



# CONTINUOUS NETWORK AUDIT

NICHOLAS CARROLL

ISACA TALLAHASSEE

JUNE 2018

# FISMA

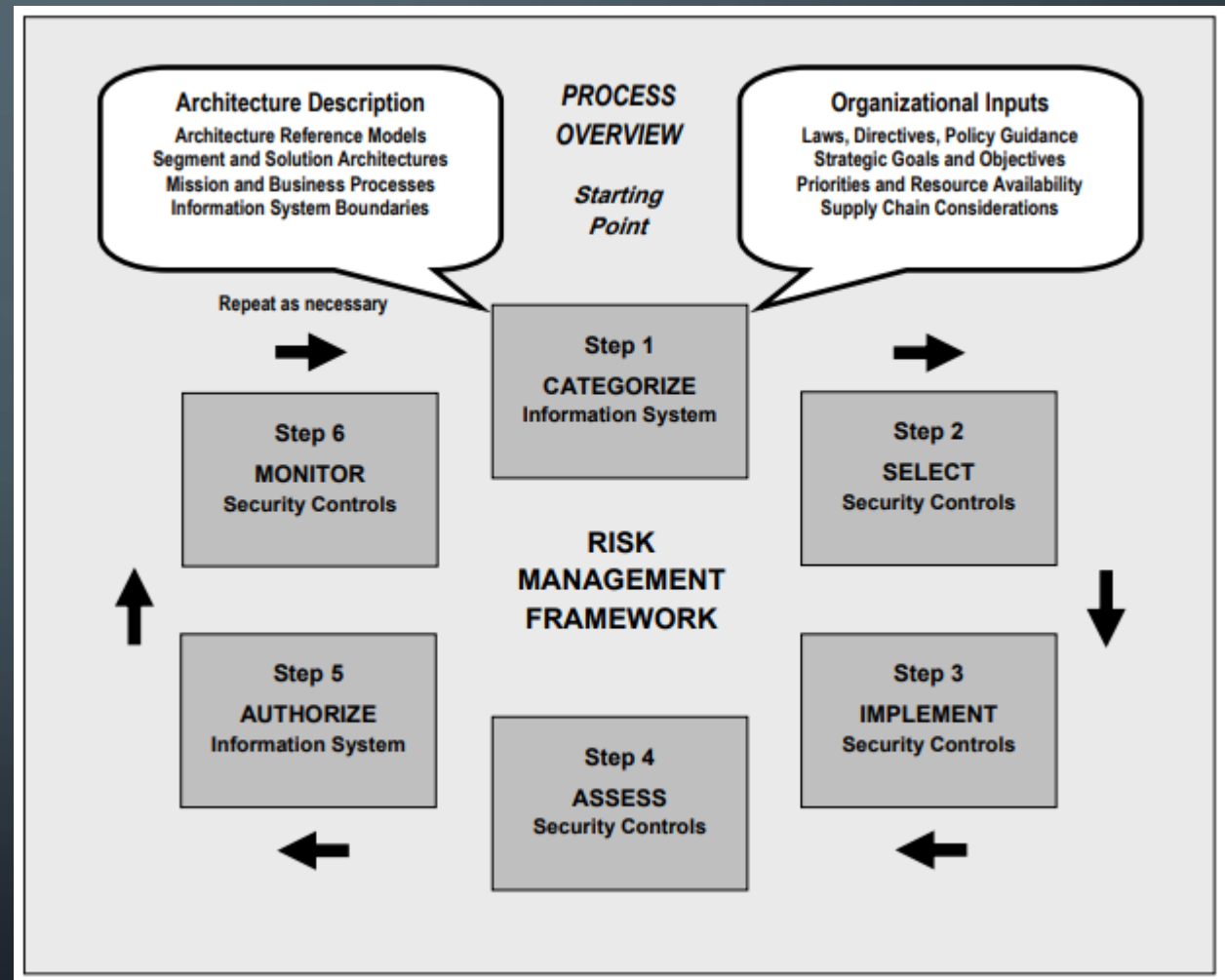
- Federal Information Security Management Act
- Originally laid out in 2002 as part of the Electronic Government Act
- Called for continuous monitoring with a major focus on compliance for Federal agencies
- Updated in 2014 to re-emphasize continuous monitoring over simple “check the box” compliance

# FISMA

- Requirements now include...
  - “the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.”
- We must become *proactive* and move beyond summary data with our audits

# NIST 800-37

- Incorporates the FISMA continuous monitoring standard as part of the RMF
- Monitoring and auditing must become regular parts of our lives



# AUDIT BEYOND EVERY NOW AND THEN...

- Many organizations are still auditing once a year, or maybe once a quarter
- Often a staffing or budget issue, but we can all move beyond this point with a little extra effort
- Many of you already have SIEMs and excellent policies and tools in place, but if you don't, here's a few ideas to help you take a more proactive approach to your testing...

# LAYOUT YOUR OWN FRAMEWORK

- If you haven't already, make sure you are using some sort of plan
- Keep it as simple as possible...
  - 1. Set your scope
    - Internal and external hosts, Software in use, etc.
  - 2. Define the threats to your organization
    - Malware, Insiders, Natural disasters, etc.
  - 3. Prioritize your risks
    - Look at trends, Compliance needs, Organization history, etc.
  - 4. Check your current posture
    - Mind your gaps!
  - 5. Create automated responses
    - Runbooks for CIRST employees to follow, Continuous monitoring tools, etc.

# AUTOMATION IS KEY


- The more we automate, the less our burden
- This may have some upfront administrative cost, but it can pay dividends
- How you automate depends on your organizations needs and the tools you use
- We'll take a high level overview of some ideas and examples for automation
- Everything mentioned today has been compiled at...
- <https://github.com/ContinuousAudit/ISACA>

# POWERSHELL

- Handy if you're in a primarily Windows environment
- Most things you can think of have been written for you!
- Easy to write for, modify existing scripts to match, and works great for automation
- Can be set for output to generate alert emails, CSVs for easy Excel reports, etc.
- Check out...
  - <https://gallery.technet.microsoft.com/>
  - <https://blogs.technet.microsoft.com/heyscriptingguy/>



# POWERSHELL – GPO REPORT

- Let's start with something simple; the report for our current GPOs
  - [https://github.com/ContinuousAudit/ISACA/blob/master/GPO\\_Report.ps1](https://github.com/ContinuousAudit/ISACA/blob/master/GPO_Report.ps1)
- Open PowerShell ISE
- Start a New Script (  )
- Paste in the report script from the GitHub and change the domain parameter

```
Untitled1.ps1* X
1 Import-Module ActiveDirectory
2 Import-Module GroupPolicy
3 $dc = Get-ADDomainController -Discover -Service PrimaryDC
4 Get-GPOReport -All -Domain your.domain -Server $dc -ReportType HTML -Path C:\Temp\GPOReportsAll.html
```

- Run it by pressing F5 or 

# POWERSHELL – GPO REPORT

- Now go open your report in C:\temp
- We can combine PowerShell, Task Scheduler, email, and more to minimize the need to manually pull such information
- Let's look at a slightly more involved example

Domain Password Policy	
Data collected on: 3/25/2016 12:05:45 PM	
General	
Computer Configuration (Enabled)	
Policies/Windows Settings/Security Settings/Account Policies/Password Policy	
Policy	Setting
Enforce password history	12 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Enabled

# POWERSHELL – ACCOUNT LOCKOUT

- Here's a Technet script to email you whenever someone's account locks out
  - [https://github.com/ContinuousAudit/ISACA/blob/master/account\\_locked\\_out.ps1](https://github.com/ContinuousAudit/ISACA/blob/master/account_locked_out.ps1)
- Anyone on the receiving end gets an email that looks like this:

## User is locked in the Active Directory

Account name	Account Domain	Caller Computer Name	Date
TEST	TEST-DOMAIN	PCTEST	16-4-2013 9:53:41

- Setup Task Scheduler to call the script on a DC with a trigger on EventID 4740
- Task should call the application PowerShell with arguments that match the script name
- Ex. - powershell -command "& 'C:\Powershell\account\_locked\_out.ps1' "

# POWERSHELL – ACCOUNT LOCKOUT

- Change “smtp.yoursmtpserver” to be your email server’s name or IP
- Set the from address to your liking
- Set the to addresses to your liking



```
$Report= "c:\powershell\html.html"

$HTML=@"
<title>Account locked out Report</title>
<!--mce:0-->
"@

$Account_Name = @{n='Account name';e={$_.ReplacementStrings[-1]}}
$Account_domain = @{n='Account Domain';e={$_.ReplacementStrings[-2]}}
$Caller_Computer_Name = @{n='Caller Computer Name';e={$_.ReplacementStrings[-1]}}

$event= Get-EventLog -LogName Security -InstanceId 4740 -Newest 1 |
Select TimeGenerated,ReplacementStrings,"Account name","Account Domain","Caller Computer Name" |
% {
    New-Object PSObject -Property @{
        "Account name" = $_.ReplacementStrings[-7]
        "Account Domain" = $_.ReplacementStrings[5]
        "Caller Computer Name" = $_.ReplacementStrings[1]
        Date = $_.TimeGenerated
    }
}

$event | ConvertTo-Html -Property "Account name","Account Domain","Caller Computer Name",Date -
head $HTML -body "<H2> User is locked in the Active Directory</H2>" |
Out-File $Report -Append

$MailBody= Get-Content $Report
$MailSubject= "User Account locked out"
$SMTPClient = New-Object system.net.mail.smtpClient
$SMTPClient.host = "smtp.yoursmtpserver"
$MailMessage = New-Object system.net.mail.mailmessage
$MailMessage.from = "account_locked_out@.....com"
$MailMessage.To.add("youremail@youremail.com")
$MailMessage.Subject = $MailSubject
$MailMessage.IsBodyHtml = 1
$MailMessage.Body = $MailBody
$SMTPClient.Send($MailMessage)

del c:\powershell\html.html
```

# POWERSHELL – GROUP MODIFICATIONS

- Here's a favorite compliments of LazyWinAdmin
- Monitors and reports on AD group changes
- Perfect for auditing unnecessary admin accounts away
- Can be scheduled with Task Scheduler to run at your convenience
- Ex. - "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe" -command "C:\Scripts\LazyWinAdmin\Monitor-ADGroupMembership.ps1 -group \"Domain Admins\", \"Enterprise Admins\", \"Example Group\" -Emailfrom \"example@email.com\" -Emailto \"your@email.com\" -Emailserver \"your.email.server\""

# POWERSHELL – GROUP MODIFICATIONS

- Download the script from the GitHub
  - <https://github.com/ContinuousAudit/ISACA/blob/master/Monitor-ADGroupMembership.ps1>
- Install in PowerShell “Install-Script –name Monitor-ADGroupMembership.ps1”
- Let it run once on the schedule to create your baseline
- Any subsequent changes will be logged in your report
- This report is saved as a CSV you can use, as well as the HTML email

# POWERSHELL – GROUP MODIFICATIONS

Create Basic Task Wizard

Start a Program

Create a Basic Task

Trigger

Weekly

Action

Start a Program

Finish

Program/script:

"C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe" -coi

Browse...

Add arguments (optional):

Start in (optional):

< Back Next > Cancel

PS MONITORING - FX\FXGROUP02 Membership Change - Messa...

FILE MESSAGE

Sun 2013-11-17 4:05 AM

Reporting@fx.lab

PS MONITORING - FX\FXGROUP02 Membership Change

To catfx@fx.lab

### Group: FX\FXGROUP02

Group Description:

Group DN: CN=FXGROUP02,OU=Groups,OU=TEST,DC=FX,DC=LAB

Group CanonicalName: FX.LAB/TEST/Groups/FXGROUP02

Group SID: S-1-5-21-1547484852-1734975818-1172947732-1191

Group Scope/Type: DomainLocal / Security

### Membership Change

The membership of this group changed. See the following **Added** or **Removed** members.

DateTime	State	DisplayName	SamAccountName	DN
20131117-04:04:51	Removed		Administrator	CN=Administrator,CN=Users,DC=FX,DC=LAB

### Change History

List of the previous changes on this group observed by the script

DateTime	State	DisplayName	SamAccountName	DN
20131117-02:54:26	Removed		AnneD	CN=AnneD,CN=Users,DC=FX,DC=LAB
20131117-02:54:26	Removed		AnnR	CN=AnnR,CN=Users,DC=FX,DC=LAB
20131117-02:50:59	Added		admcatfx	CN=admcatfx,OU=Admin Users,OU=Administration,DC=FX,DC=LAB
20131117-02:48:25	Added		Administrator	CN=Administrator,CN=Users,DC=FX,DC=LAB

Report Time: 20131117\_040450

Account: FX\ADMINISTRATOR on LAB1DC01



# SCANS

- Vulnerability scans can be an integral part of any security audit
- Though most commercial scanners aren't terribly priced, budget restricted organizations can still setup scheduled scans with a little extra elbow grease
- To start this recipe, you need some flavor of Linux running on whatever you want to run it on (VM, retired desktop, Griffin Connected Toaster, etc.)





# SCANS - OPENVAS

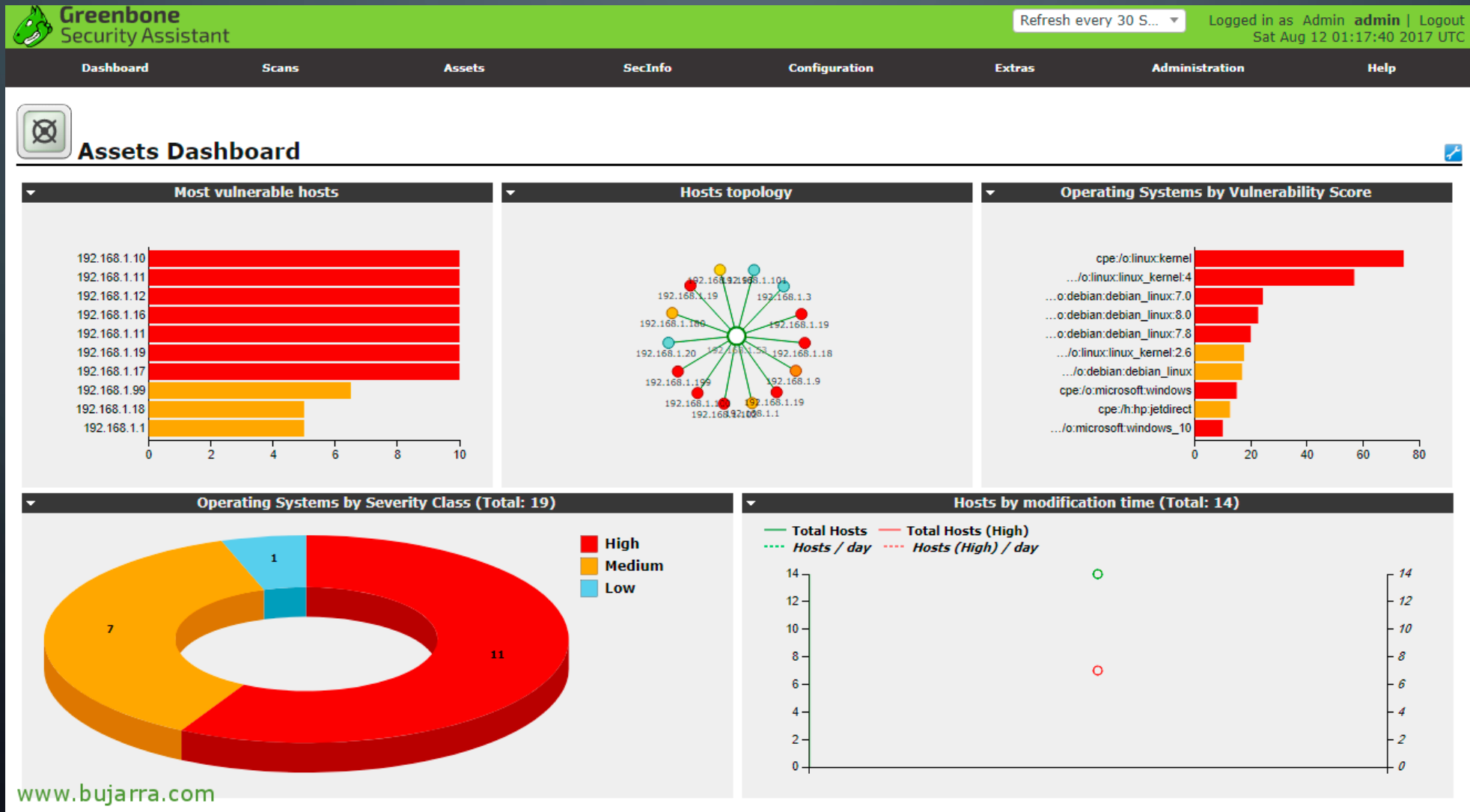
- OpenVAS (Open Vulnerability Assessment System) is a Nessus fork currently maintained by Greenbone Security and the open source community
- You can download a standalone, easy setup VM (Greenbone Security Manager) at [https://dl.greenbone.net/download/VM/gsm\\_ce\\_4.2.17.iso](https://dl.greenbone.net/download/VM/gsm_ce_4.2.17.iso)
- GSM does not have the ability to run scans on a schedule unless you license it
- But an OpenVAS install you do yourself does retain that ability



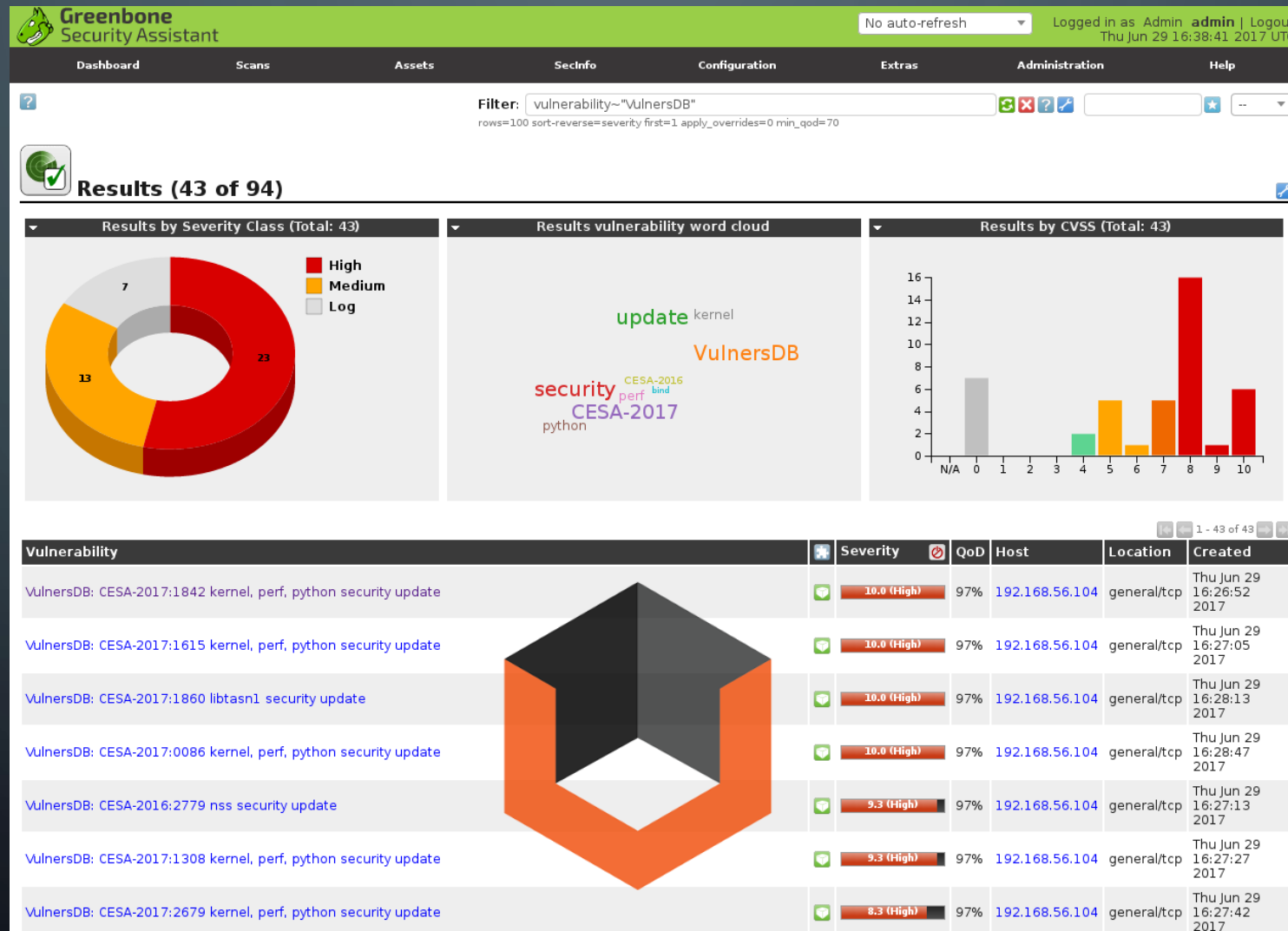
# SCANS - OPENVAS

- There are plenty of good tutorials for installing OpenVAS in Linux
  - Debian\Ubuntu:
    - <https://launchpad.net/~mrazavi/+archive/ubuntu/openvas>
    - <http://www.bujarra.com/instalando-usando-openvas/?lang=en>
    - <https://www.vultr.com/docs/how-to-install-openvas-vulnerability-scanner-on-ubuntu-16-04>
  - RHEL\CentOS:
    - <https://forums.atomicorp.com/viewtopic.php?f=31&t=8539#p44057>
    - <https://www.itzgeek.com/how-tos/linux/centos-how-tos/install-openvas-on-centos-7-rhel-7.html>

# SCANS - OPENVAS



# SCANS - OPENVAS



# SCANS - OPENVAS

The screenshot displays the OpenVAS Greenbone Security Assistant web interface. The browser address bar shows the URL: `https://192.168.1.6/omp?cmd=get_report&type=prognostic&host=192.168.1.8&pos=1&host_search_phrase=&hc`. The main content area is titled "Filtered Prognostic Results 1 - 4 of 4".

Host	OS	Start	End	High	Medium	Low	Log	False Pos	Total
192.168.1.8 (ubuntu32.domain.home)		Aug 13, 00:58:46	Aug 13, 01:15:47	1	3	0	0	0	4
Total: 0				1	3	0	0	0	4

### Security Issues reported for 192.168.1.8

**High (CVSS: 5.1)** cpe:/a:apache:http\_server:2.2.22  
CVE-2013-1862

The host carries the product: cpe:/a:apache:http\_server:2.2.22  
It is vulnerable according to: CVE-2013-1862.

mod\_rewrite.c in the mod\_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

**Medium (CVSS: 4.3)** cpe:/a:apache:http\_server:2.2.22  
CVE-2012-3499

The host carries the product: cpe:/a:apache:http\_server:2.2.22  
It is vulnerable according to: CVE-2012-3499.

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod\_imagemap, (2) mod\_info, (3) mod\_ldap, (4) mod\_proxy\_ftp, and (5) mod\_status modules.

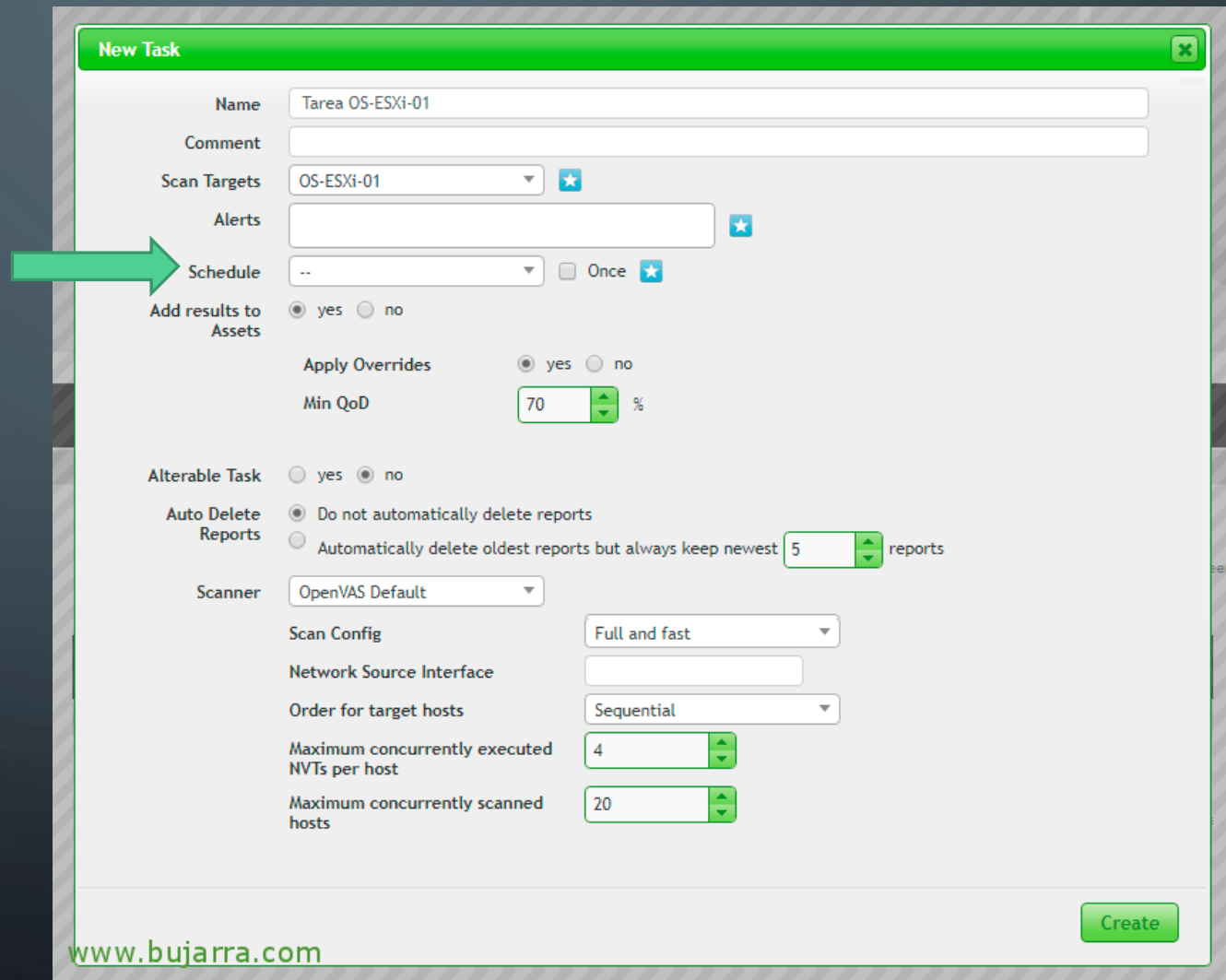
**Medium (CVSS: 4.3)** cpe:/a:apache:http\_server:2.2.22  
CVE-2012-4558

The host carries the product: cpe:/a:apache:http\_server:2.2.22  
It is vulnerable according to: CVE-2012-4558.

Multiple cross-site scripting (XSS) vulnerabilities in the balancer\_handler function in the manager interface in mod\_proxy\_balancer.c in the mod\_proxy\_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via crafted strings.

# SCANS - OPENVAS

- Scans, or tasks, can be set to run on a schedule and generate PDF reports
- If interested, check one of the earlier tutorial links for a complete walkthrough



The screenshot shows the 'New Task' configuration window in OpenVAS. The window has a green title bar with the text 'New Task' and a close button. The form contains the following fields and options:

- Name:** Tarea OS-ESXi-01
- Comment:** (empty text box)
- Scan Targets:** OS-ESXi-01 (dropdown menu with a star icon)
- Alerts:** (empty text box with a star icon)
- Schedule:** -- (dropdown menu) with a checkbox for 'Once' and a star icon. A green arrow points to this field.
- Add results to Assets:** ☒ yes ☐ no
- Apply Overrides:** ☒ yes ☐ no
- Min QoD:** 70 (spin box) %
- Alterable Task:** ☐ yes ☒ no
- Auto Delete Reports:**
  - ☒ Do not automatically delete reports
  - ☐ Automatically delete oldest reports but always keep newest 5 (spin box) reports
- Scanner:** OpenVAS Default (dropdown menu)
- Scan Config:** Full and fast (dropdown menu)
- Network Source Interface:** (empty text box)
- Order for target hosts:** Sequential (dropdown menu)
- Maximum concurrently executed NVTs per host:** 4 (spin box)
- Maximum concurrently scanned hosts:** 20 (spin box)

At the bottom right, there is a green 'Create' button. The URL [www.bujarra.com](http://www.bujarra.com) is visible at the bottom left of the window.



# SCANS – SHODAN

- [Shodan.io](https://www.shodan.io) is great for checking what you've exposed to the world

The screenshot shows the Shodan website interface. The main header includes the Shodan logo, navigation links (Shodan, Developers, Blog, View All...), a search bar, and buttons for Explore, Enterprise Access, Contact Us, New to Shodan?, and Login or Register. The main content area features the tagline "The search engine for the Web" and a sub-header "Shodan is the world's first search engine for Internet-connected devices." Below this, a search result for IP 212.187.208.158 is displayed. The result includes a table with the following information:

Field	Value
Country	United Kingdom
Organization	Level 3 Communications
ISP	Level 3 Communications
Last Update	2015-12-01T22:46:09.977768
ASN	AS3356

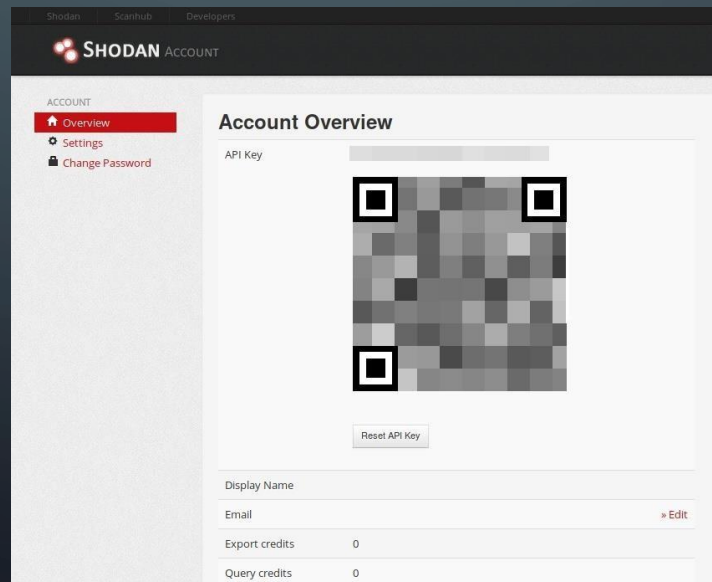
Below the table, there is a "Services" section with a list of services: 27015, udp, and steam-a2s. The "Left 4 Dead 2" server details are also shown, including the version (2.1.4.1), name (SGC Guns #3 - Eagle's Nest), players (0/4), operating system (Linux), map (c2m1\_highway), and version (2.1.4.1).

The screenshot shows the Shodan search results page for the query "port:4786 country:US". The page includes the Shodan logo, a search bar with the query, and buttons for Exploits, Maps, and Share Search. The main content area displays the following information:

- TOTAL RESULTS:** 55,353
- TOP COUNTRIES:** A world map showing the United States highlighted in red.
- United States:** 55,353
- TOP CITIES:** A list of cities and their corresponding result counts: San Antonio (1,388), Dallas (1,367), Los Angeles (1,342), New York (1,256), and Atlanta (366).
- TOP ORGANIZATIONS:** (Section header visible, but no data is shown in the screenshot).

# SCANS – SHODAN AUTOMATION

- [Shodan.io](https://shodan.io) features an API that can be called with Python
- This allows us to create automated tasks to monitor our organizations public systems
- Create a Shodan account, and go under the “My Account” section to get your API key





# SCANS – SHODAN AUTOMATION

- Install Python on your Windows (or Linux) system
  - Get it from: <https://github.com/ContinuousAudit/ISACA/blob/master/python-2.7.15.amd64.msi>
- Open Command Prompt, navigate to your python directory
  - “cd C:\Python27\”
- Install PIP
  - Download from: <https://github.com/ContinuousAudit/ISACA/blob/master/get-pip.py>
  - Copy it to your Python directory
  - Run “python get-pip.py”

Command Prompt

```
Microsoft Windows [Version 10.0.17134.112]  
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\Nick>cd C:\Python27\
```

```
C:\Python27>python get-pip.py
```

# SCANS – SHODAN AUTOMATION

- Change to your scripts directory

- cd “.\scripts”

```
C:\Python27>cd .\scripts
C:\Python27\Scripts>
```

- Install the Shodan library using Pip

- “pip install shodan”

- Install PIP

- Download from: <https://github.com/ContinuousAudit/ISAC>
  - Copy it to your Python directory
  - Run “python get-pip.py”

```
C:\Python27\Scripts>pip install shodan
Collecting shodan
  Downloading https://files.pythonhosted.org/packages/fe/cd
/shodan-1.8.1.tar.gz (43kB)
    100% |#####| 51kB 1.0MB/s
Collecting click (from shodan)
  Downloading https://files.pythonhosted.org/packages/34/c1
/click-6.7-py2.py3-none-any.whl (71kB)
    100% |#####| 71kB 1.3MB/s
Collecting click-plugins (from shodan)
  Downloading https://files.pythonhosted.org/packages/77/05
/click-plugins-1.0.3.tar.gz
Collecting colorama (from shodan)
  Downloading https://files.pythonhosted.org/packages/db/c8
/colorama-0.3.9-py2.py3-none-any.whl
Collecting requests>=2.2.1 (from shodan)
  Downloading https://files.pythonhosted.org/packages/65/47
/requests-2.19.1-py2.py3-none-any.whl (91kB)
    100% |#####| 92kB 1.5MB/s
Collecting XlsxWriter (from shodan)
  Downloading https://files.pythonhosted.org/packages/33/50
/XlsxWriter-1.0.5-py2.py3-none-any.whl (142kB)
    100% |#####| 143kB 2.0MB/s
Collecting idna<2.8,>=2.5 (from requests>=2.2.1->shodan)
  Downloading https://files.pythonhosted.org/packages/4b/2a
/idna-2.7-py2.py3-none-any.whl (58kB)
    100% |#####| 61kB 1.2MB/s
(c) 2018 Microsoft Corporation. All rights reserved.
```

C:\> Command Prompt

Microsoft Windows [Version 6.0.6002.18005]

(c) 2018 Microsoft Corporation. All rights reserved.

```
C:\Users\Nick>cd C:\Python27\
```

```
C:\Python27>python get-pip.py
```

# SCANS – SHODAN AUTOMATION

- Change to your scripts directory
  - cd “.\scripts”
- Install the Shodan library using Pip
  - “pip install shodan”

```
C:\Python27>cd .\scripts  
C:\Python27\Scripts>
```

```
C:\Python27\Scripts>pip install shodan  
Collecting shodan  
  Downloading https://files.pythonhosted.org/packages/fe/cd/  
/shodan-1.8.1.tar.gz (43kB)  
    100% |#####| 51kB 1.0MB/s  
Collecting click (from shodan)  
  Downloading https://files.pythonhosted.org/packages/34/c1/  
/click-6.7-py2.py3-none-any.whl (71kB)  
    100% |#####| 71kB 1.3MB/s  
Collecting click-plugins (from shodan)  
  Downloading https://files.pythonhosted.org/packages/77/05/  
/click-plugins-1.0.3.tar.gz  
Collecting colorama (from shodan)  
  Downloading https://files.pythonhosted.org/packages/db/c8/  
/colorama-0.3.9-py2.py3-none-any.whl  
Collecting requests>=2.2.1 (from shodan)  
  Downloading https://files.pythonhosted.org/packages/65/47/  
/requests-2.19.1-py2.py3-none-any.whl (91kB)  
    100% |#####| 92kB 1.5MB/s  
Collecting XlsxWriter (from shodan)  
  Downloading https://files.pythonhosted.org/packages/33/50/  
/XlsxWriter-1.0.5-py2.py3-none-any.whl (142kB)  
    100% |#####| 143kB 2.0MB/s  
Collecting idna<2.8,>=2.5 (from requests>=2.2.1->shodan)  
  Downloading https://files.pythonhosted.org/packages/4b/2a/  
/idna-2.7-py2.py3-none-any.whl (58kB)  
    100% |#####| 61kB 1.2MB/s
```

# SCANS – SHODAN AUTOMATION

- Open your text editor of choice
- We're going to create our actual script
- Shodan allows for many filters depending on what we want to monitor, ex.-
  - country: Country
  - city: City
  - geo: Coordinates
  - hostname: Hostname
  - net: IP\Prefix
  - os: Operating System
  - port: Ports
  - org: Organization
  - product: Specific software

# SCANS – SHODAN AUTOMATION

- Grab the sample script from:  
[https://github.com/ContinuousAudit/ISACA/blob/master/shodan\\_automation\\_sample.py](https://github.com/ContinuousAudit/ISACA/blob/master/shodan_automation_sample.py)
- Script should include a few things
  - “import shodan” to import the library
  - Your API key
  - Whatever you want to find or monitor
- The example script looks for  
XP systems with RDP open in Tallahassee  
and outputs their IPs as a CSV

```
shodan_automation_sample - Notepad
File Edit Format View Help
import shodan

SHODAN_API_KEY = "YOUR API KEY IN THESE QUOTES"

api = shodan.Shodan(SHODAN_API_KEY)

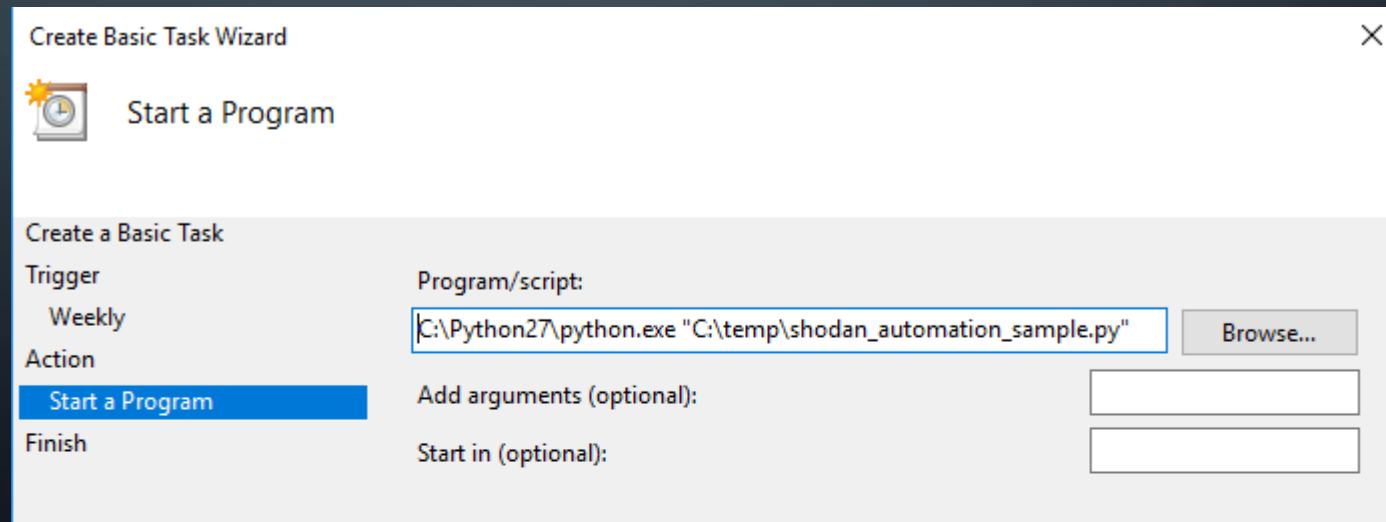
try:
    #Search\Monitor Item
    results = api.search('whatever you want')

    #Gather Info
    for result in results['matches']:
        print '%s' % result['ip_str']

import csv
```

# SCANS – SHODAN AUTOMATION

- Now we can use Task Scheduler to automatically run this report item for us
- Save your .py script file and use it in the program name in quotes
  - Ex. – C:\Python27\python.exe "C:\whereyourfileis\shodan\_automation\_sample.py"
- Set whatever schedule you like and enjoy



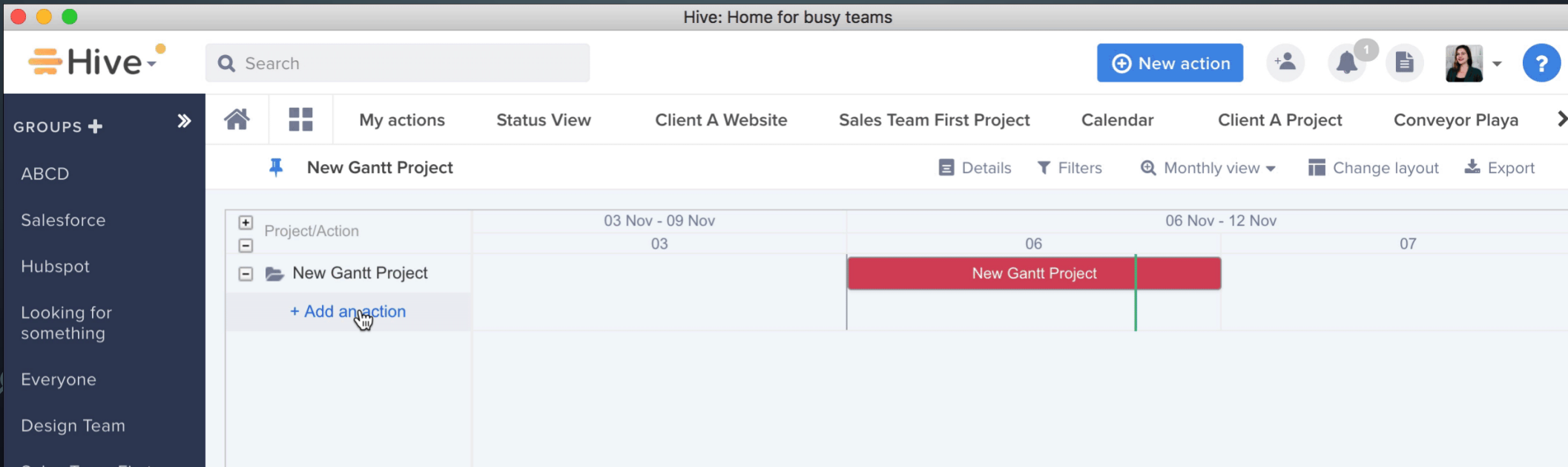


# KEEPING TRACK OF IT ALL

- Now that you've started automating some of your tasks, how to keep track of it all?
- Gathered audit information, and the logs needed to generate it, can be assembled with your SIEM or other logging tool
- If the budget doesn't allow for a commercial tool, try standing up an open source option such as Graylog or TheHive
- Leveraging some form of SIEM or similar tracking tool allows for quick access to any related data or gathered alerts and reports
- This takes the sting out of compiling all your new automated reports and alerts and converting it into actionable data

# KEEPING TRACK OF IT ALL

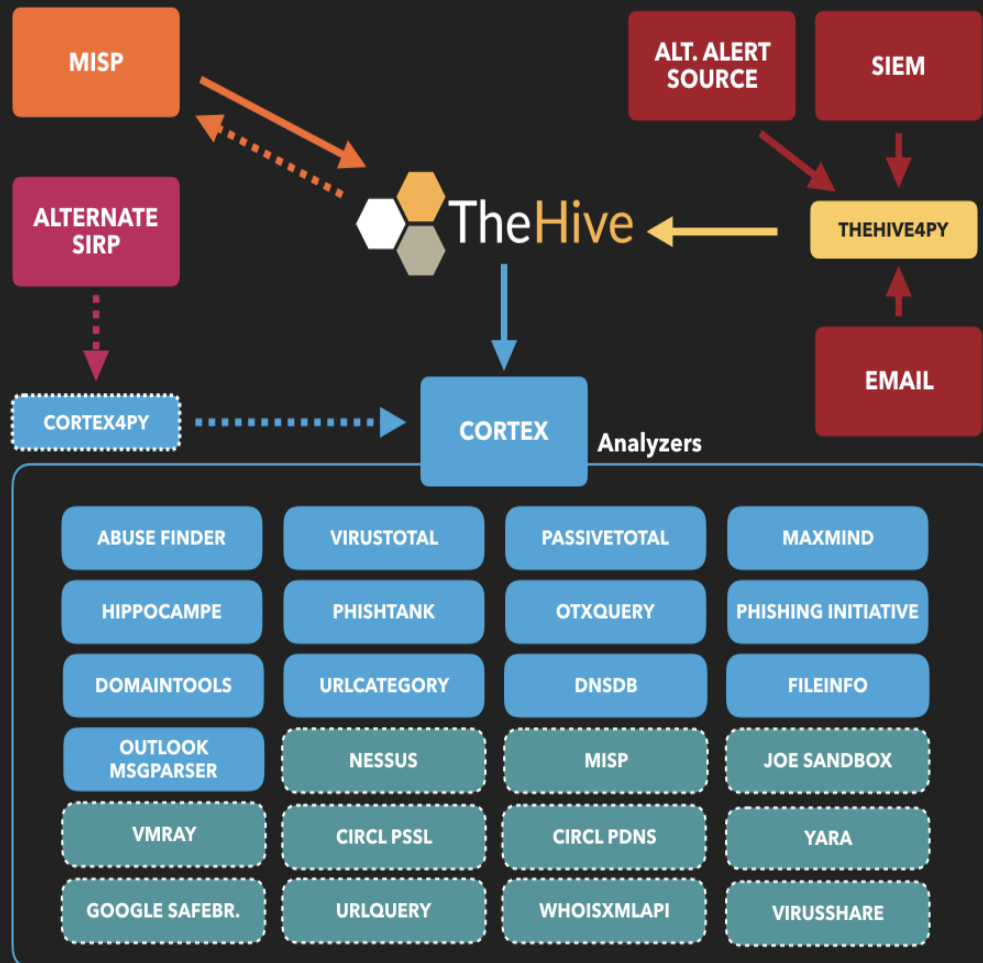
- TheHive allows for easy searching and collection of audit and incident response materials
- There's a test VM available to play with at:
- <https://drive.google.com/open?id=0B3G-Due88gfQMzIfZ2t6RVhqTUK>



The screenshot displays the TheHive web application interface. At the top, the header includes the 'Hive' logo, a search bar, and a 'New action' button. Below the header, a navigation bar shows various tabs: 'My actions', 'Status View', 'Client A Website', 'Sales Team First Project', 'Calendar', 'Client A Project', and 'Conveyor Playa'. The main content area is titled 'New Gantt Project' and features a Gantt chart. The chart has two columns: '03 Nov - 09 Nov' and '06 Nov - 12 Nov'. A red bar labeled 'New Gantt Project' spans from the start of the second column to the end of the first column. On the left side of the chart, there is a list of project actions, including 'Project/Action', 'New Gantt Project', and a '+ Add action' button. The interface also includes a sidebar on the left with a 'GROUPS +' section and a list of groups: 'ABCD', 'Salesforce', 'Hubspot', 'Looking for something', 'Everyone', and 'Design Team'.



# KEEPING TRACK OF IT ALL



**TheHive** + New Case ▾ My tasks **2** Waiting tasks **25** MISP **543** | Statistics

Case, user, URL, hash, IP, domain

Quick Filters ▾ Sort by ▾

Stats Filters 15 per page

List of cases (10 of 21)

1 filter(s) applied: status: Open Clear filters

Title	Tasks	Observables	Assignee	Date
#19 - [MISP] #3150 OSINT - Sofacy's 'Komplex' OS X Trojan by Palo Alto networks Tags: <b>circl:incident-classification="malware"</b> <b>misp</b> <b>ioc</b> <b>src:CIRCL</b>	5 Tasks	34		01/24/17 9:00
#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook Tags: <b>osint:source-type="blog-post"</b> <b>misp</b> <b>ioc</b> <b>src:CIRCL</b>	5 Tasks	54		01/24/17 11:37
#20 - [MISP] #3107 OSINT - Turbo Twist: Two 64-bit Derusbi Strains Converge Tags: <b>Type:OSINT</b> <b>misp</b> <b>ioc</b> <b>src:CIRCL</b>	5 Tasks	78		01/24/17 9:04
#17 - #3024 OSINT - In the Shadows: Vawtrak Aims to Get Stealthier by adding New Data Cloaking Tags: <b>Type:OSINT</b> <b>src:CIRCL</b>	No Tasks	179		01/22/17 12:17
#15 - #13:#3395 Malspam 2016-09-22 (js in .zip) - campaign: "Delivery #D-{integer}" / #14:Suspicious URL Tags: <b>circl:incident-classification="malware"</b> <b>src:CIRCL</b> <b>suspicious</b> <b>url</b> <b>user report</b> Merged from Case #13 and Case #14	No Tasks	155		12/13/16 13:17

Open in new window

Added by Antoine Stega

**Job Fortiguard\_URL**

status: Success  
startDate: Tue, Jan 24  
endDate: Tue, Jan 24

#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook

Added by Antoine Stega

**Job PhishingInitiative**

status: Success  
startDate: Tue, Jan 24  
endDate: Tue, Jan 24

#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook

Added by Antoine Stega

**[MISP] #4855 OSINT - Nemucod downloader spreading via Facebook**

This case contains 5 observables  
This case contains 5 tasks

description: Imported at Mon Nov 21 12:17:17  
tributes : - https://bar...  
1/nemucod-downloa

#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook



# CONTINUOUS NETWORK AUDIT

NICHOLAS CARROLL

ISACA TALLAHASSEE

JUNE 2018