - Virtual machine
  - Special service on a host
  - Special file on a host
- Never meant for legitimate use
  - Any access is either accidental *or* malicious

Quick and Dirty?

- Q: Why don’t I just install some old unpatched OS and service software in my datacenter? It’ll be attractive to attackers, right?
- A: Method would be possible if the *only* system on your network was the honeypot. But risky in a full datacenter. What if the attackers springboard from the honeypot system to attack legitimate services next?

Wrap-Up

- Questions?
- Concerns?

- **Last Lab**
  - **Lab 14** – Ansible