

The background is a dark blue gradient with faint, semi-transparent technical and financial graphics. It includes terms like 'VIRTUAL SWITCH', 'NODES ROUTER', and 'COM' scattered across the top. On the right side, there are two line charts: one showing a fluctuating line graph and another showing a bar chart with numerical labels like '34,0366' and '43,1234'.

Réaliser son premier test de sécurité

Desjardins - Forum Sécurité / Fraude 2018

**Qu'entend-on par
“test de sécurité” ?**

Ce que ce n'est pas

Dans le contexte de cette présentation, un “Test de Sécurité” n'est pas:

- Un test d'intrusion (Pentest).
- Un audit à des fins de conformité réglementaire.
- Un test réalisé à l'externe / mandat de sécurité.
- Une liste exhaustive de toutes les options possibles pour exécuter un tel test.

Objectif de la présentation

- Rappeler les bases et leur priorité en matière de sécurité TI.
- Démontrer une façon dont des compagnies actuellement sous-outillées en matière de sécurité peuvent obtenir une vision détaillée de la sécurité de leur périmètre et de leurs actifs internes.
- Expliquer pourquoi les limites de ressources de ces compagnies limite leur capacité d'effectuer ce travail efficacement en continu.

Qu'est-ce qu'un test de sécurité ?

Une ressource de référence, le CIS Top 20, priorise les besoins en matière de sécurité comme tel:

1. **Inventory and Control of Hardware Assets**
2. **Inventory and Control of Software Assets**
3. **Continuous Vulnerability Management (detection + Remediation)**
- ...
9. Limitation and Control of Network Ports, Protocols, and Services (Firewalls, IPS)
- ...
20. Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

1 et 2 : Obtenir un inventaire matériel et logiciel

Vérification de l'existence d'appareils sur le réseau en mode "black box/attaquant":

- Trouver les appareils connectés, gérés ET non-gérés
- Vérifier ce qu'ils exposent au réseau
- Vérifier ce qui y est installé (si possible)
- Trouver les sites Web exposés (dev, prod, intranet, etc.)
- Catégoriser le tout (ligne d'affaire, sous-réseau, type de matériel, etc)

3 : Effectuer de la détection et remédiation de vulnérabilité en continu

Vérifier à la fois les machines et les sites Web pour des vulnérabilités et produire des données “digestes” pour remédiation:

- Balayage de vulnérabilité machine
- Balayage de vulnérabilité Web
- Filtrer les faux positifs
- Extraire les données / Produire des rapports
- Prioriser la remédiation
- Gérer les vulnérabilités “Out-Of-Band”

Obtenir un inventaire matériel et logiciel

Trouver les appareils connectés, gérés ET non-gérés

Point de départ habituel: une liste d'IPs, de Subnets, de sites Web connus de la compagnie

Réseau Externe	Responsable	Réseau Interne	Responsable
www.monsite.com	Compagnie	www.dev.monsite.com	Compagnie
127.254.238.0/28	Compagnie / Personne 2	www.qa.monsite.com	Compagnie / Personne 2
127.226.55.0/29	Compagnie / Personne 1	192.168.10.0/24	Compagnie / Équipe 1
127.256.9.0/32	Compagnie / Personne 1	10.0.20.0/24	Compagnie / Équipe 2
127.254.45.0/24
127.109.20.0/27
...
www.beta.monsite.com	Compagnie	10.0.1.0/24	Compagnie / Équipe 2
www.client1.com/test/	Client1	10.0.60.0/24	Compagnie / Équipe 1
www.client2.com	Client2		
mtl.client1.portal.com	Client1		
mtl.client2.portal.com	Client2		

Trouver les appareils connectés, gérés ET non-gérés

1 - Trouvons les machines qui répondent

Outils disponibles

nmap, zmap, fmg, zenmap, dmitry, p0f, unicornscan, ...

```
$nmap -oG - -sP 10.0.60.0/24
```

```
...
```

```
Host: 10.0.60.101 (hostname1) Status: Up
```

```
Host: 10.0.60.118 (hostname2) Status: Up
```

```
...
```

Trouver les appareils connectés, gérés ET non-gérés

2 - Vérifier ce qui y est installé et exposé au réseau:

Quels sont les ports communs ouverts de ces machines, leur OS et de l'information sur leurs services:

- Quels ports TCP et UDP sont intéressants ?
 - **TCP:** 21-23,25,53,80,110-111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080,etc.
 - **UDP:** 53,67-69,123,135,137-139,161-162,445,500,514,520,631,1434,1900,4500,49152, etc.

```
$sudo nmap --privileged -n -PE -PS<PORTS_TCP> -PU<PORTS_UDP> -sS -sU -O --osscan-guess
--max-os-tries 1 -p T:<PORTS_TCP>,U:<PORTS_UDP> --max-retries 3 --min-rtt-timeout 100ms
--max-rtt-timeout 3000ms --initial-rtt-timeout 500ms --defeat-rst-ratelimit --min-rate 450
--max-rate 15000 -oG - 10.0.60.0/24
...
Host: 192.168.10.253 () Ports: 22/open/tcp//ssh///, 53/open/tcp//domain//ISC BIND 9.09/,
152/filtered/tcp//bftp///, 168/filtered/tcp//rsvd///, 443/open/tcp//ssl|https//VMware ESXi SOAP
API 6.0.0/, 8080/open/tcp//ssl|https//Apache/, OS: Linux 3.2 - 4.8
...
```

Trouver les appareils connectés, gérés ET non-gérés

3 - Rapportons les trouvailles dans notre document de suivi:

Machine	OS	Port	Software / Banner
127.254.238.1	Linux 2.6.32 - 3.10	22/open/tcp//ssh	OpenSSH 7.3 (protocol 2.0)
127.254.238.3	Linux 2.6.32 - 3.10	8080/open/tcp//http?	HTTP unknown
192.168.10.253	Linux 3.2 - 4.8	22/open/tcp//ssh	OpenSSH 7.6 (protocol 2.0)
192.168.10.253	Linux 3.2 - 4.8	8080/open/tcp//http	Apache
...			
192.168.10.10	Linux 2.6.22 (embedded, ARM)	22/open/tcp//ssh	OpenSSH 6.5 (protocol 2.0)
192.168.10.10	Linux 2.6.22 (embedded, ARM)	8080/open/tcp//http	lighthttpd
192.168.10.101	Microsoft Windows XP	135/open/tcp//msrpc	MS RPC
192.168.10.101	Microsoft Windows XP	3389/open/tcp//ms-wbt-server	MS RDP
10.0.1.10	Microsoft Windows Server 2008	8080/open/tcp//http	Microsoft IIS Webserver 7.5

Trouver les sites Web exposés par ces appareils (dev, prod, intranet,...)

1 - Partons du document de suivi, pour tous les ports exposant du HTTP interne ou externe, vérifier le Web service qui répond

Outils disponibles

curl, wget, nmap, VHostscan, dns[brute|enum|recon], recon-ng, shodan, censys.io, ...

```
$curl -k -vvv 192.168.10.253:8080
```

```
...
```

```
> GET / HTTP/1.1
```

```
> Host: 192.168.10.253:8080
```

```
> User-Agent: curl/7.58.0
```

```
> Accept: */*
```

```
...
```

```
<html>
```

```
<head>
```

```
... contenu retourné ...
```

```
</head>
```

```
</html>
```

Trouver les sites Web exposés par ces appareils (dev, prod, intranet,...)

2 - Tentons aussi de trouver des Virtual Hosts cachés, trouvons des sous-domaines, puis vérifions le contenu avec curl (est-il différent ?):

Outils disponibles

curl, wget, nmap, VHostscan, dns[brute|enum|recon], recon-ng, shodan, censys.io, ...

```
$VHostScan -t 192.168.10.253 -b monsite.com --fuzzy-logic -w subdomains.txt --waf --random-agent -p 8080
...
[+] Most likely matches with a unique count of 1 or less.
dev.monsite.com
beta.monsite.com

[+] Match similarity using fuzzy logic:
    [>] 51dab16e190358264a5d57163923e8e35ab820f14f5f320ee675aa3292c99af5 is 80% similar to
4954b1093aa83613e0cfefb36492e468ca2d711526bb2a7911dfb82a7c66b486b
...
```

Trouver les sites Web exposés par ces appareils (dev, prod, intranet,...)

3 - Rapportons les trouvailles dans notre document de suivi:

Machine	Zone	Port	Website	Visible / VHost Caché
192.168.10.253	Interne-1	80	http://192.168.10.253	Visible
192.168.10.253	Interne-1	8080	http://dev.monsite.com	VHost Caché
192.168.10.253	Interne-1	8080	http://beta.monsite.com	VHost Caché
127.254.238.3	Publique-1	443	http://www.monsite.com	Visible
...				
127.254.238.3	Publique-1	80	http://www.monsite.com	Visible
127.254.238.3	Publique-1	443	https://www.monsite.com	Visible
127.254.238.3	Publique-1	8080	https://beta.monsite.com	VHost Caché
192.168.10.10	Interne-1	8080	http://192.168.10.10	Visible
10.0.1.10	Interne-2	8080	https://dev.client2.com	Visible

Obtenir un inventaire matériel et logiciel

État des lieux de notre inventaire:

- ✓ Liste des machines connectées au réseau interne
- ✓ Liste des machines exposées publiquement.
- ✓ Liste des services que ces machines exposent au réseau.
- ✓ Inventaire des logiciels exposés au réseau (données partielles).
- ✓ Liste des sites Web du réseau interne (visibles ou VHost cachés).
- ✓ Liste des sites Web exposés publiquement(visibles ou VHost cachés).

Vs

1. **Inventory and Control of Hardware Assets.** ~ 99.9%
2. **Inventory and Control of Software Assets.** ~ 80% *

**Effectuer de la détection
et remédiation de
vulnérabilité en continu**



Balayage de vulnérabilité machine

Point de départ: notre liste de machines internes et externes.

Machine	Zone	OS	Port	Software / Banner
127.254.238.1	Publique-1	Linux 2.6.32 - 3.10	22/open/tcp//ssh	OpenSSH 7.3 (protocol 2.0)
127.254.238.3	Publique-1	Linux 2.6.32 - 3.10	8080/open/tcp//http?	HTTP unknown
192.168.10.253	Interne-1	Linux 3.2 - 4.8	22/open/tcp//ssh	OpenSSH 7.6 (protocol 2.0)
192.168.10.253	Interne-1	Linux 3.2 - 4.8	8080/open/tcp//http	Apache
...				
192.168.10.10	Interne-1	Linux 2.6.22 (embedded, ARM)	22/open/tcp//ssh	OpenSSH 6.5 (protocol 2.0)
192.168.10.10	Interne-1	Linux 2.6.22 (embedded, ARM)	8080/open/tcp//http	lighthttpd
192.168.10.101	Interne-1	Microsoft Windows XP	135/open/tcp//msrpc	MS RPC
192.168.10.101	Interne-1	Microsoft Windows XP	3389/open/tcp//ms-wbt-server	MS RDP
10.0.1.10	Interne-2	Microsoft Windows Server 2008	8080/open/tcp//http	Microsoft IIS Webserver 7.5

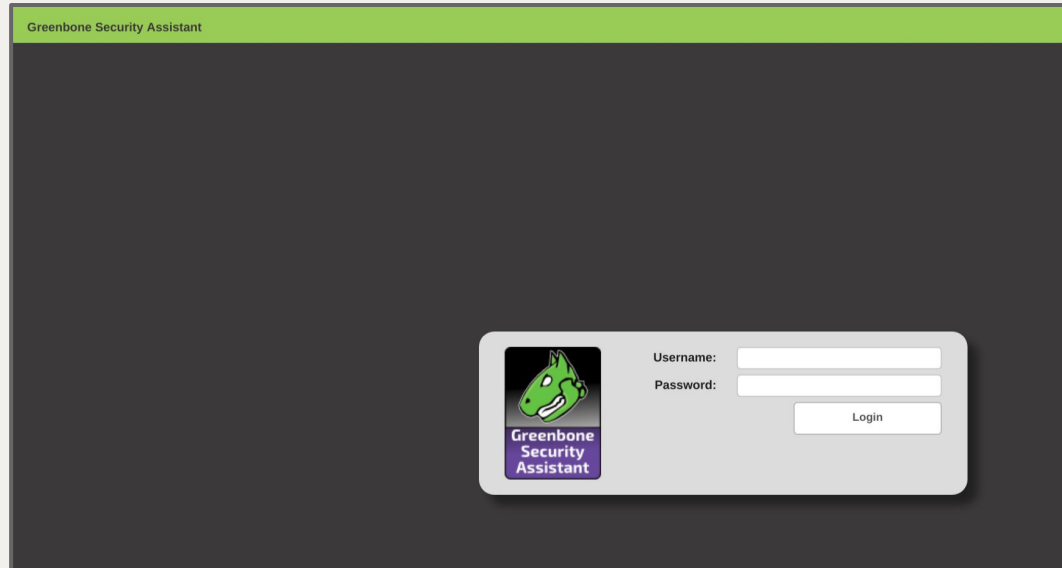


Balayage de vulnérabilité machine

Exécuter de la détection de vulnérabilités (VA) sur les IPs trouvés ci-haut:

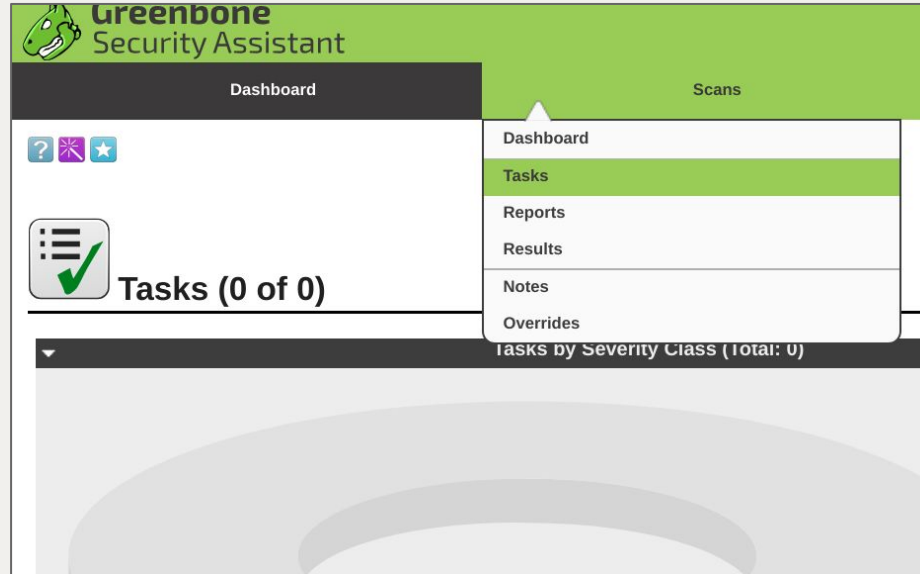
Outils disponibles

OpenVAS, Nessus, Retina CS free, nmap



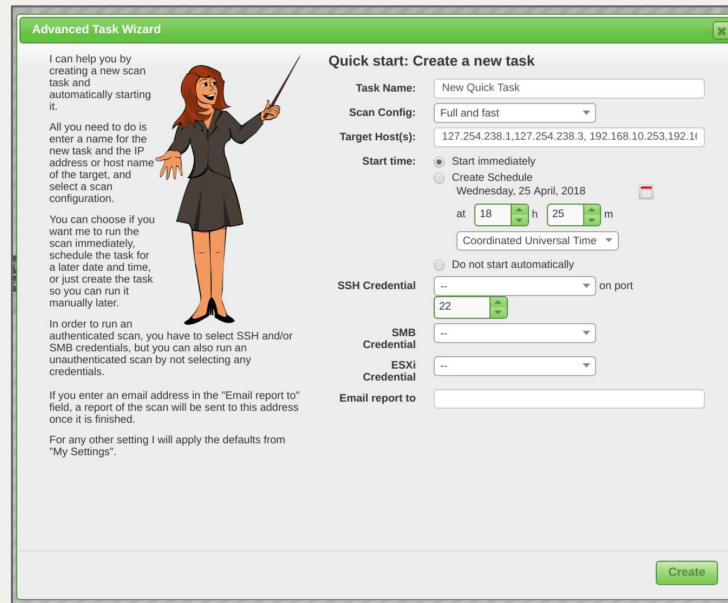
Balayage de vulnérabilité machine

Exécuter de la détection de vulnérabilités (VA) sur les IPs trouvés ci-haut:



Balayage de vulnérabilité machine

Exécuter de la détection de vulnérabilités (VA) sur les IPs trouvés ci-haut:



Advanced Task Wizard

I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.

For any other setting I will apply the defaults from "My Settings".

Quick start: Create a new task

Task Name:

Scan Config:

Target Host(s):

Start time: ☒ Start immediately
☐ Create Schedule
Wednesday, 25 April, 2018
at 18 h 25 m

☐ Do not start automatically

SSH Credential: on port

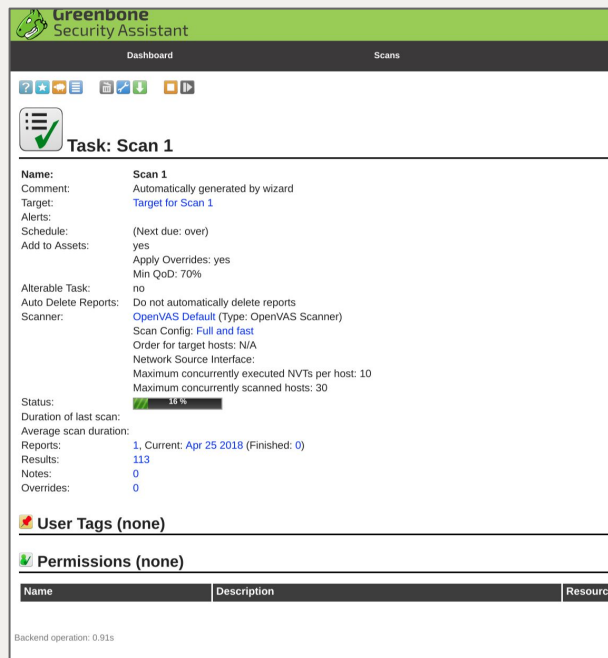
SMB Credential:

ESXi Credential:

Email report to:

Balayage de vulnérabilité machine

Exécuter de la détection de vulnérabilités (VA) sur les IPs trouvés ci-haut:



The screenshot displays the Greenbone Security Assistant (GSA) interface. At the top, there's a green header with the logo and 'Greenbone Security Assistant'. Below it, a dark navigation bar contains 'Dashboard' and 'Scans'. The main content area shows a 'Task: Scan 1' configuration page. It includes a list of settings on the left and their values on the right. A progress bar indicates the task is 10% complete. At the bottom, there are sections for 'User Tags (none)', 'Permissions (none)', and a table with columns 'Name', 'Description', and 'Resource'. The footer shows 'Backend operation: 0.01s'.

Task: Scan 1

Name: Scan 1

Comment: Automatically generated by wizard

Target: [Target for Scan 1](#)

Alerts:

Schedule: (Next due: over)

Add to Assets: yes

Apply Overrides: yes

Min QoD: 70%

Alterable Task: no

Auto Delete Reports: Do not automatically delete reports

Scanner: [OpenVAS Default](#) (Type: OpenVAS Scanner)


Scan Config: Full and fast

Order for target hosts: N/A

Network Source Interface:

Maximum concurrently executed NVTs per host: 10

Maximum concurrently scanned hosts: 30

Status:  10 %

Duration of last scan:

Average scan duration:

Reports: 1, Current: [Apr 25 2018](#) (Finished: 0)

Results: 113

Notes: 0

Overrides: 0

User Tags (none)







Permissions (none)

Name	Description	Resource
------	-------------	----------

Backend operation: 0.01s

Balayage de vulnérabilité machine

Exécuter de la détection de vulnérabilités (VA) sur les IPs trouvés ci-haut:

Vulnerability		Severity	QoD	Host	Location	Actions
ProFTPD Multiple Remote Vulnerabilities		10.0 (High)	80%	192.168.111.130	21/tcp	 
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.111.130	1524/tcp	 
ProFTPD Multiple Remote Vulnerabilities		10.0 (High)	80%	192.168.111.130	2121/tcp	 
X Server		10.0 (High)	80%	192.168.111.130	6000/tcp	 
distcc Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.111.130	3632/tcp	 
SSH Brute Force Logins with default Credentials		9.0 (High)	95%	192.168.111.130	22/tcp	 
MySQL weak password		9.0 (High)	95%	192.168.111.130	3306/tcp	 
PostgreSQL weak password		9.0 (High)	99%	192.168.111.130	5432/tcp	 
PostgreSQL Multiple Security Vulnerabilities		8.5 (High)	80%	192.168.111.130	5432/tcp	 
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.111.130	21/tcp	 
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.111.130	21/tcp	 
phpMyAdmin Code Injection and XSS Vulnerability		7.5 (High)	75%	192.168.111.130	80/tcp	 
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities		7.5 (High)	75%	192.168.111.130	80/tcp	 
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	75%	192.168.111.130	80/tcp	 
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.111.130	80/tcp	 
phpinfo() output accessible		7.5 (High)	80%	192.168.111.130	80/tcp	 
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.111.130	2121/tcp	 

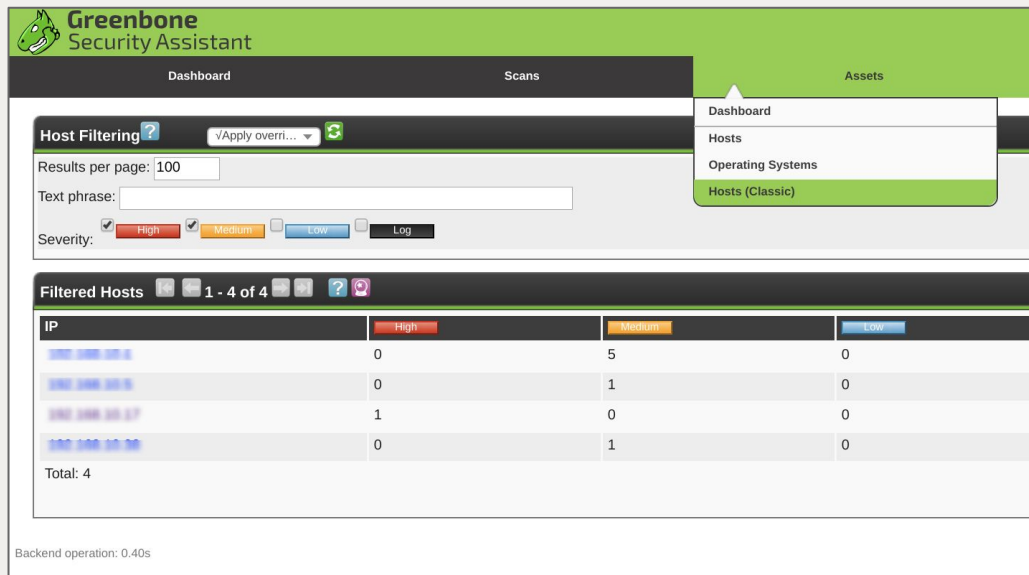
Filtrer les faux positifs

Pour chacune des vulnérabilités:

- Vérifier le détail de la vulnérabilité.
- Est-ce que ce logiciel est bel et bien installé sur mon équipement ?
- Y-a-t'il des patchs *backported* qui n'ont pas été détectés ?
- Est-ce que la détection est de suffisamment bonne qualité ?
- Est-ce que ça s'exploite vraiment ?

Extraire les données (#1 et #2)

Récupérer l'information additionnelle sur les logiciels installés et combiner le tout dans notre chiffrier existant.

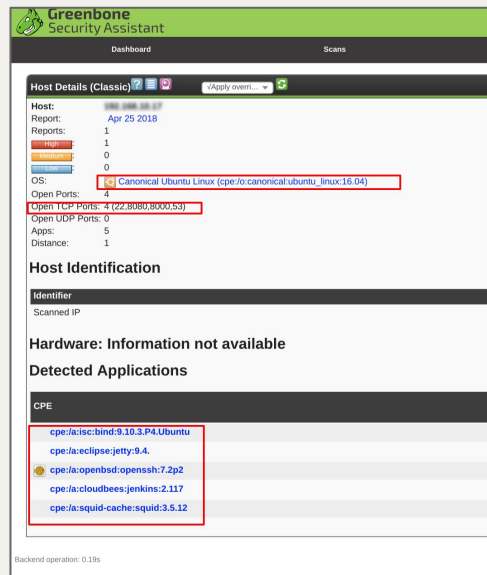


The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes 'Dashboard', 'Scans', and 'Assets'. The 'Host Filtering' section is active, showing a search bar with '100' results per page and a 'Text phrase' input field. Below this, there are severity filters for 'High', 'Medium', 'Low', and 'Log'. A table titled 'Filtered Hosts' displays 4 hosts with columns for IP, High severity count, Medium severity count, and Low severity count. The table data is as follows:

IP	High	Medium	Low
192.168.1.1	0	5	0
192.168.1.2	0	1	0
192.168.1.3	1	0	0
192.168.1.4	0	1	0

Total: 4

Backend operation: 0.40s



The screenshot shows the Greenbone Security Assistant interface for 'Host Details (Classic)'. The 'Host' section displays the following information:

- Host: 192.168.1.1
- Report: Apr 25 2018
- Reports: 1
- Severity: High
- OS: Canonical Ubuntu Linux (cpe:/o:canonical:ubuntu_linux:16.04)
- Open Ports: 4
- Open TCP Ports: 4 (22,8080,8000,63)
- Open UDP Ports: 0
- Apps: 5
- Distance: 1

The 'Host Identification' section shows the 'Identifier' as 'Scanned IP'. The 'Hardware' section states 'Information not available'. The 'Detected Applications' section lists the following CPEs:

- cpe:/a:isc:bind:9.10.3.P4.Ubuntu
- cpe:/a:eclipse:jetty:9.4.
- cpe:/a:openbsd:openssh:7.2p2
- cpe:/a:cloudbees:jenkins:2.117
- cpe:/a:squid-cache:squid:3.5.12

Backend operation: 0.13s

Extraire les données (#1 et #2)

Récupérer l'information additionnelle sur les logiciels installés et combiner le tout dans notre chiffrier existant.

1. Inventory and Control of Software Assets ~ 80% -> 99%

Machine	OS	Port	Software / Banner
127.254.238.1	Ubuntu 16.04	22/open/tcp//ssh	OpenSSH 7.2p2
127.254.238.1	Ubuntu 16.04	8008/open/tcp//http?	Jetty 9.4
127.254.238.1	Ubuntu 16.04	53/open/tcp//bind	Bind 9.70.3.P4.Ubuntu
127.254.238.1	Ubuntu 16.04	8080/open/tcp//http	Squid 3.5.12
127.254.238.1	Ubuntu 16.04	8080/open/tcp//http	Jenkins 2.117
...			
192.168.10.10	VMWare ESXi 6.5	22/open/tcp//ssh	OpenSSH 6.5 (protocol 2.0)
192.168.10.10	VMWare ESXi 6.5	8080/open/tcp//http	lighthttpd
192.168.10.101	Microsoft Windows XP	135/open/tcp//msrpc	MS RPC
192.168.10.101	Microsoft Windows XP	3389/open/tcp//ms-wbt-server	MS RDP

Prioriser la remédiation

Pour chaque vulnérabilité, faire un “light threat modeling” prenant en compte:

- Score CVSS2/3
- Âge de la vulnérabilité
- Exploitabilité de la vulnérabilité
- “Popularité” de la vulnérabilité
- Type d’actif vulnérable
- Position et impact dans le réseau


Extraire les données de vulnérabilité prioritées & initier la remédiation

Récupérer l'information additionnelle sur les logiciels installés et combiner le tout dans notre chiffrier existant.

Machine	Vulnérabilité	Date découverte	Responsable résolution
127.254.238.1	OpenSSH Denial of Service And User Enumeration Vulnerabilities CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708	15 / 05 / 2018	Mr Untel 1 / email@compagnie.com
127.254.238.1	Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities CVE-2017-9788	15 / 05 / 2018	Mr Untel 1 / email@compagnie.com
127.254.238.1	SSL/TLS: Vulnerable Cipher Suites for HTTPS CVE-2016-2183, CVE-2016-6329	15 / 05 / 2018	Mr Untel 1 / email@compagnie.com
...			
192.168.10.10	ISC BIND Denial of Service Vulnerability CVE-2016-2776	15 / 05 / 2018	Équipe 2
192.168.10.10	ISC BIND RTYPE ANY Query Denial of Service Vulnerability CVE-2016-9131	15 / 05 / 2018	Équipe 2



[illegible]





Greenbone


security Assistant

Dashboard

Scans

Assessment




Credentials (2 of 2)

Name	Type
admin (test)	snmp (SNMP)
test1 (test)	ip (username + password)

(Applied filter: rows=10 test=1 hostname=)

Backend operation: 0.00s




Greenbone

Security Assistant

Dashboard

Scans



Schedule: schedule1

Name: schedule1

Comment: test

First Run: Thu Apr 26 14:25:00 2018 UTC

Next Run: Fri Apr 27 14:25:00 2018 UTC

Timezone: UTC

Period: 1 day

Duration: 2 hours

Tasks using this Schedule (none)

Name

User Tags (none)

Permissions (none)

Name	Description	Resource
------	-------------	----------

Balayage de vulnérabilités Web

Point de départ: notre liste de sites Web internes et externes.

Website	Zone	Visible / VHost Caché
http://192.168.10.253:80	Interne-1	Visible
http://dev.monsite.com:8080	Interne-1	VHost Caché
http://beta.monsite.com:80	Interne-1	VHost Caché
https://www.monsite.com	Publique-1	Visible
...
http://www.monsite.com:80	Publique-1	Visible
https://www.monsite.com	Publique-1	Visible
https://beta.monsite.com:8080	Publique-1	VHost Caché
http://192.168.10.10:8080	Interne-1	Visible
https://dev.client2.com:8080	Interne-2	Visible

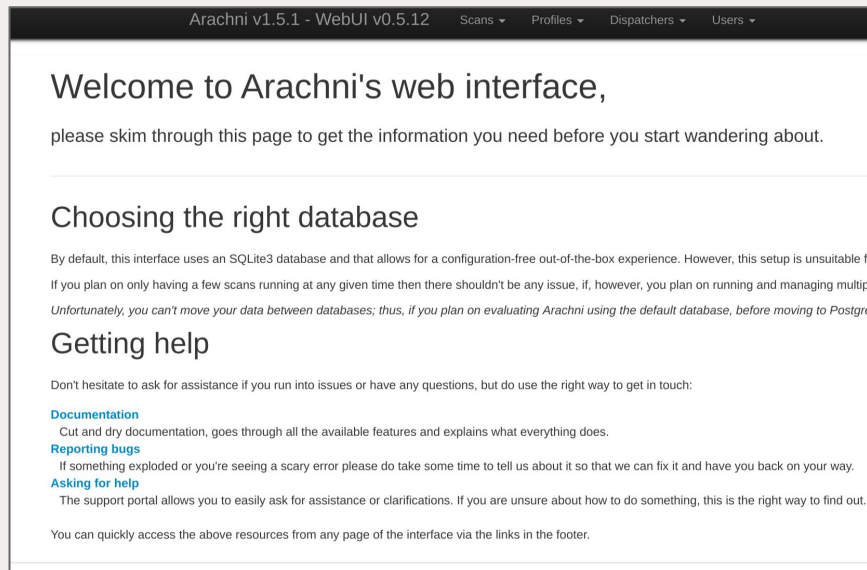


Balayage de vulnérabilités Web

Exécuter de la détection de vulnérabilités (DAST) sur les sites Web ci-haut:

Outils disponibles

Arachni, ZAP, Burp, etc.



Balayage de vulnérabilités Web

Exécuter de la détection de vulnérabilités (DAST) sur les sites Web ci-haut:

Arachni v1.5.1 - WebUI v0.5.12 Scans Profiles Dispatchers Users Administrator

Start a scan

The only thing you need to do is provide some basic information and make a simple choice about the type of scan you want to perform.

Full URL of the targeted web application (must include the appropriate protocol, http or https).

Description

You can use Markdown for text formatting.

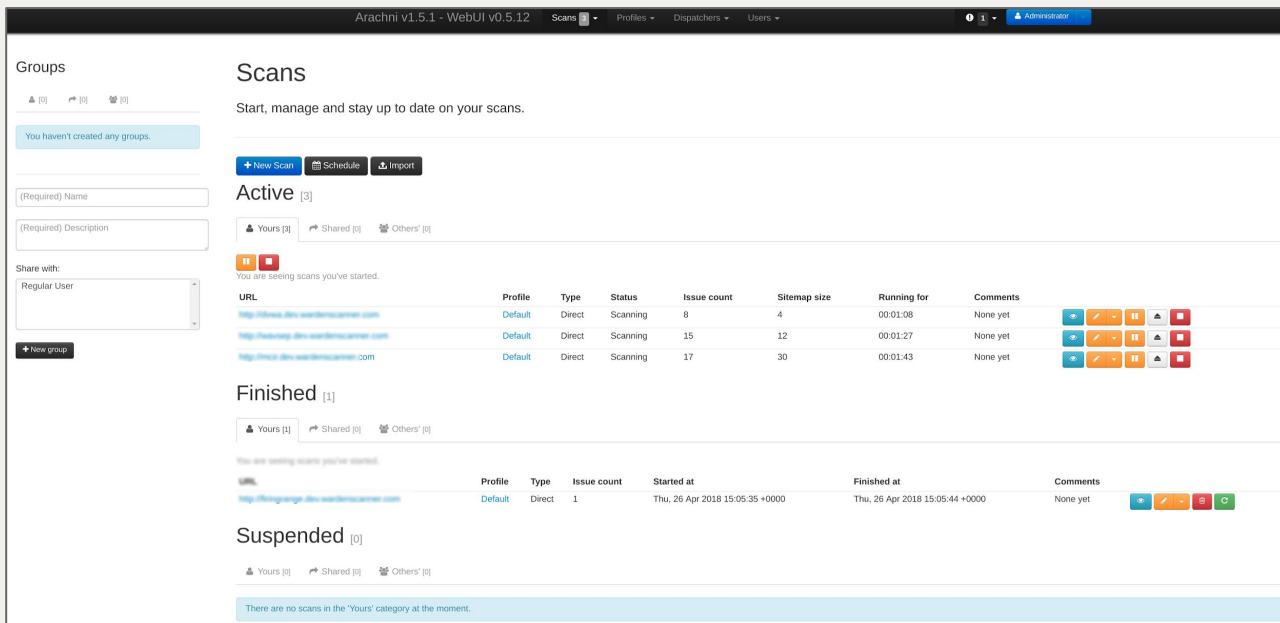
Default (Global)

Configuration profile to use.

Share with:
Regular User

Balayage de vulnérabilités Web

Exécuter de la détection de vulnérabilités (DAST) sur les sites Web ci-haut:



Arachni v1.5.1 - WebUI v0.5.12

Scans Profiles Dispatchers Users

Groups

You haven't created any groups.

(Required) Name

(Required) Description

Share with:

Regular User

+ New group

Scans

Start, manage and stay up to date on your scans.

+ New Scan Schedule Import

Active [3]

Yours [3] Shared [0] Others' [0]

You are seeing scans you've started.

URL	Profile	Type	Status	Issue count	Sitemap size	Running for	Comments
http://www.dns-wadentecanet.com	Default	Direct	Scanning	8	4	00:01:08	None yet
http://testing.dns-wadentecanet.com	Default	Direct	Scanning	15	12	00:01:27	None yet
http://dev.dns-wadentecanet.com	Default	Direct	Scanning	17	30	00:01:43	None yet

Finished [1]

Yours [1] Shared [0] Others' [0]

You are seeing scans you've started.

URL	Profile	Type	Issue count	Started at	Finished at	Comments
http://testing.dns-wadentecanet.com	Default	Direct	1	Thu, 26 Apr 2018 15:05:35 +0000	Thu, 26 Apr 2018 15:05:44 +0000	None yet

Suspended [0]

Yours [0] Shared [0] Others' [0]

There are no scans in the 'Yours' category at the moment.

Balayage de vulnérabilités Web

Exécuter de la détection de vulnérabilités (DAST) sur les sites Web ci-haut:

✓ The scan completed in 00:13:49 .

Issues [108]

All [108] * Fixed [0] ✓ Verified [0] ⓘ Pending verification [0] ✖ False positives [0] ⓘ Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

Reset Show all Hide all

High 73

Low 3

Informational 32

NAVIGATE TO

Cross-Site Scripting (XSS) in script context 31

Cross-Site Scripting (XSS) in HTML tag 19

Cross-Site Scripting (XSS) in event tag of HTML element 2

Cross-Site Scripting (XSS) 21

Missing 'X-Frame-Options' header 1

Private IP address disclosure 2

Interesting response 25

Allowed HTTP methods 1

HTML object 6

URL

Input

Element

Cross-Site Scripting (XSS) in script context 31

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.

If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS).

Arachni has discovered that it is possible to force the page to execute custom JavaScript code.

(CWE)

q

q

q

q

q

q

Link

Link

Link

Link

Link

Link

Filtrer les faux positifs

Pour chacune des vulnérabilités:

- Vérifier le détail de la vulnérabilité et déterminer si ce *payload* semble s'exécuter sur le site en question (ex XSS)

```
HTTP data
Request
Response
Proof is highlighted in red and scroll-centered.
<script>
/* arachni_js_namespace_initialize_start */ _arachni_js_namespaceTaintTracer.initialize({"window.top._%s_taint_tracer.log_execution_flow_sink()":{"stop_at_first":false,"trace":true}}) /* arachni_js_namespace_i
nitialize_stop */
window._arachni_js_namespace = true;

/* arachni_js_namespace_code_start */ /* arachni_js_namespace_code_stop */
</script> <!-- Injected by Arachni::Browser::Javascript -->
<html>
<body>
<script>

// Injected by Arachni::Browser::Javascript
_arachni_js_namespaceTaintTracer.update_trackers();
_arachni_js_namespaceDOMMonitor.update_trackers();

;window.top._arachni_js_namespace_taint_tracer.log_execution_flow_sink();</script>
<script type="text/javascript">_arachni_js_namespaceTaintTracer.update_trackers();_arachni_js_namespaceDOMMonitor.update_trackers();</script> <!-- Injected by Arachni::Browser::Javascript -->

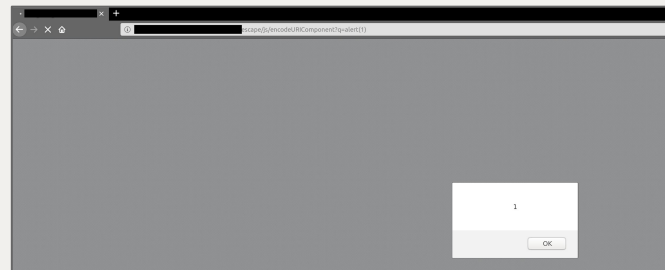
</body>
</html>
```

Filtrer les faux positifs

Pour chacune des vulnérabilités:

- Utiliser un autre *payload* pour déterminer si c'est une vraie vulnérabilité (ex XSS / GET).

Browser data			
Transitions			
#	Time	Event	Element
0	0.550399258	load	page
1	0.099933378	request	<div>q=window.top._arachni_js_namespace_taint_tracer.log_execution_flow_sink()</div>



Filtrer les faux positifs

Pour chacune des vulnérabilités:

→ Autres options pour déterminer si la vulnérabilité est exploitable:

- ◆ SQLis: Curl, fureteur (GET), SQLMap, Burp, ZAP, etc.
- ◆ XSS: Fureteur non-protégé (Firefox), Burp, ZAP, Fiddler, etc.
- ◆ XXE: Curl, wget, Fureteur, Burp, ZAP, etc.
- ◆ LFI/Path traversal: Curl, wget, Fureteur, Burp, ZAP, etc.

Prioriser la remédiation

Pour chaque vulnérabilité, faire un “light threat modeling” prenant en compte:

- Sévérité rapportée par l'outil & classement OWASP Top 10
- Âge de la vulnérabilité
- Exploitabilité de la vulnérabilité
- Type d'actif vulnérable (public, interne, transactionnel, données sensibles)
- Position et impact dans le réseau (relation aux autres vulnérabilités)

Extraire les données de vulnérabilité prioritaires & initier la remédiation

Récupérer l'information additionnelle sur les logiciels installés et combiner le tout dans notre chiffrier existant.

Website	Vulnérabilité	URL/Param/Payload	Date découverte	Responsable résolution
www.beta.monsite.com	XSS / Reflected	www.beta.monsite.com/page1.php?q=<script>alert(1)</script> www.beta.monsite.com/page2.php?q=<script>alert(1)</script>	15 / 05 / 2018	Équipe Dev 1
www.beta.monsite.com	XSS / DOM	www.beta.monsite.com/page1.php?q=;alert(1) // www.beta.monsite.com/index1.php?q=;alert(1))//	15 / 05 / 2018	Équipe Dev 1
www.beta.monsite.com	SQLi / Blind	www.beta.monsite.com/page1.php?r=" OR 1=1 --	15 / 05 / 2018	Équipe Dev 1
...				
www.client2.com	XSS / Reflected	www.client2.com/site/index.html?param="<script>alert(1)</script>	15 / 05 / 2018	Équipe Dev 2
www.client2.com	Missing 'X-Frame-Options'	www.client2.com/site/index.html www.client2.com/site/page2.html www.client2.com/site/login/client.html	15 / 05 / 2018	Équipe Dev 2



Autres Options de Balayage Web

Configuration personnalisées de balayage, balayages authentifiés, balayages cédulés

Checks The security checks to be run again the web application

Filter modules by name or description

These checks will actively engage the web application via its inputs (links, forms, etc.)

Active

<input type="checkbox"/> Code Injection (code_injection)	<input type="checkbox"/> SQL Injection (sql_injection)
<input type="checkbox"/> Code Injection (http input wrapper) (code_injection_http_input_wrapper)	<input type="checkbox"/> Blind SQL Injection (differential analysis) (sql_injection_differential)
<input type="checkbox"/> Code Injection (timing) (code_injection_timing)	<input type="checkbox"/> Blind SQL Injection (timing attack) (sql_injection_timing)
<input type="checkbox"/> CSRF (csrf)	<input type="checkbox"/> Trainer (trainer)
<input type="checkbox"/> File Inclusion (file_inclusion)	<input type="checkbox"/> Unvalidated redirect (unvalidated_redirect)
<input type="checkbox"/> LDAP Injection (ldap_injection)	<input type="checkbox"/> Unvalidated DOM redirect (unvalidated_redirect_dom)
<input type="checkbox"/> NoSQL Injection (no_sql_injection)	<input type="checkbox"/> XPath Injection (xpath_injection)
<input type="checkbox"/> Blind NoSQL Injection (differential analysis) (no_sql_injection_differential)	<input type="checkbox"/> XSS (xss)
<input type="checkbox"/> OS command injection (os_cmd_injection)	<input type="checkbox"/> DOM XSS (xss_dom)
<input type="checkbox"/> OS command injection (timing) (os_cmd_injection_timing)	<input type="checkbox"/> DOM XSS in script context (xss_dom_script_context)
<input type="checkbox"/> Path Traversal (path_traversal)	<input type="checkbox"/> XSS in HTML element event attribute (xss_event)
<input type="checkbox"/> Response Splitting (response_splitting)	<input type="checkbox"/> XSS in path (xss_path)
<input type="checkbox"/> Remote File Inclusion (rfi)	<input type="checkbox"/> XSS in script context (xss_script_context)
<input type="checkbox"/> Session fixation (session_fixation)	<input type="checkbox"/> XSS in HTML tag (xss_tag)
<input type="checkbox"/> Source code disclosure (source_code_disclosure)	<input type="checkbox"/> XML External Entity (xxe)

Passive These checks will passively collect data

<input type="checkbox"/> Allowed methods (allowed_methods)	<input type="checkbox"/> HTTP PUT (http_put)
<input type="checkbox"/> Backdoors (backdoors)	<input type="checkbox"/> Insecure client-access policy (insecure_client_access_policy)
<input type="checkbox"/> Backup directories (backup_directories)	<input type="checkbox"/> Insecure cookies (insecure_cookies)
<input type="checkbox"/> Backup files (backup_files)	<input type="checkbox"/> Insecure CORS policy (insecure_cors_policy)
<input type="checkbox"/> CAPTCHA (captcha)	<input type="checkbox"/> Insecure cross-domain policy (allow-access-from) (insecure_cross_domain_policy_access)
<input type="checkbox"/> Common administration interfaces (common_admin_interfaces)	<input type="checkbox"/> Insecure cross-domain policy (allow-http-request-headers-from) (insecure_cross_domain_policy_headers)
<input type="checkbox"/> Common directories (common_directories)	<input type="checkbox"/> Interesting responses (interesting_responses)

HTTP How the scanner will communicate with the web application

Http authentication username

Http authentication type

Advanced options

Start at

Recurring

Every

Stop after

Use storage of previous revisions:
☐ instead of crawling
☐ in addition to crawling

...en continu !

Gérer les vulnérabilités “*Out-Of-Band*”

Option 1: Créer un balayage personnalisé dans OpenVAS pour balayer toutes les machines pour cette vulnérabilité.

Option 2: Utiliser nmap + script NSE de la communauté pour détecter sur votre parc.

```
$nmap -p445 --script smb-vuln-ms17-010  
192.168.10.0/24
```

Option 3: Autres outils command-line de la communauté.

```
$/CVE-2017-5689.py 192.168.10.0/24
```



Recap: Effectuer son premier test de sécurité

État des lieux de notre premier test de sécurité

☑ **Inventory and Control of Hardware Assets.**

Amélioration: exécution de nmap + VHostScan en continu, combiner avec "*Discovery scans*" d'OpenVAS.

☑ **Inventory and Control of Software Assets.**

Amélioration: exécution de balayages machines authentifiés (SMB/SSH).

☑ **Continuous Vulnerability Management (detection + Remediation).**

Amélioration: Configurer les cédules de balayages pour machines trouvées (autorisées ou non), configurer les cédules de balayage pour sites Web trouvés.

Recap: Effectuer son premier test de sécurité

Comment s'améliorer? Règle des trois "A":

- Automatiser
- Automatiser
- Automatiser

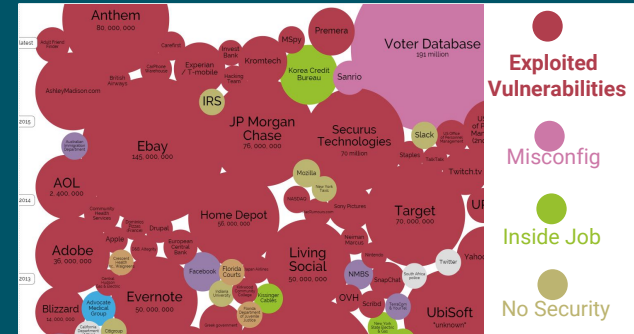
Pourquoi ?

L'état de la cybersécurité actuel

En 2017, le top 3 des sources de cyber attaques était encore:

- Des **Vulnérabilités connues avec correctifs disponibles**
- Des **données exposées** malencontreusement
- De **l'injection Web** de base (XSS/SQLis)

Pas des vulnérabilités "0days" par des adversaires avancés !



<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

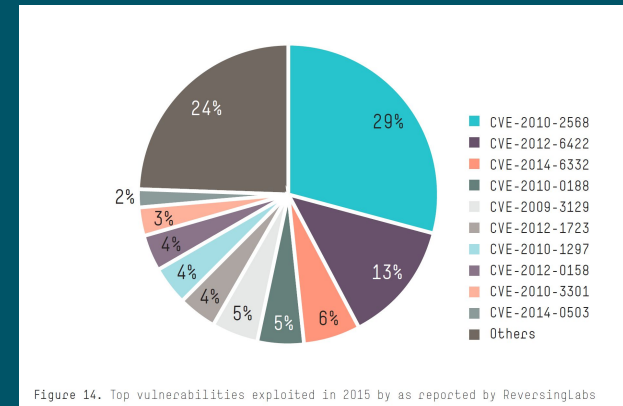


Figure 14. Top vulnerabilities exploited in 2015 by as reported by ReversingLabs
HPE Cyber Risk Report 2016

L'état de la cybersécurité actuel



"Current threat and vulnerability management has proven to be ineffective."

"70% of the market is dominated by three vendors"

(Rapid7, Tenable Network Security and Qualys).

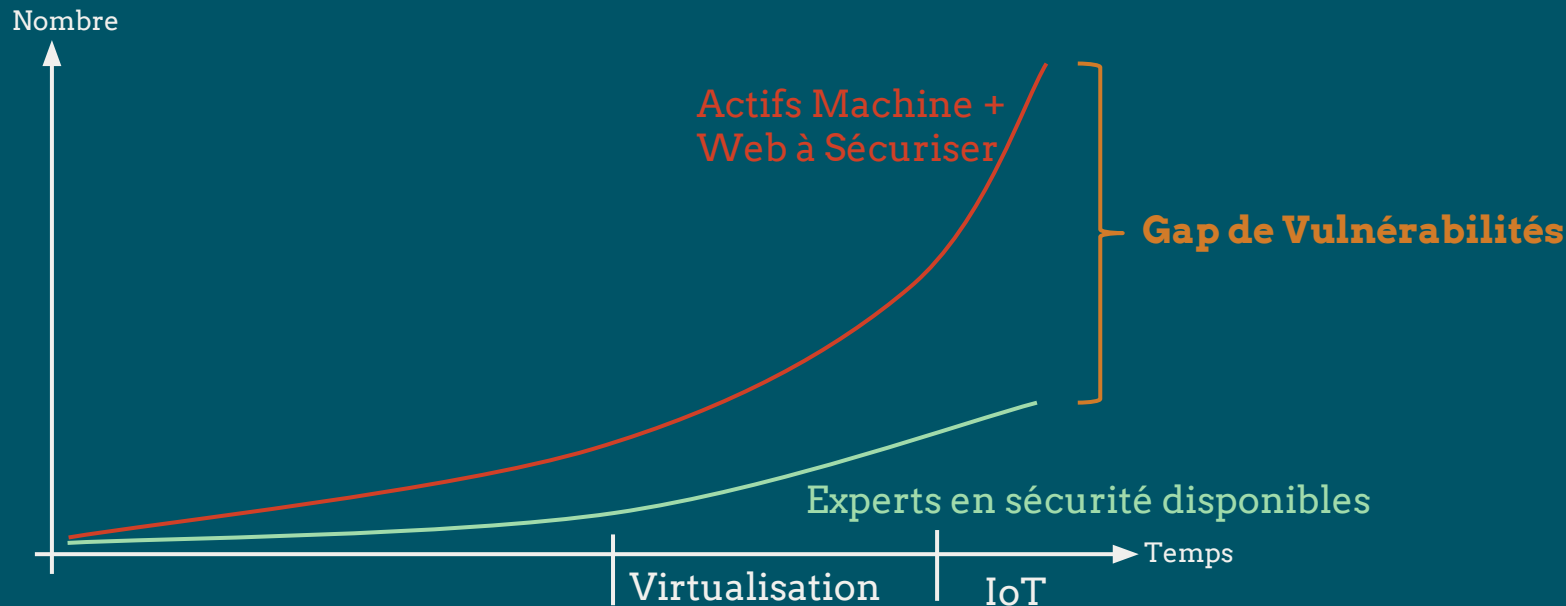
"Vulnerability assessment is a standard component of most information security management and regulatory frameworks."

"99.99% of exploits are based on vulnerabilities that have already been known to security and IT professionals for at least one year"

Qu'est-ce qui limite l'efficacité des équipes TI & Sécurité vis-à-vis la détection et remédiation de leurs vulnérabilités ?

1 - Le manque d'experts en sécurité dans l'industrie

- **2M** d'experts seront manquants d'ici 2019 [1]
- Moins de 20% des compagnies balayent 100% de leurs actifs **critiques** [2]
- **70%** des compagnies **balayent moins de 50%** de leur réseau [3] sur une base mensuelle seulement [4]



[1] <https://www.isaca.org/cyber/PublishingImages/Cybersecurity-Skills-Gap-1500.jpg>

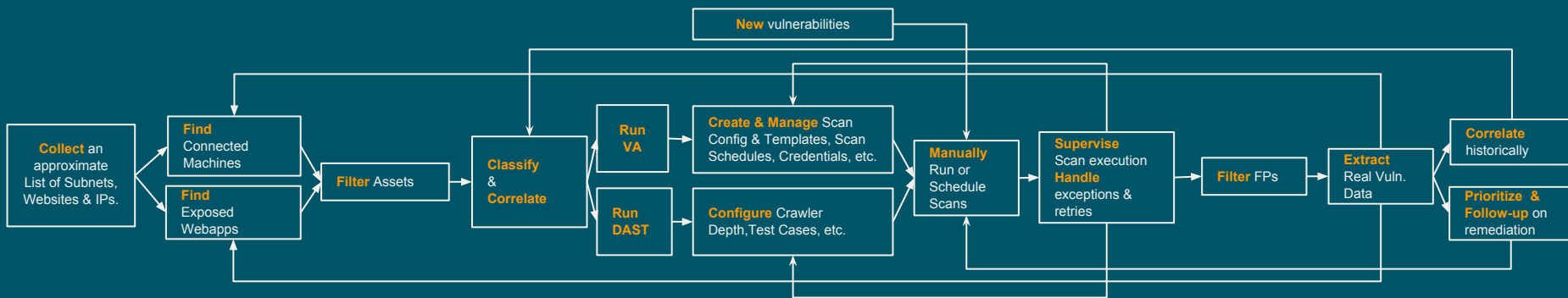
[2] <https://uk.sans.org/reading-room/whitepapers/analyst/reducing-attack-surface-sans%E2%80%99second-survey-continuous-monitoring-programs-37417>

[3] http://lp.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox_Security_Vulnerability_Management_Survey.pdf

[4] <http://lp.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox-Security-Vulnerability-Management-Survey-EN.pdf>

2 - L'approche "classique" des outils VA actuels est trop manuelle et nécessite une connaissance technique avancée

- **Les outils** sont **manuels & centrés sur les balayages** rendent le processus **Inefficace**.^[3]
- La détection de vulnérabilité classique a un taux de **Faux-Positifs** de **50% à 90%** ^[1]
- Ce processus cause une accumulation de tâches répétitives et rébarbatives pour les experts^[2]



[1] <https://www.nccgroup.trust/us/about-us/newsroom-and-events/news/2016/march/the-register-auto-vulnerability-scanners-turn-up-mostly-false-positives/>

[2] http://p.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox_Security_Vulnerability_Management_Survey.pdf

[3] <https://uk.sans.org/reading-room/whitepapers/analyst/reducing-attack-surface-sans%E2%80%9999-second-survey-continuous-monitoring-programs-37417>

WARDEN

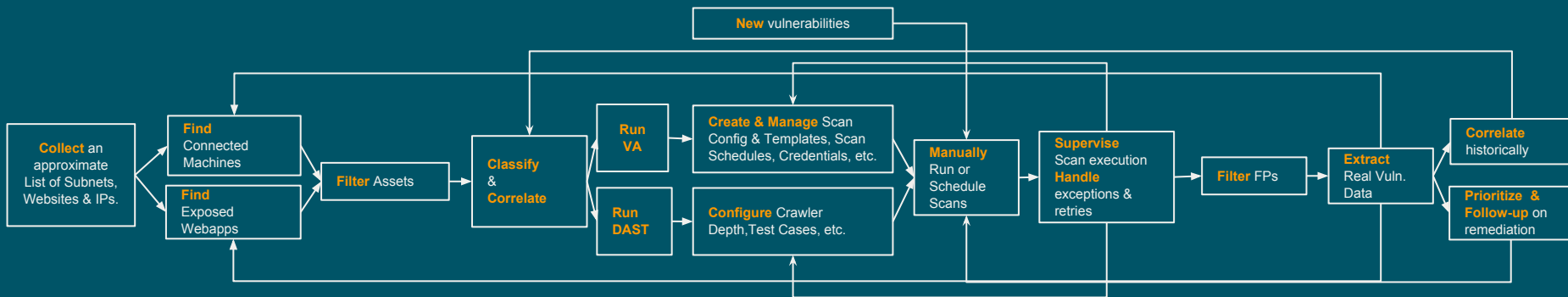
AI-DRIVEN VULNERABILITY ASSESSMENT

Comment Warden automatise ce processus

AI-DRIVEN



- **Système Expert** auto-évolutif conduisant la découverte et le balayage d'actifs
- **Apprentissage Machine** pour détection et classification des Faux-Positifs
- **Meta-Simulation de "pentest"** par l'AI pour pré-prioriser la remédiation



Comment Warden automatise ce processus

VA + DAST SIMPLIFIÉ



- **Fonctionne 24/7** virtuellement sans configuration ou supervision
- Approche centrée sur les actifs, balayage **Systems & Web** continu
- Vue **historique** complète, suivant l'évolution du réseau
- **Architecture** "JSON **API-First**" permettant une intégration rapide



WARDEN

AI-DRIVEN VULNERABILITY ASSESSMENT