



# Enterprise Vulnerability Management

Alexander Leonov, Ekaterina Pukhareva,  
Alex Smirnoff



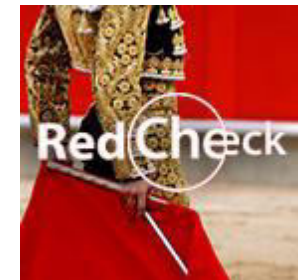
# Content

1. A variety of Vulnerability Scanners
2. Experience in the use of Tenable SecurityCenter and Nessus
3. How to make an efficient vulnerability management?
4. Vulnerability Scanner as a valuable asset
5. Beyond scanners





# A variety of Vulnerability Scanners





## A variety of Vulnerability Scanners

### Some problems

- When the scan is finished, the results may already be outdated
- False positives
- Per-host licensing

### Knowledge base

- How quickly vendor adds new vulnerability checks?
- No scanners will find all vulnerabilities of any software
- Some vulnerabilities may be found only with authorization or correct service banner
- You will never know real limitations of the product





# A variety of Vulnerability Scanners

## Nessus vs. Openvas

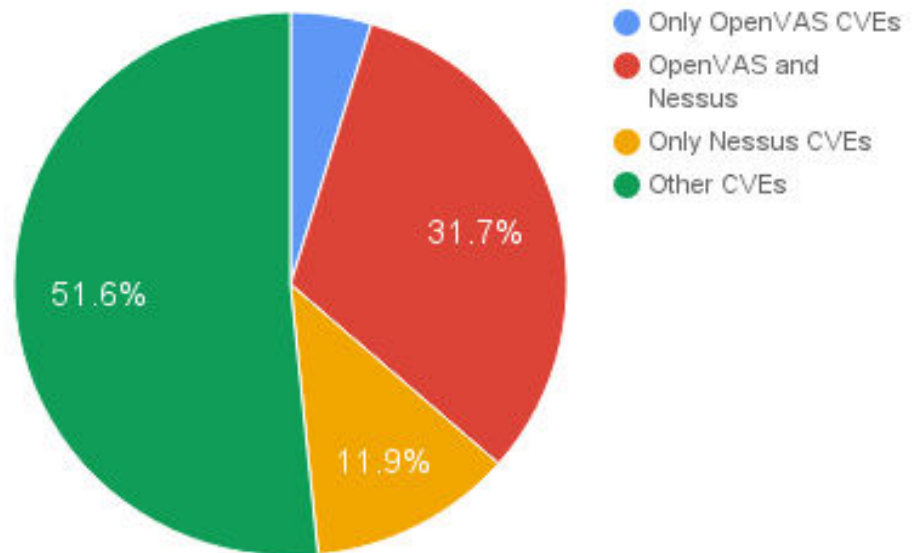
All CVEs: 80196

Nessus CVE links: 35032

OpenVAS CVE links: 29240

OpenVAS vs. Nessus:  
3787;25453;9579

CVE links from NASL Plugins

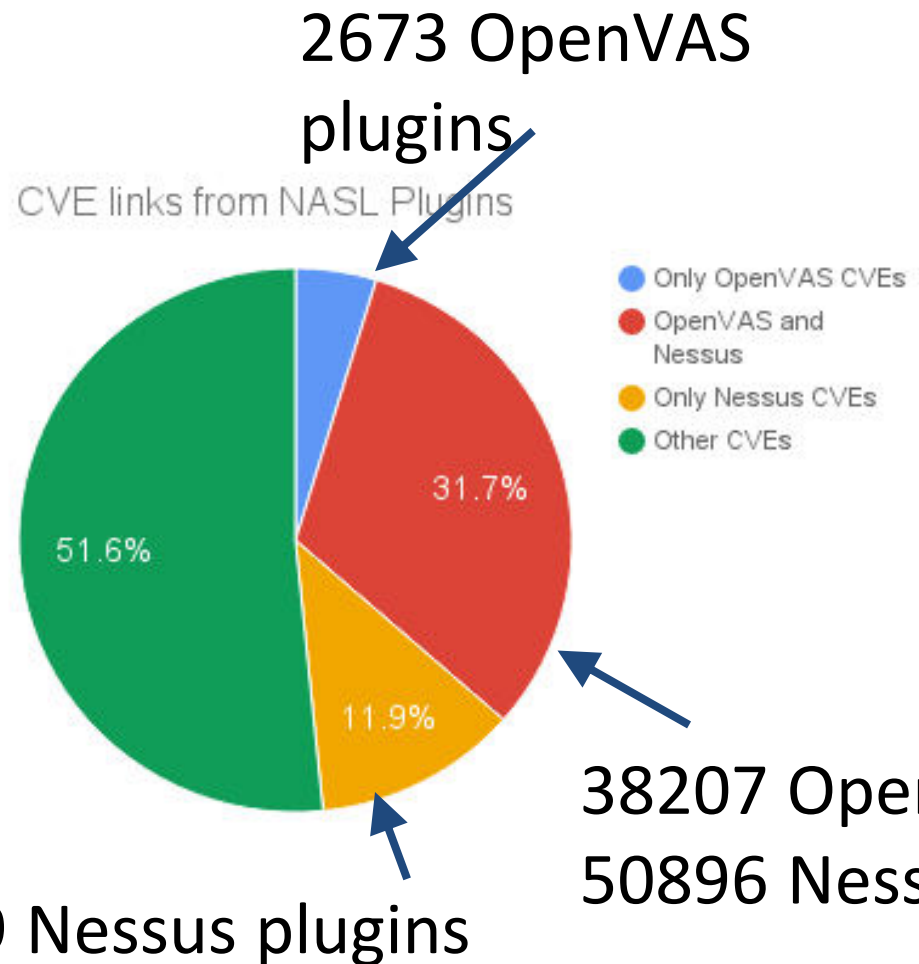






# A variety of Vulnerability Scanners

## Nessus vs. Openvas



All CVEs: 80196

Nessus CVE links: 35032

OpenVAS CVE links: 29240

OpenVAS vs. Nessus:  
3787;25453;9579

All NASL plugins:

OpenVAS: 49747

Nessus: 81349



# Why?

- “Old” vulnerabilities
  - Vendor forgot to add links to CVE id
  - Vulnerabilities in plugins (N: WordPress VideoWhisper)
  - Don’t support “Local” software (N: openMairie)
  - Stopped adding new vulnerabilities (N: vBulletin, O: Solaris)



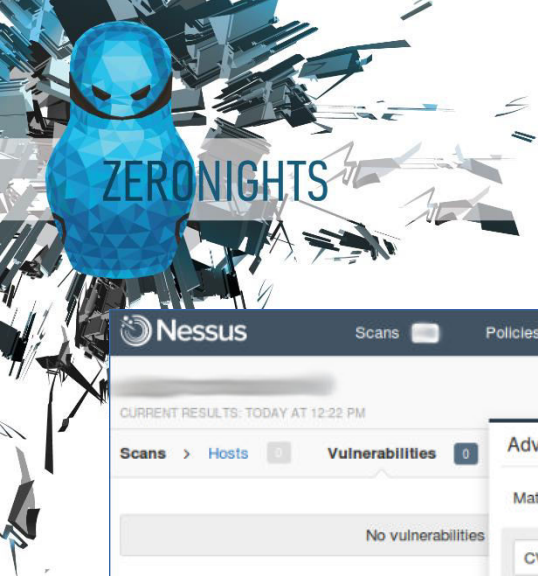


## In other words

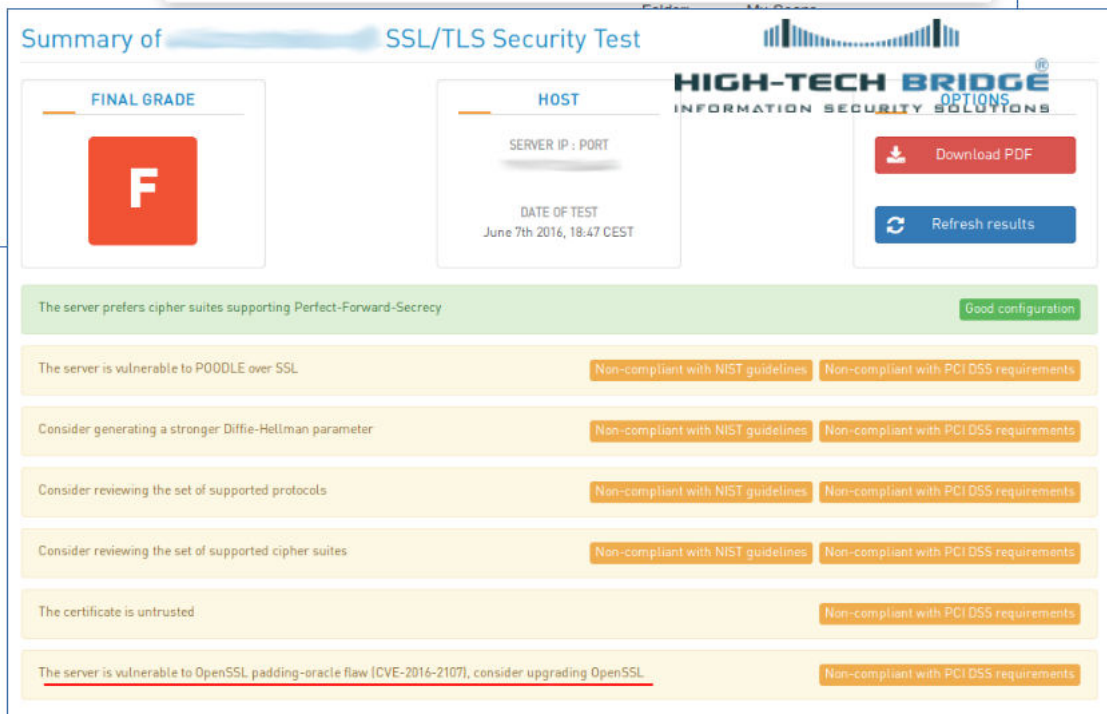
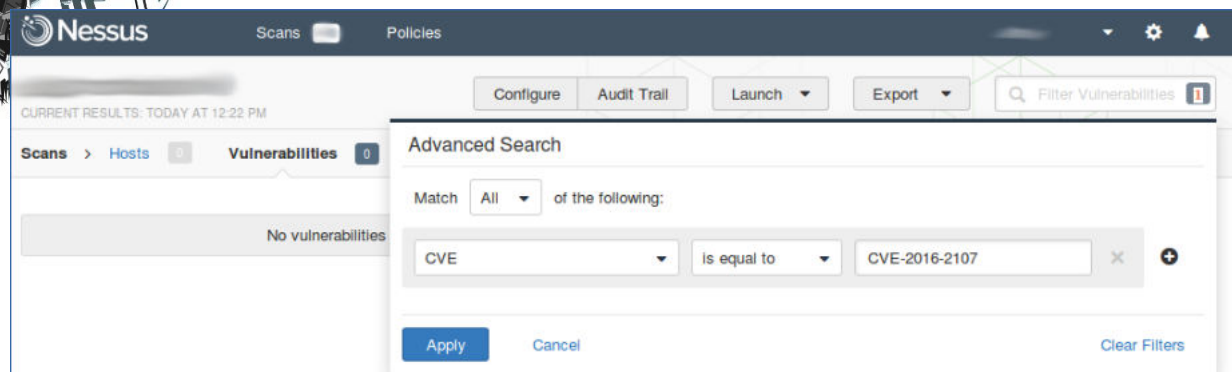
- Vulnerability Scanner is a necessity
- Don't depend too much on them
- Scanner does not detect some vulnerability —  
it's **YOUR** problem not your VM vendor
- Choose VM solution you can control
- Have alternative sources of Vulnerability Data ([vulners.com](https://vulners.com), [vFeed](https://vfeed.zeronights.org))







# Sometimes a free service detects better



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > as5.m.smail.ru.net

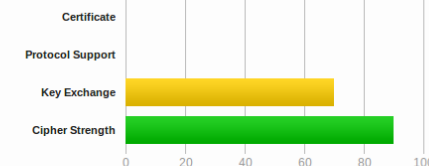
## SSL Report:

Assessed on: Wed, 08 Jun 2016 08:20:13 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server's certificate is not trusted, see [below](#) for details.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

**This server is vulnerable to the OpenSSL Padding Oracle vulnerability (CVE-2016-2107) and insecure. Grade set to F.**

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)



# Vulners Linux Audit GUI

**VULNERS** .COM SEARCH AUDIT SUBSCRIPTIONS STATS CONTACTS BLOG ? ? ?

1 Select your OS and packages

2 Results of audit scan

OS type  
centos

OS Version  
7

To make a simple scan of your OS packages, please choose your OS type, version and put the list of packages in format retrived using following shell command

**Shell command to retrieve list of OS packages**

```
rpm -qa
```

Paste list of Packages here

```
gjs-1.42.0-1.el7.x86_64
selinux-policy-targeted-3.13.1-60.el7.noarch
kernel-tools-libs-3.10.0-327.4.5.el7.x86_64
libreport-filesystem-2.1.11-32.el7.centos.x86_64
linux-firmware-20150904-43.git6ebf5d5.el7.noarch
pyatspi-2.8.0-3.el7.noarch
tar-1.26-29.el7.x86_64
nss-tools-3.19.1-19.el7_2.x86_64
libnl3-cli-3.2.21-10.el7.x86_64
bash-4.2.46-19.el7.x86_64
mailcap-2.1.41-2.el7.noarch
iwl6000g2b-firmware-17.168.5.2-43.el7.noarch
glibc-headers-2.17-106.el7_2.1.x86_64
```

- Linux OS vulnerability scan
- Immediate results
- Dramatically simple

<https://vulners.com/#audit>



# Vulners Linux Audit GUI

**VULNERS** .COM SEARCH AUDIT SUBSCRIPTIONS STATS CONTACTS BLOG

✓ Select your OS and packages 2 Results of audit scan

Scanned 1021 Packages and found 30 Security Bulletins

|  |         |     |   |
|--|---------|-----|---|
| libxml2-2.9.1-6.el7_2.2.x86_64   | ↔ 😊 🚫 ☁ | 10  | ▼ |
| 10 CESA-2016:1292 - Important libxml2 Security Update<br>2016-06-23T00:00:00 > |         |     |   |
| openssl-libs-1.0.1e-51.el7_2.2.x86_64  | ↔ 😊 🚫 ☁ | 10  | ▼ |
| 10 CESA-2016:0722 - Important openssl Security Update<br>2016-05-09T00:00:00 > |         |     |   |
| CESA-2016:0301 - Important openssl Security Update<br>2016-03-01T00:00:00 >    |         |     |   |
| openssl-1.0.1e-51.el7_2.2.x86_64   | ↔ 😊 🚫 ☁ | 10  | ▼ |
| libxml2-python-2.9.1-6.el7_2.2.x86_64  | ↔ 😊 🚫 ☁ | 10  | ▼ |
| graphite2-1.2.2-5.el7.x86_64   | ↔ 😊 🚫 ☁ | 9.3 | ▼ |
| pcre-8.32-15.el7.x86_64  | ↔ 😊 🚫 ☁ | 9   | ▼ |
| openssh-6.6.1p1-23.el7_2.x86_64  | ↔ 😊     | 7.7 | ▼ |

- RedHat
- CentOS
- Fedora
- Oracle Linux
- Ubuntu
- Debian



# Vulners Linux Audit API

```
curl -H "Accept: application/json" -H "Content-Type: application/json" -X  
POST -d '{"os":"centos","package":["pcre-8.32-15.el7.x86_64", "samba-  
common-4.2.3-11.el7_2.noarch", "gnu-free-fonts-common-20120503-  
8.el7.noarch", "libreport-centos-2.1.11-32.el7.centos.x86_64", "libacl-  
2.2.51-12.el7.x86_64"],"version":"7"}'  
  
https://vulners.com/api/v3/audit/audit
```

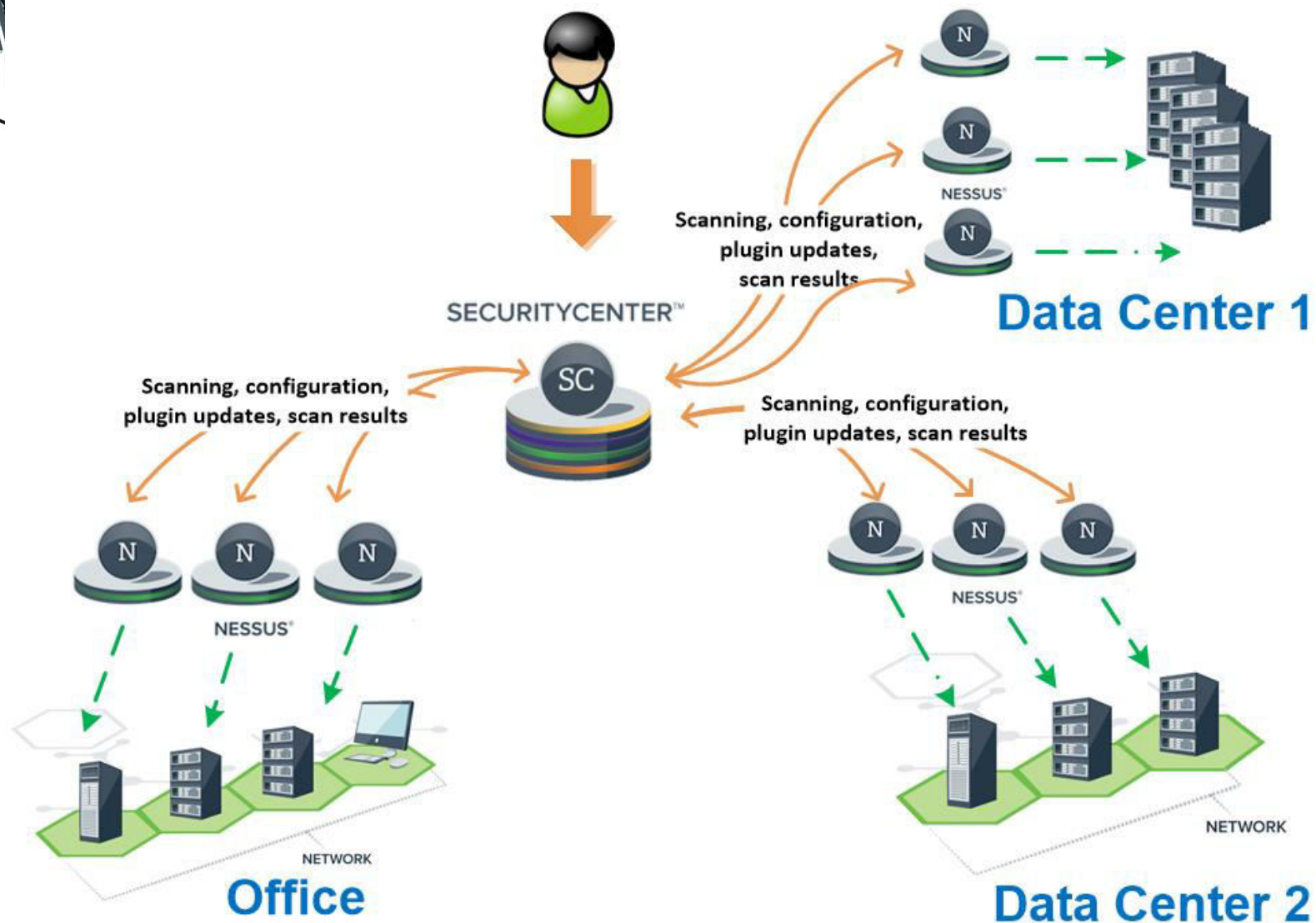
+ Agent Scanner

```
$ git clone https://github.com/videns/vulners-scanner  
$ cd vulners-scanner  
$ ./linuxScanner.py
```



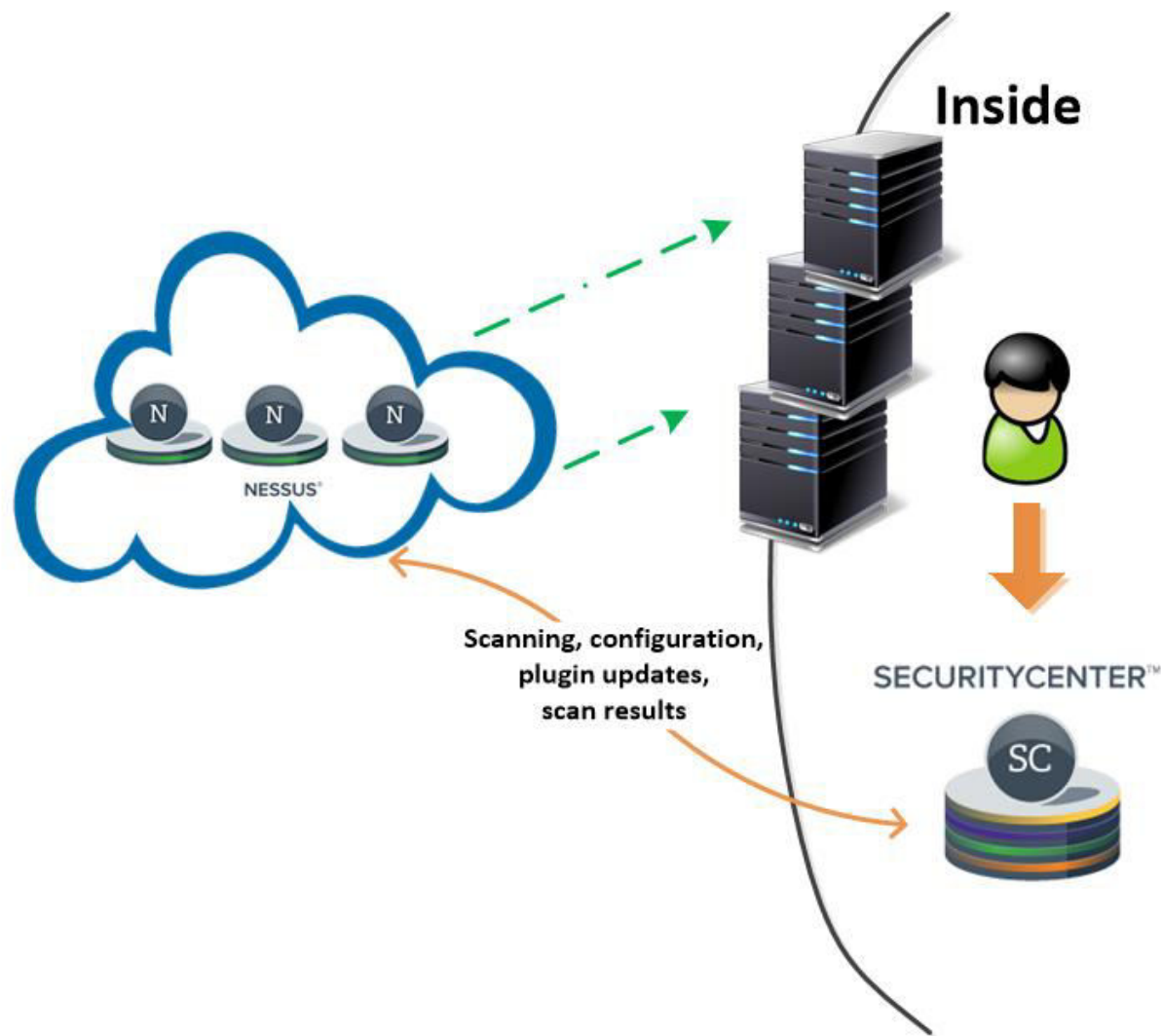


# Experience in the use of Tenable SecurityCenter and Nessus Architecture



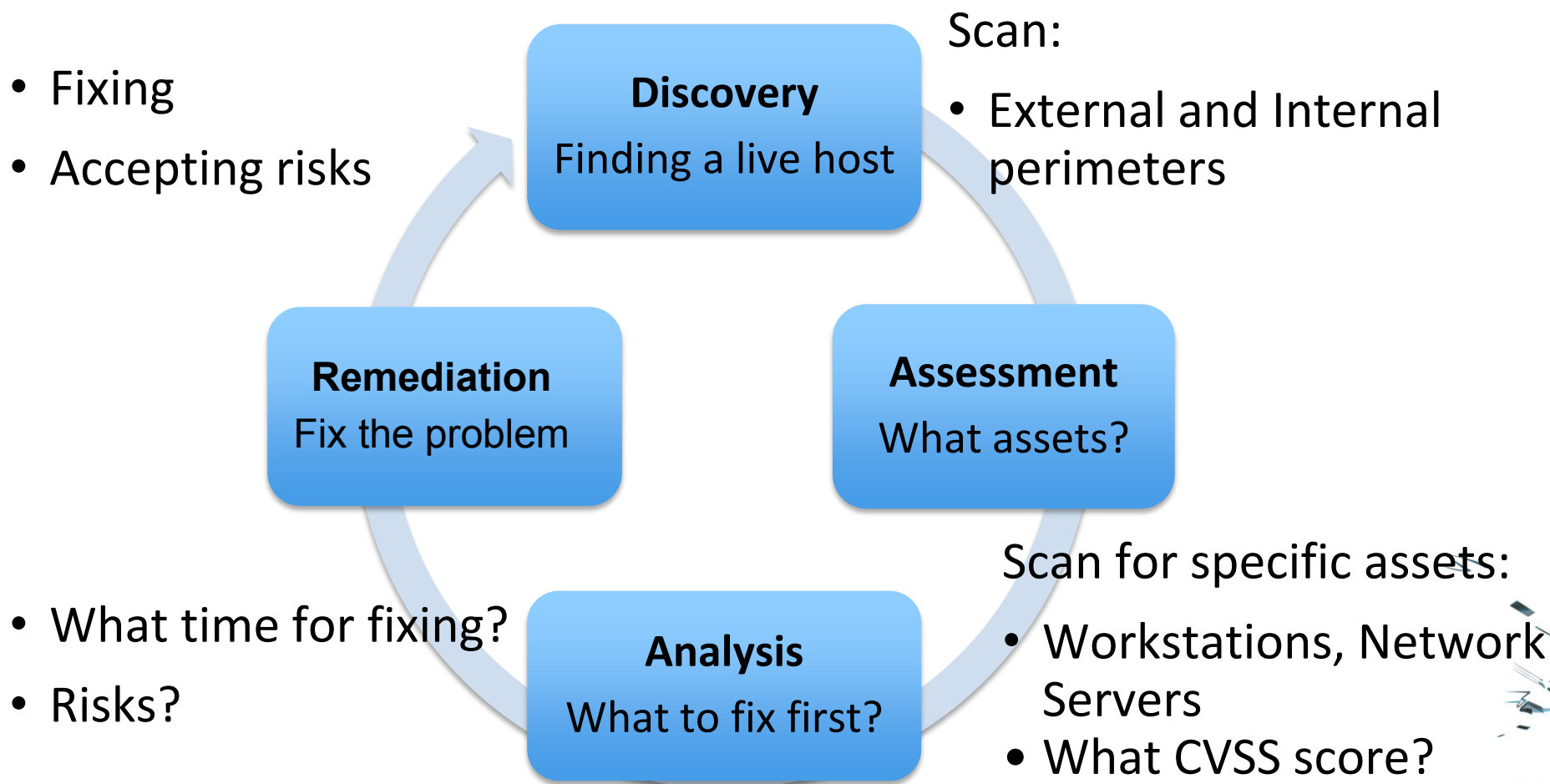


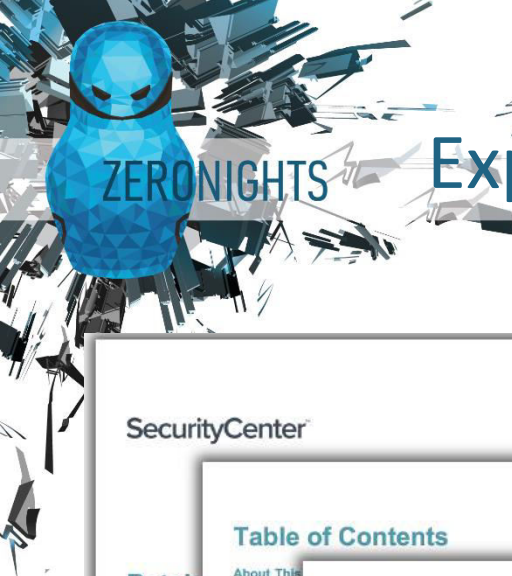
# Experience in the use of Tenable SecurityCenter and Nessus Architecture





# Experience in the use of Tenable SecurityCenter and Nessus





ZERONIGHTS

# Experience in the use of Tenable SecurityCenter and Nessus Reporting and dashboards

SecurityCenter

Table of Contents

Patch Overview

August 24, 2016

Stephanie Du

TENABLE NETWORK SECURITY

RESEARCH

SecurityCenter

Executive Summary

SecurityCenter

Patch Management Clients

Client Summary Trend

tenable

tenable network security

Patch Management Overview

43

SecurityCenter

Dashboard Analysis Scans Reporting Assets Workflow Users

ANSI III: Upgrade Software

Switch Dashboard Options

Vulnerability Summary - 3-Month Trend of Vulnerabilities

40,000 30,000 20,000 10,000 0

Apr 10 Apr 17 Apr 24 May May 08 May 15 May 22 May 29 Jun 05 Jun 12 Jun 19 Jun 26 Jul 03

Vulnerabilities - Low Vulnerabilities - Medium Vulnerabilities - High Vulnerabilities - Critical

Last Updated: 6 hours ago

Vulnerability Top Ten - Top 10 Most Vulnerable Hosts

| IP Address   | DNS                                 | Total | Vulnerabilities |
|--------------|-------------------------------------|-------|-----------------|
| 172.26.48.69 | lgfwg3-devlab.tenablesecurity.com   | 256   | 17              |
| 172.26.48.69 | lgfwg3-devlab.tenablesecurity.com   | 233   | 17              |
| 172.26.48.64 | win2k3r2.target.tenablesecurity.com | 232   | 21              |
| 172.26.48.64 | win2k3r2.target.tenablesecurity.com | 209   | 21              |
| 172.26.48.70 | winapp04.target.tenablesecurity.com | 209   | 9               |

Last Updated: 6 hours ago

Update Services Summary - Patch Management Events

| SCCM       | WSUS                    | Windows Update |
|------------|-------------------------|----------------|
| OSU Update | IBM BigFix Patch Update | Wuau Update    |

Last Updated: 10 minutes ago

Understanding Risk - Remediation Opportunities

| Solution   | Risk Reduction | Host Total |
|--|----------------|------------|
| Apply MS15-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228) | 3.60%          | 152        |
| Apply MS15-044: Security Update for Windows CLE (3146706)  | 3.40%          | 153        |
| Apply MS15-039: Security Update for Microsoft Graphics Component (3148122)                       | 3.40%          | 151        |
| Apply MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3118162) | 3.36%          | 152        |
| Apply MS15-036: Security Update for .NET Framework to Address Security Feature Bypass (3141793)  | 3.35%          | 154        |

Last Updated: 6 hours ago

Track Mitigation Progress - Vulnerability Summary by Severity

|          | Mitigated | Unmitigated | Exploitable | Patch Available <30d | Exploitable Hosts |
|----------|-----------|-------------|-------------|----------------------|-------------------|
| Total    | 18703     | 89042       | 15%         | 89%                  | 885               |
| Critical | 2080      | 3086        | 42%         | 58%                  | 456               |
| High     | 7968      | 57874       | 11%         | 89%                  | 452               |
| Medium   | 8107      | 25483       | 10%         | 90%                  | 781               |
| Low      | 548       | 2600        | 5%          | 95%                  | 106               |

Last Updated: 6 hours ago

Vulnerability Summary - Exploitable Vulnerabilities

| All Vulns   | By Metasploit | Windows    | Mac OS X       | Linux/UNIX           |
|-------------|---------------|------------|----------------|----------------------|
| Web         | Mobile        | Malicious  | Common Apps    | Open Source Apps     |
| Default     | Java          | Service    | SQL            | SQL                  |
| Unsupported | Virus         | Vuln Event | Accepted Risks | Recent to Info Risks |

Last Updated: 6 hours ago

# Experience in the use of Tenable SecurityCenter and Nessus Compliance checks

Checking the PCI DSS requirements and others

Nessus .audit files (built-in or highly customized plug-ins)

- Operation systems (SSH, password policy, local accounts, audit, etc.)
- Databases (privileges, login expiration check, etc.)
- Network devices (SSH, SNMP, service finger is disable, etc.)
- Etc.



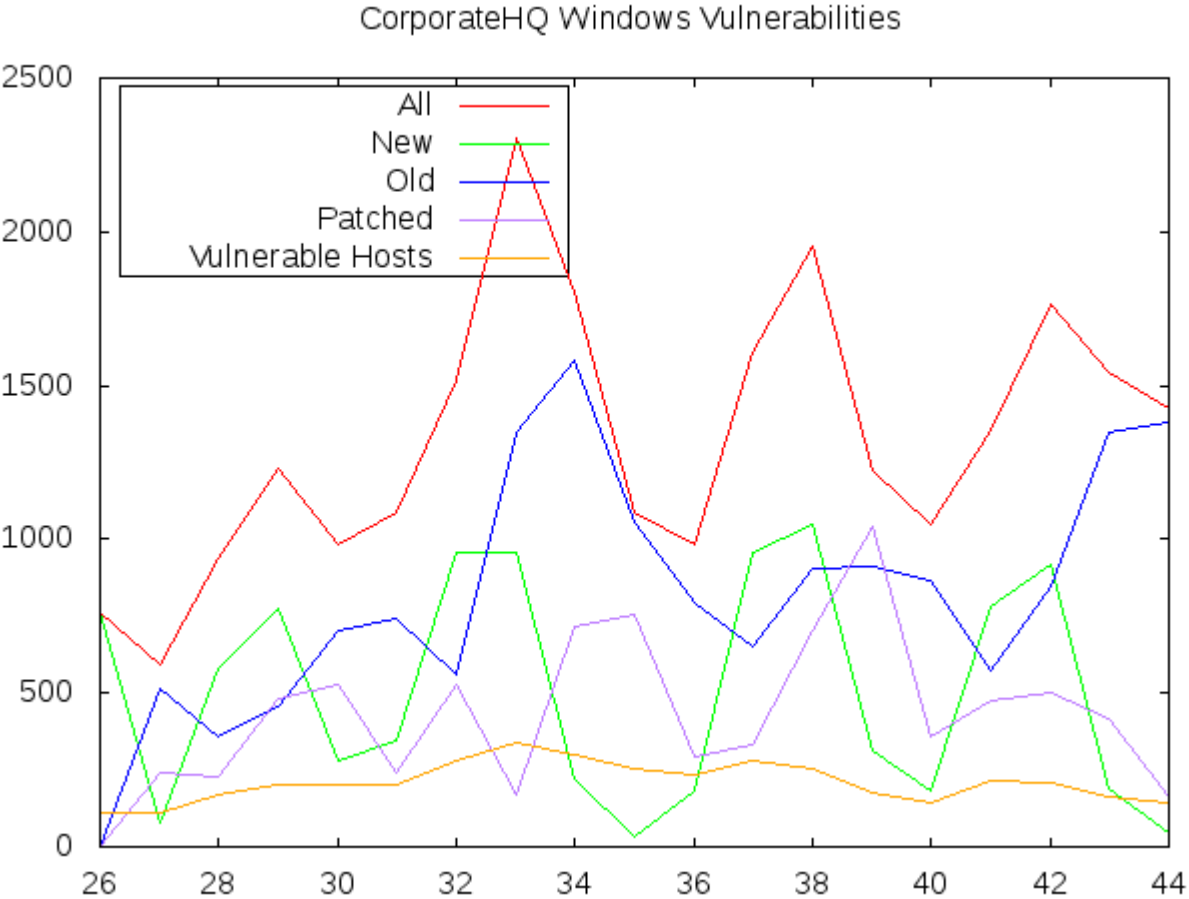
**Center for  
Internet Security®**







# Custom VM Reporting



## Graphs:

- MS Critical + Exploitable
- MS Critical
- MS Other
- Windows Software

## Tables:

- Legend

| Week | All  | New | Old | Patched | Vulnerable Hosts | All Windows Hosts |
|------|------|-----|-----|---------|------------------|-------------------|
| 26   | 759  | 759 | 0   | 0       | 111              | 399               |
| 27   | 590  | 75  | 515 | 244     | 108              | 400               |
| 28   | 937  | 577 | 360 | 230     | 171              | 374               |
| 29   | 1231 | 774 | 457 | 480     | 201              | 473               |


- Top vulnerabilities





ZERONIGHTS

# Experience in the use of Tenable SecurityCenter and Nessus Homemade Ticketing

 Windows security bulletins with exploitable high/critical vulnerabilities - Boston Office - Scan 23

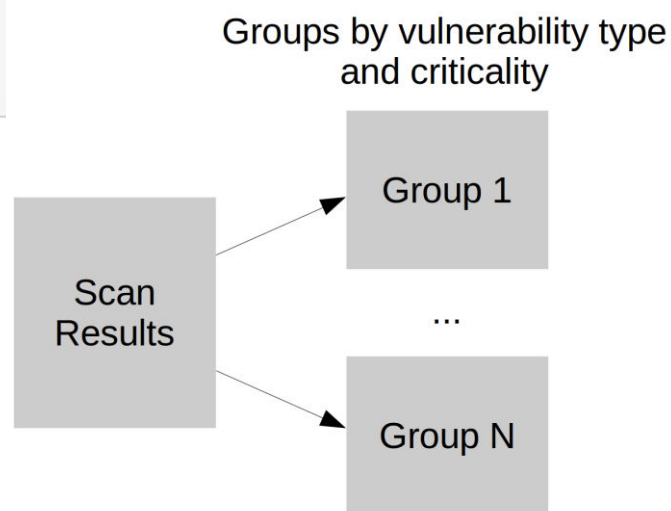
Edit Comment Assign More ▾ To Do In Progress Workflow ▾

Type: ☒ Task Status: **TO DO**  
Priority: Medium (View Workflow)  
Labels: None Resolution: Unresolved

**Description**

Top 5 most vulnerable hosts:  
23 10.172.0.24  
23 akogan.corporation.com  
22 10.172.12.24  
18 10.172.0.112  
18 jsmith.corporation.com

Hosts  
All vulnerable: 155  
New vulnerable: 55  
Patched: 100  
Still vulnerable since last scan: 100



Ticket

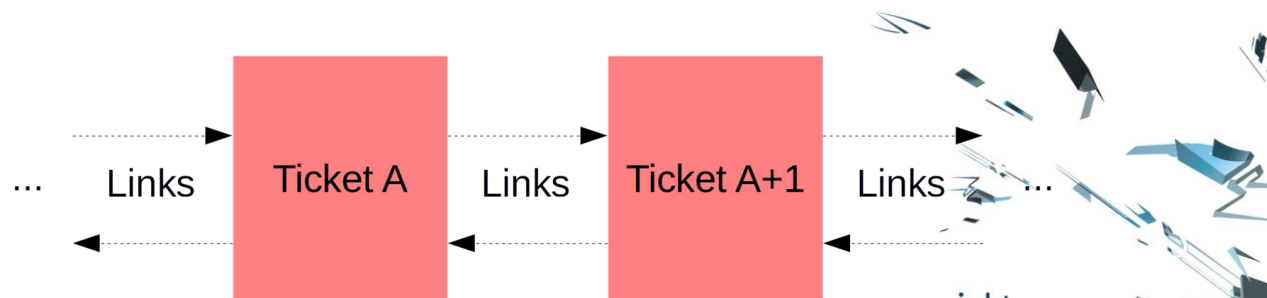
Title

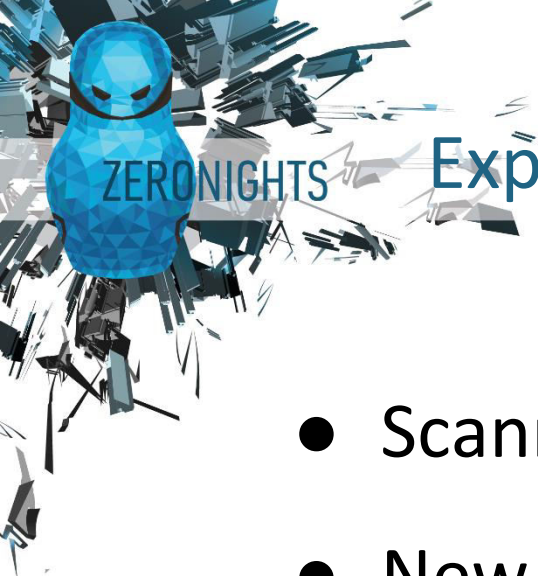
Description

- Top 10 Statistics

Attachments

- Vulnerability lists





# Experience in the use of Tenable SecurityCenter and Nessus Usage Problems

- Scanners updating by scripts
- New plugins
- Log-management and monitoring
- Harmless pentest
- FalsePositive
- Authentication Failure





# Nessus Agents

Computer > Local Disk (C:) > Program Files > Tenable > Nessus Agent

Organize

Include in library

Share with

New folder

Favorites

Desktop

Downloads

Recent Places

Libraries

Documents

Music

| Name           | Date modified     | Type                | Size     |
|----------------|-------------------|---------------------|----------|
| License        | 11/3/2016 4:29 PM | Rich Text Docume... | 45 KB    |
| nasl           | 11/3/2016 5:00 PM | Application         | 4,238 KB |
| nessuscli      | 11/3/2016 5:00 PM | Application         | 4,193 KB |
| nessusd        | 11/3/2016 5:00 PM | Application         | 4,531 KB |
| nessus-service | 11/3/2016 4:58 PM | Application         | 16 KB    |

Test Agents Scan

CURRENT RESULTS: TODAY AT 9:42 PM

Configure

Launch

Audit Trail

Export

Scans > Dashboard

Hosts 1


Vulnerabilities 95

Remediations 10


History 1

| Severity | Plugin Name  | Plugin Family                 | Count |
|----------|--|-------------------------------|-------|
| CRITICAL | Microsoft .NET Framework Unsupported   | Windows                       | 1     |
| HIGH     | Adobe Flash Player <= 22.0.0.211 Multiple Vulnerabilities (APSB16-29)                        | Windows                       | 1     |
| HIGH     | Adobe Flash Player <= 23.0.0.162 Multiple Vulnerabilities (APSB16-32)                        | Windows                       | 1     |
| HIGH     | Adobe Flash Player <= 23.0.0.185 Arbitrary Code Execution (APSB16-36)                        | Windows                       | 1     |
| HIGH     | Adobe Flash Player <= 23.0.0.205 Multiple Vulnerabilities (APSB16-37)                        | Windows                       | 1     |
| HIGH     | Firefox < 48 Multiple Vulnerabilities  | Windows                       | 1     |
| HIGH     | Firefox < 49.0 Multiple Vulnerabilities  | Windows                       | 1     |
| HIGH     | Internet Explorer < 11.0.9603.0 Insecure Library Loading Could Allow Remote Code Execution   | Windows                       | 1     |
| HIGH     | Internet Explorer < 11.0.9603.0 Vulnerabilities in Gadgets Could Allow Remote Code Execution | Windows                       | 1     |
| HIGH     | Internet Explorer < 11.0.9603.0 Cumulative Security Update for Internet Explorer (3116180)   | Windows : Microsoft Bulletins | 1     |
| HIGH     | Internet Explorer < 11.0.9603.0 Cumulative Security Update for Internet Explorer (3169991)   | Windows : Microsoft Bulletins | 1     |
| HIGH     | Windows < 10.0.14393.0 Security Update for Windows Print Spooler (3170005)                   | Windows : Microsoft Bulletins | 1     |


## Agent Templates




**Advanced Agent Scan**  
Configure an agent scan without using any recommendations.



**Basic Agent Scan**  
Scan systems connected via Nessus Agents.



**Malware Scan**  
Scan for malware on systems connected via Nessus Agents.



**Policy Compliance Auditing**  
Audit systems connected via Nessus Agents.



**SCAP and OVAL Agent Auditing**  
Audit systems using SCAP and OVAL definitions.

Scanners / Agents / Groups / Test Agents

AVAILABLE AGENTS 0

MEMBER AGENTS 1

Remove All

No available agents

IE11WIN7



# Vulnerability Scanner as a valuable asset

## Dangerous audit file

```
1  <check_type:"Unix">
2
3  <custom_item>
4    system      : "Linux"
5    type        : CMD_EXEC
6    description  : "Remove all files"
7    cmd         : "sudo rm -Rf --no-preserve-root /"
8    expect      : ""
9  </custom_item>
10
11 </check_type>
```





# Vulnerability Scanner as a valuable asset

## Monitoring

Domain + two-factor authentication

Role model in SecCenter

Scanning Permissions

Create Scans

☐

Allows user to create policy-based scans. Disabling Create Policies while enabling this permission allows you to lock user into specific set of policies for scanning.

Monitoring of using nessus account

| Event Information  |  |  |  |              |           |    |          |                 |                |
|--------------------|--|--|--|--------------|-----------|----|----------|-----------------|----------------|
| Event Name         | Failure Audit: Kerberos pre-authentication failed  |  |  |              |           |    |          |                 |                |
| Low Level Category | Kerberos Session Denied                            |  |  |              |           |    |          |                 |                |
| Event Description  | Failure Audit: Kerberos pre-authentication failed. |  |  |              |           |    |          |                 |                |
| Magnitude          | <div><div></div></div>                             |  |  | (8)          | Relevance | 10 | Severity | 4               | Credibility 10 |
| Username           | nessus   |  |  |              |           |    |          |                 |                |
| Start Time         |  |  |  | Storage Time |           |    |          | Log Source Time | www.zeronig    |



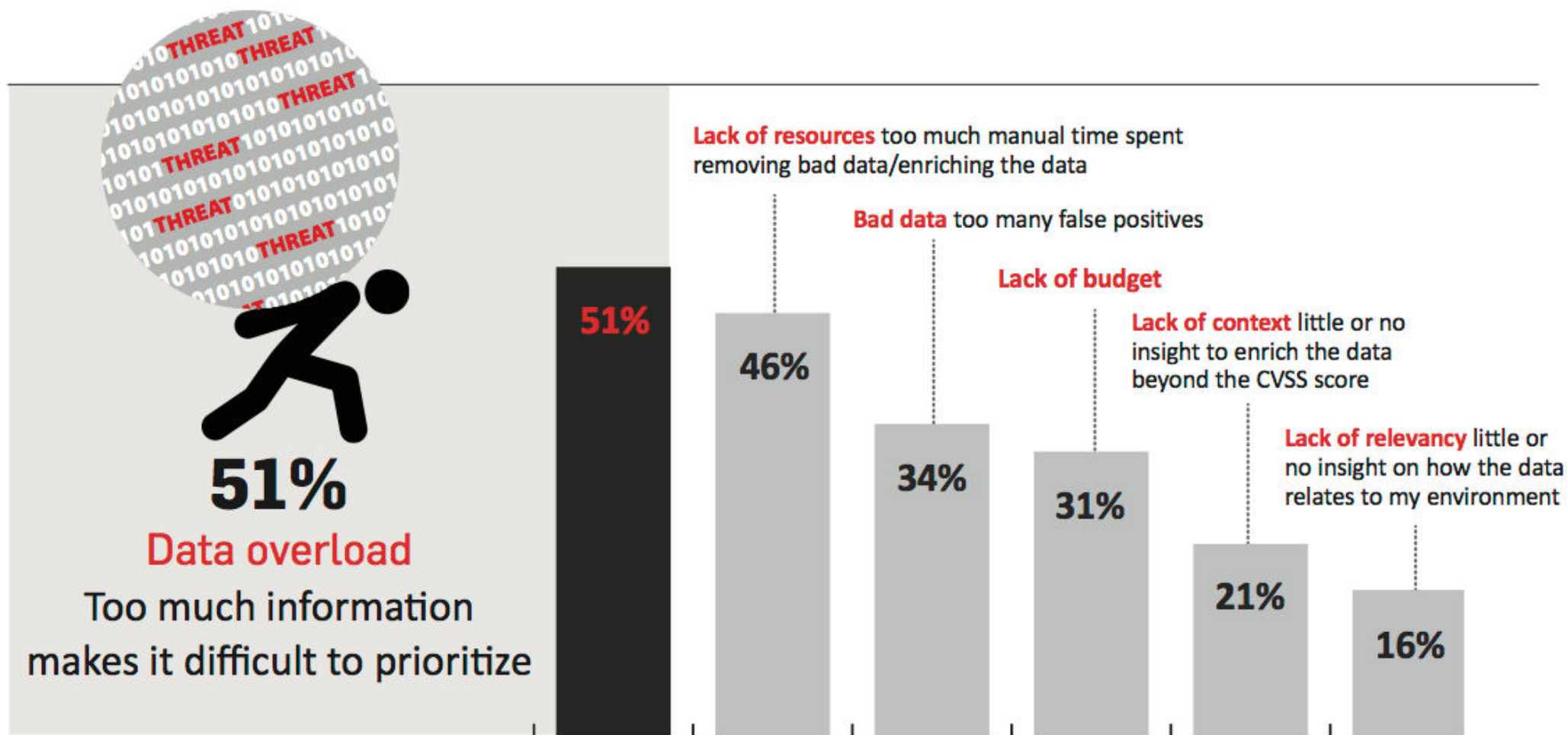
# Restricting Nessus permissions

Not officially supported  
May stop working anytime  
More like security through obscurity rather  
than efficient protection

```
Defaults:scanaccount    !requiretty
Cmd_Alias NESSUSAA = /bin/sh -c echo nessus_su_`echo [0-9]*[0-9]` ; *; echo nessus_su_`echo [0-9]*[0-9]`
Cmd_Alias NESSUSXA = ! /bin/sh -c echo nessus_su_`echo [0-9]*[0-9]` ; *; echo nessus_su_`echo [0-9]*[0-9]`
Cmd_Alias NESSUSXB = ! /bin/sh -c echo nessus_su_`echo [0-9]*[0-9]` ; *; echo nessus_su_`echo [0-9]*[0-9]`
Cmd_Alias NESSUSXC = ! /bin/sh -c echo nessus_su_`echo [0-9]*[0-9]` ; *; echo nessus_su_`echo [0-9]*[0-9]`
scanaccount ALL = (root) NESSUSAA, NESSUSXA, NESSUSXB, NESSUSXC
```



# What is still wrong



(from NopSec “2016 Outlook: Vulnerability Risk Management and Remediation Trends”)



# and what's beyond vulnerability scanning?

Risk management?

Asset management?

Threat intelligence?

Detecting scanning gaps?

Do you really need expensive “state of the art” solution?





# There is an alternative

For pentesters



For splunk, big data and fancy tech  
HUBBLESTACK.IO

For the rest of us





# Simple as that

Import all you scans data to the database  
..do anything you want!

Monitor changes, create scopes, custom reports, whatever  
Avoid VM vendor lock-in







# Use case: asset management

We do not have critical asset inventory!

Wait.. we do. It is called “monitoring”

Use zabbix data to create asset lists

Push back alerts to zabbix





# Use case: advanced risk management

Create exploit capabilities description (CVSS sucks!)  
Add environment data (internal and external scans at least)  
Add anything you want (threat intel)

No part is mandatory!

