

Scrappling 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

Scraping for Pennies

Maturing to a Scalable Operation

Scaling the Mountain



Equifax data breach response...



EXECUTIVE PERSPECTIVE



SALES

- Advertising
- Sales Growth



R&D

- New Products
- New Efficiencies



FINANCE

- New Investments



IT

- New Efficiencies



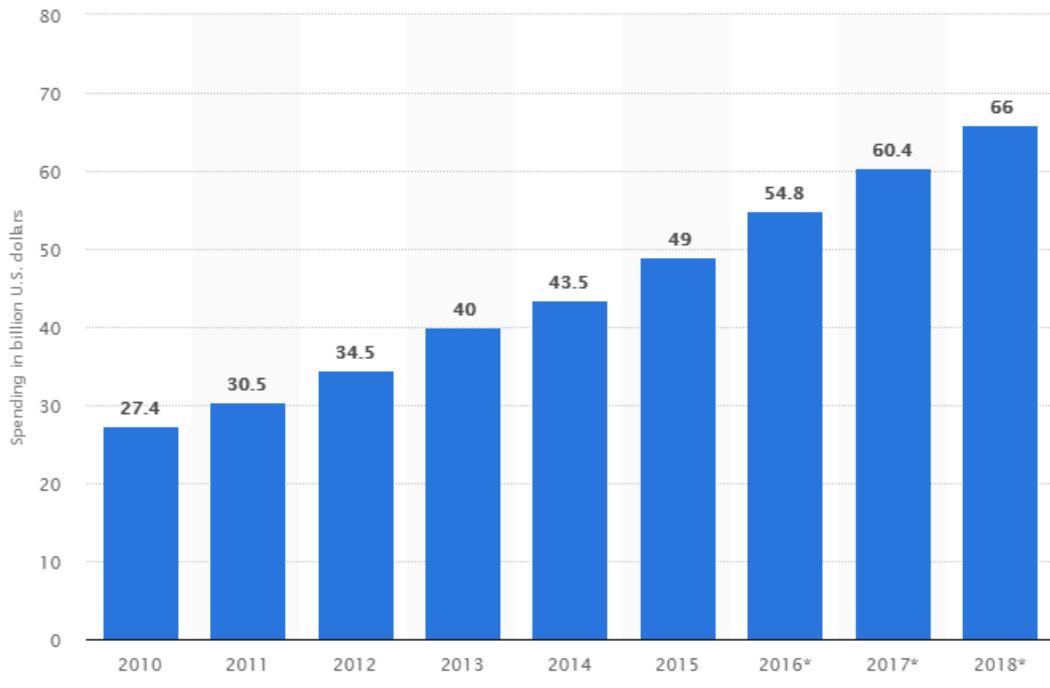
SECURITY

- ???



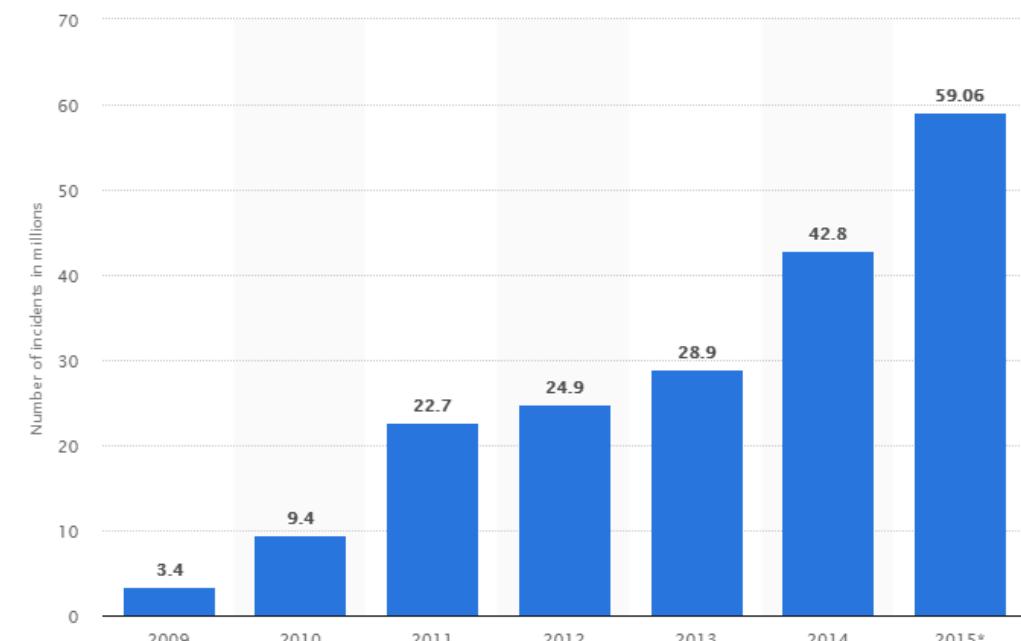
MORE INVESTMENT = PREVENT ATTACKS!

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



© Statista 2019

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



© Statista 2019

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...

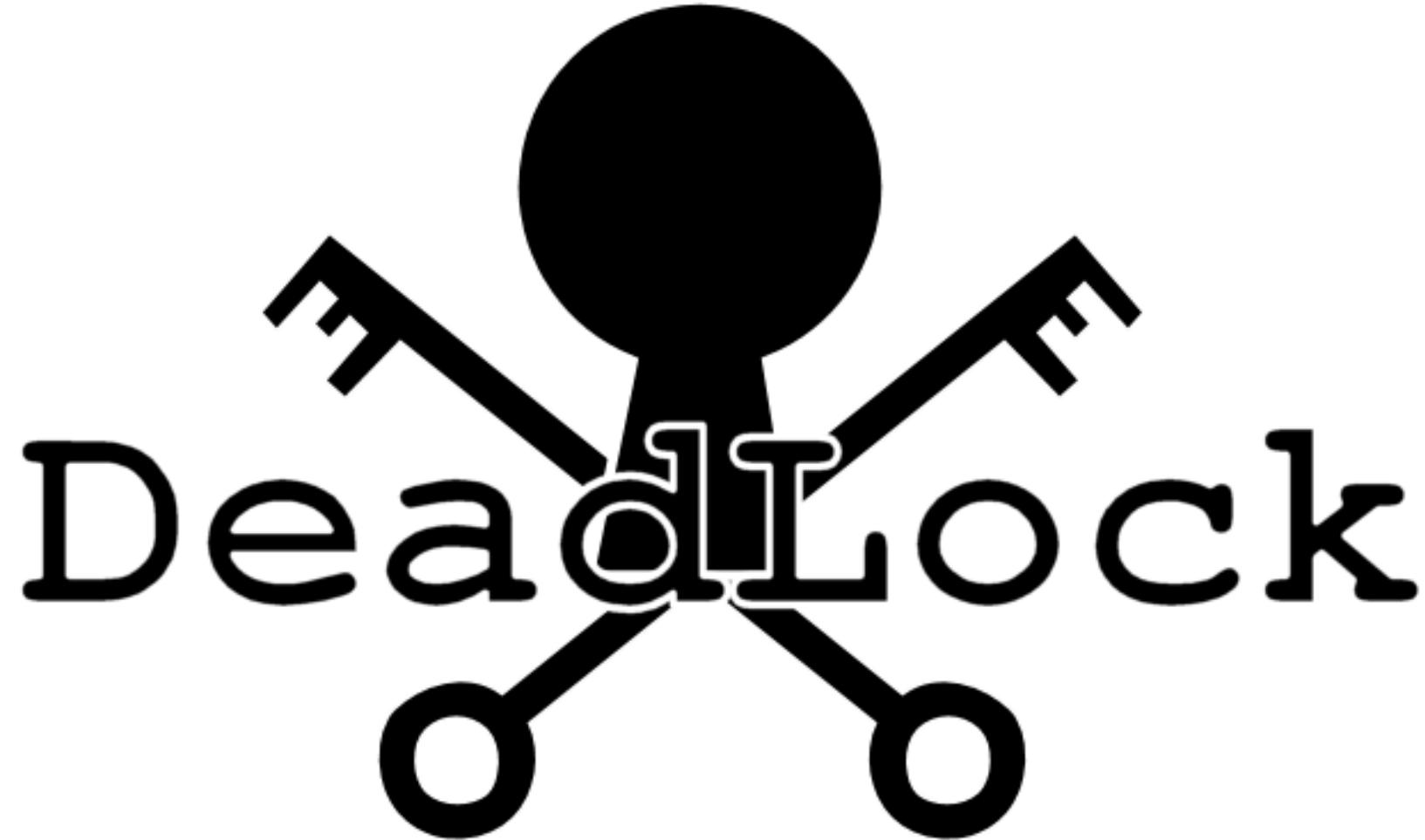
We investigate
650
Incidents/year

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!!!



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



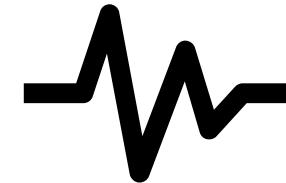
Step 1:
Discover



Step 2:
Define



Step 3:
Enforce



Step 4:
Monitor



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

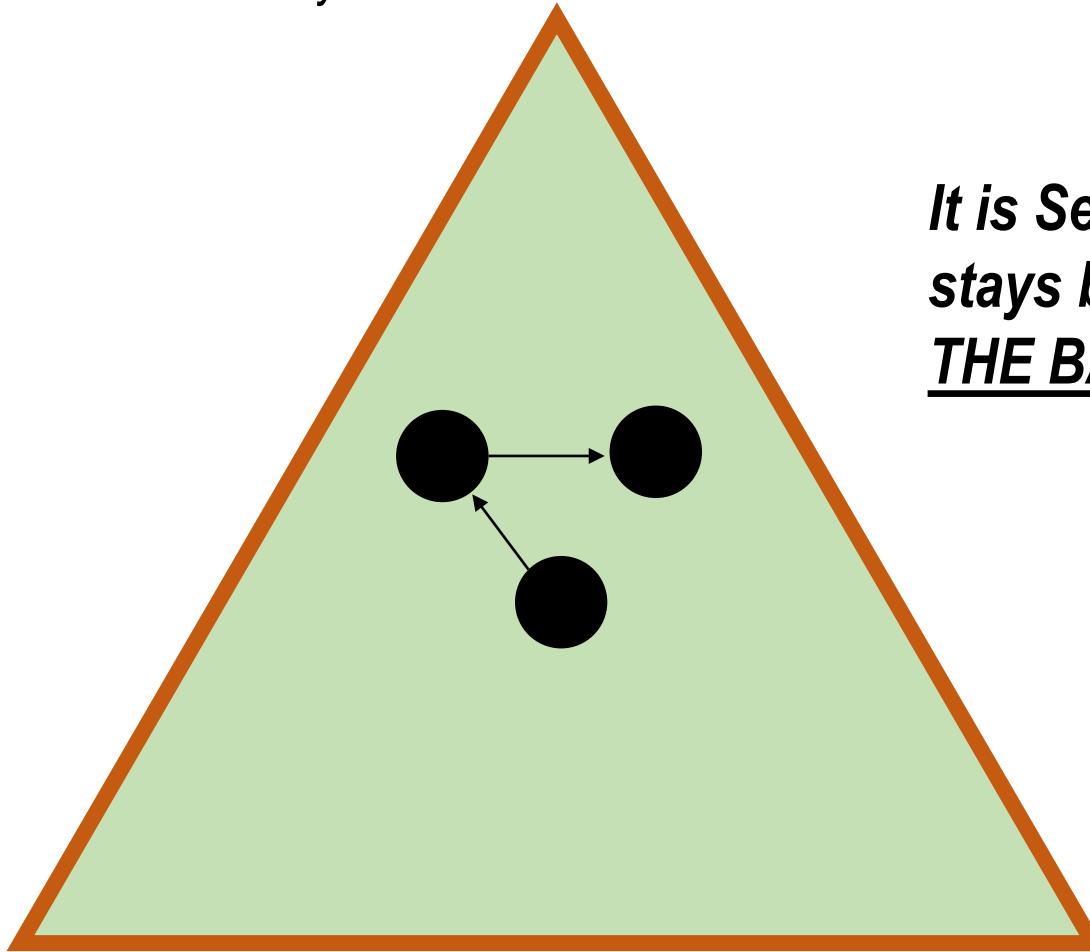
20 Penetration Tests and Red Team Exercises

Functionality

Systems do things for us

Convenience

Systems make our life easier



Security

Systems protect us

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

🔍 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?



NMAP



MASSCAN



PowerShell



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

🔍 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 --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:

Scan Top 100 ports from list:

Scan Specific Port (ie 22):

```
nmap -sP 10.10.10.0/24 -oA output  
nmap -F -iL list-of-ips.txt -oA output  
nmap -p 22 -iL list-of-ips.txt -oA output
```

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



Pingsweep:

Scan Specific Port (ie 22):

```
masscan 10.0.0.0/8 --ping -oL ips.txt  
masscan 10.0.0.0/8 -p 22 -oX output.xml
```

<https://github.com/robertdavidgraham/masscan>

<https://www.youtube.com/watch?v=nX9JXI4I3-E>

🔍 Step 1: Discover

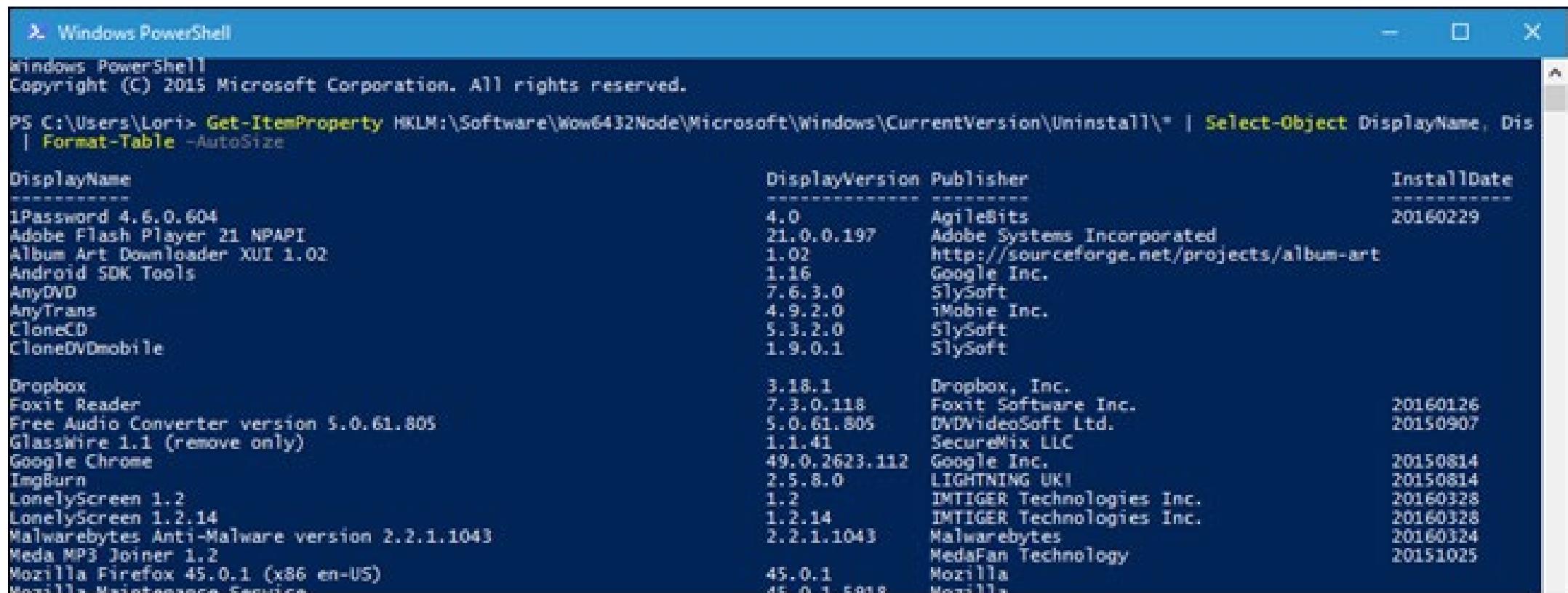
nmap_scan.csv - Excel

	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%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%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-header	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
```



The screenshot shows a Windows PowerShell window titled "Windows PowerShell". The command entered is:

```
PS C:\Users\Lori> Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, Dis | Format-Table -AutoSize
```

The output displays a table of installed software with columns: DisplayName, DisplayVersion, Publisher, and InstallDate.

DisplayName	DisplayVersion	Publisher	InstallDate
1Password 4.6.0.604	4.0	AgileBits	20160229
Adobe Flash Player 21 NPAPI	21.0.0.197	Adobe Systems Incorporated	
Album Art Downloader XUI 1.02	1.02	http://sourceforge.net/projects/album-art	
Android SDK Tools	1.16	Google Inc.	
AnyDVD	7.6.3.0	SlySoft	
AnyTrans	4.9.2.0	iMobile Inc.	
CloneCD	5.3.2.0	SlySoft	
CloneDVDmobile	1.9.0.1	SlySoft	
Dropbox	3.18.1	Dropbox, Inc.	
Foxit Reader	7.3.0.118	Foxit Software Inc.	20160126
Free Audio Converter version 5.0.61.805	5.0.61.805	DVDVideoSoft Ltd.	20150907
GlassWire 1.1 (remove only)	1.1.41	SecureMix LLC	
Google Chrome	49.0.2623.112	Google Inc.	20150814
ImgBurn	2.5.8.0	LIGHTNING UK!	20150814
LonelyScreen 1.2	1.2	IMTIGER Technologies Inc.	20160328
LonelyScreen 1.2.14	1.2.14	IMTIGER Technologies Inc.	20160328
Malwarebytes Anti-Malware version 2.2.1.1043	2.2.1.1043	Malwarebytes	20160324
Media MP3 Joiner 1.2		MediaFan Technology	
Mozilla Firefox 45.0.1 (x86 en-US)	45.0.1	Mozilla	20151025
Mozilla Maintenance Service	45.0.1.2016	Mozilla	



Step 2: Define

4 Controlled Use
of Administrative
Privileges

Privileged Account Usage Policy

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

Hardened Image for Clients and Servers

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

Network Security Framework

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

Hardened Image for Network Devices

14 Controlled Access
Based on the Need
to Know

Data Classification and Access Policy

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



Step 2: Define

4 Controlled Use
of Administrative
Privileges

Privileged Account Usage Policy

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Step 2: Define

4 Controlled Use
of Administrative
Privileges

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

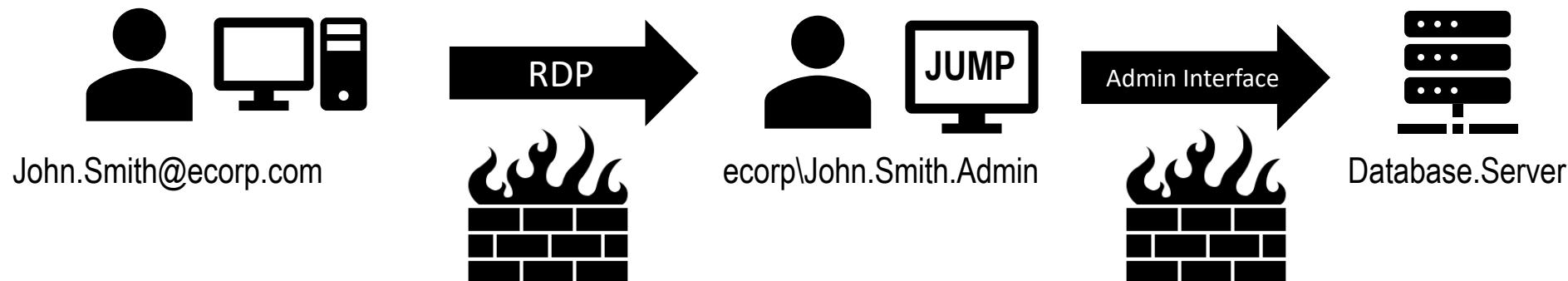
18

19

20

Privileged 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

Privileged Account Usage Policy

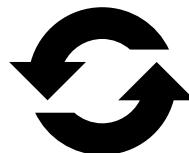
No default admin passwords



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!

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



Step 2: Define

4 Controlled Use
of Administrative
Privileges

Privileged Account Usage Policy

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

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      agreeen
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:\> -
```



Ronnie Flathers
@ropnop

[Follow](#)

Always remember that "net group /domain" doesn't show members that are groups. Might look like this domain only has 2 DAs, in fact it has 15

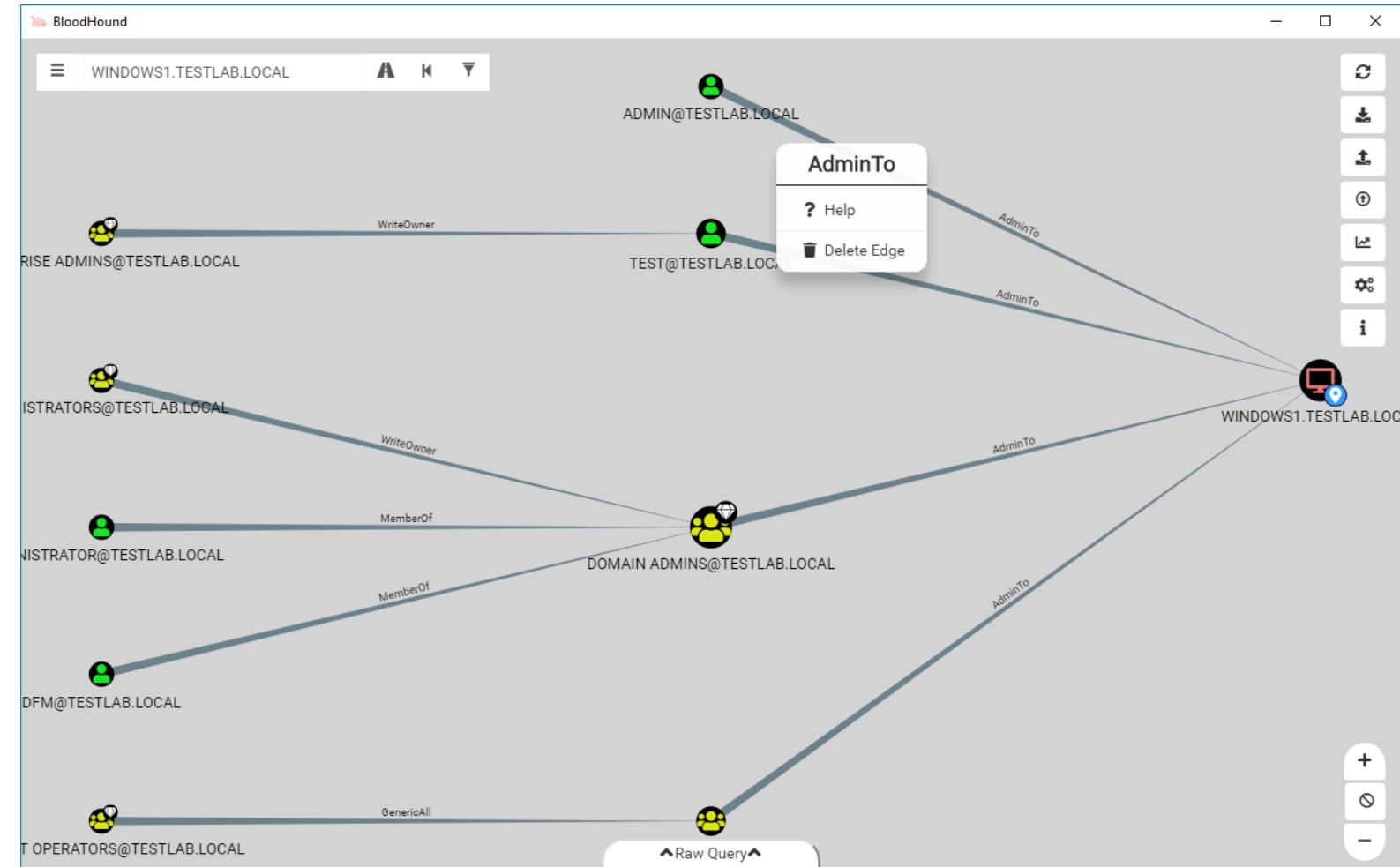
Step 2: Define

4 Controlled Use
of Administrative
Privileges

Privileged Account Usage Policy



<https://github.com/BloodHoundAD>



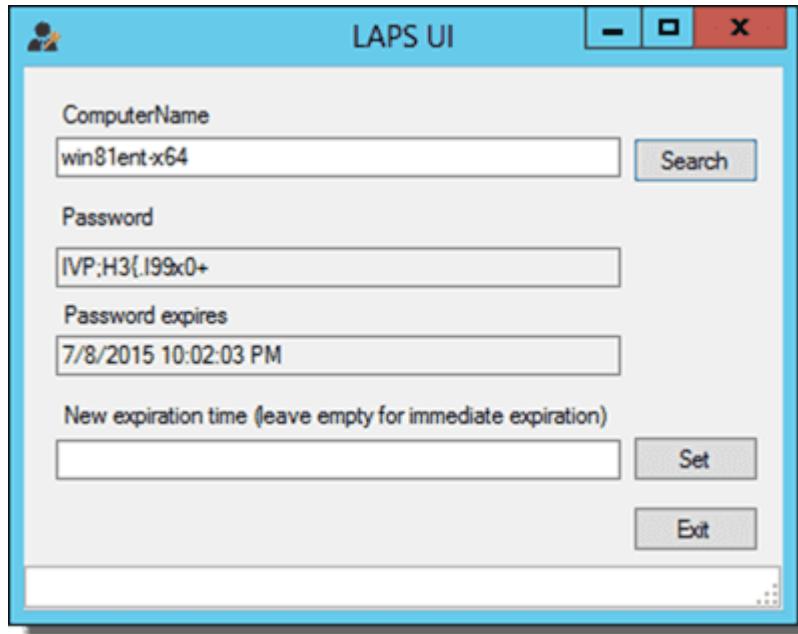


Step 2: Define

4 Controlled Use
of Administrative
Privileges

Privileged 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>

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



Step 2: Define

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

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

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20



Hardened Image for Clients and Servers

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:	<input type="text" value="Any....."/>	Content Type:	<input type="text" value="Any....."/>	Search	Reset
Authority:	<input type="text" value="Any....."/>	Tool Compatibility:	<input type="text" value="Any....."/>		
Target:	<input type="text" value="Microsoft Windows Server 2012 R2"/>	Keyword:	<input type="text"/>		

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	<ul style="list-style-type: none">- 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	E
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	BUILTIN Administrators, NT AUTHORITY AUTHENTICATED USERS
Access this computer from the network	
Act as part of the operating system	
Allow log on locally	BUILTIN Administrators
Allow log on through Terminal Services	BUILTIN Administrators
Backup files and directories	BUILTIN Administrators
Create a pagefile	BUILTIN Administrators
Create a token object	BUILTIN Administrators
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	BUILTIN Administrators
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`

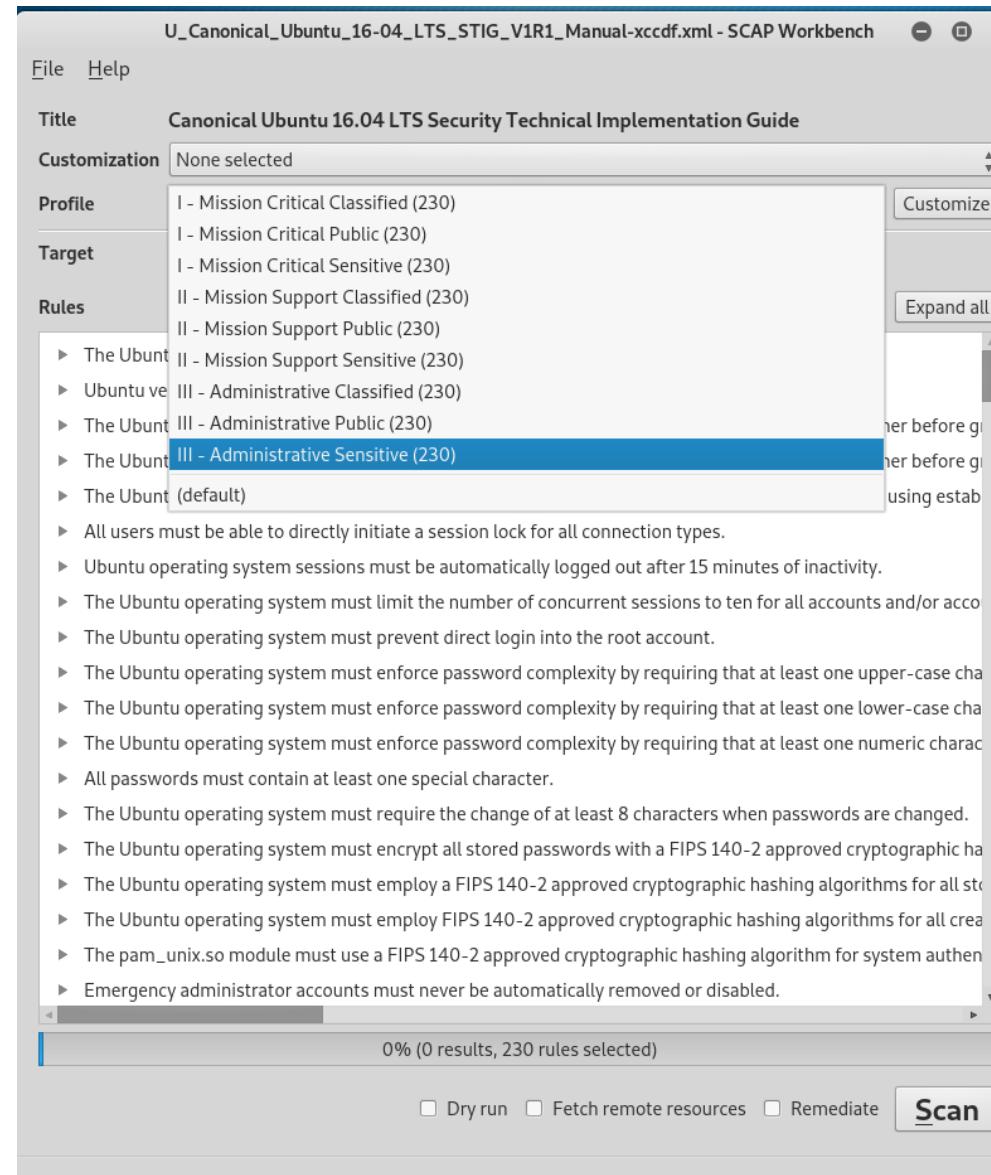


`yum install scap-workbench`

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/>

The screenshot shows the Qualys FreeScan interface for a SCAP audit. The top navigation bar includes the Qualys logo, a search bar with the URL <https://freescan.qualys.com/freescan-front/module/freescan/#scans>, and a dropdown menu for the user "Vanessa Follys". Below the header, the "Welcome Vanessa" message is displayed, along with a note about quickly verifying business security. A "More Results" link is on the left, and a "Take the trial" button is on the right. The main content area is titled "View by: SCAP Report Patch Report Threat Report" with "SCAP Report" selected. It shows a summary of the "SCAP scan on 01/28/2013" which was completed at 17:41 on January 28, 2013. The scan summary indicates 96.04% compliance. On the left, there's a box showing "227 Total rules". On the right, the target IP address is listed as "10.10.30.32" with the host name "client-XP-30-32.fdcc.ad.vuln.qa.qualys.com" and the operating system "Windows XP Service Pack 3". Below this, the "SCAP Checklist details" section provides benchmark information: "Benchmark: xccdf_gov.nist_benchmark_USGCB-Windows-XP", "Policy: USGCB: Guidance for Securing Microsoft Windows XP Systems", "Version: v1.2.3.1", "Published by: National Institute of Standards and Technology", "Status date: 02/23/2012", "CPE: cpe:/o:microsoft:windows_xp", and "Profile: xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1". At the bottom, a "Filter by:" section allows filtering by "All Rules (227)", "Compliant (218)", "Not Compliant (9)", and "Ignored (0)". The interface uses a light gray background with blue highlights for active tabs and buttons.

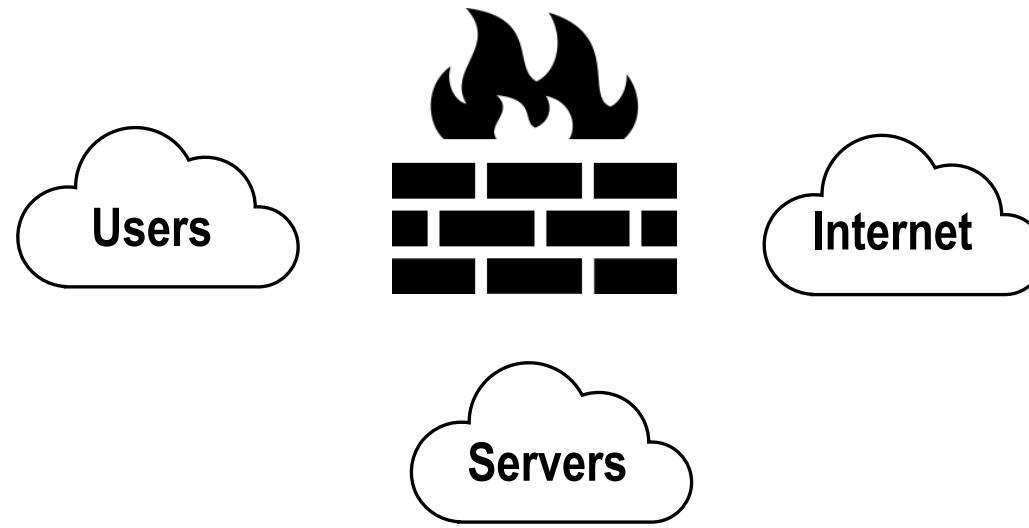


Step 2: Define

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

Network Security Framework

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



System-Concentric View

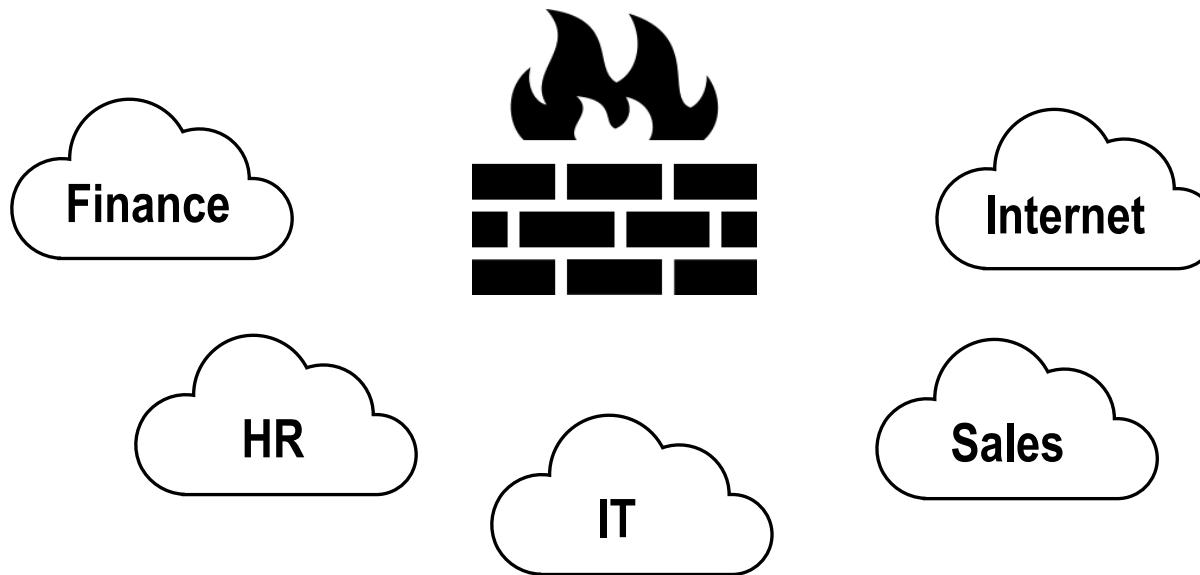


Step 2: Define

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

Network Security Framework

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



User-Concentric View



Step 2: Define

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

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

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

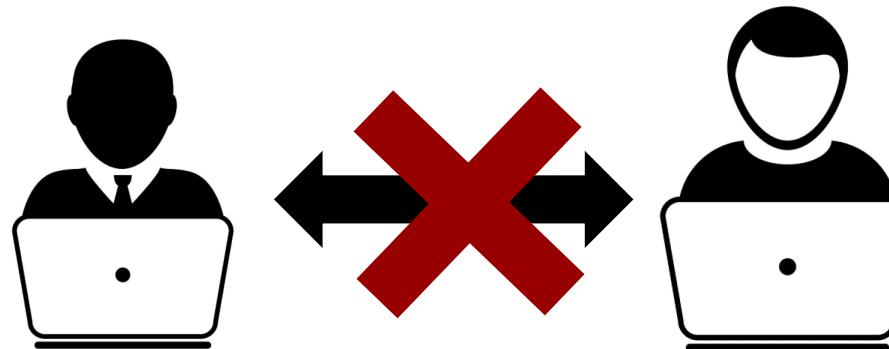
18

19

20

Network Security Framework

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

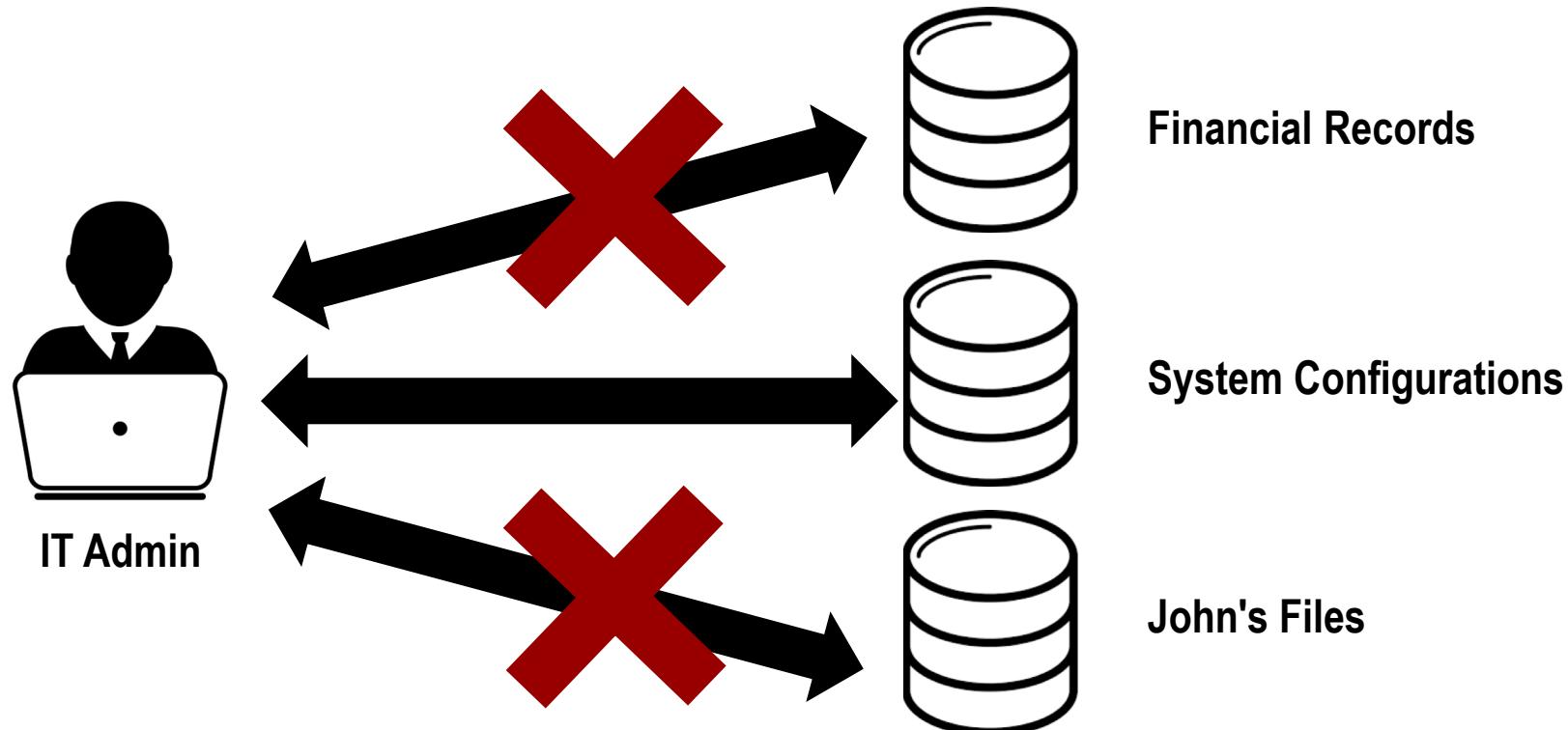




Step 2: Define

14 Controlled Access
Based on the Need
to Know

Data Classification and Access Policy



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



Step 2: Define

14 Controlled Access
Based on the Need
to Know

Data Classification and Access Policy

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

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

12 Boundary Defense

Implement firewalls on trust boundaries

13 Data Protection

Encrypt drives and disable writeable USBs

7 Email and Web Browser Protections

Implement DNS Filtering

10 Data Recovery Capabilities

Ensure Backups

8 Malware Defenses

Ensure your AV

15 Wireless Access Control

Ensure Secure Wireless Deployments

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

Step 3: Enforcement

12 Boundary Defense

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**

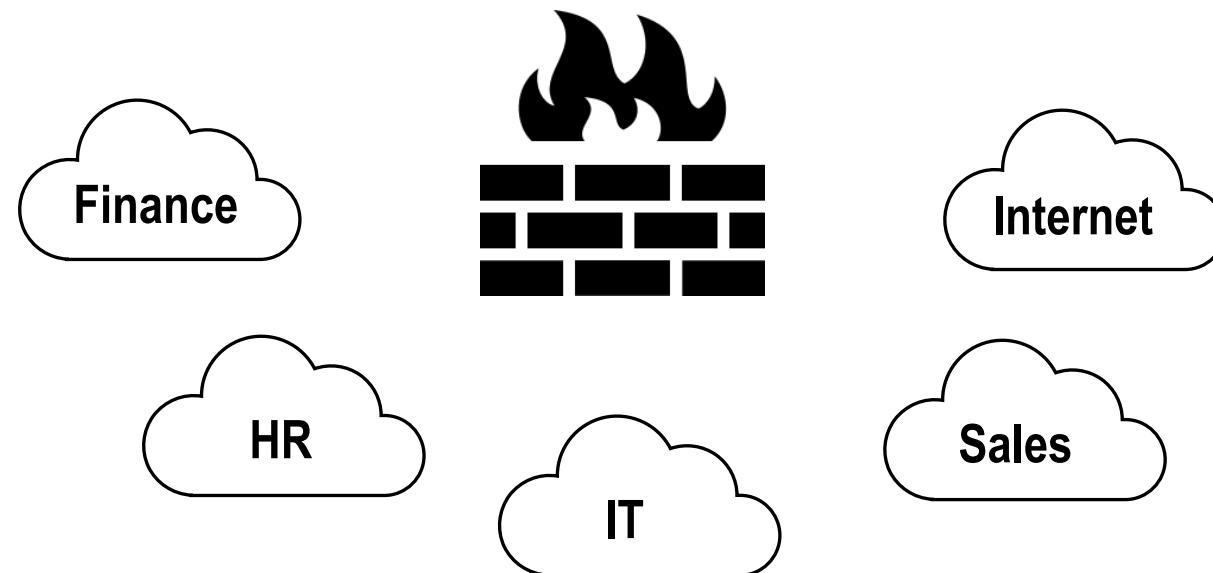
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Step 3: Enforcement

12 Boundary Defense

Implement firewalls on trust boundaries

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20





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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

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](#)

SHA256 Checksum for compressed (.gz) file:
a5ca11eab11e2cdc33a11ded4df69eab7ae48399004588562f5f305ae3c0246

Supported by netgate

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](#))



2. Install

ESX Guide

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

Hyper-V Guide

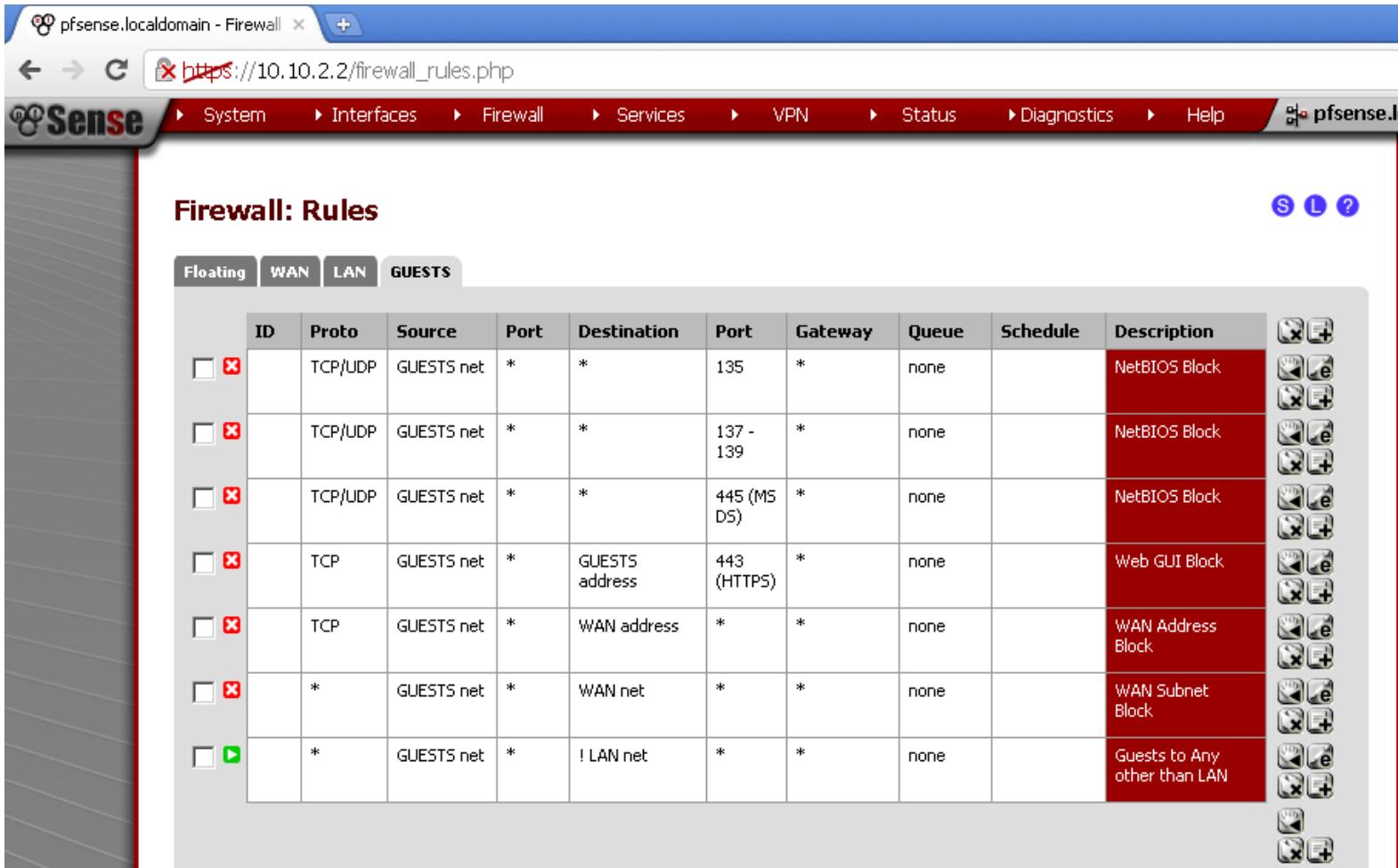
<https://docs.netgate.com/pfsense/en/latest/virtualization/virtualizing-pfsense-with-hyper-v.html>

Bare Metal Guide

<https://docs.netgate.com/pfsense/en/latest/install/installing-pfsense.html>



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



The screenshot shows the PFSense Firewall Rules configuration page. The URL in the browser is https://10.10.2.2/firewall_rules.php. The navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a pfSense logo. The main title is "Firewall: Rules". Below it, there are tabs for Floating, WAN, LAN, and GUESTS, with GUESTS selected. The table lists the following rules:

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action
	TCP/UDP	GUESTS net	*	*	135	*	none		NetBIOS Block	 
	TCP/UDP	GUESTS net	*	*	137 - 139	*	none		NetBIOS Block	 
	TCP/UDP	GUESTS net	*	*	445 (MS DS)	*	none		NetBIOS Block	 
	TCP	GUESTS net	*	GUESTS address	443 (HTTPS)	*	none		Web GUI Block	 
	TCP	GUESTS net	*	WAN address	*	*	none		WAN Address Block	 
	*	GUESTS net	*	WAN net	*	*	none		WAN Subnet Block	 
	*	GUESTS net	*	! LAN net	*	*	none		Guests to Any other than LAN	 

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Step 3: Enforcement

13 Data Protection

Encrypt drives and disable writeable USBs

- Encrypt client hard drives
- No writing to external drives

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

Step 3: Enforcement

☐ Encrypt client hard drives

GPO:

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

The screenshot shows the Group Policy Management Editor window. The left pane displays a navigation tree under 'BitLocker [WIN-BUQ4IBVF3I8.EXAMPLE.COM]'. The 'BitLocker Drive Encryption' node is selected and expanded, showing sub-categories: Fixed Data Drives, Operating System Drives, Removable Data Drives, and Camera. The right pane is a table titled 'Setting' with columns for 'Setting', 'State', and 'Comment'. It lists nine policy settings, all of which are currently 'Not configu...' and marked 'No' in the 'Comment' column. The table has a header row with three columns: Setting, State, and Comment.

Setting	State	Comment
Fixed Data Drives	Not configu...	No
Operating System Drives	Not configu...	No
Removable Data Drives	Not configu...	No
Store BitLocker recovery information in Active ...	Not configu...	No
Choose default folder for recovery password	Not configu...	No
Choose how users can recover BitLocker-protect...	Not configu...	No
Choose drive encryption method and cipher str...	Not configu...	No
Choose drive encryption method and cipher str...	Not configu...	No
Choose drive encryption method and cipher str...	Not configu...	No
Provide the unique identifiers for your organizat...	Not configu...	No
Prevent memory overwrite on restart	Not configu...	No
Validate smart card certificate usage rule compl...	Not configu...	No

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Step 3: Enforcement

No writing to external drives

GPO:

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

The screenshot shows the Group Policy Management Editor window. The left pane displays the navigation tree under Computer Configuration / Policies / Administrative Templates / System. The 'Removable Storage Access' folder is selected. The right pane shows a table of 19 settings, all of which are currently 'Not configured' and have a comment of 'No'. The table has columns for Setting, State, and Comment.

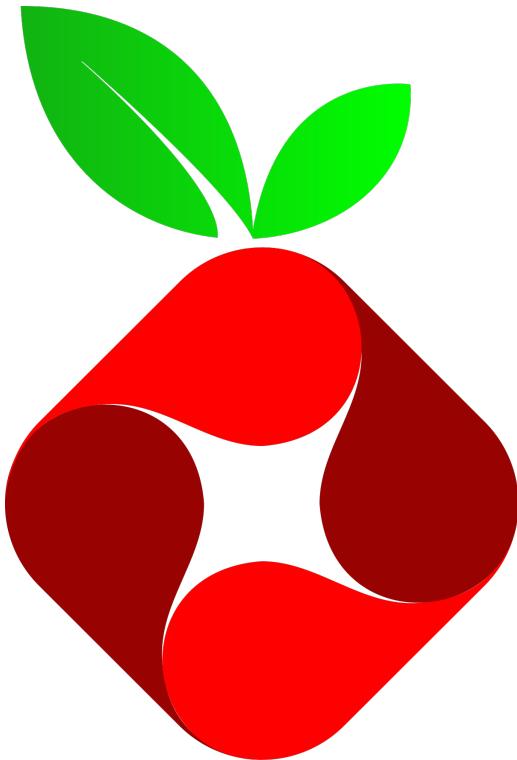
Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny execute access	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
All Removable Storage: Allow direct access in remote sessions	Not configured	No
Tape Drives: Deny execute access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Step 3: Enforcement

7 Email and Web
Browser Protections

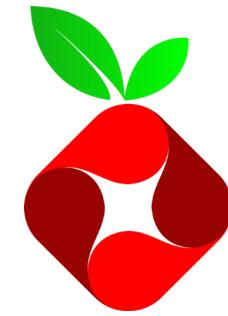
Implement DNS Filtering



Pi-hole

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

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>

Enabled	List	Delete
<input checked="" type="checkbox"/>	https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts	
<input checked="" type="checkbox"/>	https://mirror1.malwaredomains.com/files/justdomains	
<input checked="" type="checkbox"/>	http://sysctl.org/cameleon/hosts	
<input checked="" type="checkbox"/>	https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist	
<input checked="" type="checkbox"/>	https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt	
<input checked="" type="checkbox"/>	https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt	
<input checked="" type="checkbox"/>	https://hosts-file.net/ad_servers.txt	
<input checked="" type="checkbox"/>	https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienVault_reputation.ipset	
<input checked="" type="checkbox"/>	https://s3.amazonaws.com/lists.disconnect.me/simple_malvertising.txt	
<input checked="" type="checkbox"/>	https://hosts-file.net/exp.txt	
<input checked="" type="checkbox"/>	https://hosts-file.net/edn.txt	
<input checked="" type="checkbox"/>	https://hosts-file.net/psh.txt	
<input checked="" type="checkbox"/>	https://mirror.cedia.org.ec/malwaredomains/immortal_domains.txt	
<input checked="" type="checkbox"/>	https://www.malwaredomainlist.com/hostslist/hosts.txt	
<input checked="" type="checkbox"/>	https://bitbucket.org/ethanr/dns-blocklists/raw/8575c9f96e5b4a1308f2f12394abd86d0927a4a0/bad_lists/Mandiant_APT1_Report_Appendix_D.txt	

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

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



© Black Hills Information Security | @BHInfoSecurity



Step 4: Monitor

3 Continuous Vulnerability Management



OpenVAS
Open Vulnerability Assessment System

6 Maintenance, Monitoring and Analysis of Audit Logs



16 Account Monitoring and Control



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

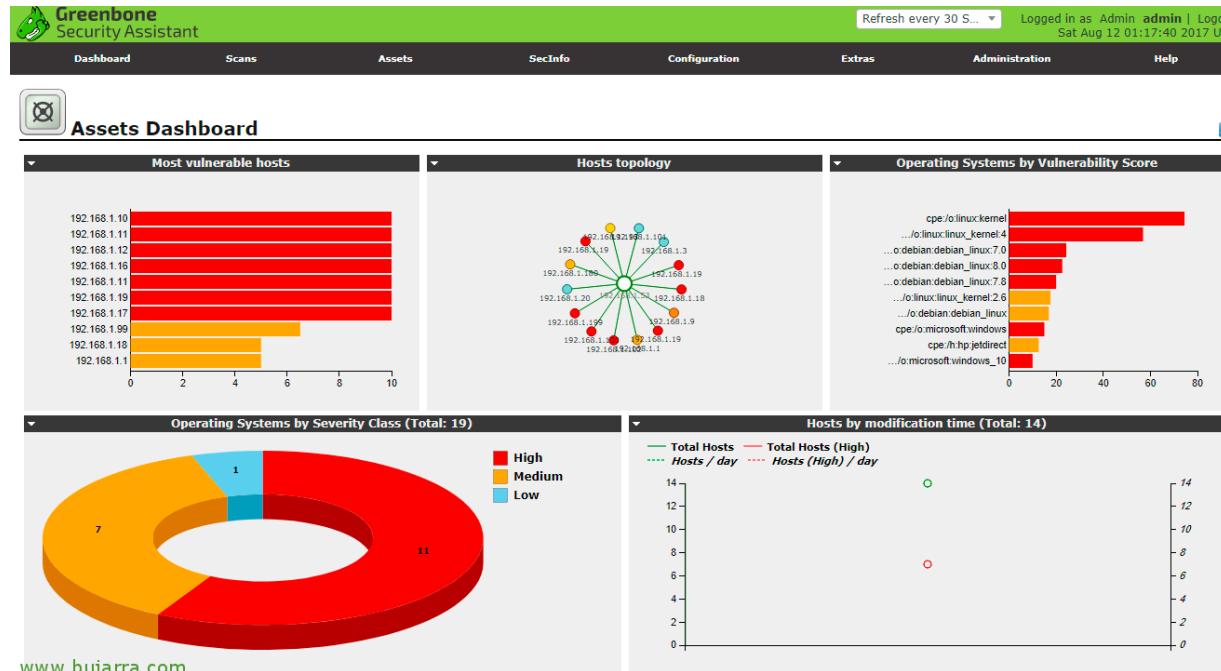
Step 4: Monitor

3 Continuous
Vulnerability
Management



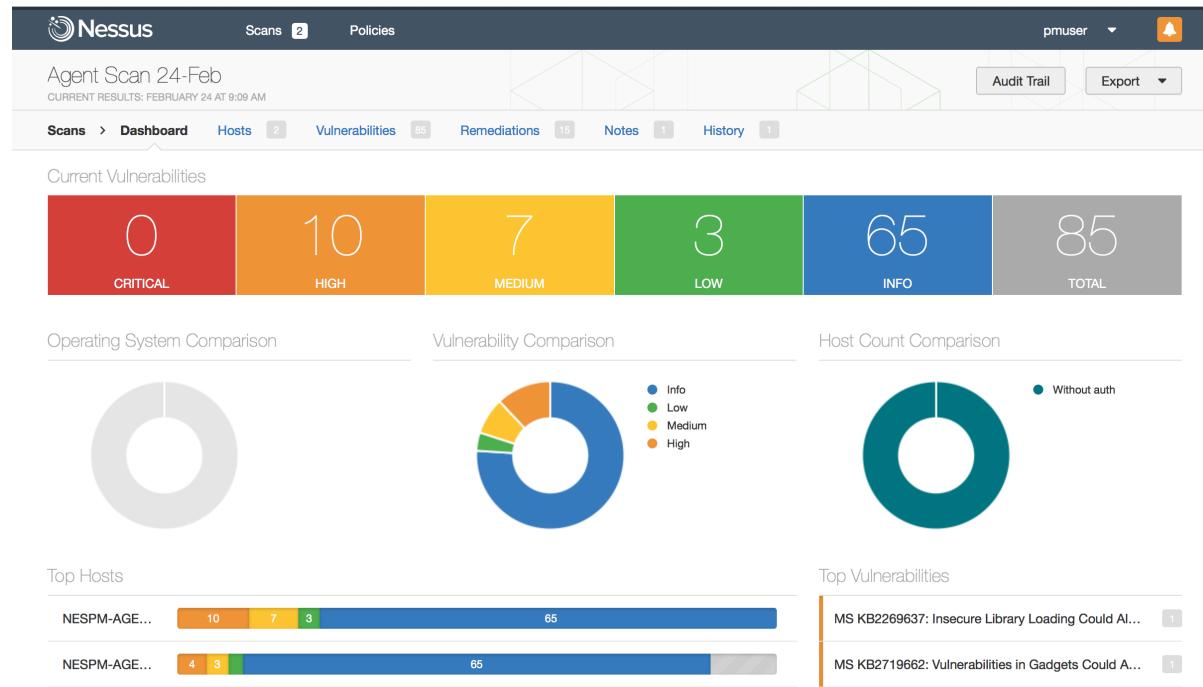
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Step 4: Monitor



<http://www.openvas.org/>

Step 4: Monitor

A screenshot of the Nessus scan results interface. It shows a sidebar with "Folders" (My Scans, All Scans, Trash), "Resources" (Policies, Plugin Rules, Customized Reports, Scanners), and "Scans" (Live Results Scan). The main area is titled "Live Results Scan" and shows a table of vulnerabilities. The table includes columns for Severity (CRITICAL, HIGH, MEDIUM, LOW, INFO), Status (LIVE), Name, Family, and Count. A note says "Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them." To the right, "Scan Details" show the scan was named "Live Results Scan", completed, used an Advanced Scan policy, a Local Scanner, and was modified today at 6:03 PM. A "Vulnerabilities" donut chart is also present.

Scans Settings
Live Results Scan Back to My Scans
Hosts 1 Vulnerabilities 45 History 1
Filter Search Vulnerabilities 45 Vulnerabilities
Sev Name Family Count
CRITICAL Mozilla Foundation Unsupported Application ... MacOS X Local Security Checks 1
HIGH Mozilla Firefox < 59 Multiple Vulnerabilities (m... MacOS X Local Security Checks 1
HIGH Mozilla Firefox < 59.0.1 Multiple Code Executi... MacOS X Local Security Checks 1
HIGH Mozilla Firefox < 59.0.2 Denial of Service Vuln... MacOS X Local Security Checks 1
HIGH Mozilla Firefox < 60 Multiple Critical Vulnerabil... MacOS X Local Security Checks 1
HIGH Mozilla Firefox < 61 Multiple Critical Vulnerabil... MacOS X Local Security Checks 1
HIGH Mozilla Firefox < 62 Multiple Critical Vulnerabil... MacOS X Local Security Checks 1
MEDIUM SSL Certificate Cannot Be Trusted General 1
INFO Netstat Portscanner (SSH) Port scanners 16
INFO Service Detection Service detection 4
INFO HTTP Server Type and Version Web Servers 2
INFO Additional DNS Hostnames General 1
Name: Live Results Scan Status: Completed Policy: Advanced Scan Scanner: Local Scanner Modified: Today at 6:03 PM (Live Results)
Vulnerabilities

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

Step 4: Monitor

6 Maintenance,
Monitoring and
Analysis of Audit
Logs

16 Account Monitoring
and Control

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

Security
union



Step 4: Monitor



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

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

The screenshot shows a GitHub repository page for 'security-onion'. The top navigation bar includes 'Code', 'Issues 117', 'Pull requests 0', 'Projects 3', 'Wiki', and 'Insights'. Below the navigation is a 'Join GitHub today' banner with a 'Sign up' button. The main content area displays a file named 'Verify_ISO.md' from the 'master' branch. The file content includes:

```
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.
```

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

Step 4: Monitor

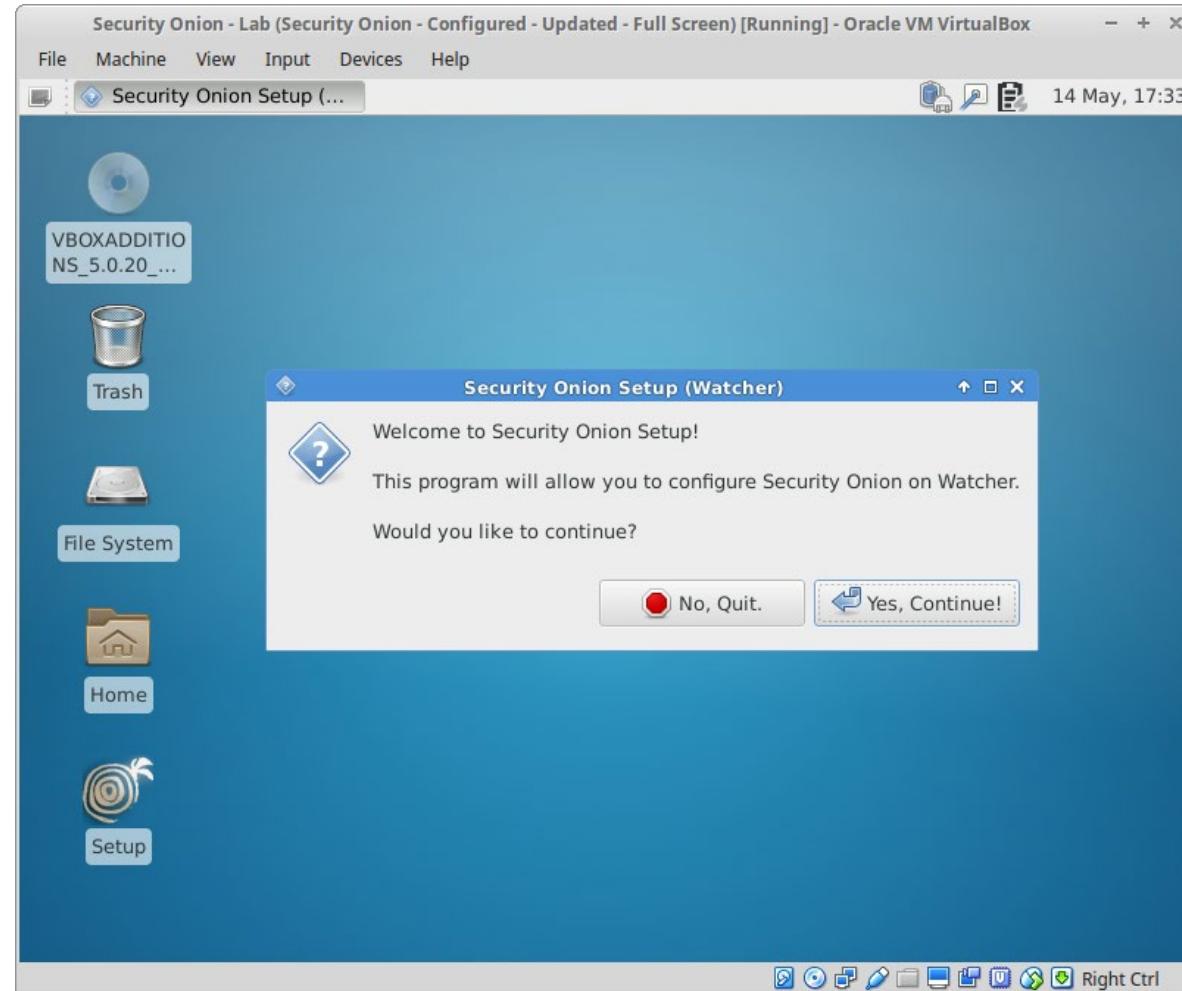
2. Install

Quick Install

<https://securityonion.readthedocs.io/en/latest/QuickISOImage>

Full Deployment Guide

<https://securityonion.readthedocs.io/en/latest/ProductionDeployment>



- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

Step 4: Monitor

3. HAVE FUN!



ELSA

Security Union

Sguil

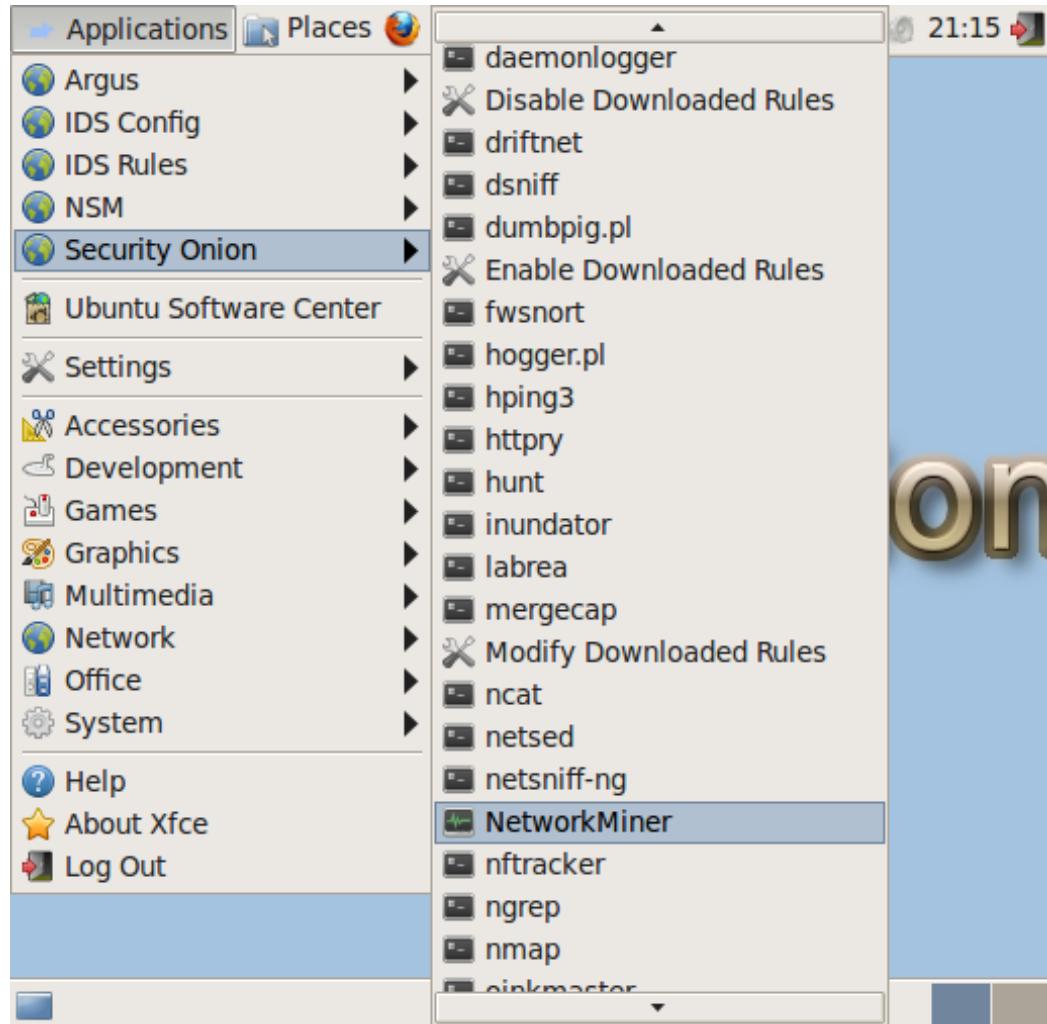
The screenshot shows the Snorby dashboard with the following details:

- Header:** Welcome Administrator | Settings | Log out
- Top Navigation:** Dashboard, My Queue (6), Events, Sensors, Search, Administration
- Section: Dashboard**
 - TODAY, YESTERDAY, THIS WEEK, THIS MONTH, THIS QUARTER, THIS YEAR
 - Last Updated: 03/19/11 12:30:00 PM
- Three large boxes showing event counts:**
 - 7 HIGH SEVERITY (7 / 17363)
 - 16782 MEDIUM SEVERITY (16782 / 17363)
 - 574 LOW SEVERITY (574 / 17363)
- Sensors Tab:** Sensors, Sensors, Protocols, Signatures, Sources, Destinations
- Event Count vs Time By Sensor:** A line graph showing event counts over time for sensor eth1. The y-axis ranges from 0K to 10K. The x-axis shows dates from March 1 to March 23. The graph shows a sharp peak around March 11.
- Right Sidebar:**
 - TOP 5 SENSOR**
 - alideid:eth1 25611
 - TOP 5 ACTIVE USERS**
 - Administrator 6
 - LAST 5 UNIQUE EVENTS**
 - http_inspect_OVERFLOW_... 8
 - POLICY Dropbox desktop_... 6
 - sensitive_date:obfuscate_... 5
 - WEB-CLIENT obfuscated_... 1
 - sig_ip: invalid Client... 3
 - ANALYST CLASSIFIED EVENTS**
 - False Positive 162
 - Unauthorized Root Access 0
 - Unauthorized User Access 0
 - Attempted Unauthorized... 0
 - Denial of Service Attack 0
 - Policy Violation 0
 - Reconnaissance 0
 - Virus Infection 0

Snorby

Step 4: Monitor

3. HAVE FUN!



...and many more
(+60 tools)

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

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20

Step 5: Homework

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

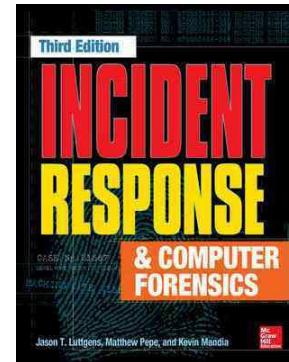
17 Implement a Security Awareness and Training Program



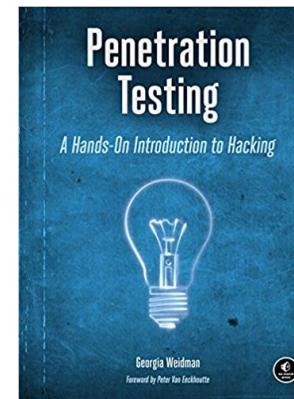
18 Application Software Security



19 Incident Response and Management



20 Penetration Tests and Red Team Exercises



QUESTIONS?



✉ RYAN@ACTIVEDEFENSE.US

🐦 @RY_WIZ

THANK YOU!