Vulnerability Management Overview

2a Jornada Ciberseguridad CUDI - 2022

André R. Landim

Brazilian Academic and Research Network CSIRT

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

CAIS

Educação, Pesquisa
e Inovação em Rede

*** INFORMATION ***

This is not a Risk Management training, the informations shown here is only about fundamentals skills related to RM process.

Who we are?

"We are an advanced national network for higher education, research and innovation. In 1992, we helped bringing the internet to Brazil and we continue promoting innovative use of Information and Communication Technologies, driving science and education for all."

- 27 Points of Presence (PoPs)
- +1500 campuses and units of education, research and health institutions throughout the country
- Benefiting more than 3.5 million users.

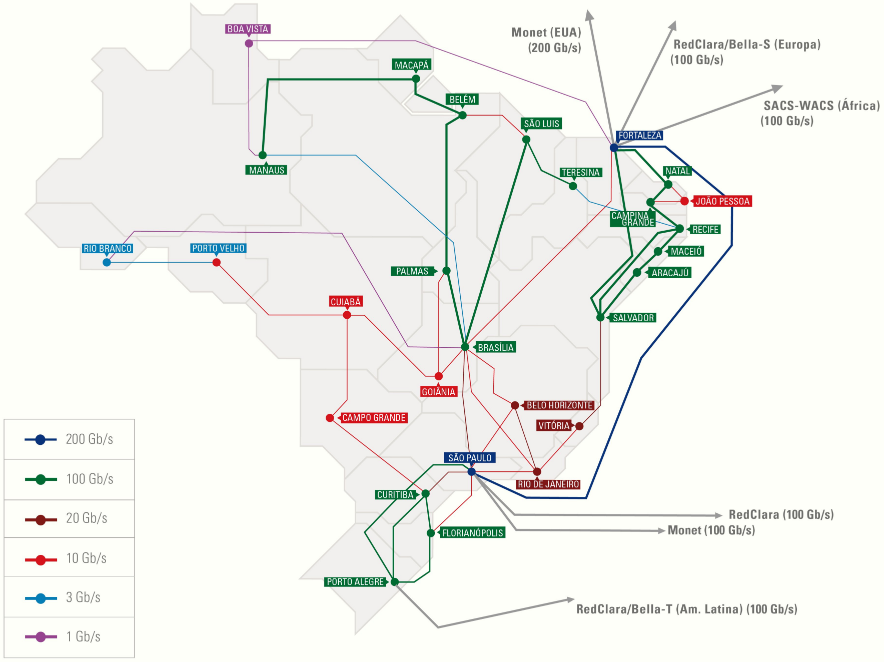
Who we are?

1,97 Tb/s

capacidade agregada

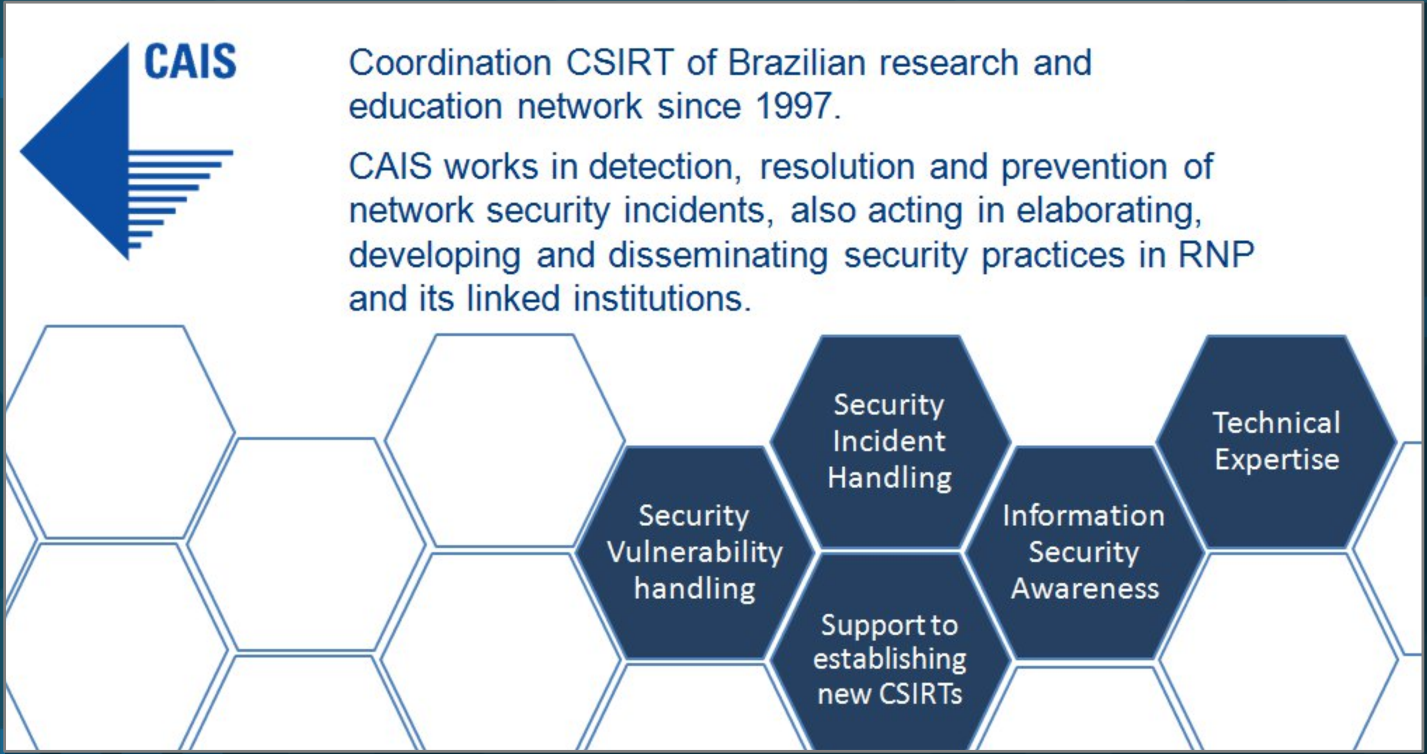
600 Gb/s

Capacidade internacional



redeIpê

Who we are?



CAIS

Coordination CSIRT of Brazilian research and education network since 1997.

CAIS works in detection, resolution and prevention of network security incidents, also acting in elaborating, developing and disseminating security practices in RNP and its linked institutions.

Security Vulnerability handling

Security Incident Handling

Support to establishing new CSIRTs

Information Security Awareness

Technical Expertise

Assets

Any object that have significant importance or value to the organization. That object can be physical or not.

- *Ex.: Informations, systems, devices, pictures, reputation and others.*

http://www.ti-e-mais.com.br/wp-content/uploads/2015/07/Gestao_Ativo_TI.png
http://www.abctec.com.br/wp-content/uploads/2015/04/imagem_adoti.jpg
http://globaw.com.br/wp-content/uploads/2015/02/data-center-TI.jpg

Information Security Risk

It's a result of combination between likelihood and impact.

$R = L \times I$

http://www.gestaoporprocessos.com.br/wp-content/uploads/2015/02/riscos.jpg

Threats

Possible occurrence of a security incident, that can result in a damage for an asset

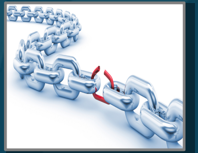
- *Ex.: system break, hurricanes/earthquake, unavailability, etc...*

http://iporto.com.br/wp-content/uploads/2014/03/IPORTO-Aprenda-a-proteger-as-informa%C3%A7%C3%B5es-da-sua-empresa.jpg

Vulnerabilities

Weakness in a device or group of devices that can be exploited

- *“The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities.”*
  - https://www.first.org/cvss/
- *“The Exploit Prediction Scoring System (EPSS) is an open, data-driven effort for predicting when software vulnerabilities will be exploited.”*
  - https://www.first.org/epss/
- *“The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.”*
  - https://www.cve.org/About/Overview
- **CVSS != EPSS != CVE**



http://www.rmcweb.com/wp-content/uploads/2012/01/Vulnerability-Assessments1.jpg

Exploits & Attacks

Intention to execute non-authorized actions like:

- ***Destroy data;***
- ***Leak or Theft of sensitive informations;***
- ***Misuses of devices;***

Exploits, in simple words, is a tool or group of tools they are used by malicious user to explore a vulnerability in a system.

https://www.scmp.com/sites/default/files/2015/07/13/_sin102_36211235.jpg

Basic “modus-operandi” of attack

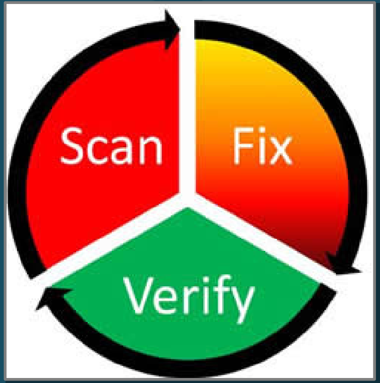
Is very close of a vulnerability assessment or pentest, but the big difference is the main objective ;)

1. *An attacker run a scan against a target network searching for vulnerable devices and services (open ports);*
2. *After this step, based on results of previous step, he tries to exploit the discovered vulnerabilities;*
3. *If the exploit get success, the attacker usually start another step that can be a “lateral movement” or a “privilege scalation”, for example;*
4. *System P0wn3d!!!*

https://www.occupycorporatism.com/wp-content/uploads/2013/04/Access-hacker-attack.jpg

Well… What is Vulnerability Management?

Is a group of coordinated activities with the main goal is to reduce at an acceptable levels the discovered vulnerabilities during a vulnerability analisys of an environment or devices.



http://www.avaintcon.com/uploads/5/8/9/1/5891023/415905635.jpg

Benefits of Vulnerability Management

If an organization don't have a risk management, a vulnerability management can help in many aspects related some technical decisions.

- **VM process don't cover aspects like "reputation".**
  - *The reputation of an organization can be impacted in case of data leak, for example.*

https://cafeemarketing.files.wordpress.com/2013/03/calcular-o-like-e-seguidores.jpg

More Benefits of Vulnerability Management Process…

Knowledge about your environment

- *A VM process enforce the needs about an updated inventory of HW and SW (ITILv3 topic)*

Clearness

- *Clear information about any asset and what is necessary to do*

Helps process of decision

- *Priority*

Some obstacles of Vulnerability Management Process…

(Un)Controlled environment

- *Complexity, chaotic growth, lack of standards…*

Operation cost

- *Tools, team training, time…*

https://grist.files.wordpress.com/2012/01/homer_control_room_600.jpg

Vulnerability Assessment != Pentest

Vulnerability assessments (VA) can generate false positives because they don't exploit the flaws.

- *Some conditions in environment maybe don’t exists in a way to possibilite real exploitation of a vulnerability*

With a pentest it is possible to determine the result of the exploitation of a specific vulnerability

- *It is possible to identify in a clearer way which possible forms of exploitation and which countermeasures can be applied.*

What about "Risk Management"?

According to what we saw earlier, the VM process is similar to the RM process. But, VM process has focus in IT environment

According ISO27001, RM is described by:

- *"Coordinated activities to direct and control an organization with regard to risk"*

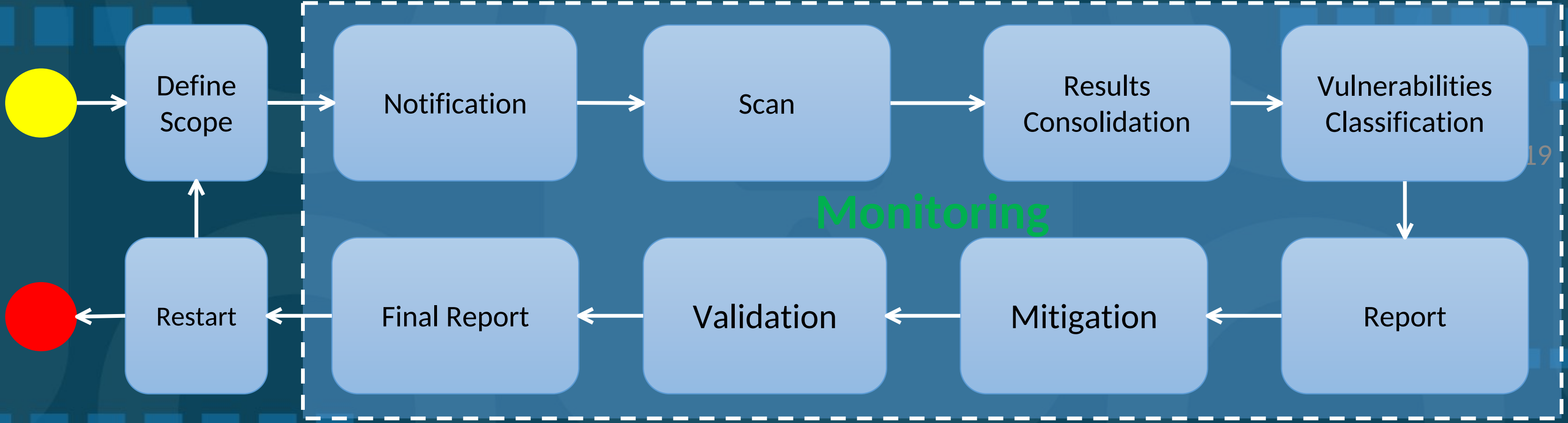
Prerequisites to Vulnerability Management

Looking for establish a minimal efective VM process, we need some basic points. Let’s see :

- *Asset Inventory & Scope definition*
- *Type of Scans & Authorization*
  - *Ondemand X Periodic Scans*
- *Mitigation process*
  - *Vulnerability Classification X Mitigation (update) schedule*
- *Status report process*
- *Restart...*

Basic activities flow

A **basic activities flow** should also be **defined**. This make **clear to** the entire **organization** what the overall **vulnerability management process** is.



VM Process - Asset Inventory

HW inventory

SW inventory

Asset contact owner

- *Licensing and support information*

How often and how to update asset inventory?

What services or group of services each asset or group of assets support

- *Help for RM process*

Scope definition

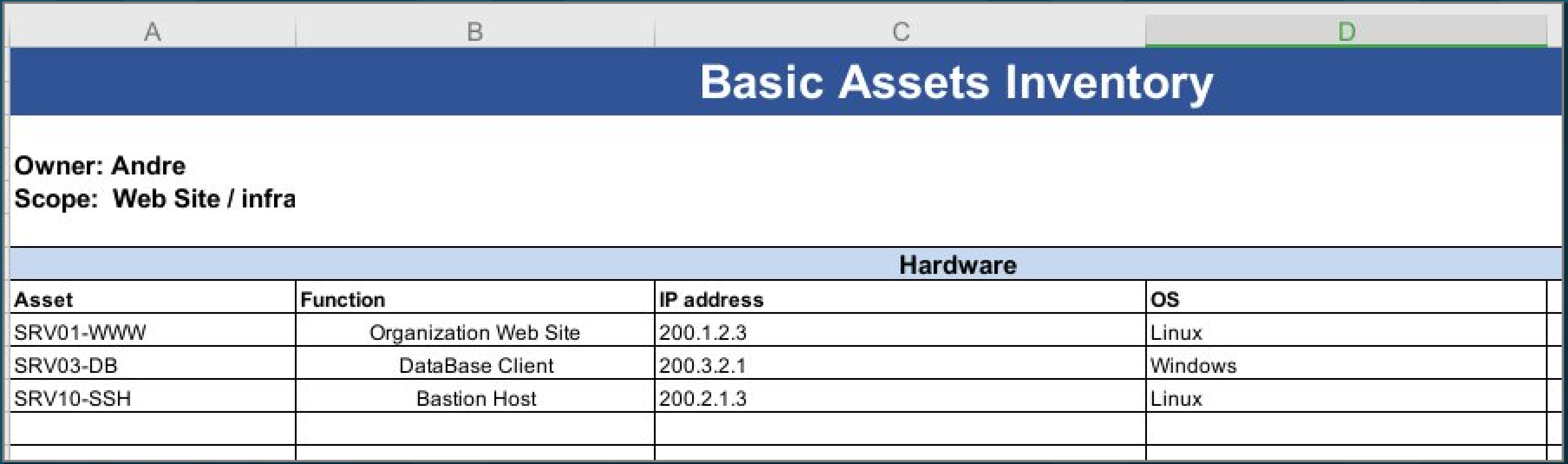
If you are running a VA for the first time, it is recommended to reduce the scan scope.

- *With a small scope, is possible to adequate the scan with some specific aspects of environment.*
- *We can reduce the types of vulnerabilities too. Instead of run a "full-scan", we can select some vulnerabilities to scan, like:*
  - *Services vulnerabilities (NTP, RDP, WWW…)*
  - *OS vulnerabilities (Linux, Windows…)*

Is very difficult define a scope without assets inventory

Scope definition

In specific cases, we can use spreadshets to help us with assets inventory.



Basic Assets Inventory

Owner: Andre
Scope: Web Site / infra

Hardware

Asset	**Function**	**IP address**	**OS**
SRV01-WWW	Organization Web Site	200.1.2.3	Linux
SRV03-DB	DataBase Client	200.3.2.1	Windows
SRV10-SSH	Bastion Host	200.2.1.3	Linux

About assets inventory…

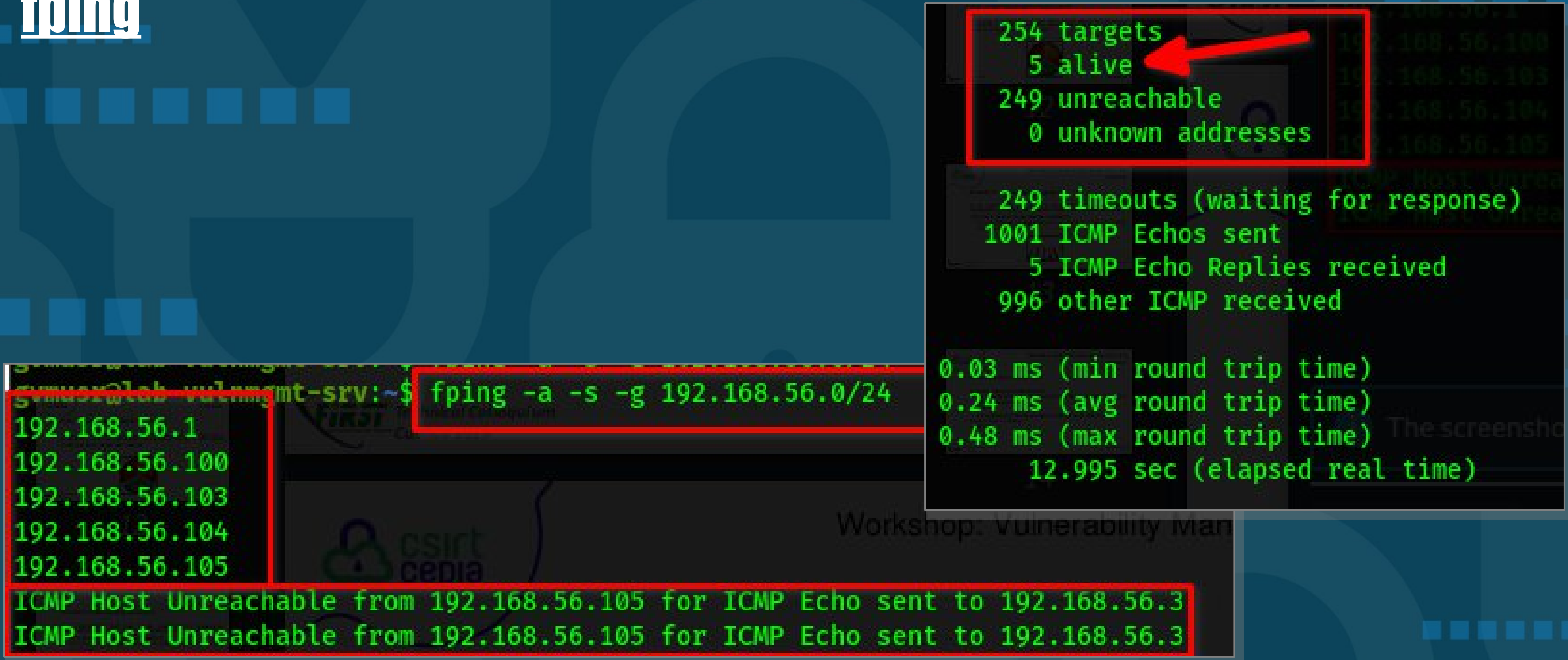
Described on ISO27001

- *It's fundamental for the organization know your assets and know each service or system supported for these assets*

If the asset inventory is not updated we can use some tools to help us discover devices in our network

- *fping*
- *NMAP*
- *GreenBone Vulnerability Management (GVM OpenVAS)*

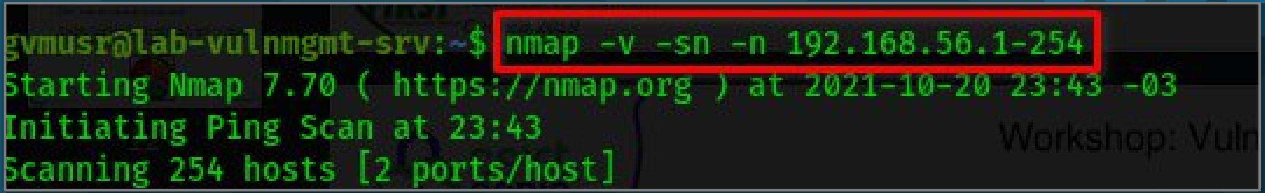
fping



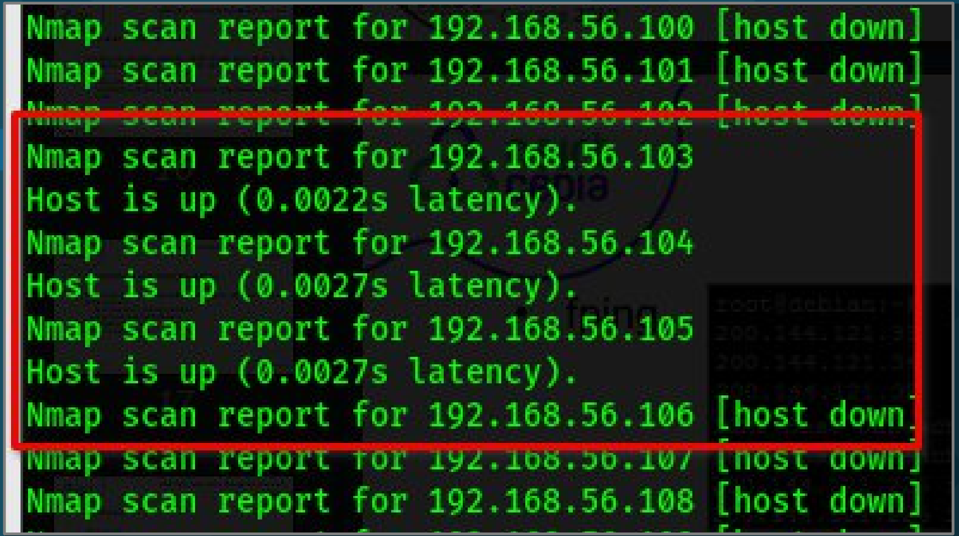
```
gvmuser@lab-vulnmgmt-srv:~$ fping -a -s -g 192.168.56.0/24
192.168.56.1
192.168.56.100
192.168.56.103
192.168.56.104
192.168.56.105
ICMP Host Unreachable from 192.168.56.105 for ICMP Echo sent to 192.168.56.3
ICMP Host Unreachable from 192.168.56.105 for ICMP Echo sent to 192.168.56.3
```

```
     254 targets
       5 alive
     249 unreachable
       0 unknown addresses

     249 timeouts (waiting for response)
    1001 ICMP Echos sent
       5 ICMP Echo Replies received
     996 other ICMP received

 0.03 ms (min round trip time)
 0.24 ms (avg round trip time)
 0.48 ms (max round trip time)
       12.995 sec (elapsed real time)
```

NMAP

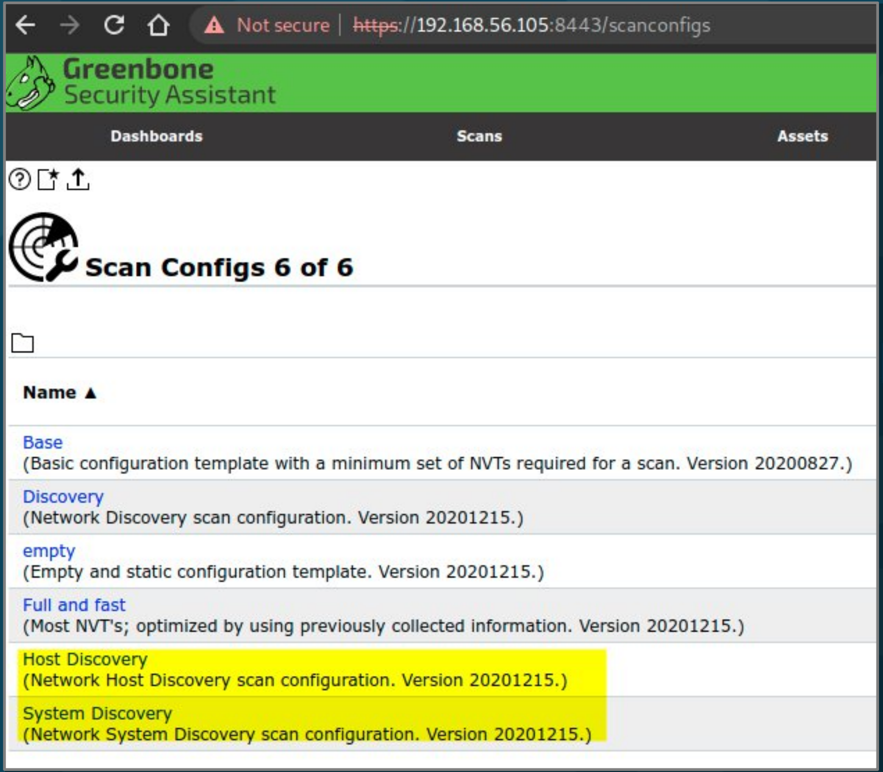


```
gvmusr@lab-vulnmgmt-srv:~$ nmap -v -sn -n 192.168.56.1-254
Starting Nmap 7.70 ( https://nmap.org ) at 2021-10-20 23:43 -03
Initiating Ping Scan at 23:43
Scanning 254 hosts [2 ports/host]
```



```
Nmap scan report for 192.168.56.100 [host down]
Nmap scan report for 192.168.56.101 [host down]
Nmap scan report for 192.168.56.102 [host down]
Nmap scan report for 192.168.56.103
Host is up (0.0022s latency).
Nmap scan report for 192.168.56.104
Host is up (0.0027s latency).
Nmap scan report for 192.168.56.105
Host is up (0.0027s latency).
Nmap scan report for 192.168.56.106 [host down]
Nmap scan report for 192.168.56.107 [host down]
Nmap scan report for 192.168.56.108 [host down]
```

GVM OpenVAS



Scan Configs 6 of 6

Name ▲

Base
(Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)

Discovery
(Network Discovery scan configuration. Version 20201215.)

empty
(Empty and static configuration template. Version 20201215.)

Full and fast
(Most NVT's; optimized by using previously collected information. Version 20201215.)

Host Discovery
(Network Host Discovery scan configuration. Version 20201215.)

System Discovery
(Network System Discovery scan configuration. Version 20201215.)

Type of scans and Authorization

We can have different scan schedules in according to type of assets or group of assets

Authorization

- *Before start a scan, we must inform the owners of assets assets about scan*

The owners of assets they are interested in receive reports immediately at the end of scans or the results must be presented in a status report meeting?

- *False Positve X "PATCH NOW!"*

Scanning…

Commercial Tools

- *Nexpose, Nessus, QualysGuard (Infrastructure – Web with additional modules)*
- *N-Stalker, Acunetix, Burp Suite (Web Applications)*

Open/free Tools

- *GreenBone Vulnerability Manager (GVM OpenVAS) & NMAP (+NSE) (Infrastructure – Web with limitations);*
- *w3af, OWASP ZAP, wapiti, arachni (Web Applications);*

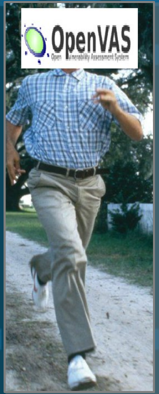
Vulnerability Analisys - RUN VA Scan... RUN!!!

The VA scan can be different focus and some tools that fits better, depending of your goals. IE:

- *Network scan + Simple vulnerability discover : NMAP + NSE Scripts*
- *Vulnerability Assessment System: GVM OpenVAS*
- *Web Application vulnerability scan: OWASP ZAP & wapiti*

ZAP

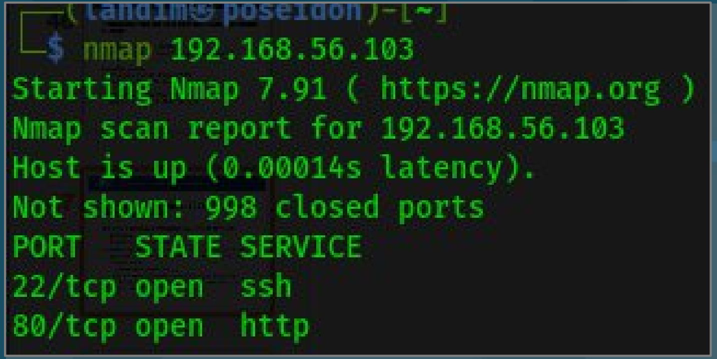
NMAP.ORG



Scanning tools - NMAP

“Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.”

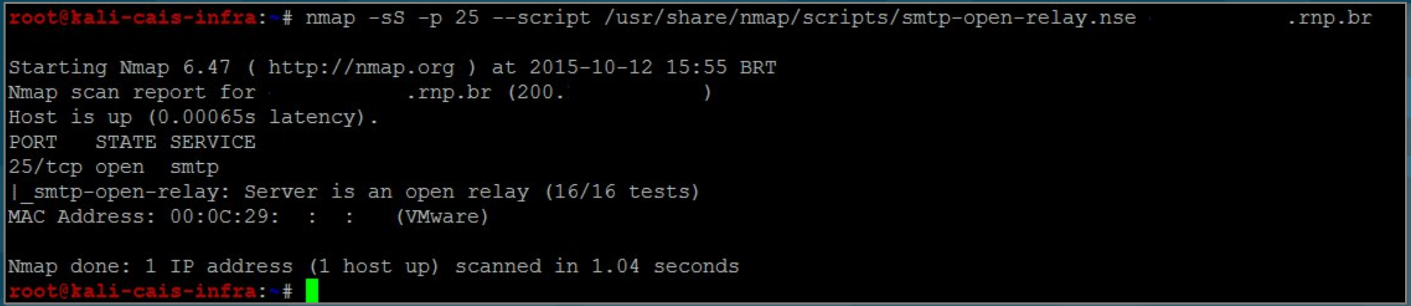
- ***https://nmap.org/***
- ***ZENMap (frontend)***
- ***XML reports***
  - ***XML to HTML with xsltproc tool***



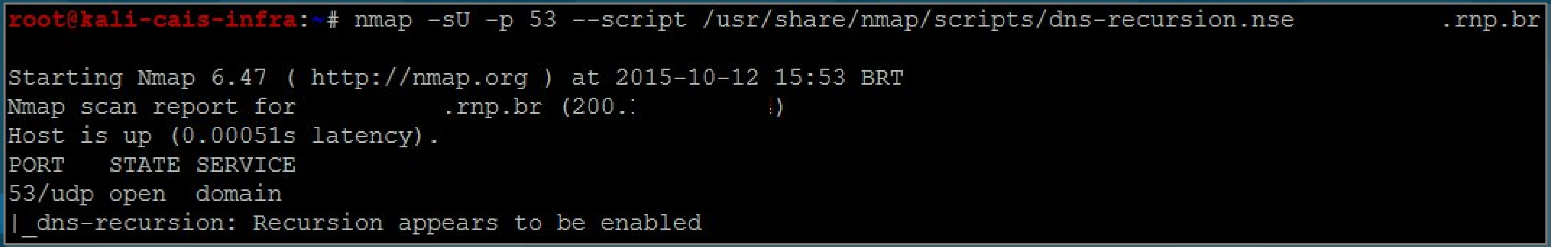
```
┌──(landim㉿poseidon)-[~]
└─$ nmap 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for 192.168.56.103
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Scanning tools - NMAP + NSE scripts

- ***SMTP Relay***
- ***DNS Recursion***



```
root@kali-cais-infra:~# nmap -sS -p 25 --script /usr/share/nmap/scripts/smtp-open-relay.nse [redacted].rnp.br

Starting Nmap 6.47 ( http://nmap.org ) at 2015-10-12 15:55 BRT
Nmap scan report for [redacted].rnp.br (200.[redacted])
Host is up (0.00065s latency).
PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server is an open relay (16/16 tests)
MAC Address: 00:0C:29:[redacted]:[redacted]:[redacted] (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
root@kali-cais-infra:~#
```



```
root@kali-cais-infra:~# nmap -sU -p 53 --script /usr/share/nmap/scripts/dns-recursion.nse [redacted].rnp.br

Starting Nmap 6.47 ( http://nmap.org ) at 2015-10-12 15:53 BRT
Nmap scan report for [redacted].rnp.br (200.[redacted])
Host is up (0.00051s latency).
PORT   STATE SERVICE
53/udp open  domain
|_dns-recursion: Recursion appears to be enabled
```

Scanning tools - GVM OpenVAS

From web site *(https://www.openvas.org/)*

- *"Open Vulnerability Assessment Scanner (OpenVAS) is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test."*
- *"OpenVAS has been developed and driven forward by the company Greenbone Networks since 2006. As part of the commercial vulnerability management product family "Greenbone Security Manager" (GSM), the scanner forms the Greenbone Vulnerability Management together with other Open Source modules."*

Scanning tools - GVM OpenVAS

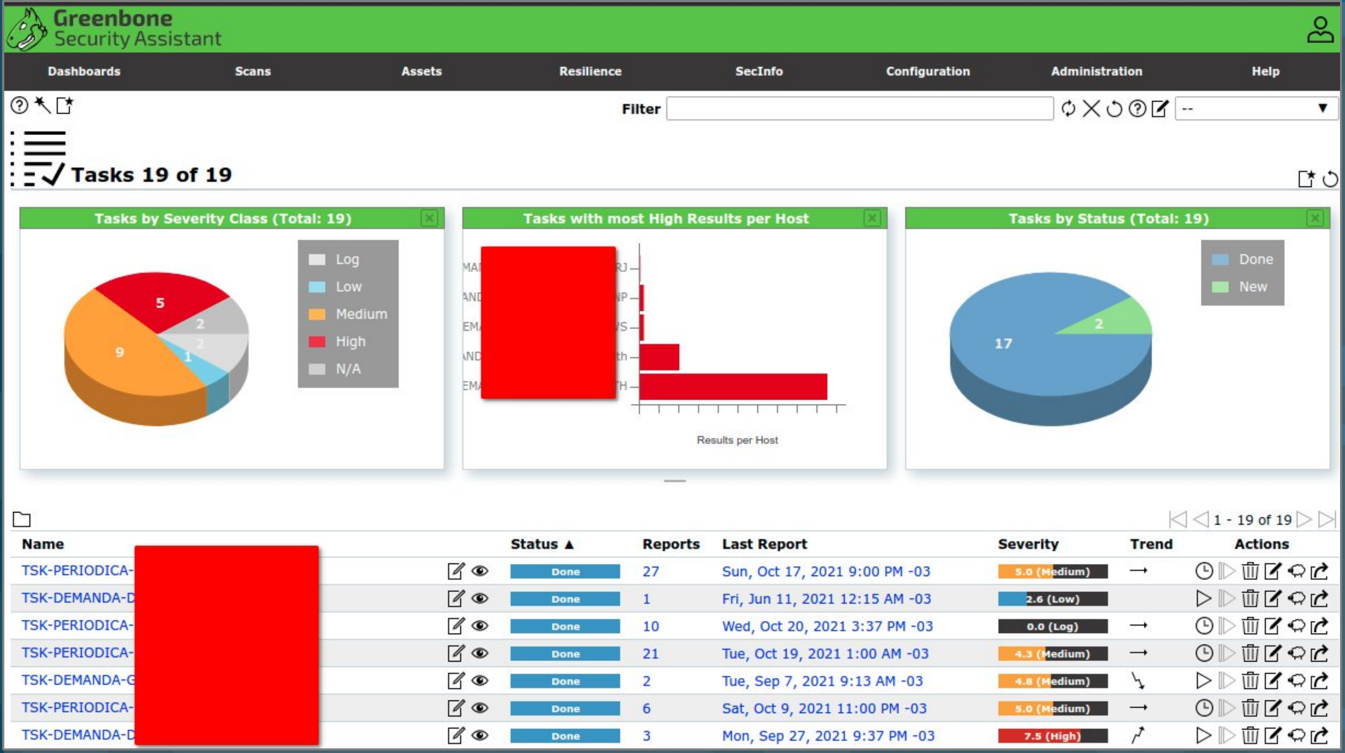
Born from Nessus (fork from old open-source version);

More than 100k Network Vulnerability Tests (NVTs);

Nowadays is on version 22.4

- *Source Code download*
- *Cloud server*
- *Commercial platform*

GVM OpenVAS

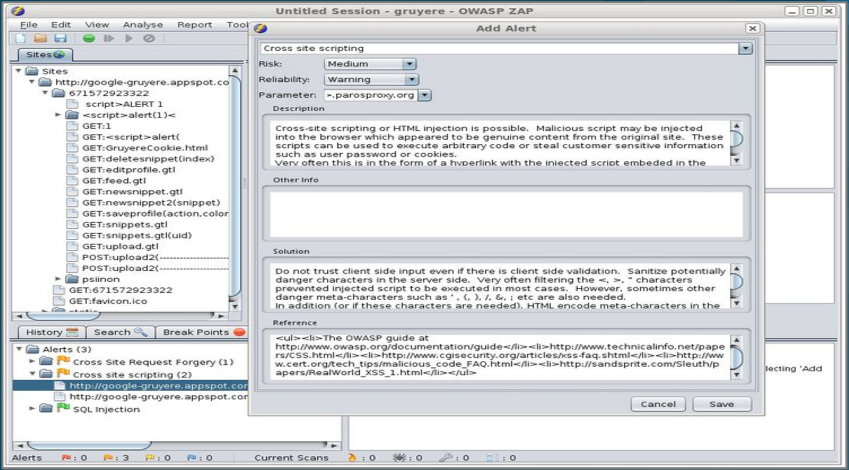


Name		Status ▲	Reports	Last Report	Severity	Trend	Actions
TSK-PERIODICA-[redacted]		Done	27	Sun, Oct 17, 2021 9:00 PM -03	5.0 (Medium)	→	
TSK-DEMANDA-D[redacted]		Done	1	Fri, Jun 11, 2021 12:15 AM -03	2.6 (Low)		
TSK-PERIODICA-[redacted]		Done	10	Wed, Oct 20, 2021 3:37 PM -03	0.0 (Log)	→	
TSK-PERIODICA-[redacted]		Done	21	Tue, Oct 19, 2021 1:00 AM -03	4.3 (Medium)	→	
TSK-DEMANDA-G[redacted]		Done	2	Tue, Sep 7, 2021 9:13 AM -03	4.8 (Medium)	↘	
TSK-PERIODICA-[redacted]		Done	6	Sat, Oct 9, 2021 11:00 PM -03	5.0 (Medium)	→	
TSK-DEMANDA-D[redacted]		Done	3	Mon, Sep 27, 2021 9:37 PM -03	7.5 (High)	↗	

Scanning tools - OWASP Zed Attack Proxy

Web Application Analysis Tool;

- *Automated Functions + Manual inspections*
- *https://owasp.org/www-project-zap/*



Cross site scripting

Risk: Medium

Reliability: Warning

Parameter: >.parosproxy.org

Description

Cross-site scripting or HTML injection is possible. Malicious script may be injected into the browser which appeared to be genuine content from the original site. These scripts can be used to execute arbitrary code or steal customer sensitive information such as user password or cookies.
Very often this is in the form of a hyperlink with the injected script embeded in the

Other Info

Solution

Do not trust client side input even if there is client side validation. Sanitize potentially danger characters in the server side. Very often filtering the <, >, " characters prevented injected script to be executed in most cases. However, sometimes other danger meta-characters such as ' , (,), /, &, ; etc are also needed.
In addition (or if these characters are needed), HTML encode meta-characters in the

Reference

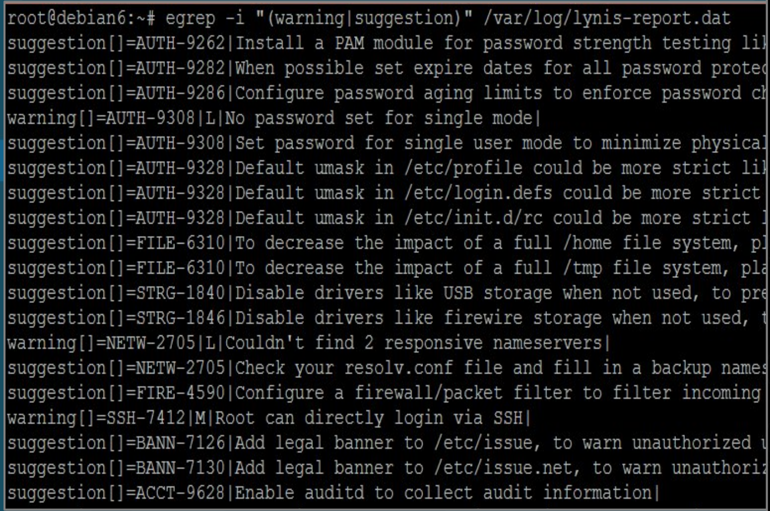
```
<ul><li>The OWASP guide at
http://www.owasp.org/documentation/guide</li><li>http://www.technicalinfo.net/pape
rs/CSS.html</li><li>http://www.cgisecurity.org/articles/xss-faq.shtml</li><li>http://ww
w.cert.org/tech_tips/malicious_code_FAQ.html</li><li>http://sandsprite.com/Sleuth/p
apers/RealWorld_XSS_1.html</li></ul>
```

Scanning tools - Lynis

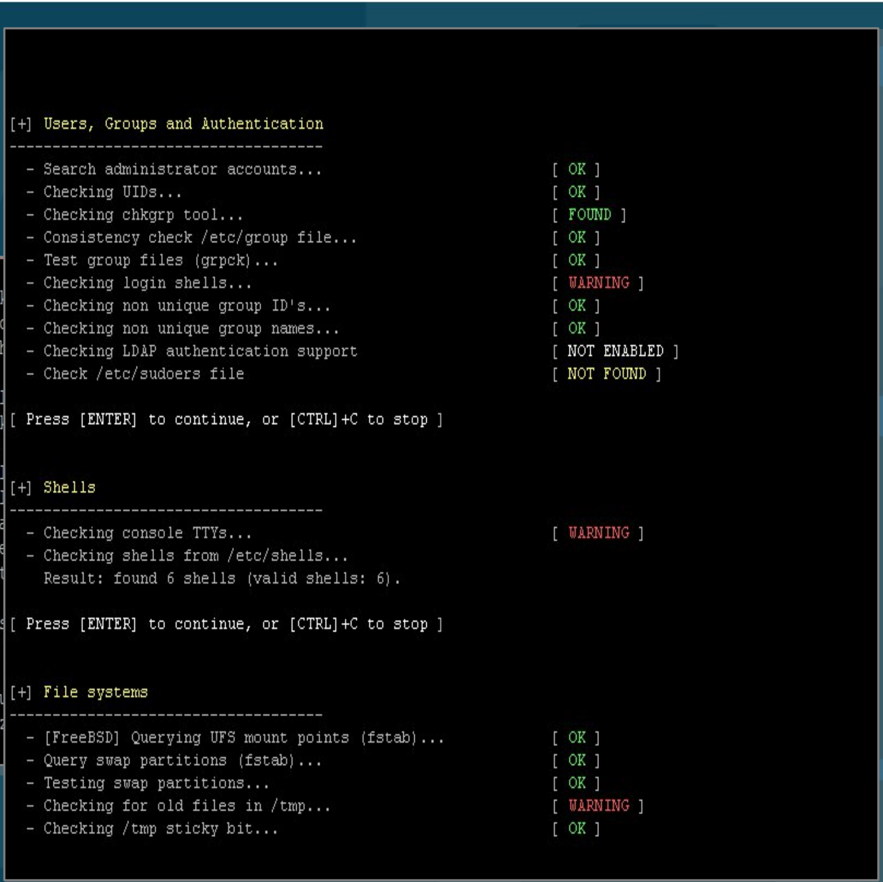
Open Source Audit Tool ("Unix-like" systems)

- *https://cisofy.com/lynis/*
- *Runs local & remote*
- *Excellent performance*
- *Perform hundreds of tests to determine the security/compliance status of a system*
- *No installation required*
- *It doesn't make corrections – it just points out the issues*
- *The information in the report is useful for inventory.*

Lynis



```
root@debian6:~# egrep -i "(warning|suggestion)" /var/log/lynis-report.dat
suggestion[]=AUTH-9262|Install a PAM module for password strength testing li
suggestion[]=AUTH-9282|When possible set expire dates for all password protec
suggestion[]=AUTH-9286|Configure password aging limits to enforce password ch
warning[]=AUTH-9308|L|No password set for single mode|
suggestion[]=AUTH-9308|Set password for single user mode to minimize physical
suggestion[]=AUTH-9328|Default umask in /etc/profile could be more strict li
suggestion[]=AUTH-9328|Default umask in /etc/login.defs could be more strict
suggestion[]=AUTH-9328|Default umask in /etc/init.d/rc could be more strict l
suggestion[]=FILE-6310|To decrease the impact of a full /home file system, pl
suggestion[]=FILE-6310|To decrease the impact of a full /tmp file system, pla
suggestion[]=STRG-1840|Disable drivers like USB storage when not used, to pre
suggestion[]=STRG-1846|Disable drivers like firewire storage when not used, t
warning[]=NETW-2705|L|Couldn't find 2 responsive nameservers|
suggestion[]=NETW-2705|Check your resolv.conf file and fill in a backup names
suggestion[]=FIRE-4590|Configure a firewall/packet filter to filter incoming
warning[]=SSH-7412|M|Root can directly login via SSH|
suggestion[]=BANN-7126|Add legal banner to /etc/issue, to warn unauthorized u
suggestion[]=BANN-7130|Add legal banner to /etc/issue.net, to warn unauthoriz
suggestion[]=ACCT-9628|Enable auditd to collect audit information|
```



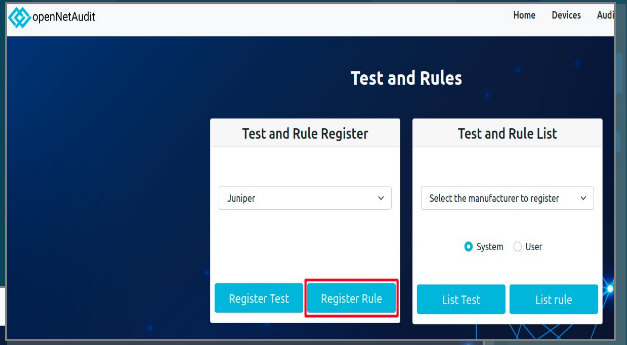
```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts...                        [ OK ]
  - Checking UIDs...                                        [ OK ]
  - Checking chkgrp tool...                                 [ FOUND ]
  - Consistency check /etc/group file...                    [ OK ]
  - Test group files (grpck)...                             [ OK ]
  - Checking login shells...                                [ WARNING ]
  - Checking non unique group ID's...                       [ OK ]
  - Checking non unique group names...                      [ OK ]
  - Checking LDAP authentication support                    [ NOT ENABLED ]
  - Check /etc/sudoers file                                 [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] Shells
------------------------------------
  - Checking console TTYs...                                [ WARNING ]
  - Checking shells from /etc/shells...
    Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] File systems
------------------------------------
  - [FreeBSD] Querying UFS mount points (fstab)...          [ OK ]
  - Query swap partitions (fstab)...                        [ OK ]
  - Testing swap partitions...                              [ OK ]
  - Checking for old files in /tmp...                       [ WARNING ]
  - Checking /tmp sticky bit...                             [ OK ]
```

Scanning tools - openNetAudit

“OpenNetAudit was build with the objective of mantaining your routers secure in a easy and simple way”

Devices supported

- *CISCO, Juniper, Extreme, Huawei & Mikrotic*
- *https://netaudit.rnp.br/*



Test and Rules

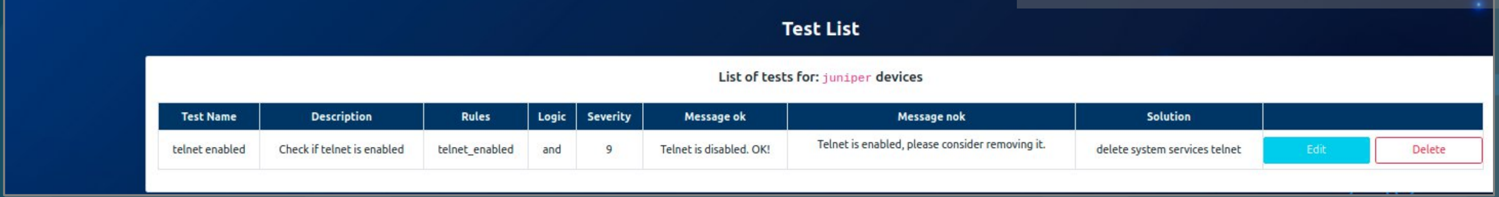
Test and Rule Register

Juniper

Test and Rule List

Select the manufacturer to register

● System ○ User



Test List

List of tests for: juniper devices

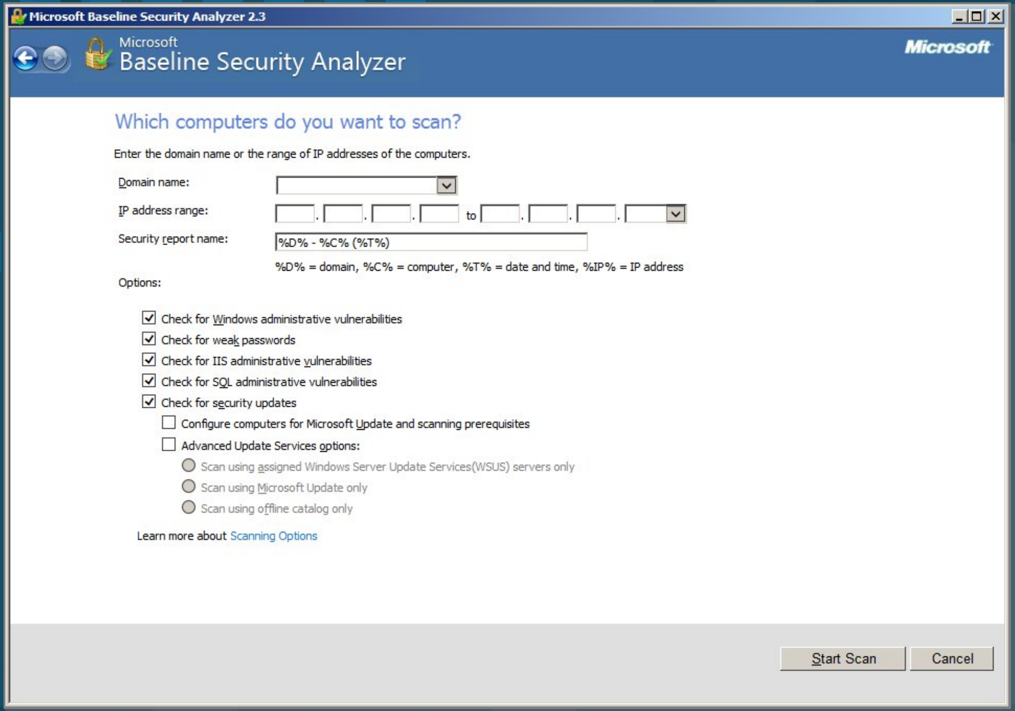
Test Name	Description	Rules	Logic	Severity	Message ok	Message nok	Solution	
telnet enabled	Check if telnet is enabled	telnet_enabled	and	9	Telnet is disabled. OK!	Telnet is enabled, please consider removing it.	delete system services telnet	Edit Delete

Scanning tools - Microsoft Baseline Security Analyzer - MBSA

Discontinued (legacy systems) =/

- Recommendations based on MS guidelines
- Supports several MS products
- Information integrated with WUA/WSUS
- Local & Remote

MBSA



Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Which computers do you want to scan?

Enter the domain name or the range of IP addresses of the computers.

Domain name:

IP address range: . . . to . . .

Security report name: %D% - %C% (%T%)

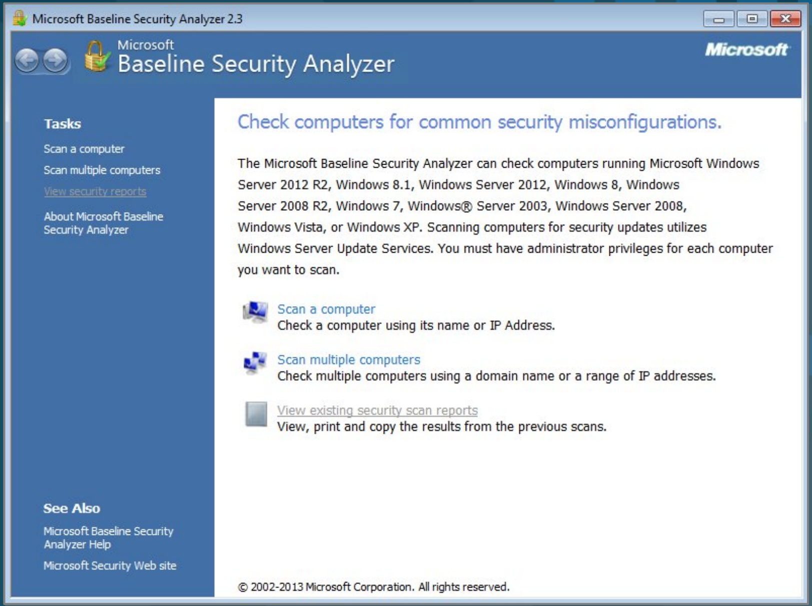
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- ☑ Check for Windows administrative vulnerabilities
- ☑ Check for weak passwords
- ☑ Check for IIS administrative vulnerabilities
- ☑ Check for SQL administrative vulnerabilities
- ☑ Check for security updates
  - □ Configure computers for Microsoft Update and scanning prerequisites
  - □ Advanced Update Services options:
    - ○ Scan using assigned Windows Server Update Services(WSUS) servers only
    - ○ Scan using Microsoft Update only
    - ○ Scan using offline catalog only

Learn more about Scanning Options

Microsoft
Start Scan
Cancel



Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2013 Microsoft Corporation. All rights reserved.

Results consolidation & Vulnerabilities classification

What information a report must have?

How frequency ?

Should critical vulnerabilities have a different process?

- *Needs to isolate environment?*
- *Emergencial maintenance windows*

Results consolidation & Vulnerabilities classification

The analyst that perfomed the VA is responsible to create a report/presentation that will be delivered/presented to those responsible for the assets or systems.

- *Analyst must understand the results and validate them looking to reduce the number of false positives, ensuring greater reliability to the process*

It's not recommended share automatically generated reports!!!

Results consolidation & Vulnerabilities classification

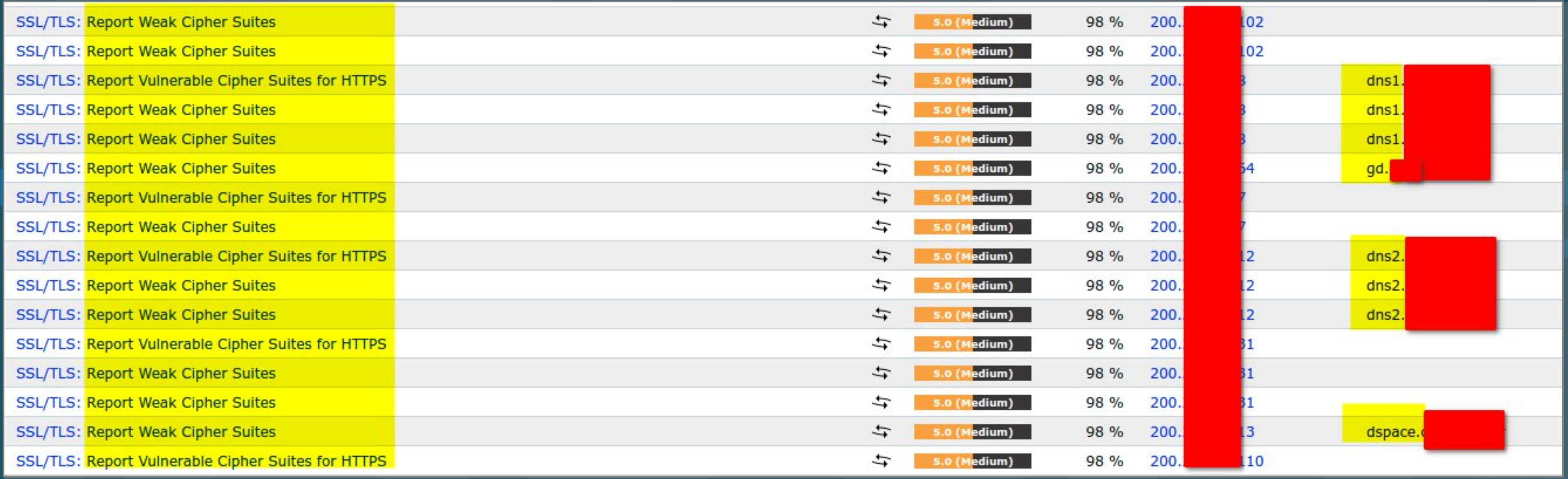
There are different type of reports, in different formats and types of informations

- *Technical: contain detailed information about each one vulnerability discovered and how to mitigate then*
- *Executive: Consolidate informations about total of vulnerabilities, total for assets, severity classification, etc.*

Informations must be aligned with recipients

- *Managers X Analysts X Auditors*

Results consolidation & Vulnerabilities classification



SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]102	
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]102	
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	5.0 (Medium)	98 %	200.[redacted]3	dns1.[redacted]
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]3	dns1.[redacted]
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]3	dns1.[redacted]
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]4	gd.[redacted]
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	5.0 (Medium)	98 %	200.[redacted]7	
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]7	
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	5.0 (Medium)	98 %	200.[redacted]12	dns2.[redacted]
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]12	dns2.[redacted]
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]12	dns2.[redacted]
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	5.0 (Medium)	98 %	200.[redacted]31	
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]31	
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]31	
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	200.[redacted]13	dspace.[redacted]
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	5.0 (Medium)	98 %	200.[redacted]110	

Results consolidation & Vulnerabilities classification

Can you see possible inconsistent data in previous informations?

Discussion…

Creating reports

Quality of information is fundamental. The informations needs focus in:

- *Public (managers, auditors, analysts...)*
- *Bring relevant information to take decisions about next steps*
- *Show the actual scenario of vulnerabilities in defined scope*

Creating reports

Recommended informations for technical staff

- *Assets & areas affected by vulnerability*
- *Description of vulnerability & Severity*
- *Exploits information*
  - *Evidence of compromisse*
- *How the vulnerability was discovered*
  - *Type of scan or tool used in this case*
- *Countermeasures available*

Creating reports

Recommended informations for managers

- *Assets & areas affected by vulnerability*
- *Description of vulnerability & Severity*
- *Mitigation process*
  - *Scheduled maintenance X Emergencial maintenance X Downtime expected*
  - *Rollback plan*

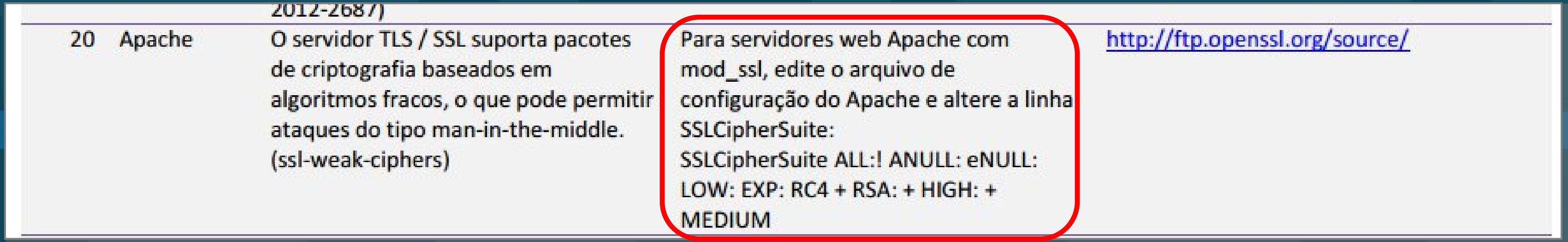
Creating reports

Recommended informations for auditors

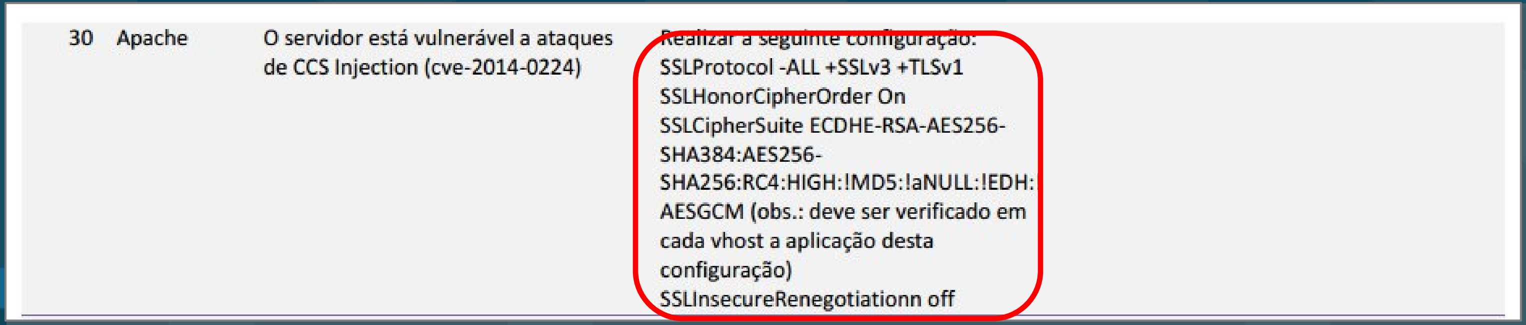
- *Assets & areas affected by vulnerability*
- *Description of vulnerability & Severity*
- *Exploits information*
- *Evidence of compromisse*
- *Applied countermeasures & Mitigation status*

Creating reports - Common mistakes

Confused mitigation informations



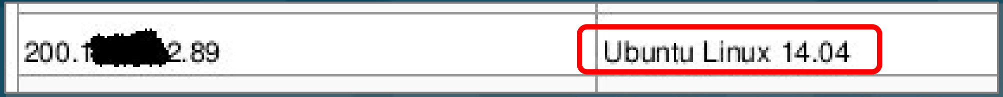
		2012-2687)		
20	Apache	O servidor TLS / SSL suporta pacotes de criptografia baseados em algoritmos fracos, o que pode permitir ataques do tipo man-in-the-middle. (ssl-weak-ciphers)	Para servidores web Apache com mod_ssl, edite o arquivo de configuração do Apache e altere a linha SSLCipherSuite: SSLCipherSuite ALL:! ANULL: eNULL: LOW: EXP: RC4 + RSA: + HIGH: + MEDIUM	http://ftp.openssl.org/source/



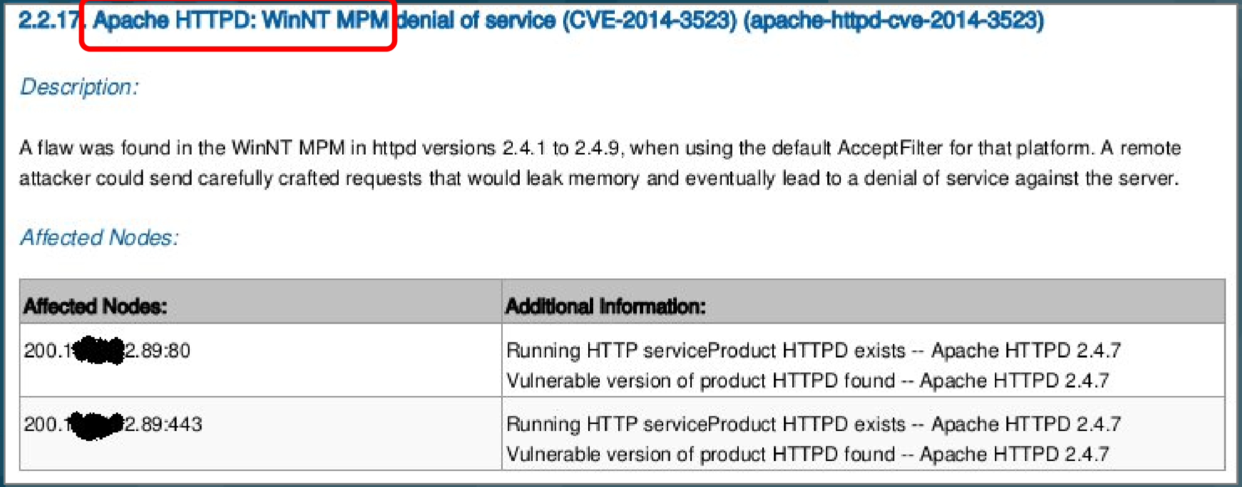
30	Apache	O servidor está vulnerável a ataques de CCS Injection (cve-2014-0224)	Realizar a seguinte configuração: SSLProtocol -ALL +SSLv3 +TLSv1 SSLHonorCipherOrder On SSLCipherSuite ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH:AESGCM (obs.: deve ser verificado em cada vhost a aplicação desta configuração) SSLInsecureRenegotiationn off

Creating reports - Common mistakes

Confused platform informations



200.1[redacted]2.89	Ubuntu Linux 14.04



2.2.17. Apache HTTPD: WinNT MPM denial of service (CVE-2014-3523) (apache-httpd-cve-2014-3523)

Description:

A flaw was found in the WinNT MPM in httpd versions 2.4.1 to 2.4.9, when using the default AcceptFilter for that platform. A remote attacker could send carefully crafted requests that would leak memory and eventually lead to a denial of service against the server.

Affected Nodes:

Affected Nodes:	Additional Information:
200.1[redacted]2.89:80	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.7 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.7
200.1[redacted]2.89:443	Running HTTP serviceProduct HTTPD exists -- Apache HTTPD 2.4.7 Vulnerable version of product HTTPD found -- Apache HTTPD 2.4.7

Mitigation process

Maintenance schedule X Emergencial update

- *Vulnerability classification X Priority patches*
- *High X Medium X Low? (CVSS / EPSS)*

What maximum expected time to apply critical patches?

- *External X Internal services*

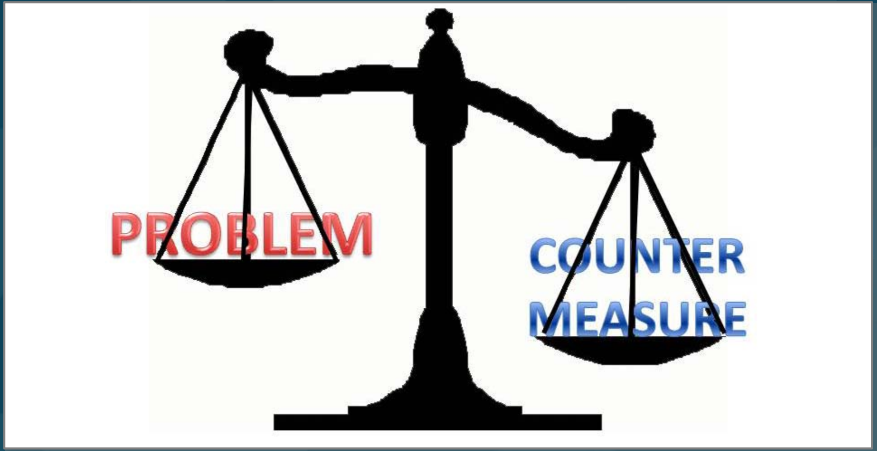
Mitigation/notification process in case of critical vulnerabilities

- *External X Internal services*

Mitigation process

Countermeasures

- *Patches*
  - *“Virtual patch”*
- *Fix configuration*
  - *Disable specific module*
- *Update system*
- *And… “C’est la vie”*



Mitigation process

What we need to consider about mitigations

- Cost of mitigation
  - Renew license, buy new version of SW…
- Downtime
- Severity
- Attack surface
  - Systems affected (exposition)
  - Impacted areas
- Fallback plan

Mitigation process

Apply mitigations in a controlled environment

- *Test environment*
  - *Used to TEST functions, configurations and updates*
- *Non-production environment*
  - *Used to VALIDATE functions, configurations and updates in an environment similar of the "production"*

Validation process

This step is like a “re-scan” of environment

Is recommended that it be executed by same analyst that who does the first execution

All premisses are they applied here

Validation process

The same tools and steps must be repeated here

- *Collect evidence about mitigations*
  - *They are fixed vulnerabilities?*
- *Create final report*

Conclusion…

- ***All areas*** **must be** ***involved*** **in** ***Vulnerability Management process***
  - *“Time is money…”*
- **Run** ***different tools*** **bring** ***more quality*** **to the process, but make this** ***more complexity***
- ***Stay update always…***

OBRIGADO!!!

André Ricardo LANDIM

andre.landim@cais.rnp.br

@a_landim_xhkl

https://www.rnp.br/sistema-rnp/cais

https://www.linkedin.com/in/andrelandim/

CAIS Centro de Atendimento a Incidentes de Segurança

RNP
REDE NACIONAL DE
ENSINO E PESQUISA