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?


CompTIA+
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

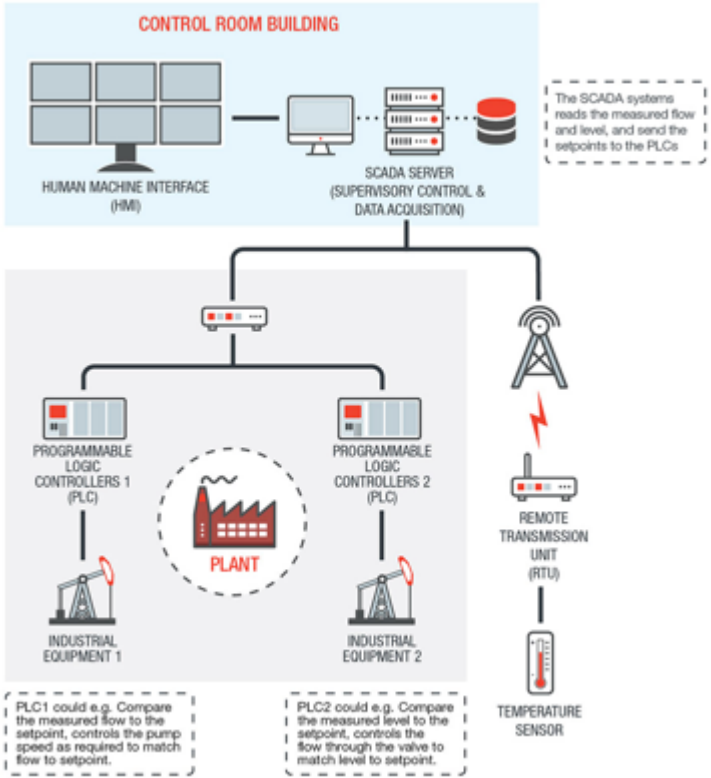
Most open source security tools are built natively in Linux

Platforms you'll be asked to secure

- Content management systems
  - Wordpress
  - SharePoint (has other uses)
- Web servers
- Databases
- Network infrastructure
  - Firewalls, routers and VPN servers
  - Edge devices (e.g., micro datacenters)
  - Mobile
  - DNS especially
- End points – from PCs to IoT devices: *Malicious processes*

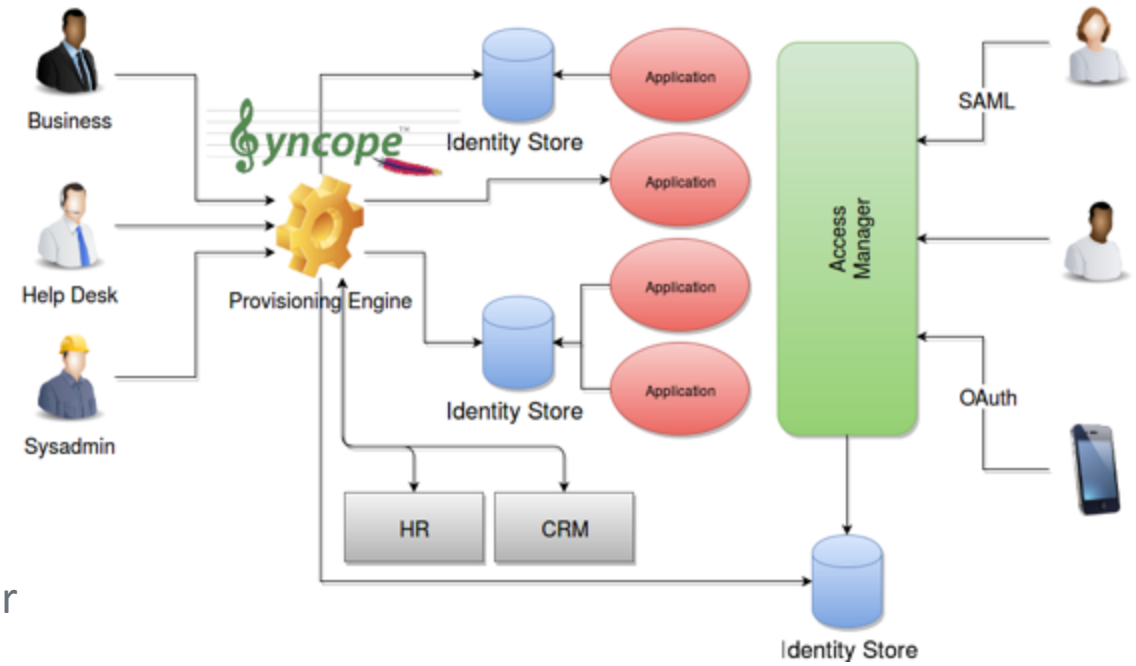
Platforms (cont'd)

- 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

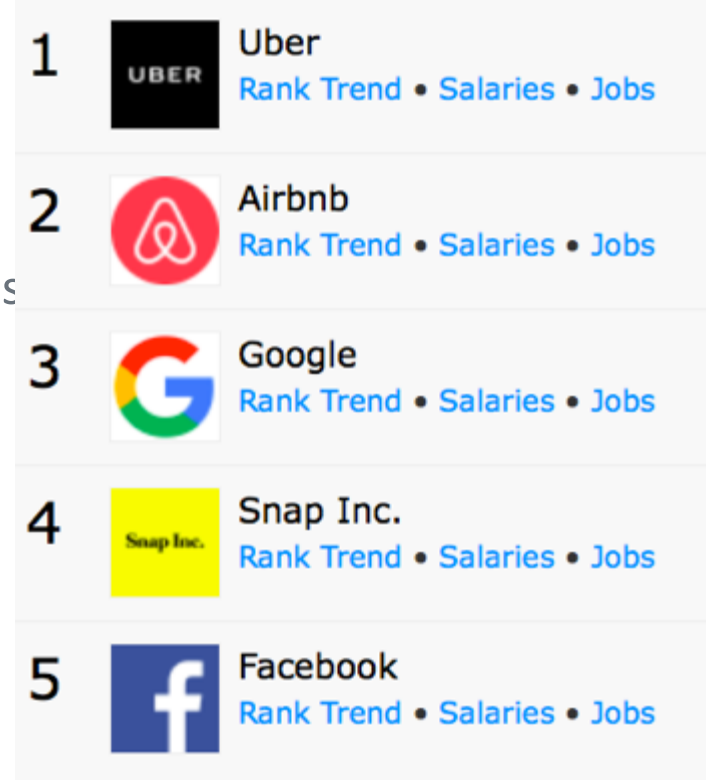


"Who has access to What, When, How, and Why?"

Linux and open source remains hot

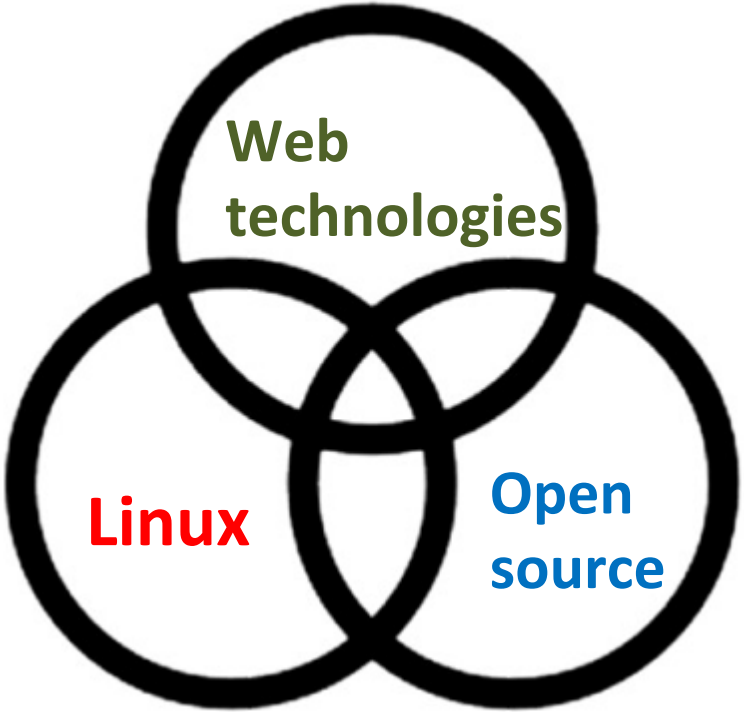
- Paysa – career advisor site
  - Surveyed top Silicon Valley companies
  - All listed Linux skills prominently
- Linux: A terrific gateway into infrastructure jobs
  - Cloud / IoT / edge
  - Security
  - Web
- Very much ”behind the scenes”
- But that’s exactly where we are as IT Pros

“The preferred operating system for engineers and programmers.”



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

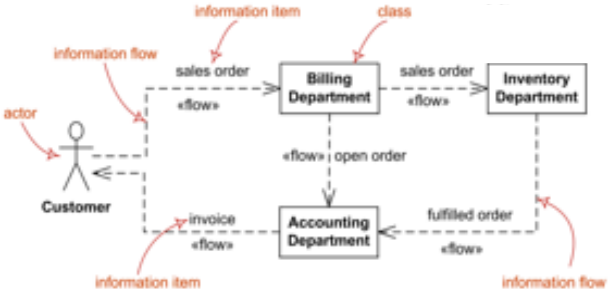
Poll question

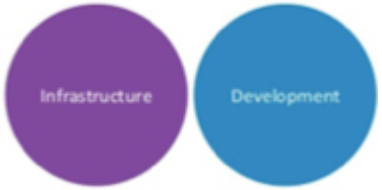
- You suspect that your company has been hit by a particular form of ransomware. Which of the following is an indicator of compromise (IoC) relevant to that ransomware?

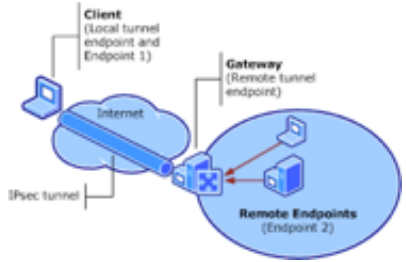
  A. A change in the size of a shared library (e.g., a DLL) on a network host.
  B. The announcement of a new form of ransomware released into the wild, based on a previous attack.
  C. The installation of an update on a Linux system.
  D. The announcement that phishing attacks have increased in the corporation.

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

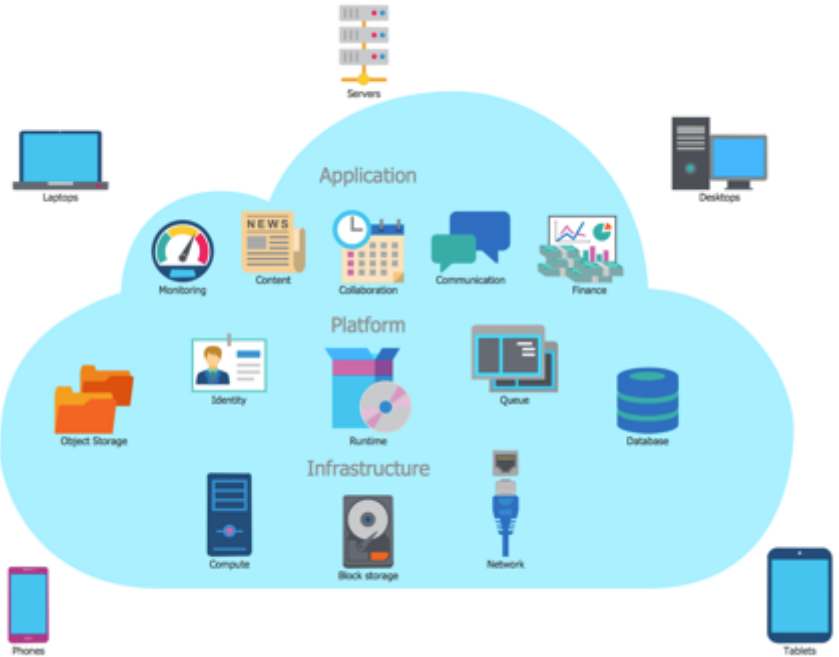






Searching for gaps - *interstices*

- 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

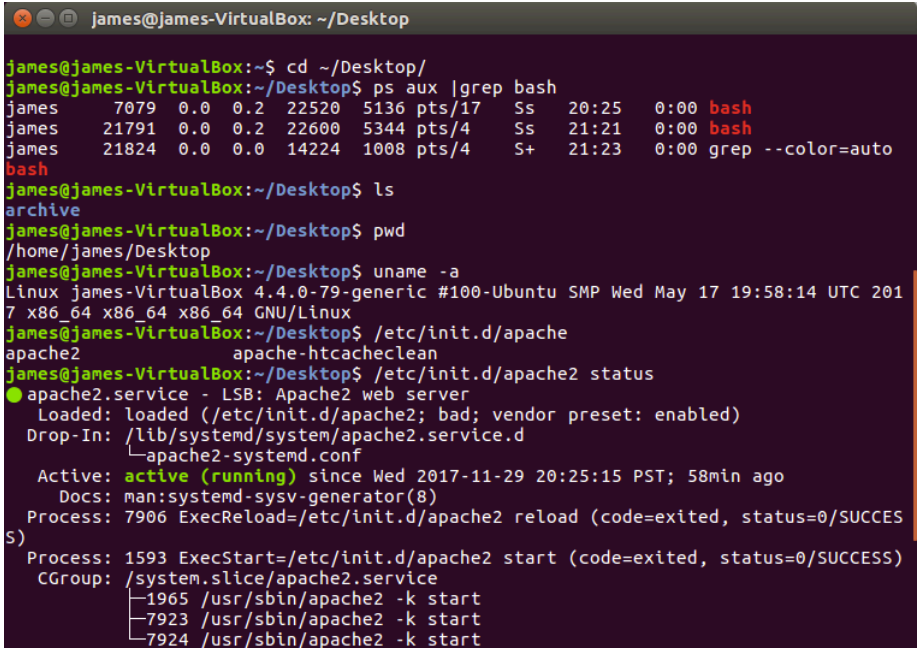
- Conveyor belt controller systems – compromised by ransomware
  - Discovered by threat hunter by noting
    - NTP and Internet-based traffic (instead of GPS)
    - Bandwidth issues
  - Solution? Keep workers from surfing the Web on the PC controlling the ICS system
  - Downtime costs: £4,000 an hour
- 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*


CompTIA.
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



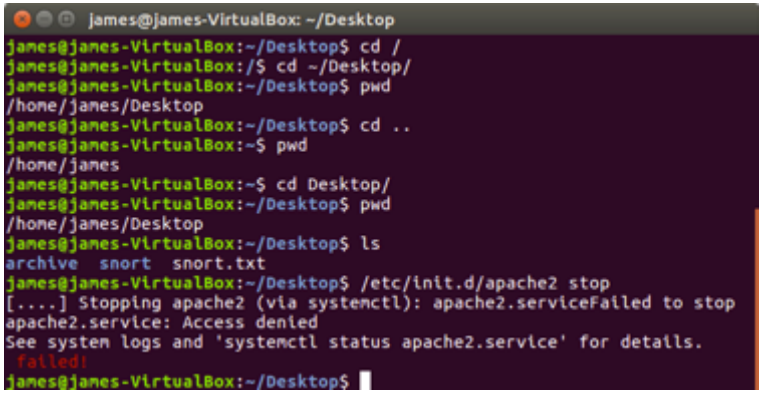
Poll question

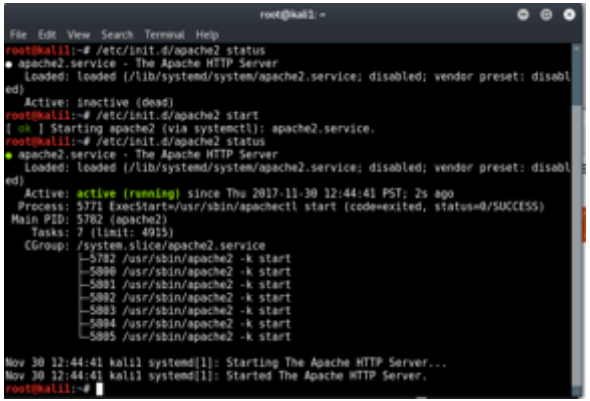
- How well do you know the command line?
  A. I've heard of the ls command before
  B. Pretty well – I know how to list hidden files and use grep
  C. Give me root on the command line, and I'll take over the world
  D. Why use the command line? Doesn't Linux have a GUI interface, for heaven's sake?

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





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**

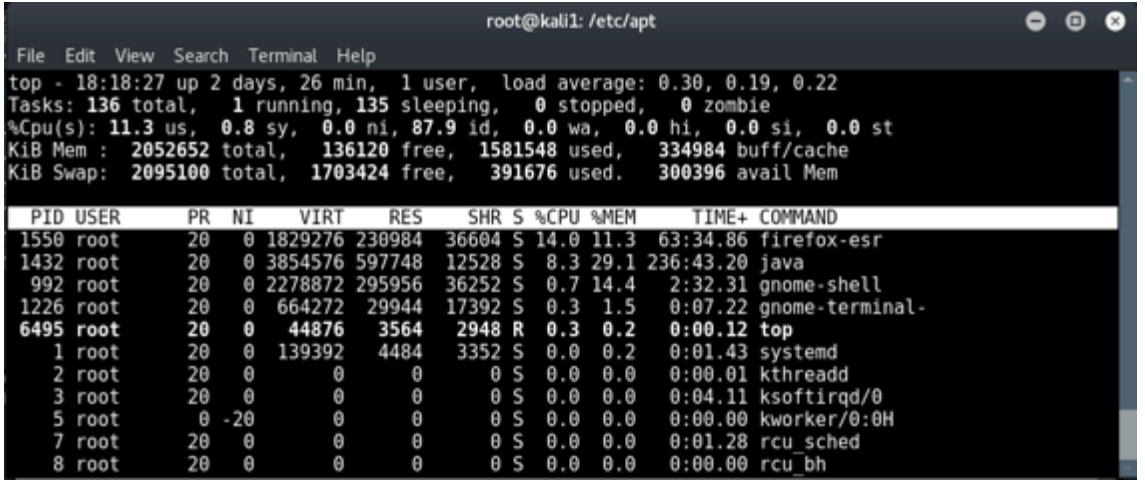
*Don't forget command line history and the **ctrl + r** keystroke combination*

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**



- Quick overview of processes running: **ps** **$ ps aux**

  $ ps aux | grep wireshark

  $ ps aux | less

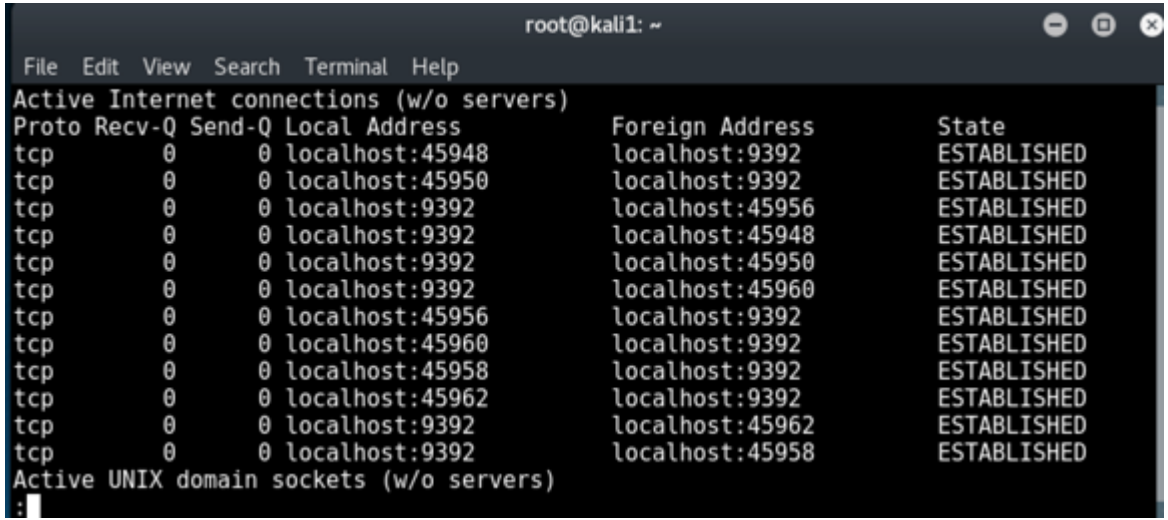
Network commands

- Network configuration information

$ ifconfig -a

$ netstat |less

$ netstat |grep *textstring*



- dig:

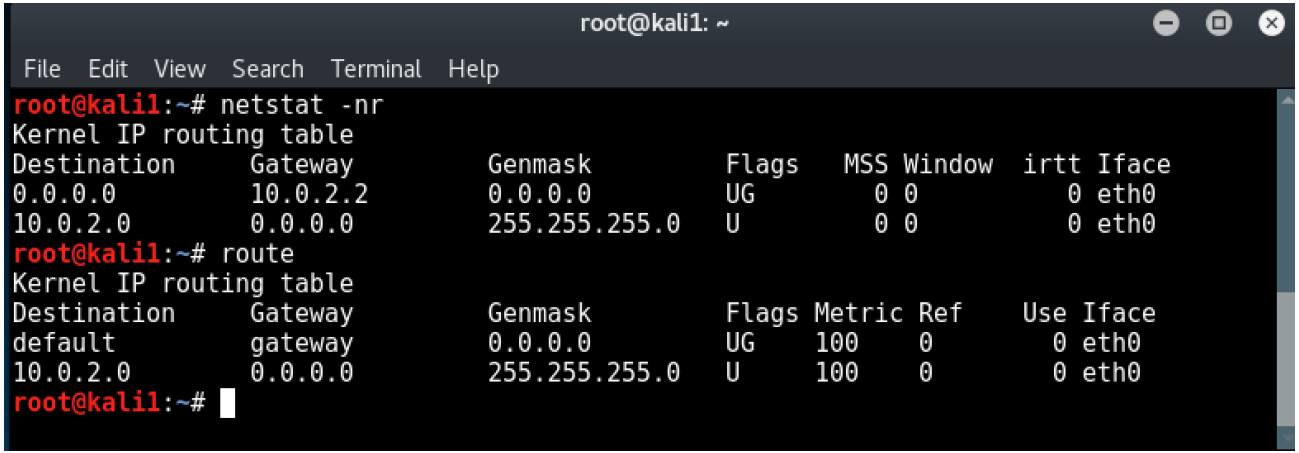
$ dig mt-example.com A +noall +answer
$ dig mt-example.com MX +noall +answer
$ dig @ns1.mediatemple.net mt-example.com

More network commands

- Network configuration information

$ netstat -nr

$ route



$ route add default gw 192.168.54.1

$ route -Cn

$ route add -host 192.168.54.2 reject

$ route add -net 192.168.54.0 netmask 255.255.255.0 reject


CompTIA.
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

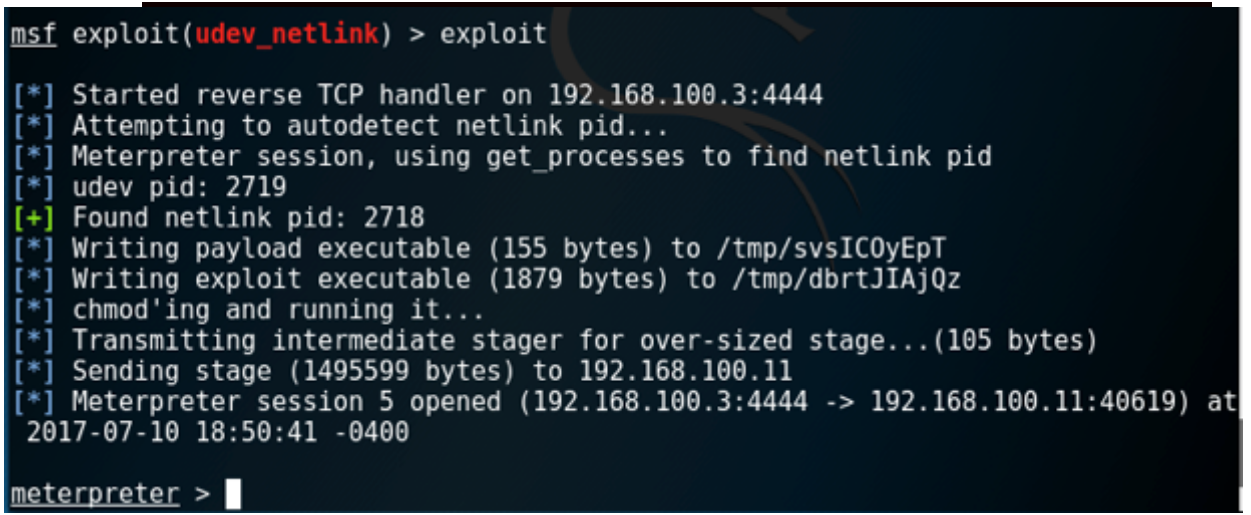
Penetration testing and Linux

- 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*

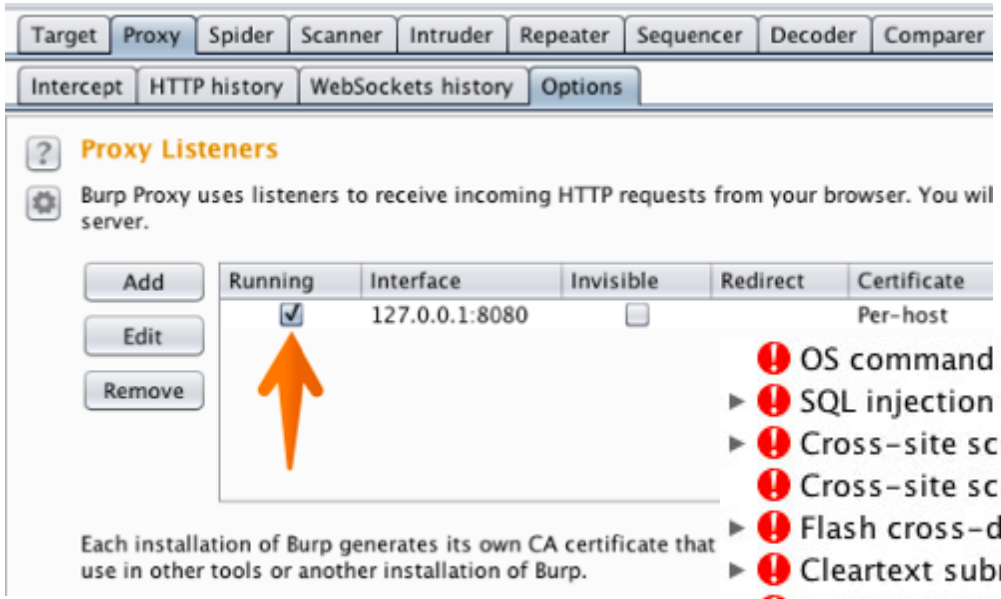
Metasploit

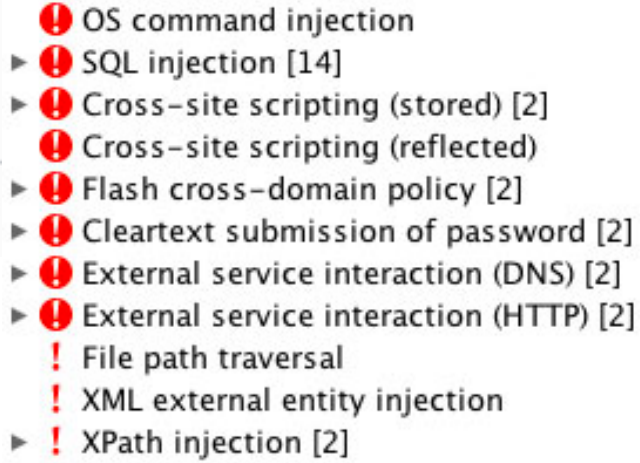
- Can be used to discover systems
- Mostly used, however, to conduct pen testing
- Contains relatively current tools for session hijacking, as well as system exploits



Burp suite

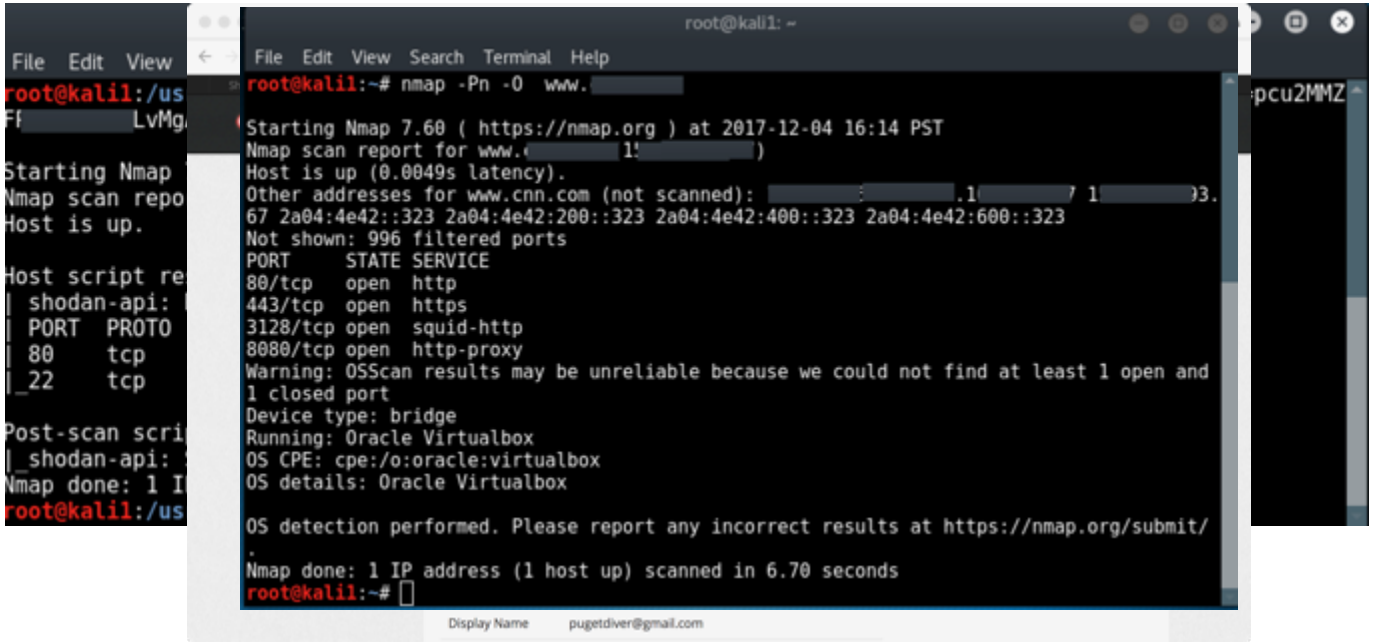
- Also used for testing systems
- Discovers issues
- Session capturing
- Code and command injection
- Screen capturing





Discovering and enumerating hosts

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



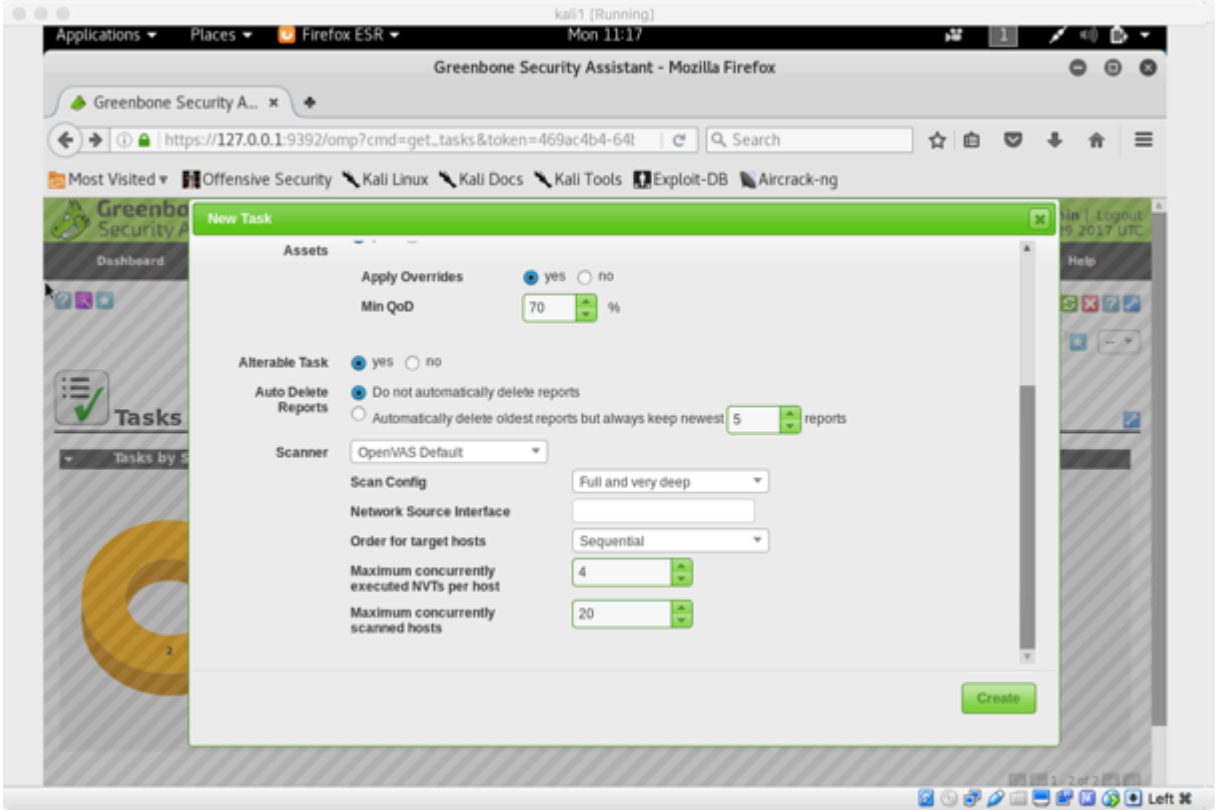
$ sudo nmap --script shodan-api a.b.c.0/24 -sn -Pn -n --script-args 'shodan-api.outfile=potato.csv,shodan-api.apikey=SHODANAPIKEY' nmap --script shodan-api --script-args 'shodan-api.target=x.y.z.a,shodan-api.apikey=SHODANAPIKEY'

Vulnerability assessment

- Set up OpenVAS
  $ sudo apt-get install openvas
  $ sudo open-vas setup
  $ netstat |grep 9392

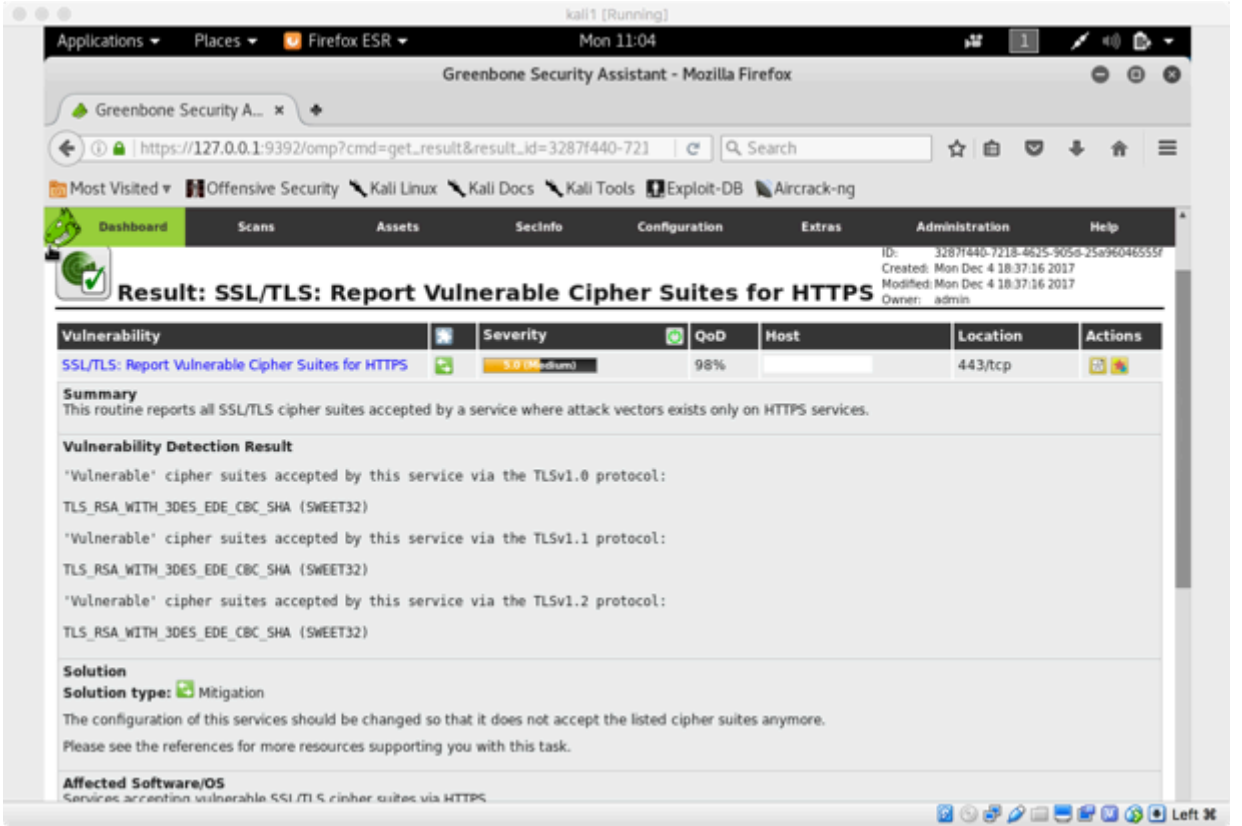
  as root: openvas-check-setup

- 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



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


CompTIA+
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:

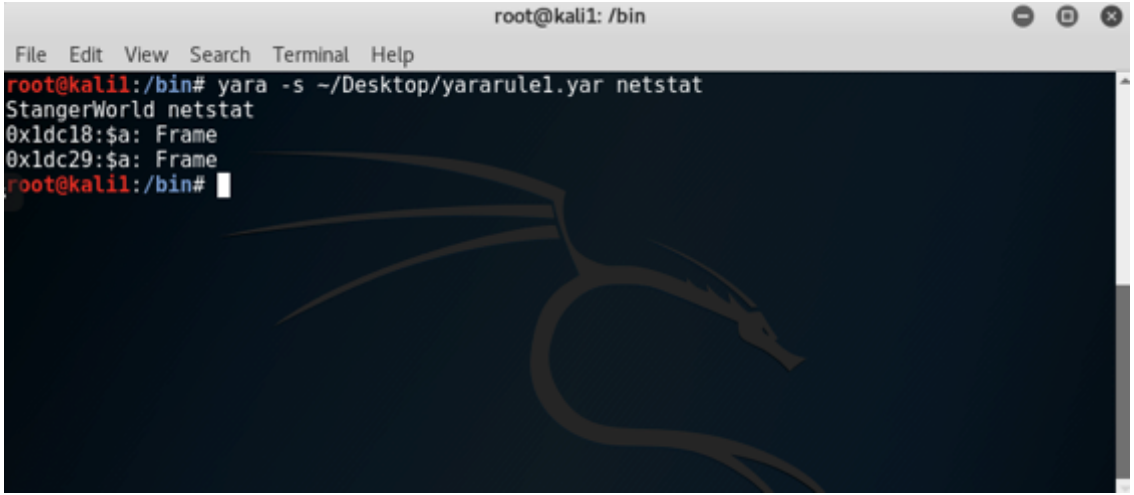
```
01 rule NameOfRule
02 {
03          strings: $test_string1= "James"
04         $test_string2= {8C 9C B5 L0}
05        conditions: $test_string1 or  $test_string2
06   }
```

To read the above contents with yar, 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



Visualization tools

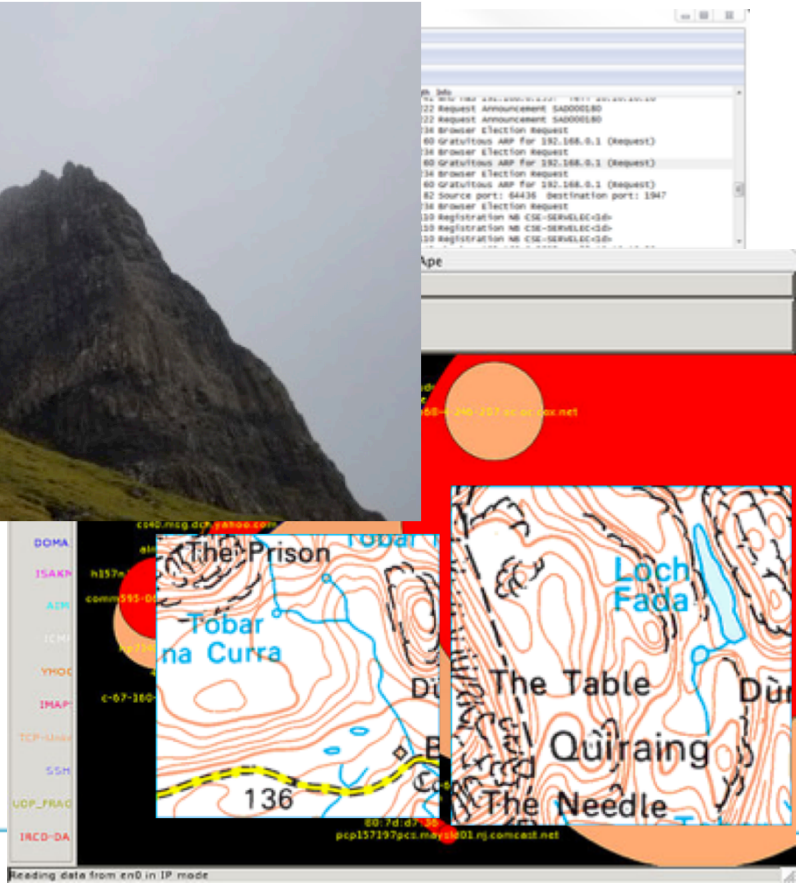
Poll question

- 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.

Security, risk management, and visuals

- Why are visuals so important?
- Because humans like to look at things – pictures
- Brief synopsis
- Allows for:
  - Quick understanding
  - Understand interconnections
  - Ability to pivot / make decisions
  - Actionable information



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"

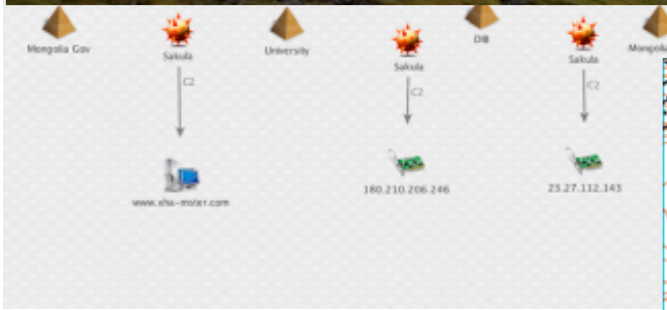
- What is normal?
- Why is traffic coming from point x to point y?

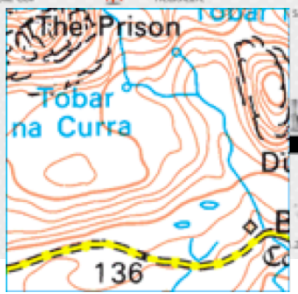
Who is talking to where, and why?

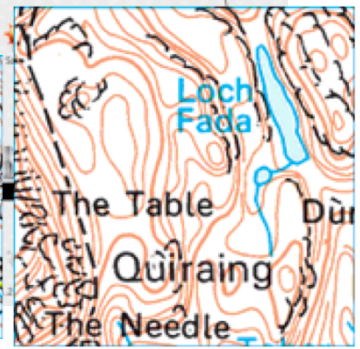
- Find context
- Suggest remediation
- Follow up

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

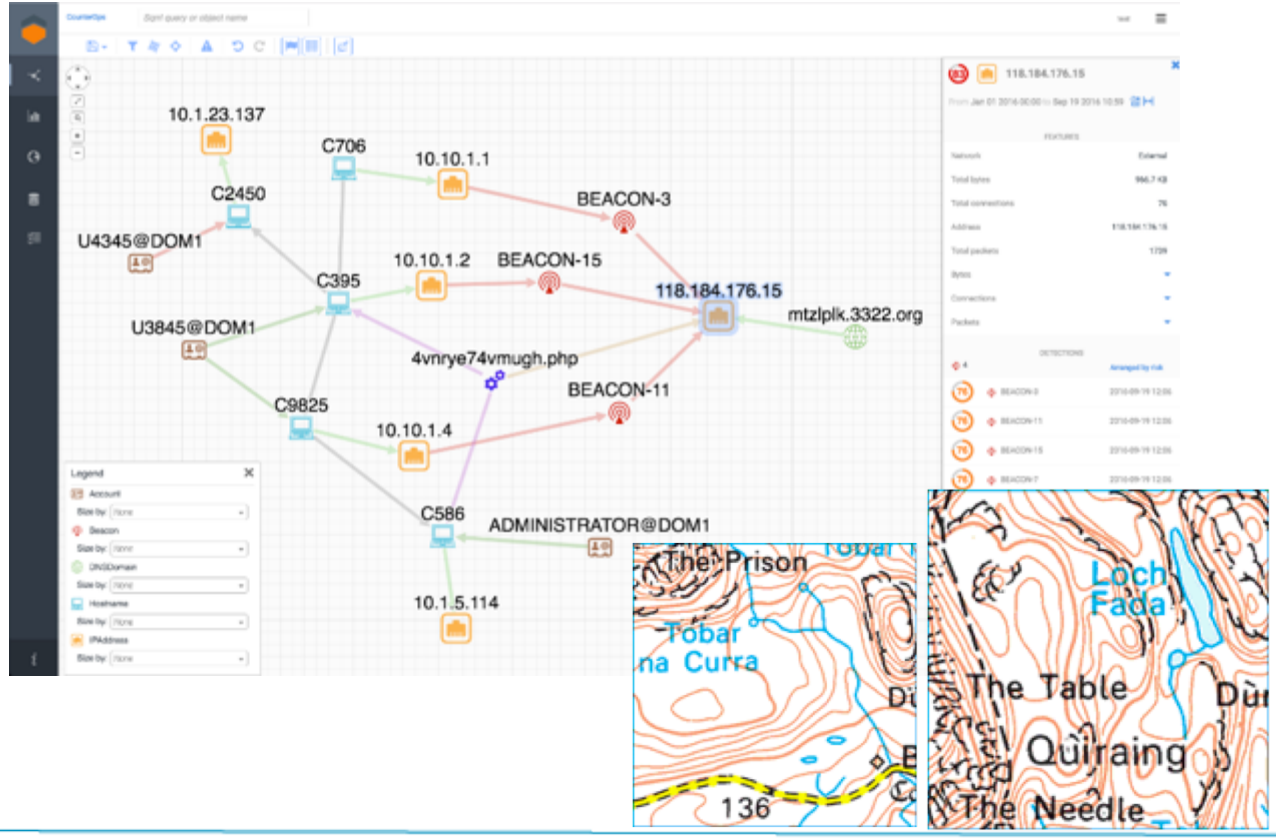






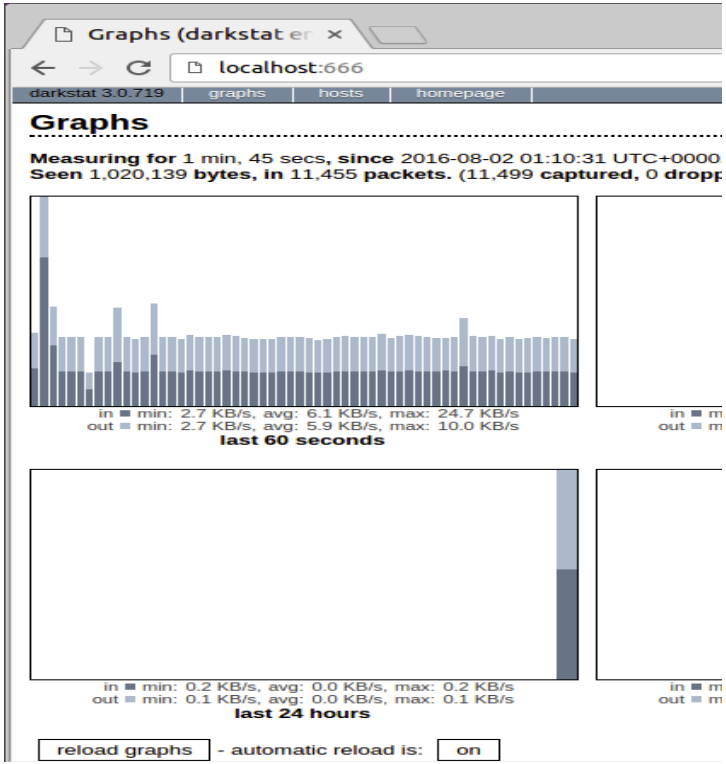
Additional visualization solutions

- Maltego
- Sqrrl
- Cacti



Additional network visualization tools

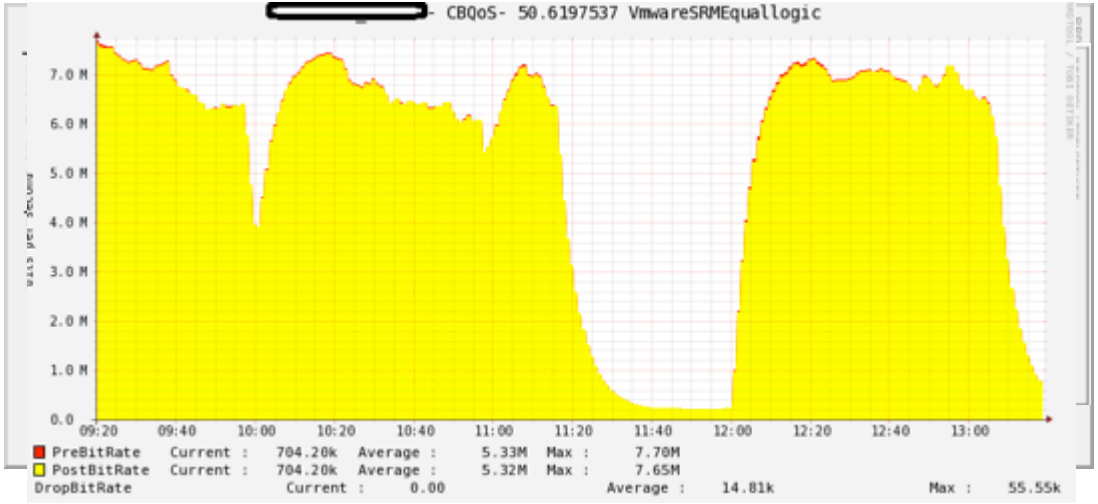
- vnstat
  - Persistent stats, even after system reboots
  - Uses kernel-based logging
- iptstate
  - Monitors traffic across iptables
  - Helps look for congestion
- Darkstat
  - Linux/FreeBSD/Mac OS
  - Captures traffic
  - Calculates stats
  - Has own Web server – Default port: 666

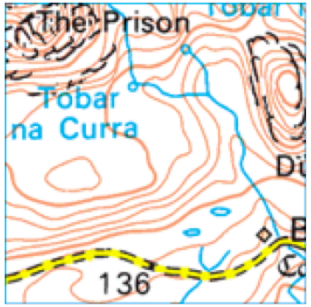


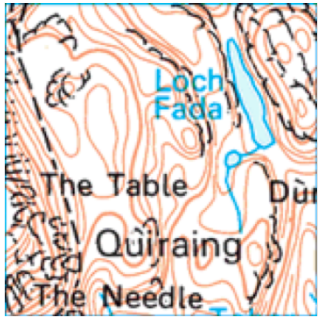
Network visualization with Cacti

- Network graphing solution
- URL:

  www.cacti.net





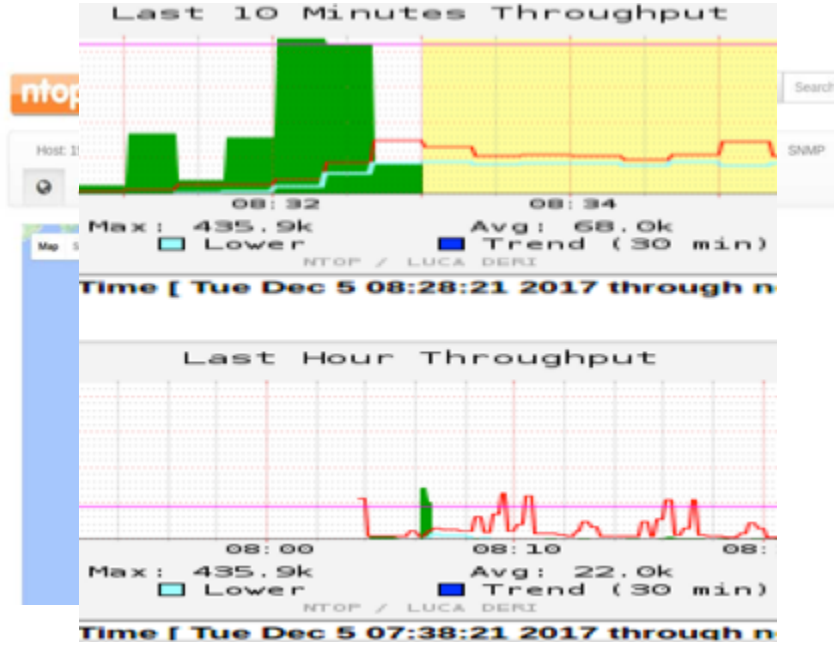


Network visualization with ntop

- Install (Ubuntu)
  - Few, if any, dependencies
  - URL: www.ntop.org
- 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

Can also use Kali Linux

Default user: admin
password – you set it



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

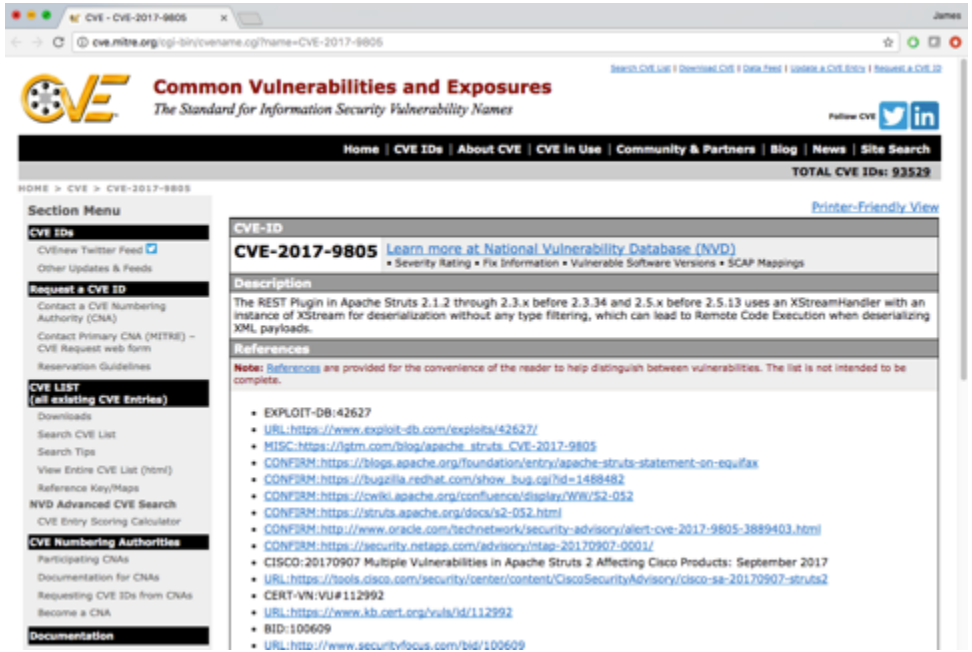
- Police force for one of the states in the United States
- Needed a collaboration site to manage extremely sensitive data
- Criteria
  - Must enable "double blind" communication
  - Highest encryption allowed
    - At rest
    - In transit
  - Low cost
- Developing their own solution


CompTIA.
Tracking open source security issues

Tracking open source issues

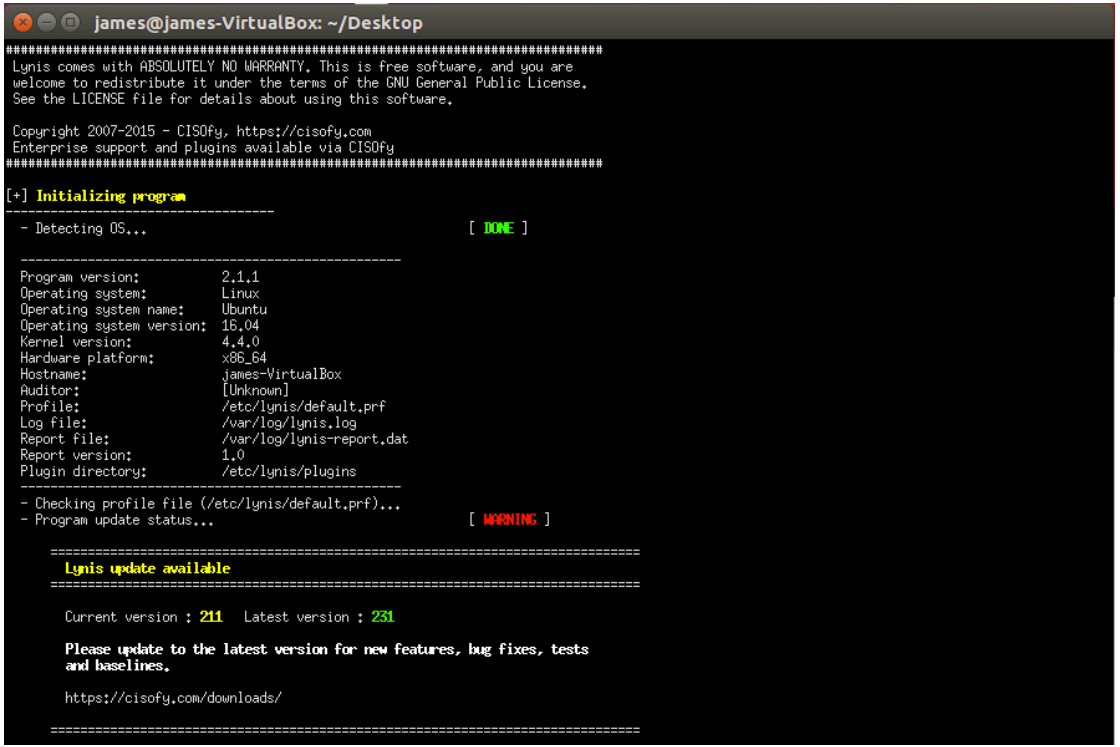
- No such thing as perfect software
  - Apache Struts - CVE-2017-5638 (Equifax) and CVE-2017-9805
  - Heartbleed (2012 – 2014)
  - Shellshock (2014)
  - IoT issues galore!
- We're going to see more successful attacks
- Where to learn more? http://cve.mitre.org
- What to do?

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



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

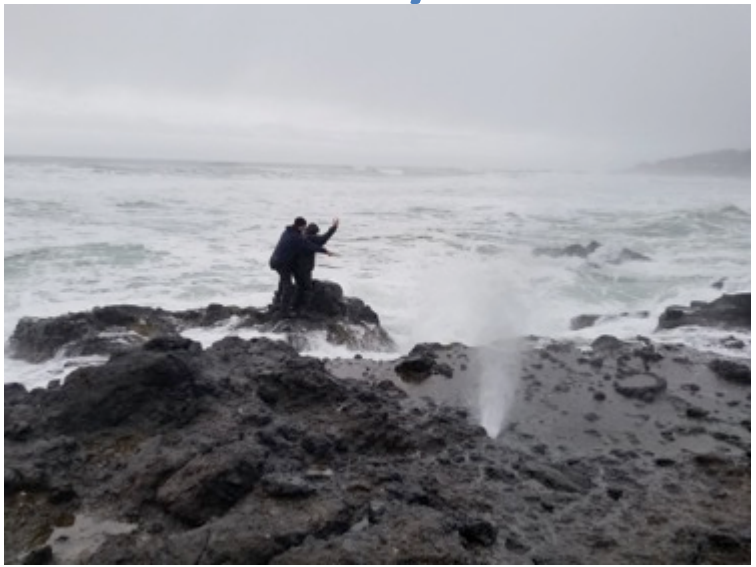
- It's office hour time!
- Join me to learn more about:
  - Linux and command line basics
  - Using Nmap in Linux

Wednesday January 10th, 2018
9:00 AM Pacific, US Time
Interested?
Send your requests to:
jstanger@comptia.org

I'll be in touch with registration details!

Office hours with James

Thank you!



James Stanger, PhD
jstanger@comptia.org
+1 (360) 970-5357
Twitter: @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/y9paj5ay

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