Scrapping for Pennies

Implementing CIS Top 20 with no budget

Ryan Wisniewski
Principle Security Consultant
Active Defense, LLC

March 1, 2019

HOUSEKEEPING

- Feel free to take notes, pictures, recordings, etc.
- **ALL SLIDES WILL BE RELEASED AT THE END OF THIS TALK!**
- If you like this presentation…

Upcoming Courses Taught By Ryan Wisniewski

Type	Course / Location	Date	Register
Mentor	MGT414: SANS Training Program for CISSP® Certification Mentor Session Chicago, IL	Apr 30, 2019 - Jun 11, 2019	Register

SECURITY IMPLEMENTATION TALKS: AN ACTIVE DEFENSE SERIES

Starting from Scratch
0Day to HeroDay

Starting from Basic IT Implementations
Scrapping for Pennies

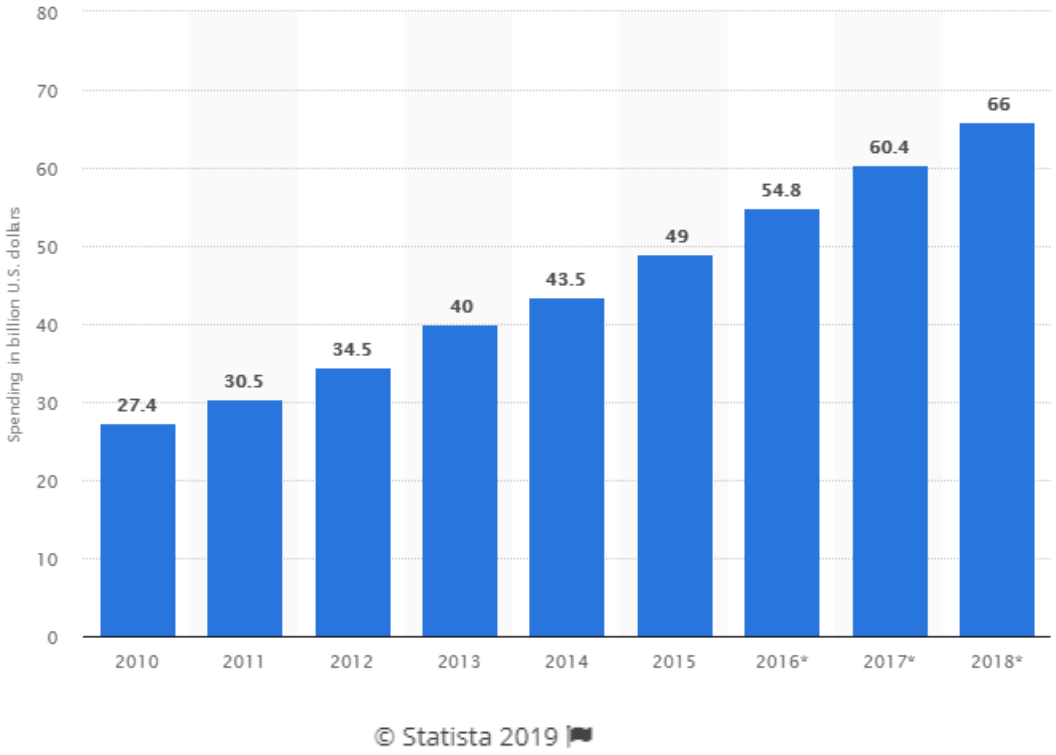
Maturing to a Scalable Operation
Scaling the Mountain

EXECUTIVE PERSPECTIVE

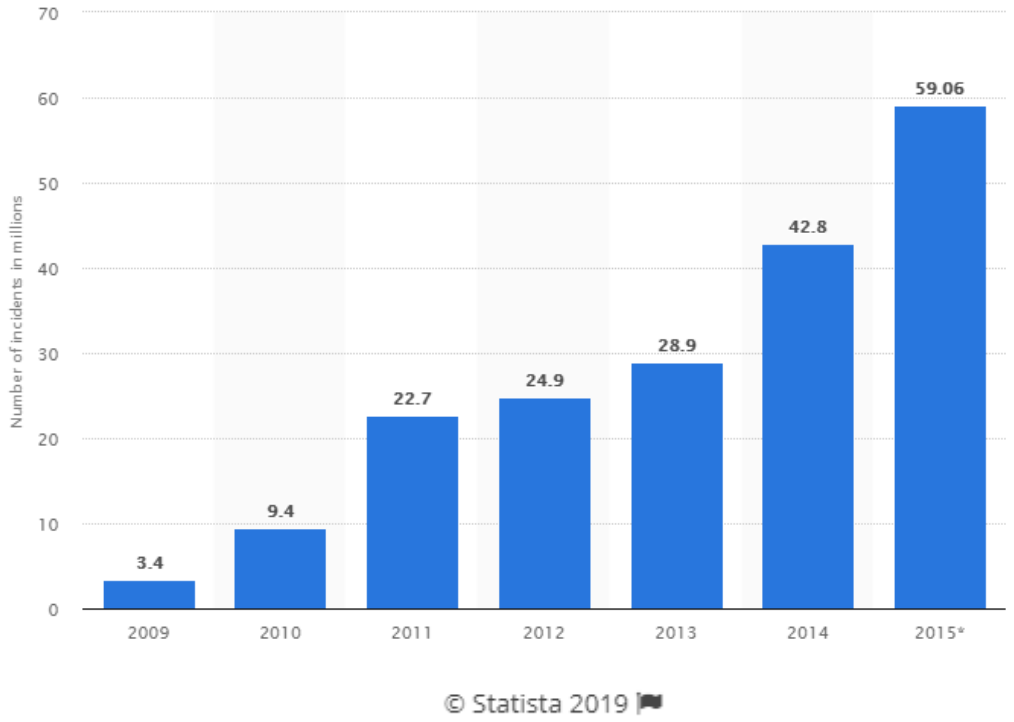
SALES	- Advertising - Sales Growth	+ 
R&D	- New Products - New Efficiencies	+ 
FINANCE	- New Investments	+ 
IT	- New Efficiencies	+ 
SECURITY	- ???	? 

MORE INVESTMENT = PREVENT ATTACKS!

Spending on cybersecurity in the United States from 2010 to 2018 (in billion $)



Global number of cyber security incidents from 2009 to 2015 (in millions)



MORE INVESTMENT = PREVENT ATTACKS!

NOVEMBER 1, 2017

Due to investments in infrastructure for growth and **spending to bolster security**, Facebook CFO Dave Wehner said capital expenditures in 2018 are forecast **to double from $7 billion to $14 billion**

SEPTEMBER 28, 2018

On the afternoon of Tuesday, September 25, our engineering team discovered a **security issue affecting almost 50 million accounts**

SPEAK THEIR LANGUAGE!

EXECUTIVES UNDERSTAND RISK! WE MITIGATE RISK!

EXAMPLE:

We investigate

650

Incidents/week

We encounter

950

Incidents/week

To keep up with demand, we need to spend $15,000 on a new tool that will allow for 300 Incidents/week

If we choose not to, we will allow 300 incidents per day, increasing our probability for breach by 33%. We estimate an average breach would cost $1.5mil. The increase of 33% risk is equal to $495k/year.

PROBLEM IS…

We investigate

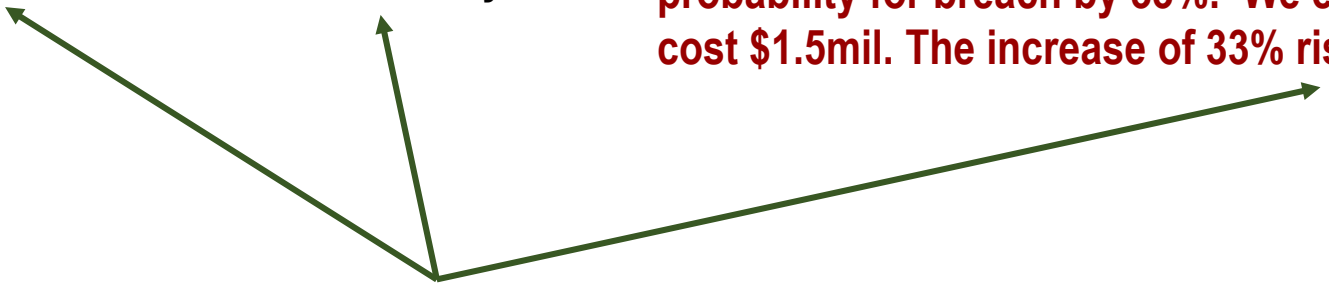
650

Incidents/year

We encounter

950

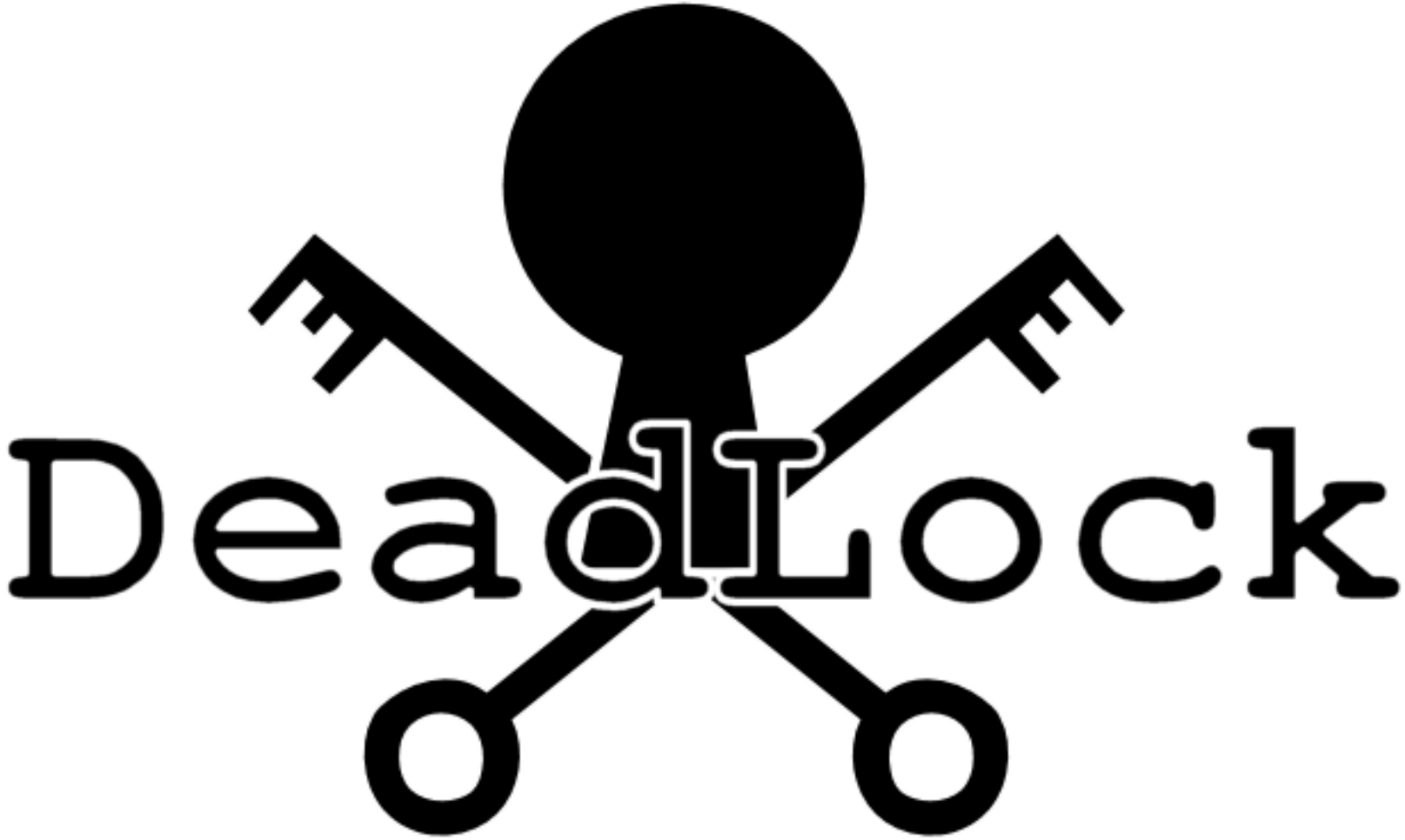
Incidents/day



To keep up with demand, we need to spend $15,000 on a new tool that will allow for 150 Incidents/day

If we choose not to, we will allow 300 incidents per day, increasing our probability for breach by 33%. We estimate an average breach would cost $1.5mil. The increase of 33% risk is equal to $495k/year.

THIS IS VERY HARD TO GET AT!!!



CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

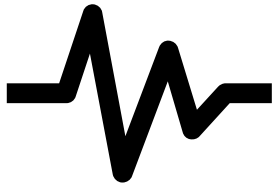
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Implementation of the CIS Top 20

Step 1:
Discover

Step 2:
Define

Step 3:
Enforce



Step 4:
Monitor

CIS Controls™ V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

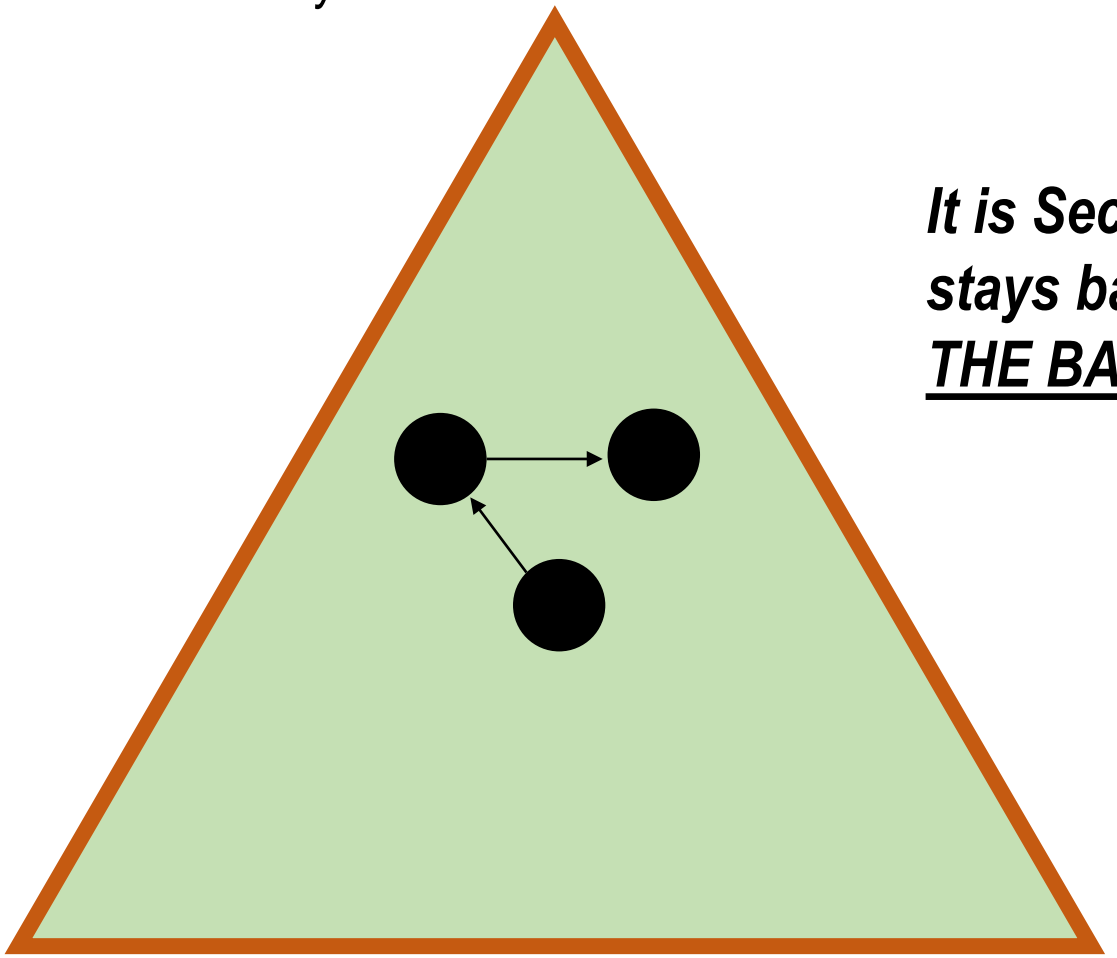
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Convenience

Systems make our life easier



It is Security's job to ensure the ball stays balanced, <u>NOT JUST DRIFT THE BALL TOWARDS SECURITY</u>

Functionality

Systems do things for us

Security

Systems protect us

Step 1: Discover

1 Inventory and Control of Hardware Assets

What are my devices?

2 Inventory and Control of Software Assets

What is running on my devices?

Step 1: Discover

- List all devices on the network


```
root@siteduzero:~# nmap 192.168.1.65

Starting Nmap 4.20 ( http://insecure.org ) at 2007-
01-26 00:18 CET
Interesting ports on 192.168.1.65:
Not shown: 1692 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
1234/tcp open  hotline
6112/tcp open  dtspc

Nmap finished: 1 IP address (1 host up) scanned in
5.622 seconds
root@siteduzero:~#
```

```
root@kali:~/masscan# bin/masscan 0.0.0.0/0 -p443

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2014-07-15 02:09:49 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 4294967295 hosts [1 port/host]
Discovered open port 443/tcp on 91.198.80.248
Discovered open port 443/tcp on 98.192.179.43
Discovered open port 443/tcp on 66.193.141.162
Discovered open port 443/tcp on 74.118.98.123
Discovered open port 443/tcp on 193.225.227.6
Discovered open port 443/tcp on 202.241.109.145
Discovered open port 443/tcp on 96.8.126.35
Discovered open port 443/tcp on 197.247.7.195
```

Step 1: Discover

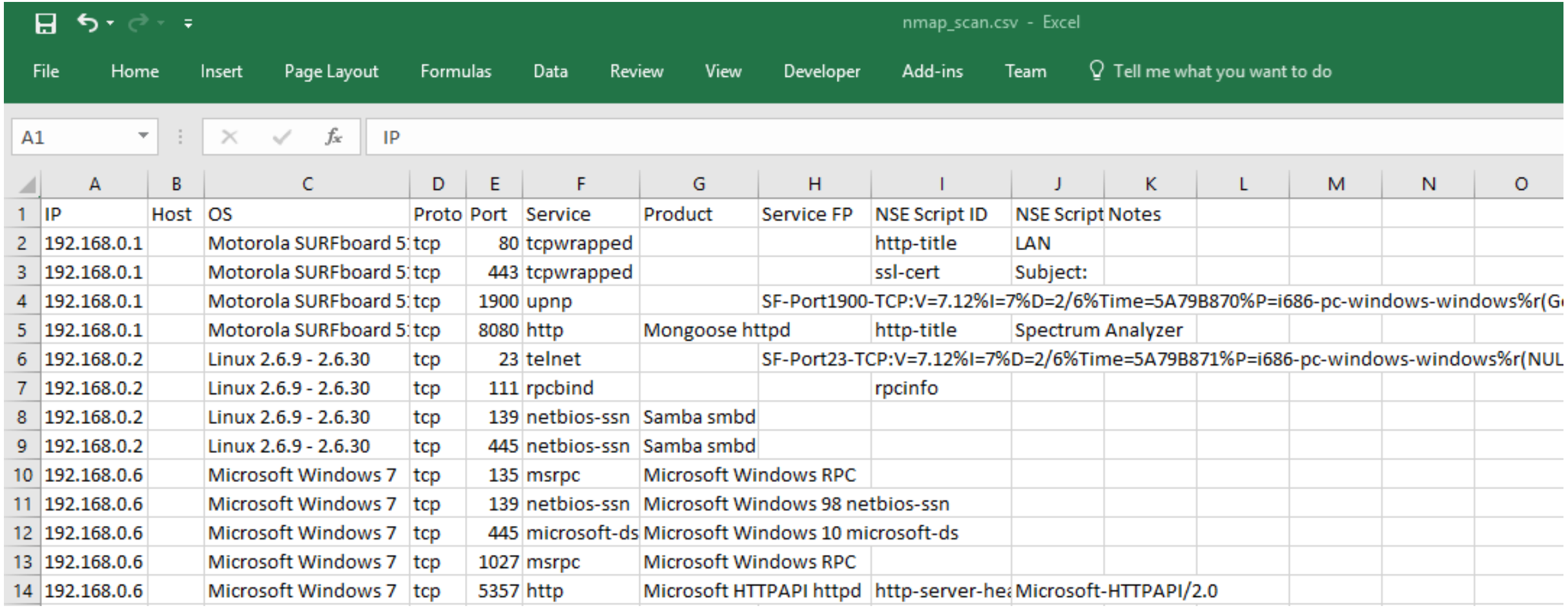
Pingsweep: `nmap –sP 10.10.10.0/24 –oA output`
Scan Top 100 ports from list: `nmap -F -iL list-of-ips.txt –oA output`
Scan Specific Port (ie 22): `nmap –p 22 -iL list-of-ips.txt –oA output`

https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.0.pdf

Pingsweep: `masscan 10.0.0.0/8 --ping –oL ips.txt`
Scan Specific Port (ie 22): `masscan 10.0.0.0/8 –p 22 –oX output.xml`

https://github.com/robertdavidgraham/masscan
https://www.youtube.com/watch?v=nX9JXI4l3-E

Step 1: Discover



nmap_scan.csv - Excel

File Home Insert Page Layout Formulas Data Review View Developer Add-ins Team Tell me what you want to do

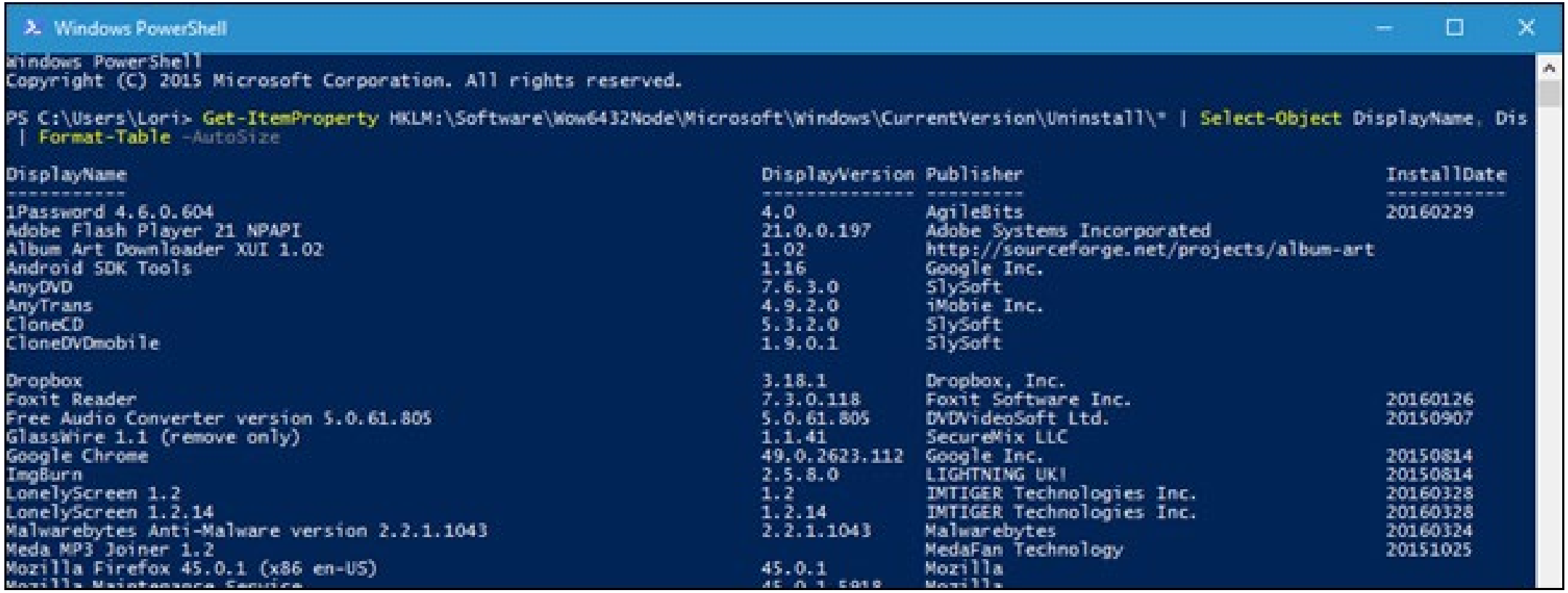
A1 IP

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	IP	Host	OS	Proto	Port	Service	Product	Service FP	NSE Script ID	NSE Script	Notes				
2	192.168.0.1		Motorola SURFboard 5	tcp	80	tcpwrapped			http-title	LAN					
3	192.168.0.1		Motorola SURFboard 5	tcp	443	tcpwrapped			ssl-cert	Subject:					
4	192.168.0.1		Motorola SURFboard 5	tcp	1900	upnp		SF-Port1900-TCP:V=7.12%I=7%D=2/6%Time=5A79B870%P=i686-pc-windows-windows%r(G							
5	192.168.0.1		Motorola SURFboard 5	tcp	8080	http	Mongoose httpd		http-title	Spectrum Analyzer					
6	192.168.0.2		Linux 2.6.9 - 2.6.30	tcp	23	telnet		SF-Port23-TCP:V=7.12%I=7%D=2/6%Time=5A79B871%P=i686-pc-windows-windows%r(NUL							
7	192.168.0.2		Linux 2.6.9 - 2.6.30	tcp	111	rpcbind			rpcinfo						
8	192.168.0.2		Linux 2.6.9 - 2.6.30	tcp	139	netbios-ssn	Samba smbd								
9	192.168.0.2		Linux 2.6.9 - 2.6.30	tcp	445	netbios-ssn	Samba smbd								
10	192.168.0.6		Microsoft Windows 7	tcp	135	msrpc	Microsoft Windows RPC								
11	192.168.0.6		Microsoft Windows 7	tcp	139	netbios-ssn	Microsoft Windows 98 netbios-ssn								
12	192.168.0.6		Microsoft Windows 7	tcp	445	microsoft-ds	Microsoft Windows 10 microsoft-ds								
13	192.168.0.6		Microsoft Windows 7	tcp	1027	msrpc	Microsoft Windows RPC								
14	192.168.0.6		Microsoft Windows 7	tcp	5357	http	Microsoft HTTPAPI httpd		http-server-hea	Microsoft-HTTPAPI/2.0					

Step 1: Discover

❑ List all software installed on a client machine

```
Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* |
Select-Object DisplayName, DisplayVersion, Publisher, InstallDate |
Format-Table –AutoSize
```



Step 2: Define

Privledged Account Usage Policy

Hardened Image for Clients and Servers

Network Security Framework

Hardened Image for Network Devices

Data Classification and Access Policy

Step 2: Define

4 Controlled Use of Administrative Privileges

Privledged Account Usage Policy

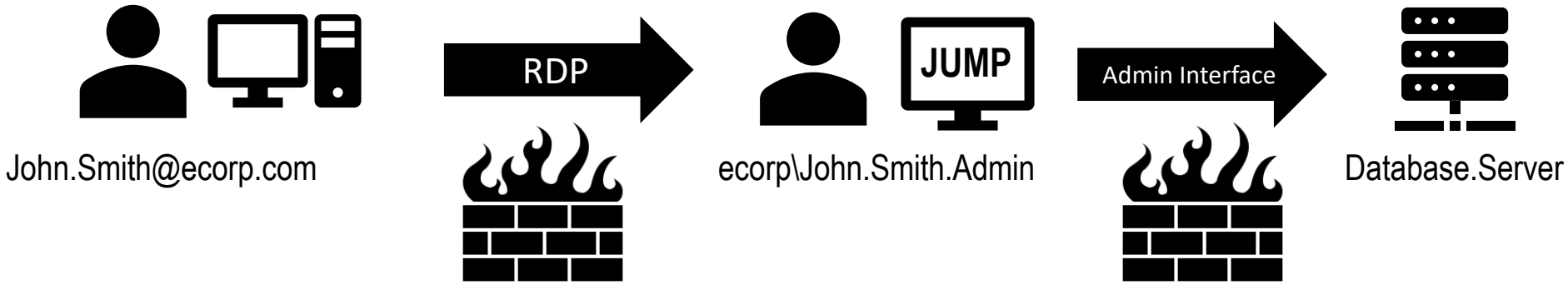
- ❑ No administration from non-admin accounts
- ❑ No administration from non-admin workstations
- ❑ No default admin passwords
- ❑ No Domain Admins
- ❑ Implement LAPS

Step 2: Define

4 Controlled Use of Administrative Privileges

Privledged Account Usage Policy

- ❑ No administration from non-admin accounts
- ❑ No administration from non-admin workstations



Firewalls MUST BE TIGHT!

Step 2: Define

4 Controlled Use of Administrative Privileges

Privledged Account Usage Policy

- ❑ No default admin passwords

Scan

```
nmap -p80 --script http-
default-accounts 10.0.0.0/8
```

https://nmap.org/nsedoc/scripts/http-default-accounts.html

Change

Long and complex

Vault

KeePass

Don't forget your printers!

Step 2: Define

4 Controlled Use of Administrative Privileges

Privledged Account Usage Policy

❑ No Domain Admins

- `net group "Domain Admins" /domain`
- `dsget group "CN=Domain Admins,CN=Users,DC=ecorp,DC=com" -members`

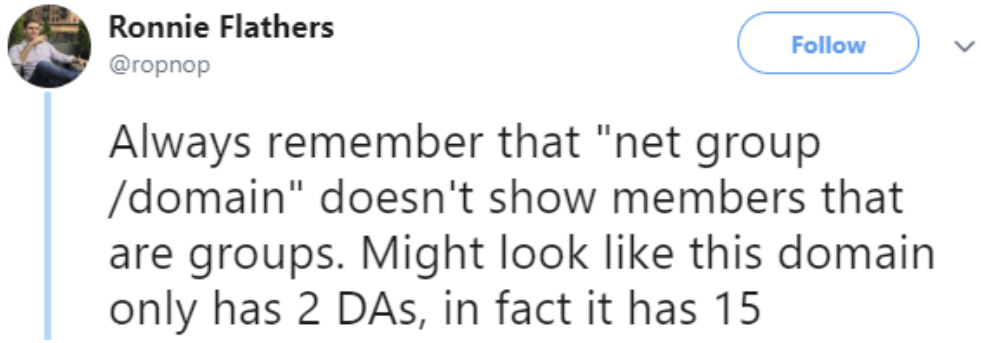
```
PS C:\> net group "Domain Admins" /domain
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            agreen
The command completed successfully.

PS C:\> dsget group "CN=Domain Admins,CN=Users,DC=lab,DC=ropnop,DC=com" -members
"CN=IT Admins,OU=groups,OU=LAB,DC=lab,DC=ropnop,DC=com"
"CN=Andy Green,OU=users,OU=LAB,DC=lab,DC=ropnop,DC=com"
"CN=Administrator,CN=Users,DC=lab,DC=ropnop,DC=com"

PS C:\> _
```



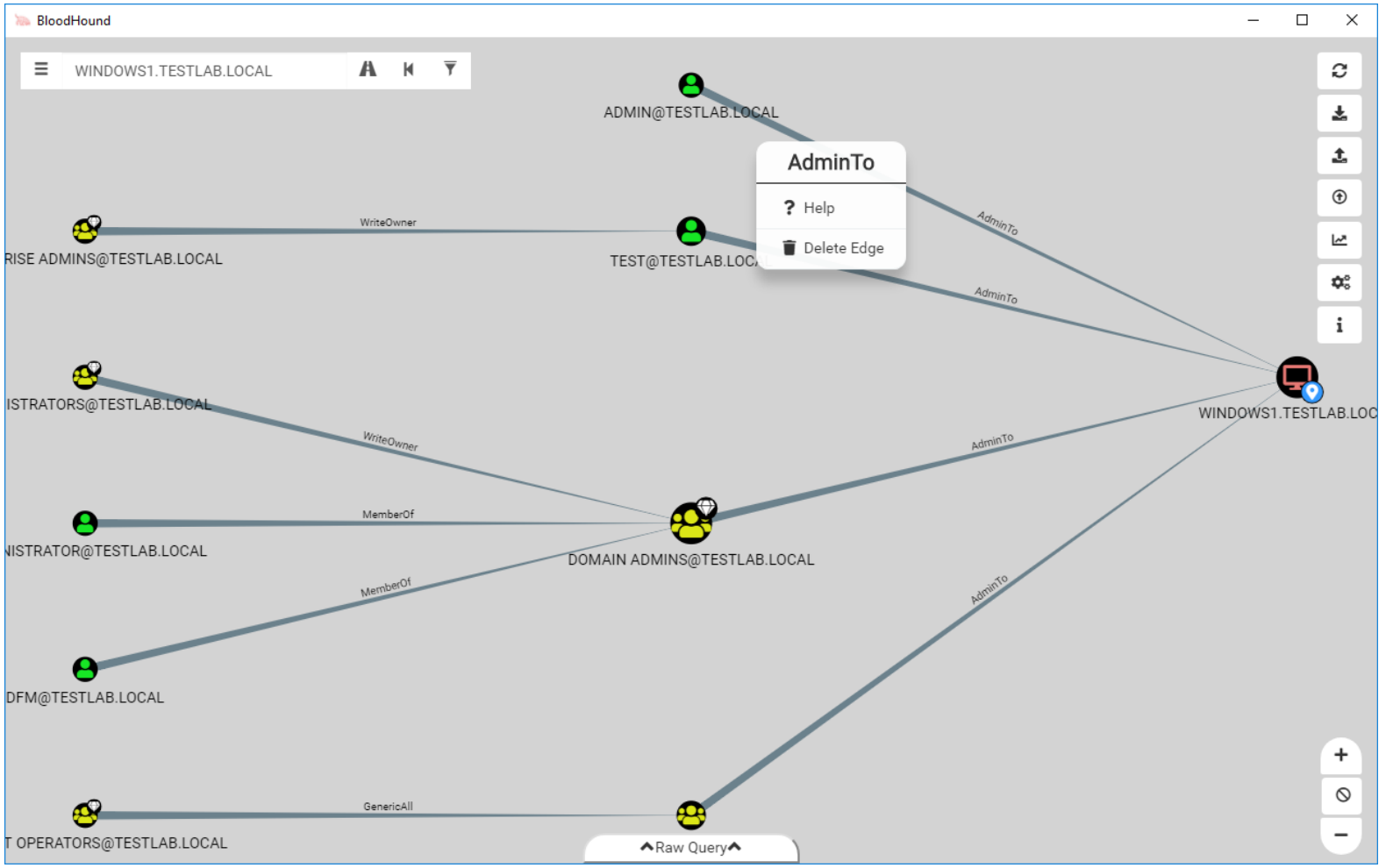
Step 2: Define

4 Controlled Use of Administrative Privileges

Privledged Account Usage Policy

BLOODHOUND

https://github.com/BloodHoundAD

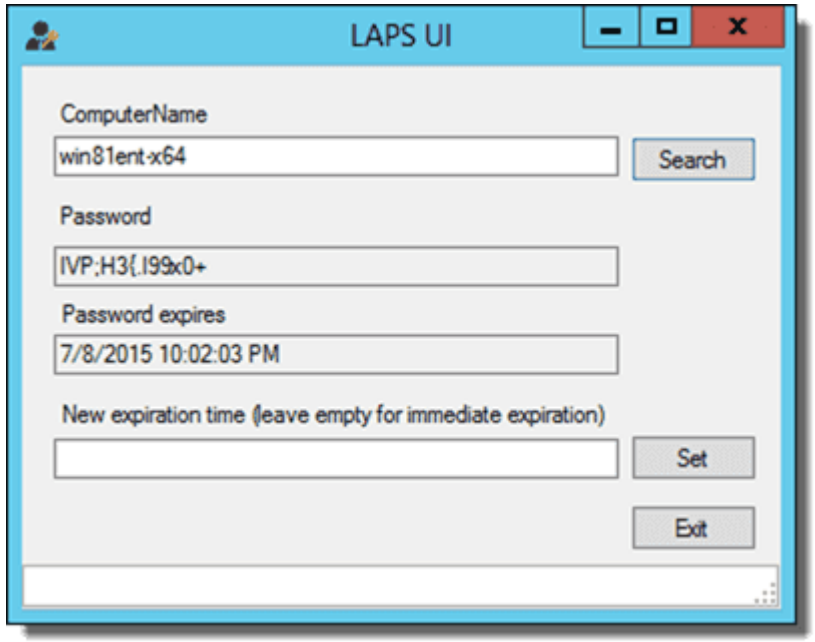


Step 2: Define

4 Controlled Use of Administrative Privileges

Privledged Account Usage Policy

- ❑ **Implement LAPS (Local Admin Password Solution)**



1. Push install .msi to clients through GPO
2. Modify AD schema with .ps script from Microsoft
3. Enable LAPS GPO
4. Remove any custom local admins you have

https://www.microsoft.com/en-us/download/details.aspx?id=46899

Step 2: Define

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Hardened Image for Clients and Servers

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Hardened Image for Network Devices

Free SCAP Compliance Audit

NIST Checklists - https://nvd.nist.gov/ncp/repository

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

NCP provides metadata and links to checklists of various formats including checklists that conform to the Security Content Automation Protocol (SCAP). SCAP enables validated security products to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms. Please note that the current search fields have been adjusted to reflect NIST SP 800-70 Revision 4.

Search for Checklists using the fields below. The keyword search will search across the name, and summary.

Checklist Type:	Any.....	**Content Type:**	Any.....
Authority:	Any.....	**Tool Compatibility:**	Any.....
Target:	Microsoft Windows Server 2012 R2	**Keyword:**	

Search Reset

There are **10** matching records.

Name (Version)	Target	Product Category	Authority	Last Modified	Resources
Windows Server 2012 / 2012 R2 STIG (Version 2, Release 14)	Microsoft Windows Server 2012 R2 Microsoft Windows Server 2012	Operating System	Defense Information Systems Agency	01/22/2019	SCAP 1.2 Content - Microsoft Windows 2012 and 2012 R2 DC STIG Benchmark - Ver 2, Rel 14 SCAP 1.2 Content - Microsoft Windows 2012 and 2012 R2 MS STIG Benchmark - Ver 2, Rel 14 GPOs - Group Policy Objects (GPOs) - November 2018 Standalone XCCDF 1.1.4 - Microsoft Windows 2012 and 2012 R2 DC STIG - Ver 2, Rel 14 Standalone XCCDF 1.1.4 - Microsoft Windows 2012 and 2012 R2 MS STIG - Ver 2, Rel 14

NIST Checklists - https://nvd.nist.gov/ncp/repository

GPOs

Root

Name	Size	Packed Size	Modified	Created	Accessed	Attributes
Checklist	0	0	2018-07-27 15:49			D
GPOs	985 688	110 429	2018-11-05 09:38			D
Reports	1 417 494	154 895	2018-11-05 10:01			D
WMI Filter	2 000	845	2018-11-05 09:38			D

GPOs

Name	Size	Pack
{0537A302-FBC2-4C43-A0C3-045419A1F221}	43 916	
{B9379DEB-619C-4313-A9EE-8F899928D4EF}	43 900	
{DAF7CEC7-3321-4455-A007-A495EF54B03D}	450 352	
{E253CCCA-26B5-4CC7-8863-AC3AADBE5C31}	445 121	
manifest.xml	2 399	

Reports

Name	Size	Packed Size	Modified	Cr
DoD Windows Server 2012 R2 DC Deltas.xlsx	11 016	8 312	2018-10-25 11:11	
DoD Windows Server 2012 R2 Domain Controller STIG Computer v2r14.html	528 148	51 287	2018-10-25 10:19	
DoD Windows Server 2012 R2 Domain Controller STIG User v2r14.html	166 088	17 406	2018-10-25 10:19	
DoD Windows Server 2012 R2 Member Server STIG Computer v2r14.html	535 254	52 262	2018-10-25 10:19	
DoD Windows Server 2012 R2 Member Server STIG User v2r14.html	166 072	17 401	2018-10-25 10:19	
DoD Windows Server 2012 R2 MS Deltas.xlsx	10 916	8 227	2018-10-25 11:12	

NIST Checklists - https://nvd.nist.gov/ncp/repository

GPO Reports

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes

Local Policies/User Rights Assignment

Policy	Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	BUILTIN\Administrators, NT AUTHORITY\Authenticated Users
Act as part of the operating system	
Allow log on locally	BUILTIN\Administrators
Allow log on through Terminal Services	BUILTIN\Administrators
Back up files and directories	BUILTIN\Administrators
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create global objects	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\SERVICE
Create permanent shared objects	
Create symbolic links	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests, NT AUTHORITY\Local account
Deny log on as a batch job	ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests
Deny log on as a service	ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS
Deny log on locally	ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests
Deny log on through Terminal Services	ADD YOUR DOMAIN ADMINS, ADD YOUR ENTERPRISE ADMINS, BUILTIN\Guests, NT AUTHORITY\Local account
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	BUILTIN\Administrators
Generate security audits	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Impersonate a client after authentication	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators
Lock pages in memory	
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Perform volume maintenance tasks	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Restore files and directories	BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Local Policies/Security Options

OpenSCAP - https://www.open-scap.org/getting-started/

1. Download and install

https://www.open-scap.org/tools/scap-workbench/download-win32

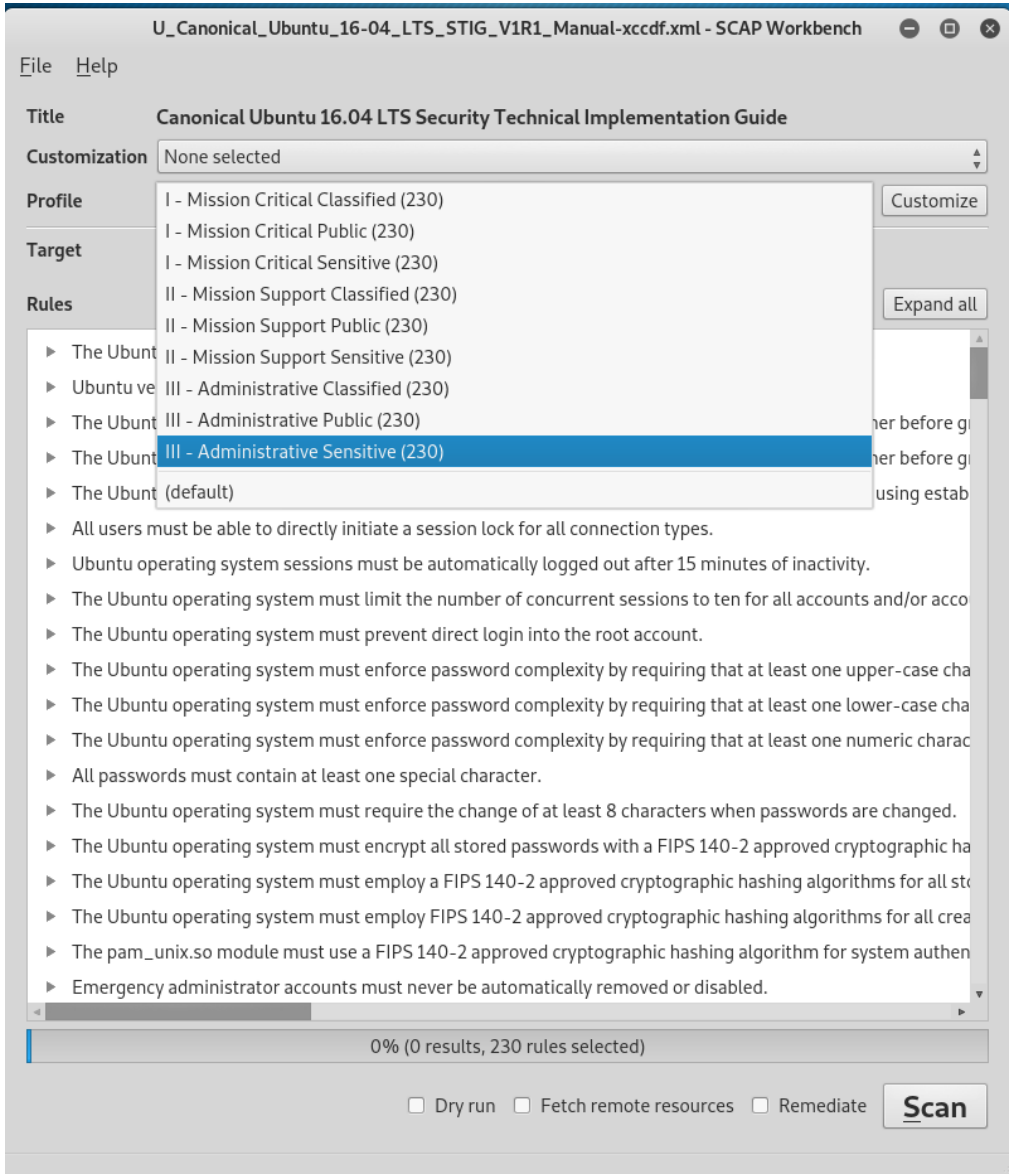
https://www.open-scap.org/tools/scap-workbench/download-osx

```
apt-get install scap-workbench
```

```
yum install scap-workbench
```

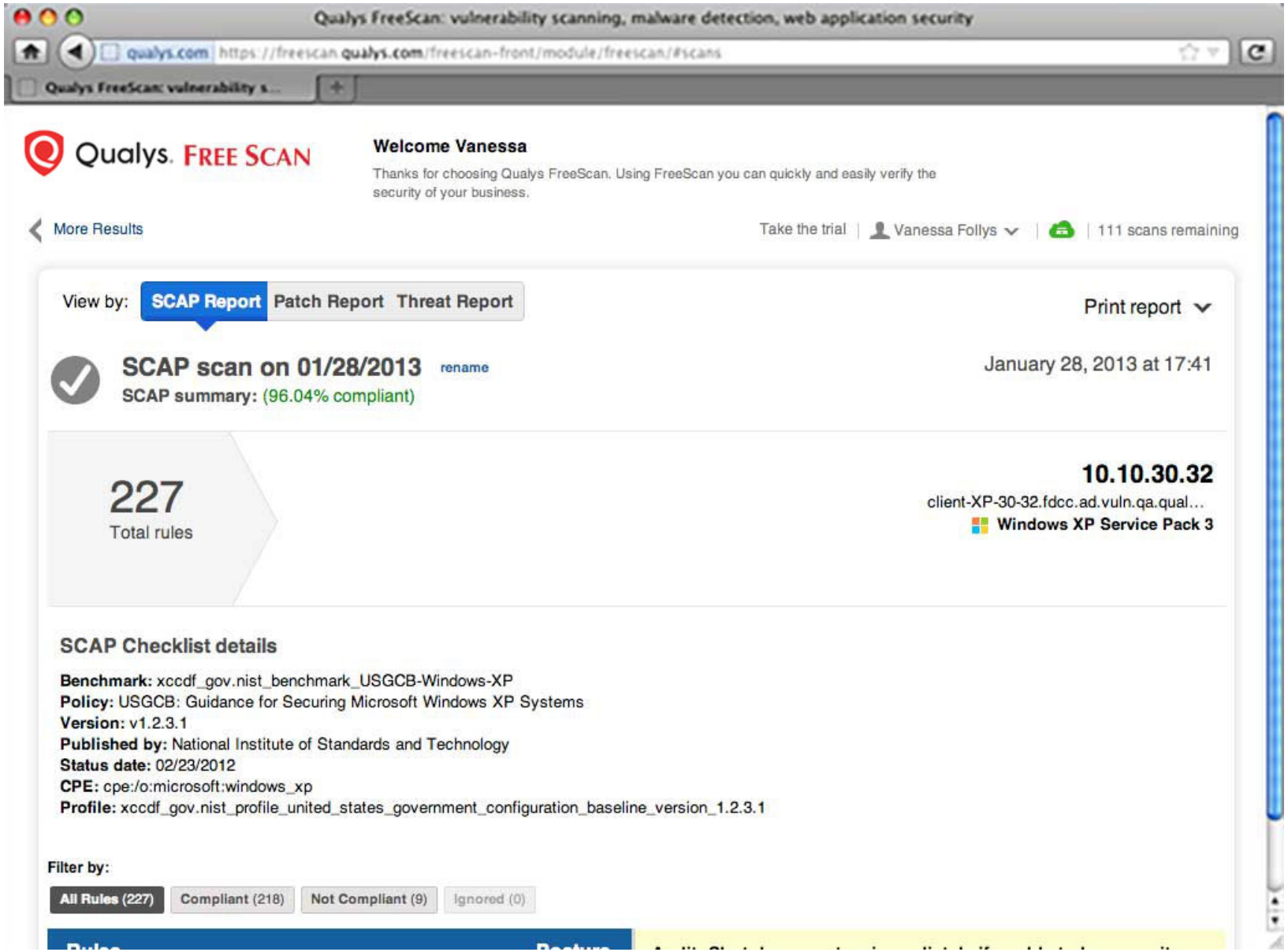
OpenSCAP - https://www.open-scap.org/getting-started/

2. Load the STIG SCAP contents
3. Scan!



*Limited to only *nix machines…

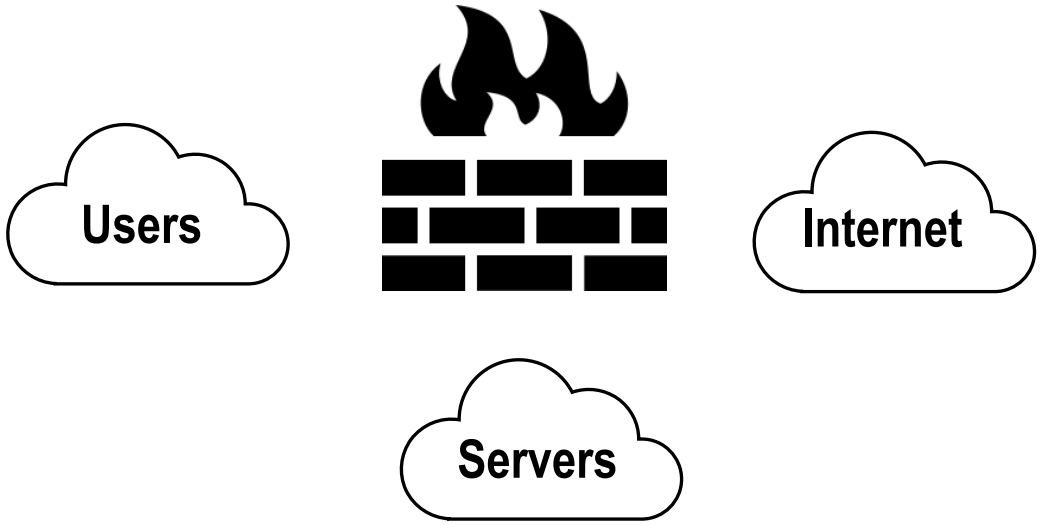
Qualys FreeScan SCAP Audit - https://www.qualys.com/forms/freescan/scap/



Step 2: Define

9 Limitation and Control of Network Ports, Protocols, and Services

Network Security Framework

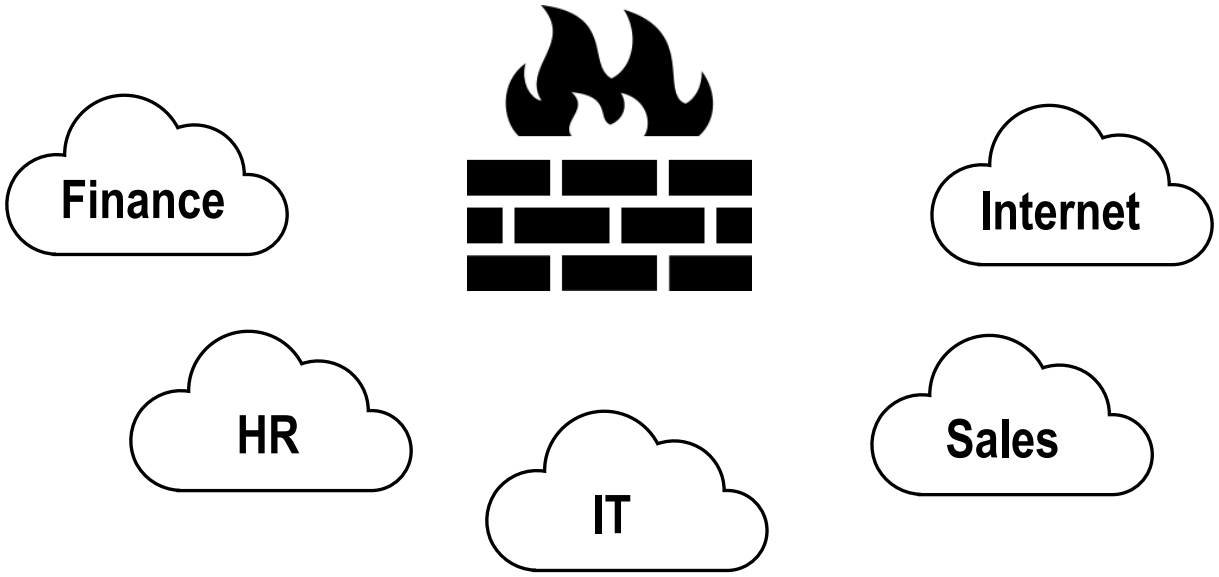


System-Conentric View

Step 2: Define

9 Limitation and Control of Network Ports, Protocols, and Services

Network Security Framework



User-Conentric View

Step 2: Define

9 Limitation and Control of Network Ports, Protocols, and Services

Network Security Framework

RBAC in Network Security

1. Categorize people, systems, applications, websites, etc. by functional role
2. Allow access to those systems, apps, sites to roles
3. Move people into those roles
4. Deny all other access

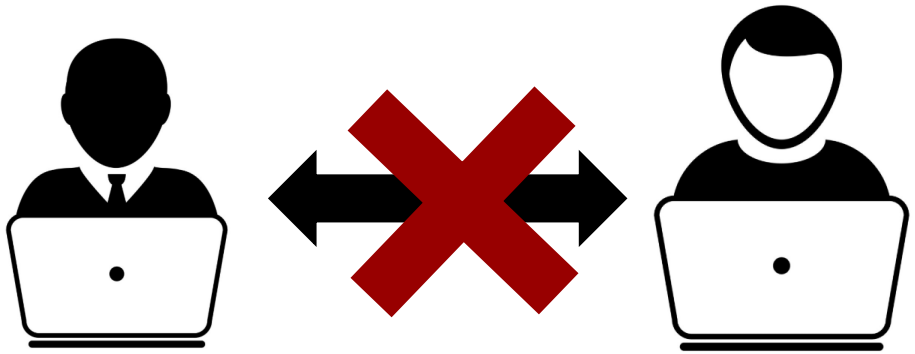
Role	Department	Internal Access	External Access
Stock Market Analyst	Finance	US-SAP-FI-001:8505 US-APP-STOCK-001:900 …	Fidelity.com/stocks Robinhood.com
IT SysAdmin	IT	ALL (Challenge this)	Google.com Reddit.com

Step 2: Define

9 Limitation and Control of Network Ports, Protocols, and Services

Network Security Framework

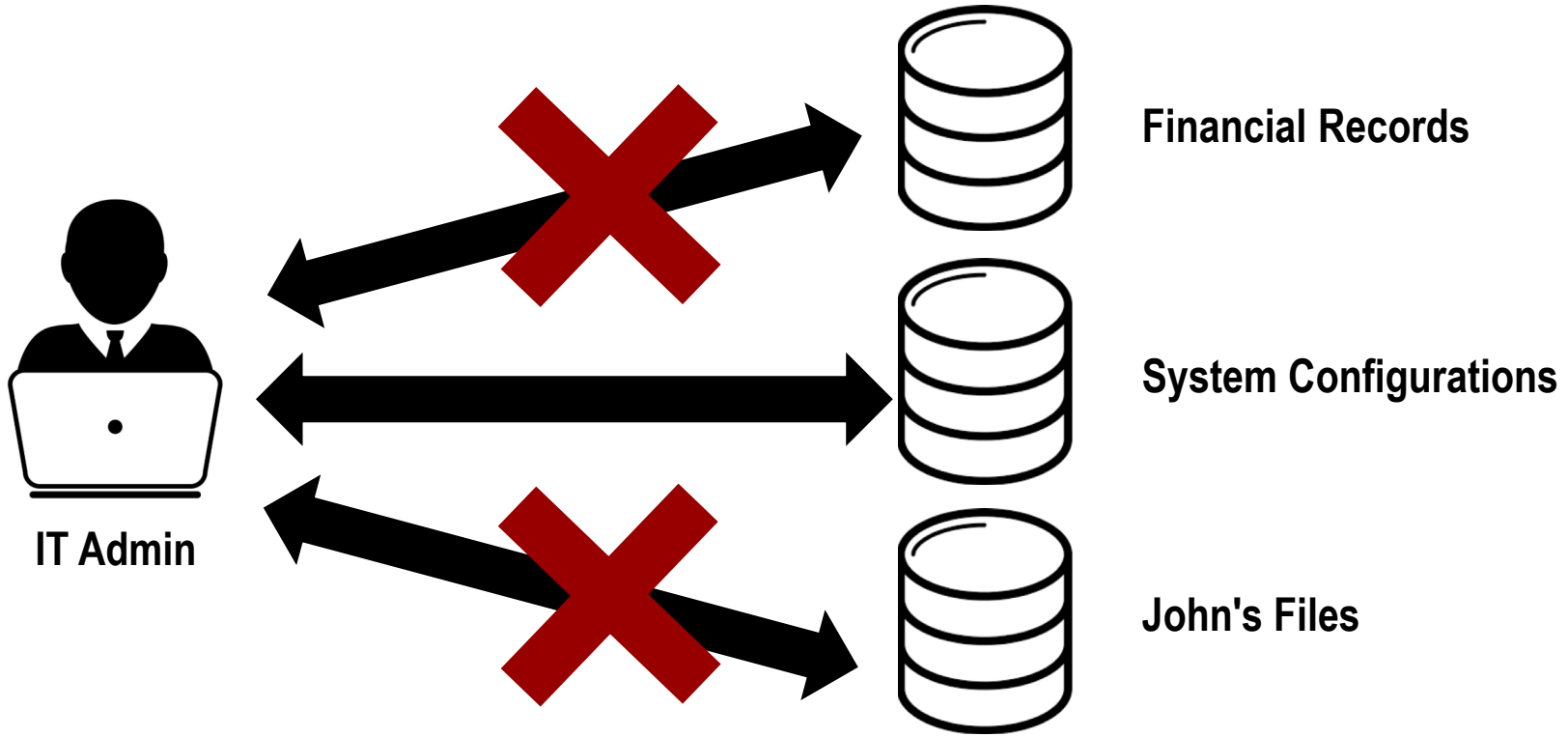
- ❑ Turn on client-side firewalls
- ❑ Don't allow peer connections



Step 2: Define

14 Controlled Access Based on the Need to Know

Data Classification and Access Policy



Step 2: Define

14 Controlled Access Based on the Need to Know

Data Classification and Access Policy

RBAC in Data

1. Categorize people, systems, applications, websites, etc. By functional role
2. Allow access to those systems, apps, sites to roles
3. Move people into those roles
4. Deny all other access

Role	Department	Data	Location
Stock Market Analyst	Finance	Historic Purchases Current Bank Accounts	\\US-STOCK\hist\001.xls \\US-BANK\acct\today.xls
IT SysAdmin	IT	Configuration database Documentation Archive	\\US-IT\configs \\US-IT\docs

Step 3: Enforcement

Implement firewalls on trust boundaries

Encrypt drives and disable writeable USBs

Implement DNS Filtering

Ensure Backups

Ensure your AV

Ensure Secure Wireless Deployments

Step 3: Enforcement

Implement firewalls on trust boundaries

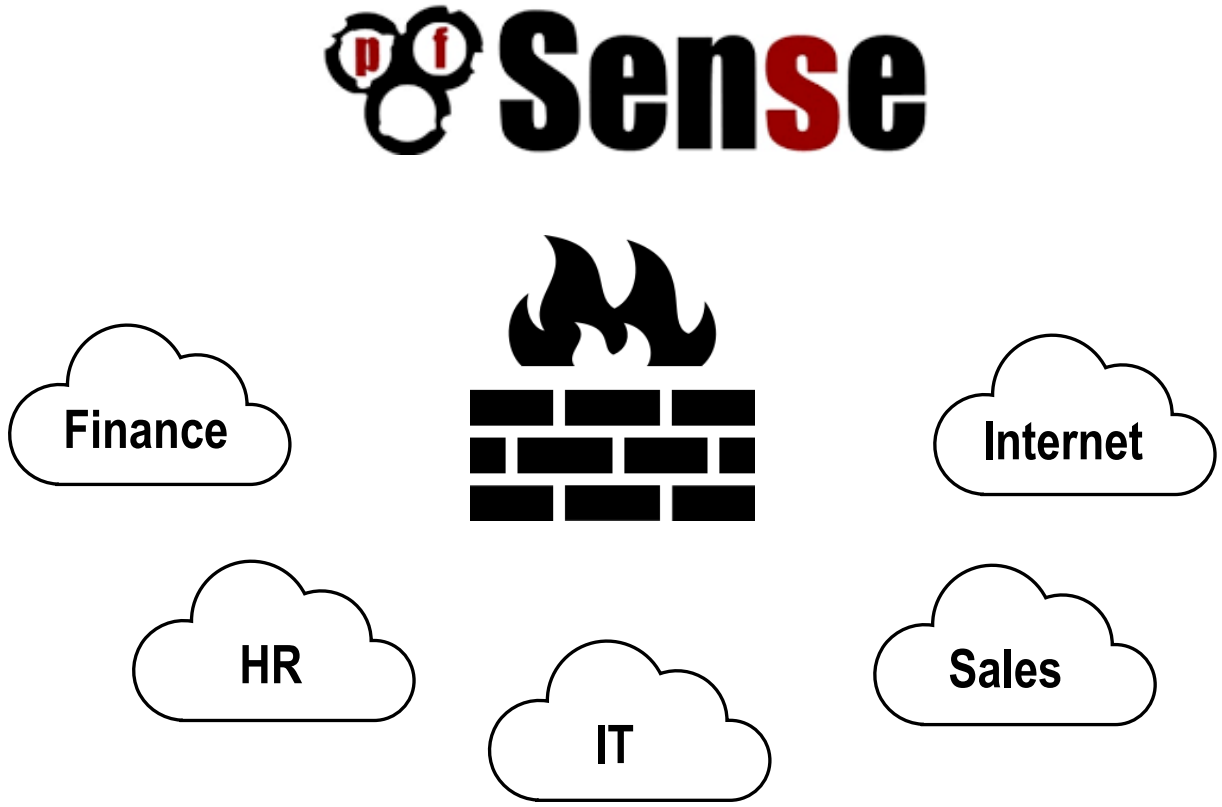
1. Define your boundaries from your RBAC policy
2. Build a PFSense VM
3. Build the PFSense policy based on your RBAC policy

A firewall is simply a technical implementation of your written policy. No more, no less

Step 3: Enforcement

12 Boundary Defense

Implement firewalls on trust boundaries



PFSENSE - https://www.pfsense.org/

1. Download ISO https://www.pfsense.org/download/

Latest Stable Version (Community Edition)

This is the most recent stable release, and the recommended version for all installations. For upgrade information, see the Upgrade Guide. For pre-configured systems, see the pfSense appliances on Netgate.

RELEASE NOTES | SOURCE CODE

Select Image To Download

Version: 2.4.4-p1

Architecture: AMD64 (64-bit)

Installer: CD Image (ISO) Installer

Mirror: New York City, USA

DOWNLOAD

Supported by netgate

SHA256 Checksum for compressed (.gz) file:
a5ca11eab11e2cddc33a11ded4df69eab7ae48399004588562f5f305ae3c0246

Subscribe To The Netgate Newsletter

Product information, software announcements, and special offers.
See our newsletter archive for past announcements.

Email*
Email Address

I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*

Subscribe

(view our privacy policy)

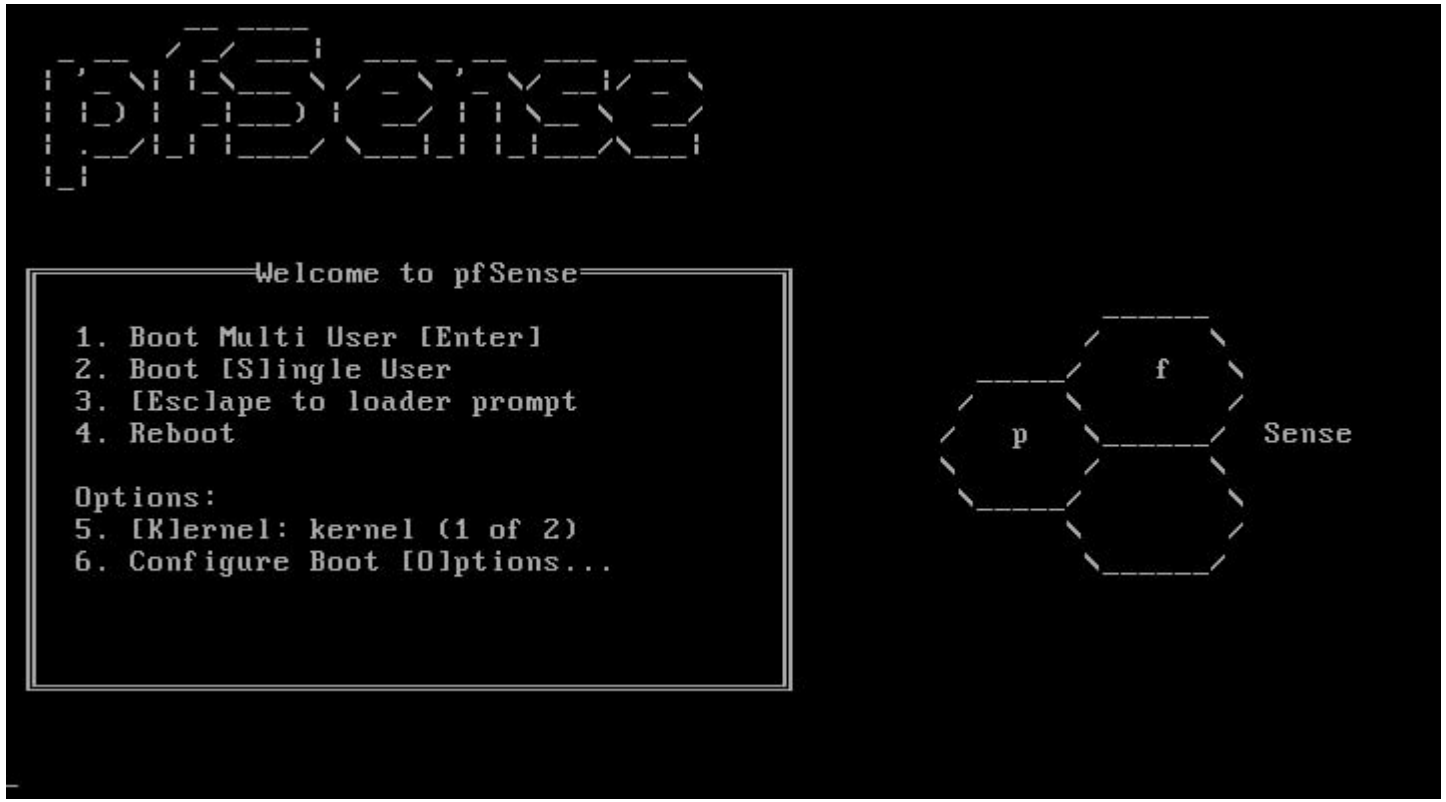
PFSENSE - https://www.pfsense.org/

2. Install

ESX Guide
https://docs.netgate.com/pfsense/en/latest/virtualization/virtualizing-pfsense-with-vmware-vsphere-esxi.html

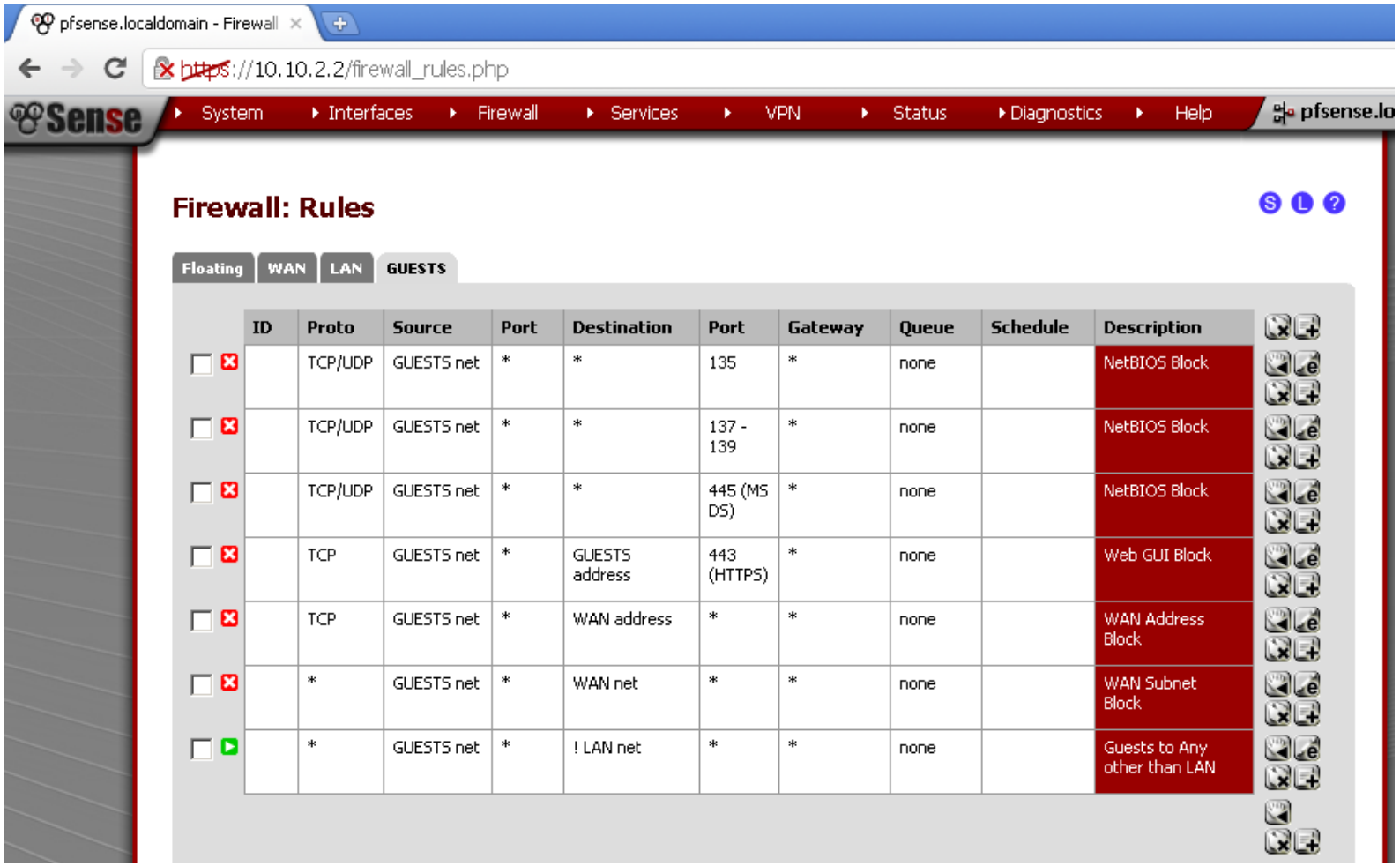
Hyper-V Guide
https://docs.netgate.com/pfsense/en/latest/virtualization/virtualizing-pfsense-with-hyper-v.html

Bare Metal Guide
https://docs.netgate.com/pfsense/en/latest/install/installing-pfsense.html



PFSENSE - https://www.pfsense.org/

3. Configure - https://docs.netgate.com/pfsense/en/latest/config/



Step 3: Enforcement

Encrypt drives and disable writeable USBs

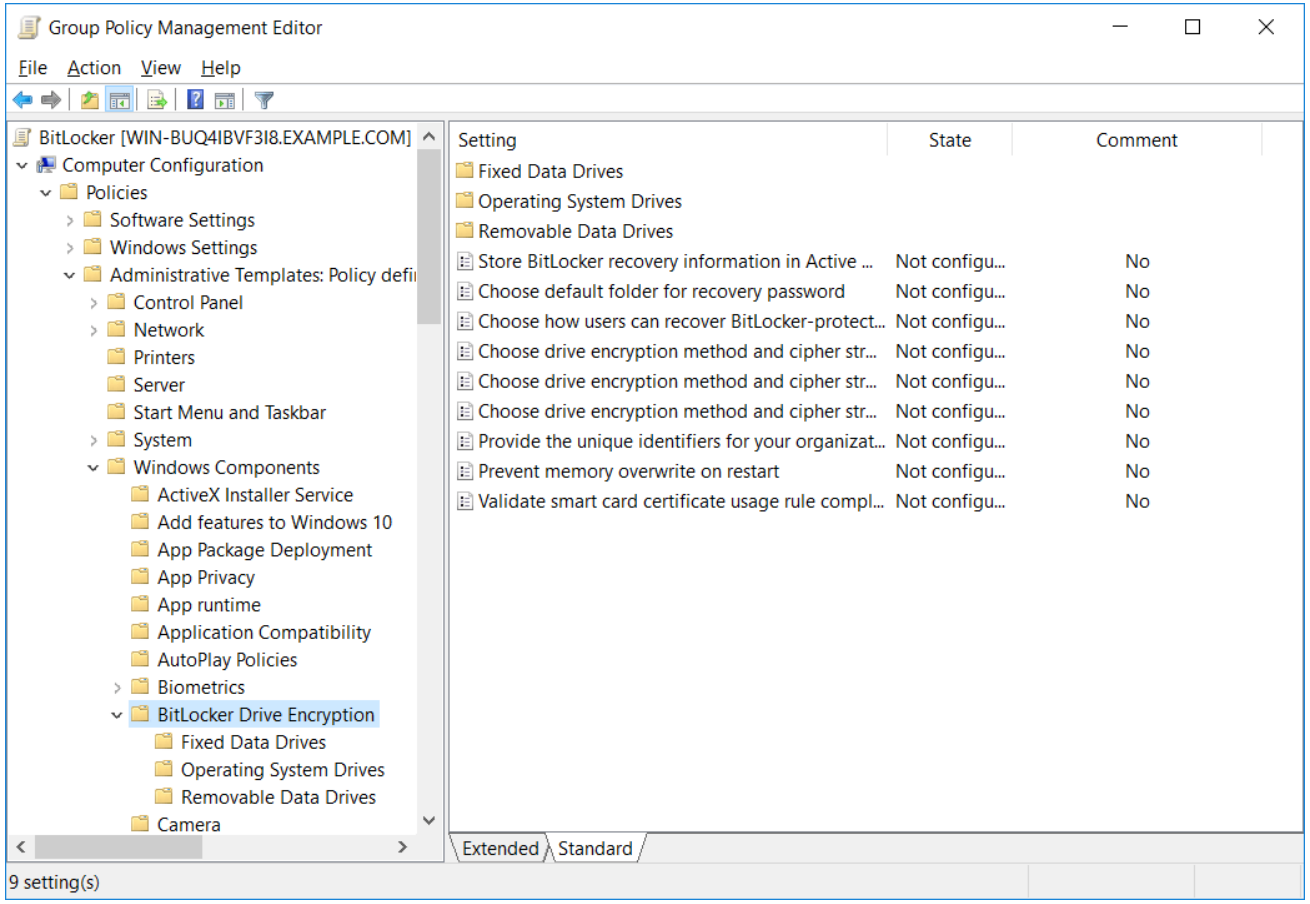
- ❑ Encrypt client hard drives
- ❑ No writing to external drives

Step 3: Enforcement

❑ Encrypt client hard drives

GPO:

Computer Configuration >
Policies >
Administrative Templates >
Windows Components >
BitLocker Drive Encryption

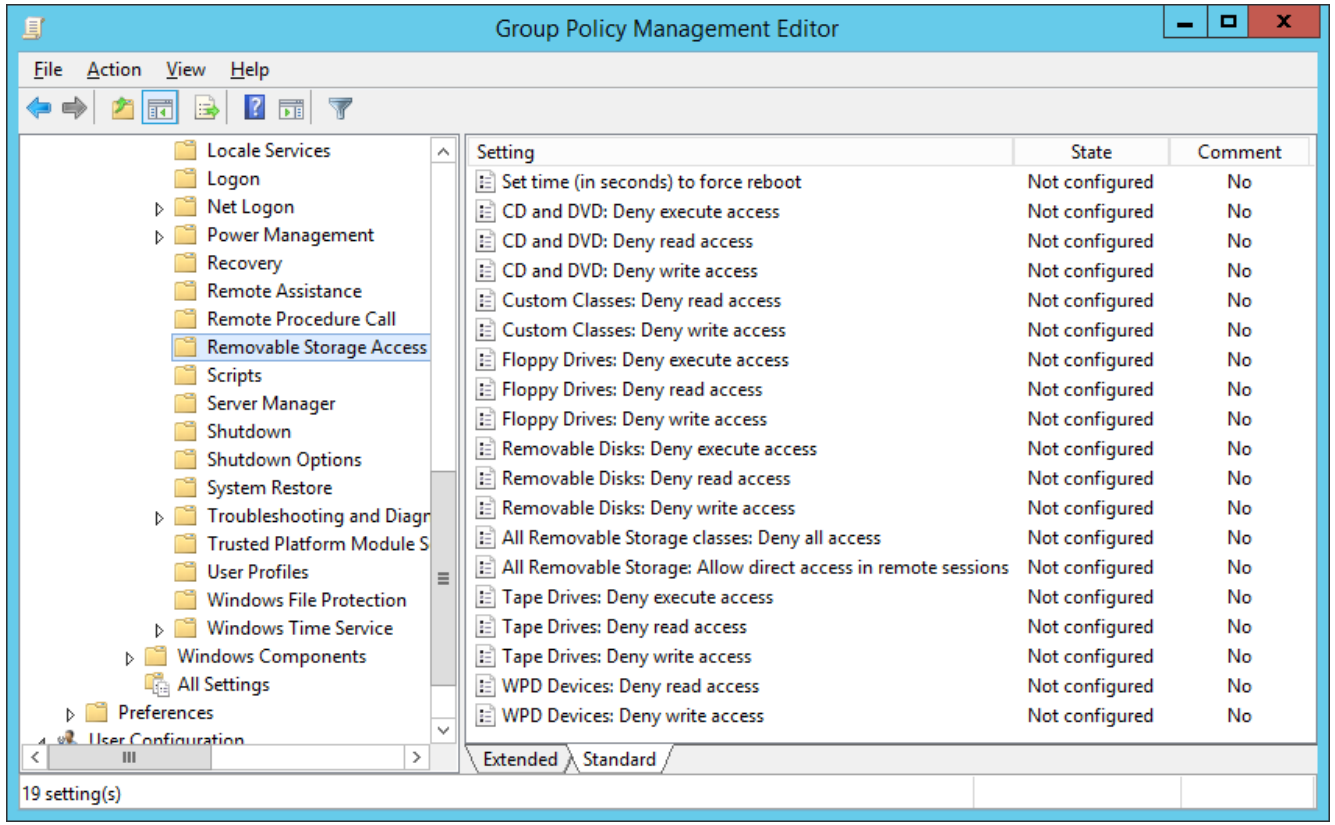


Step 3: Enforcement

❑ No writing to external drives

GPO:

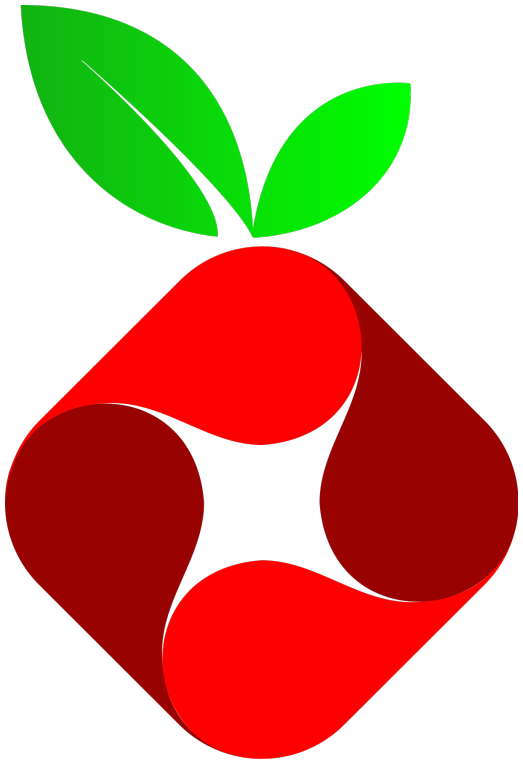
Computer Configuration >
Policies >
Administrative Templates >
System >
Removable Storage Access



Step 3: Enforcement

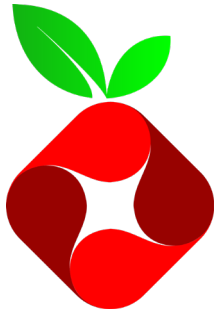
7 Email and Web Browser Protections

Implement DNS Filtering



Pi-hole

Pi-Hole - https://pi-hole.net/

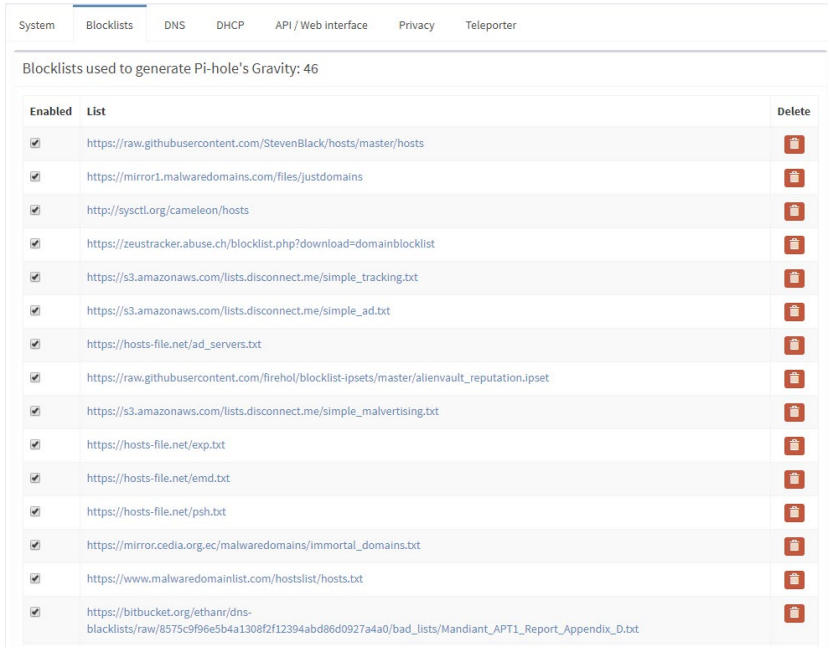


1. **Install with this command**

```
curl -sSL https://install.pi-hole.net | bash
```

2. **Configure blocklists**

```
https://raw.githubusercontent.com/setoptz/sysadmin/master/blocklist.txt
```



3. **Update your DHCP to point users to your DNS server**

Step 3: Enforcement

10 Data Recovery Capabilities

Ensure Backups*

3 – 2 – 1 Backup rule

3 copies of your data – 2 different media – 1 copy off site

15 Wireless Access Control

Ensure Secure Wireless Deployments*

- ❑ No WEP, Use WPA2
- ❑ Segment Guest Network from Corporate LAN

8 Malware Defenses

Ensure your AV*

AV Cash Cow Tipping…

"Or, kicking puppies… And Laughing."

egyp7

Thanks for the subtitle @egyp7

Step 4: Monitor

3 Continuous Vulnerability Management

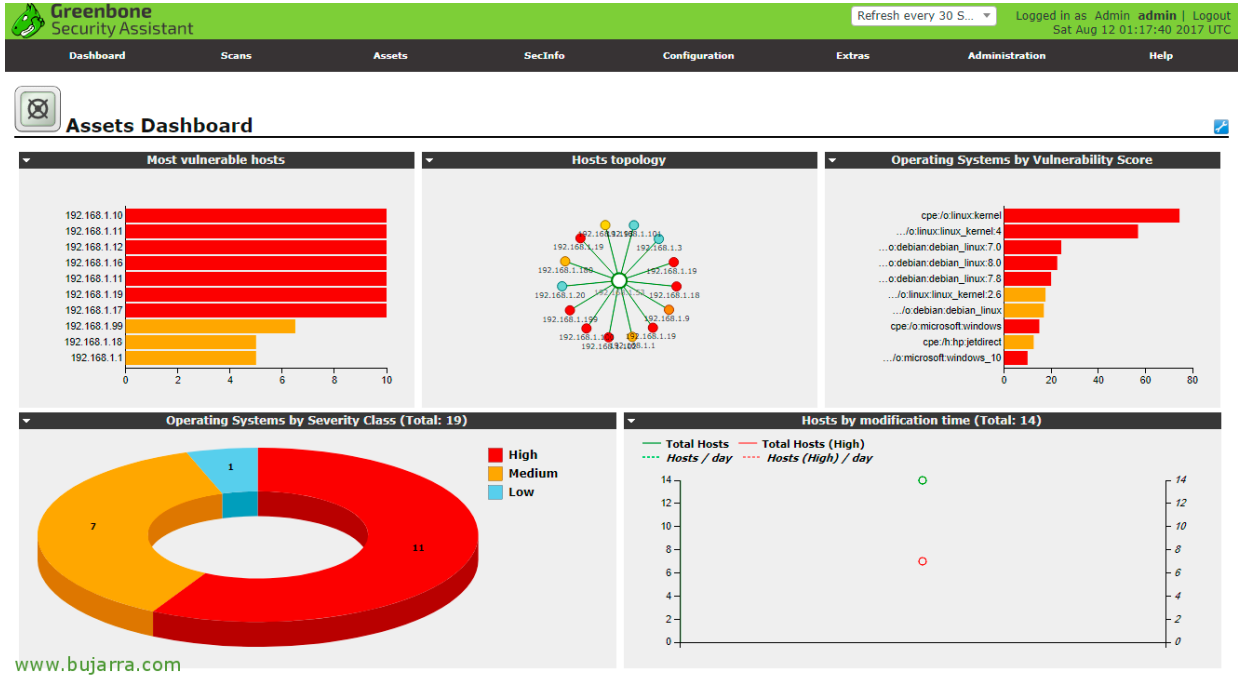
6 Maintenance, Monitoring and Analysis of Audit Logs

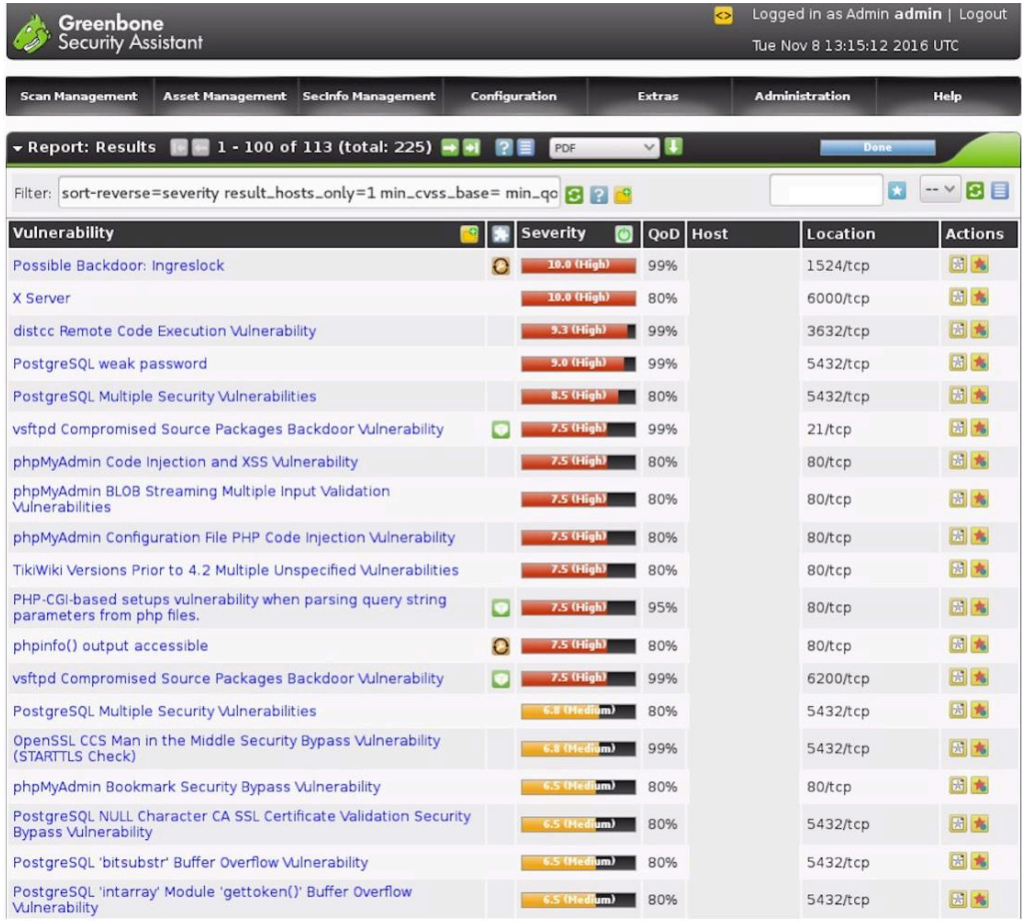
16 Account Monitoring and Control

Step 4: Monitor

3 Continuous Vulnerability Management

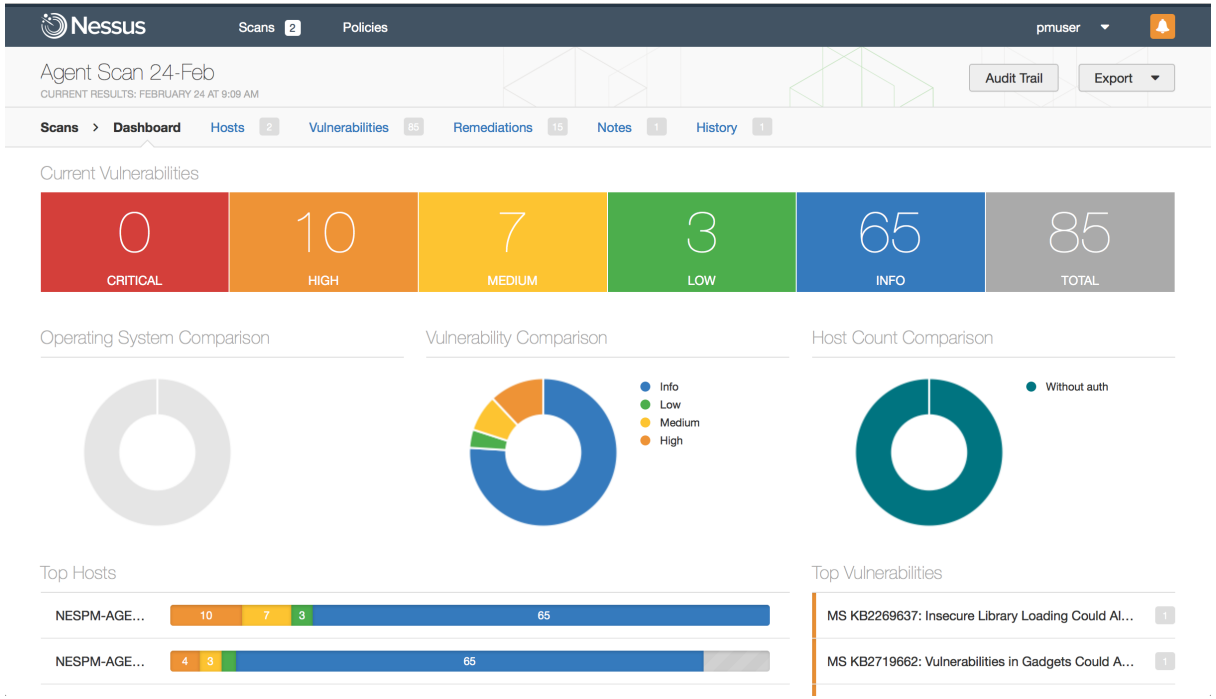
Step 4: Monitor

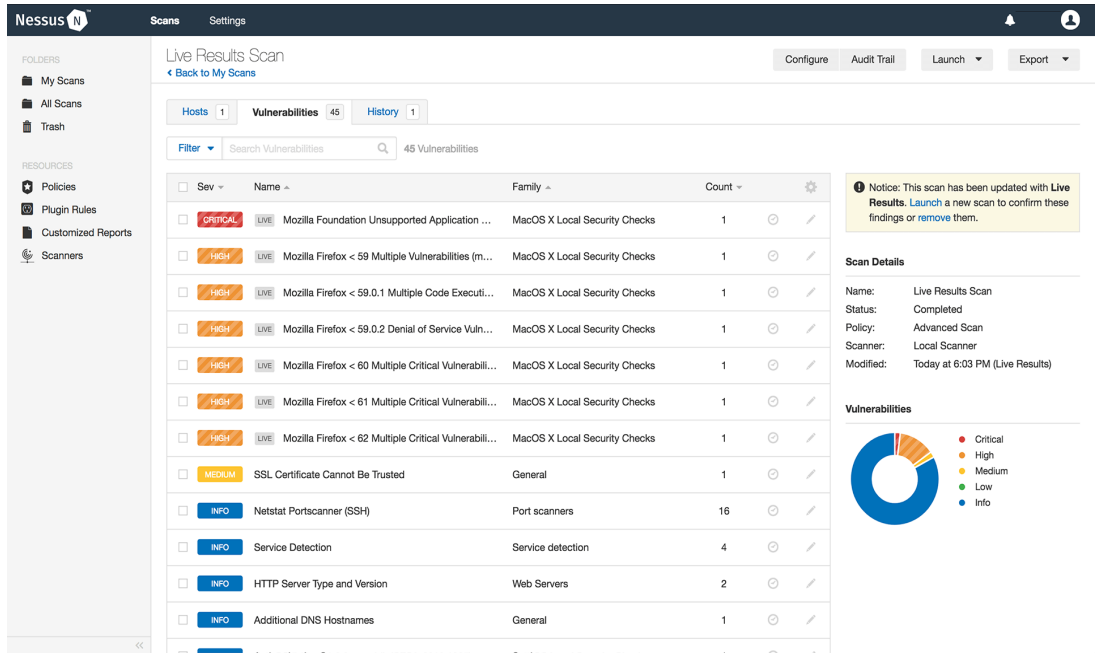




http://www.openvas.org/

Step 4: Monitor





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

Step 4: Monitor

6 Maintenance, Monitoring and Analysis of Audit Logs

16 Account Monitoring and Control

Step 4: Monitor

Security Onion

Full PCAP

netsniff-ng
the packet sniffing beast

NIDS/HIDS

Analysis/Presentation

Step 4: Monitor

1. Download ISO

https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md

Security-Onion-Solutions / security-onion

Watch 308 | Star 1,939 | Fork 320

Code | Issues 117 | Pull requests 0 | Projects 3 | Wiki | Insights

Join GitHub today

GitHub is home to over 31 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

Branch: master ▾ security-onion / Verify_ISO.md

Find file | Copy path

dougburks promote 16.04.5.6 to stable 9a24e32 on Jan 14

1 contributor

52 lines (39 sloc) | 1.83 KB

Raw | Blame | History

16.04.5.6 ISO image built on 2019/01/10

Download and Verify

16.04.5.6 ISO image:
https://github.com/Security-Onion-Solutions/security-onion/releases/download/v16.04.5.6_20190110/securityonion-16.04.5.6.iso

Signature for ISO image:
https://github.com/Security-Onion-Solutions/security-onion/raw/master/sigs/securityonion-16.04.5.6.iso.sig

Signing key:
https://raw.githubusercontent.com/Security-Onion-Solutions/security-onion/master/KEYS

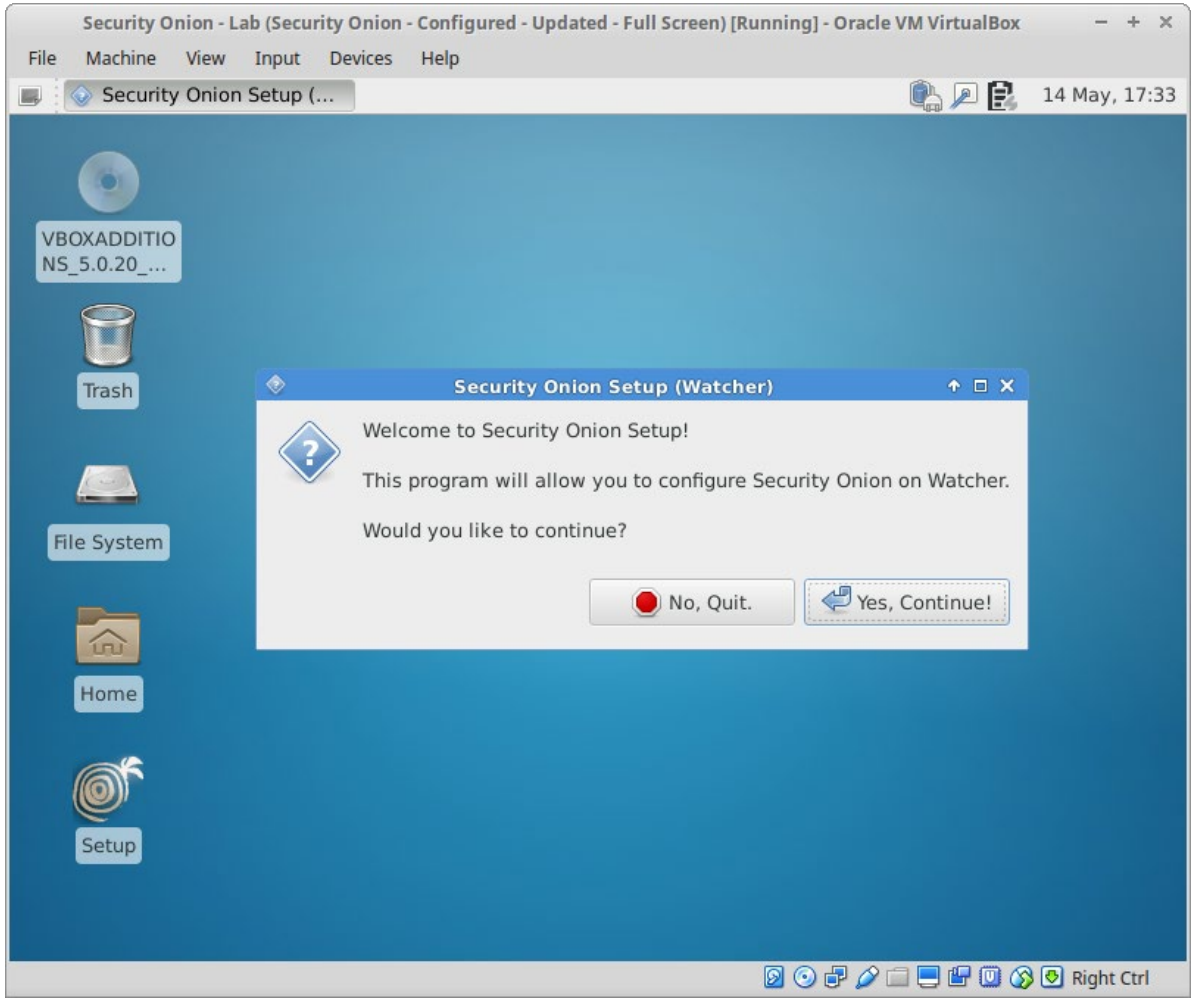
For example, here are the steps you can use on most Linux distributions to download and verify our Security Onion ISO image.

Step 4: Monitor

2. Install

Quick Install
https://securityonion.readthedocs.io/en/latest/QuickISOImage

Full Deployment Guide
https://securityonion.readthedocs.io/en/latest/ProductionDeployment

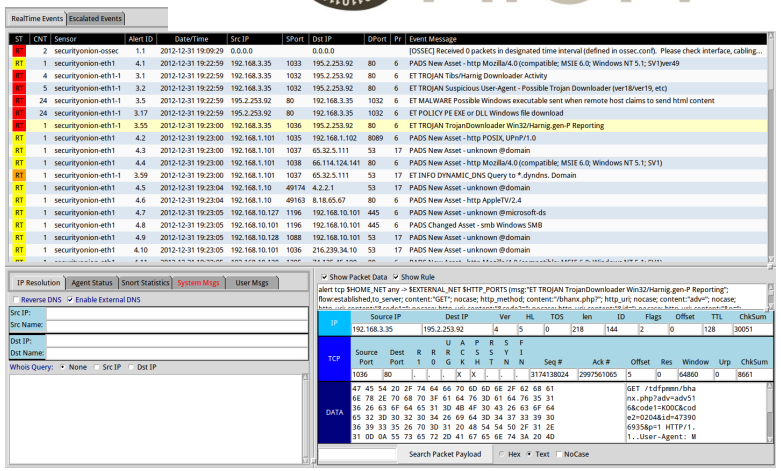


Step 4: Monitor

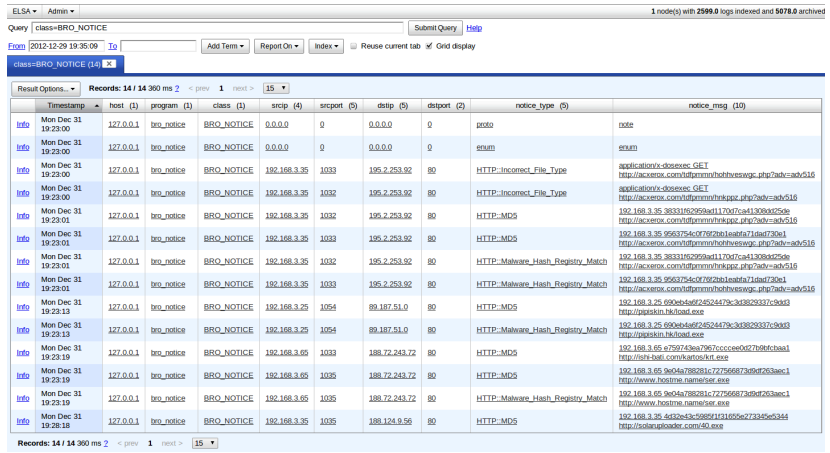
3. HAVE FUN!

Kibana

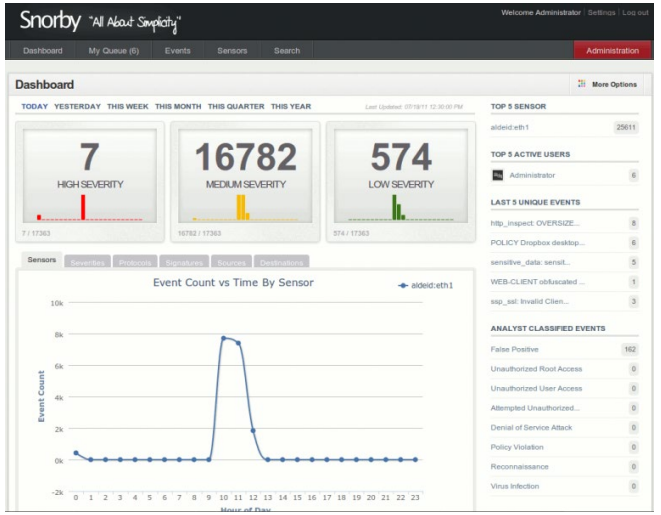
Sguil



ELSA

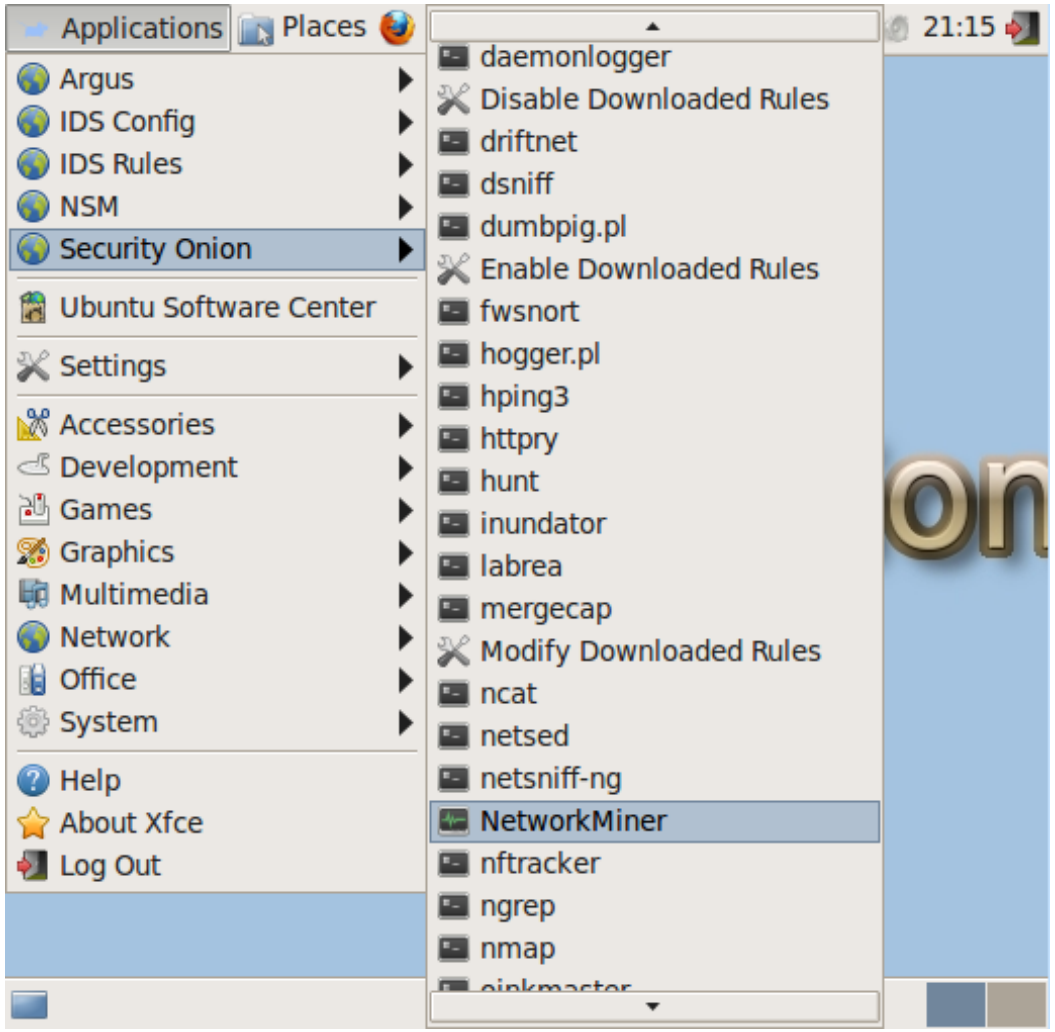


Snorby



Step 4: Monitor

3. HAVE FUN!



…and many more
(+60 tools)

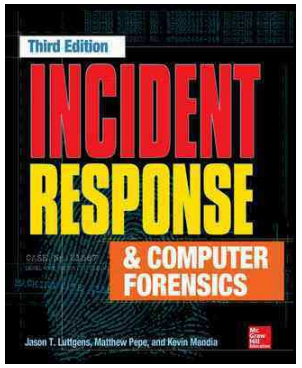
https://onlinetraining.securityonionsolutions.com/p/security-onion-101

Step 5: Homework

17 Implement a Security Awareness and Training Program

SANS SECURITY AWARENESS NEWSLETTER
OUCH!

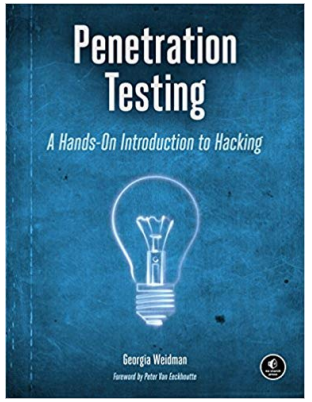
19 Incident Response and Management



18 Application Software Security

OWASP Mobile Security Project

20 Penetration Tests and Red Team Exercises



QUESTIONS?

RYAN@ACTIVEDEFENSE.US

@RY_WIZ

THANK YOU!