

# 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, fing, 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	8008/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	lighttpd
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  
4954b1093aa83613e0cfcb36492e468ca2d711526bb2a7911dfb82a7c66b486b  
...
```

# 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	8008	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	8008/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



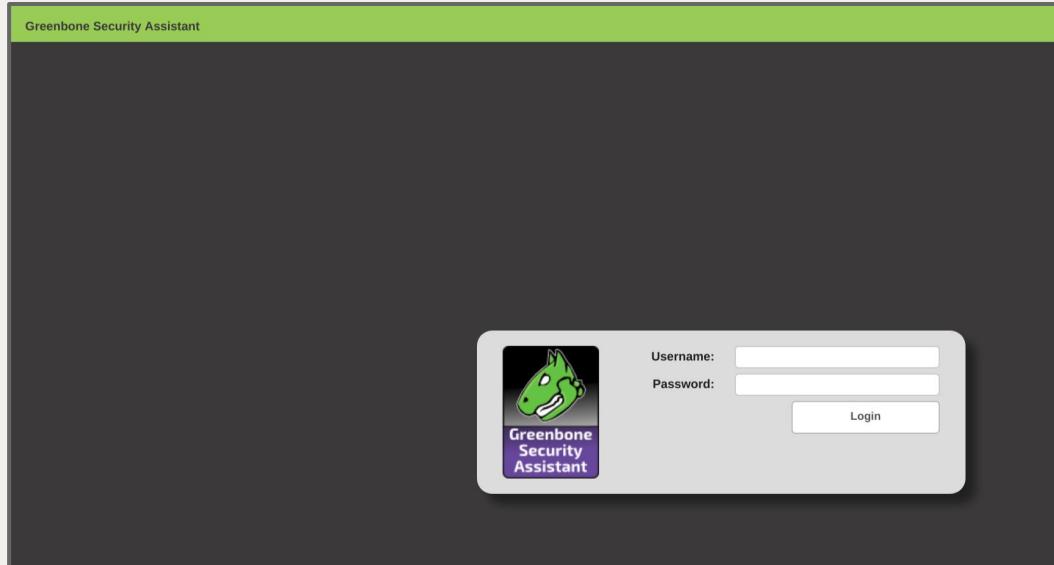
# Balayage de vulnérabilité machine

---

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

## Outils disponibles

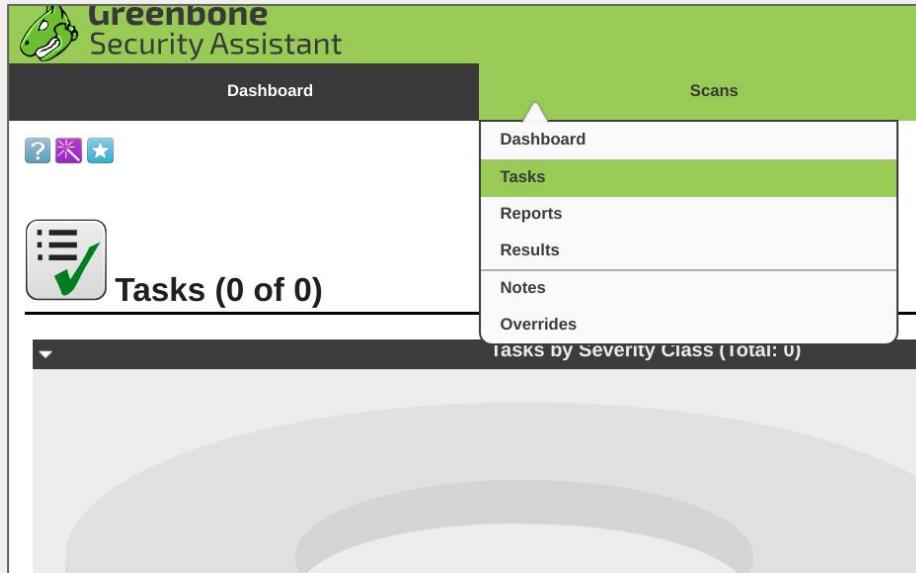
*OpenVAS, Nessus, Retina CS free, nmap*



# Balayage de vulnérabilité machine

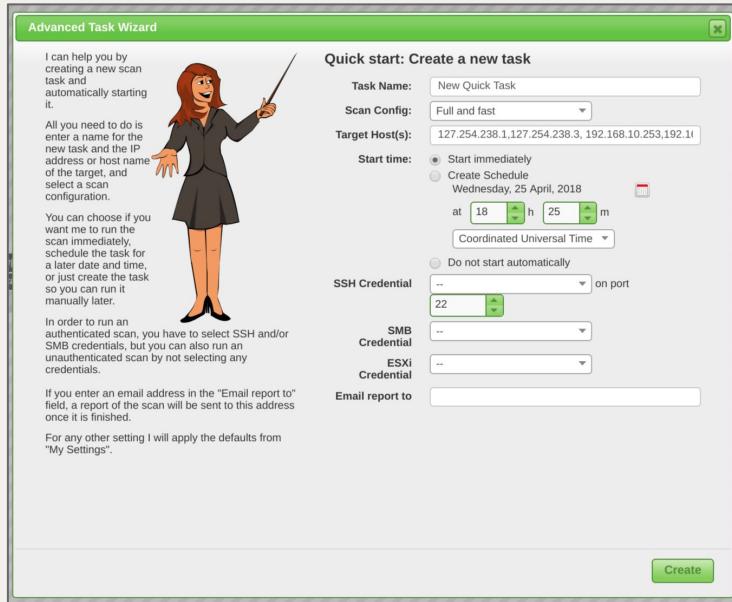
---

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:



# Balayage de vulnérabilité machine

---

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

The screenshot shows the Greenbone Security Assistant interface. The main title is "Task: Scan 1". The configuration details are as follows:

Name:	Scan 1
Comment:	Automatically generated by wizard
Target:	Target for Scan 1
Alerts:	(Next due: over)
Schedule:	yes
Add to Assets:	Apply Overrides: yes Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	<b>OpenVAS Default</b> (Type: OpenVAS Scanner) Scan Config: <b>Full and fast</b> Order for target hosts: N/A Network Source Interface: Maximum concurrently executed NVTs per host: 10 Maximum concurrently scanned hosts: 30
Status:	16 %
Duration of last scan:	
Average scan duration:	
Reports:	1, Current: Apr 25 2018 (Finished: 0)
Results:	113
Notes:	0
Overrides:	0

Below the configuration, there are sections for "User Tags (none)" and "Permissions (none)". A footer note states "Backend operation: 0.91s".

# Balayage de vulnérabilité machine

---

Exécuter 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. On the left, there's a sidebar with 'Host Filtering' options, including 'Results per page: 100', 'Text phrase:', and severity filters ('High', 'Medium', 'Low', 'Log'). Below this is a 'Filtered Hosts' table with columns for IP, High, Medium, and Low severity counts. The table shows four hosts with the following data:

IP	High	Medium	Low
192.168.0.10	0	5	0
192.168.0.15	0	1	0
192.168.0.17	1	0	0
192.168.0.18	0	1	0

Total: 4

Backend operation: 0.40s

A dropdown menu in the top right is open, showing 'Assets' and 'Hosts (Classic)'. The 'Hosts (Classic)' option is highlighted with a green background.

The screenshot shows the 'Host Details (Classic)' page for a host scanned on April 25, 2018. It lists the following information:

Host	Report	Reports	Severity
192.168.0.17	Apr 25 2018	1	High: 1 Medium: 0 Low: 0

Host OS: Canonical Ubuntu Linux (cpe:/o:canonical:ubuntu\_linux:16.04)

Open Ports: 4 (22, 8080, 8000, 53)

Host Identification

Identifier: Scanned IP

Hardware: Information not available

Detected Applications

CPE

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: 0.19s

# 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	lighttpd
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 priorisées & 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



## Autres Options de Balayage

Configuration personnalisées de balayage, alayages authentifiés, balayages cédulés

	Dashboard	Scan	Agents	Buckets	Configuration
<b>Security</b>					
20X Local Security Checks					
Windows Local Security Checks					
None (0)					
Buffer overflow				560 of 560	
CantFind Local Security Checks				560 of 560	
Crls:Inconsistent Local Security Checks				25000 of 25000	
File Read				361 of 361	
File Write				7 of 7	
Hashes				667 of 687	
Delete Local Security Checks				20000 of 2496	
File Copy				1400 of 1400	
DnsGet				1350 of 1350	
File Local Security Checks				125 of 125	
File Read (0)				135 of 135	
File Write (0)				90000 of 96600	
Futex Local Security Checks				6 of 6	
Finger absence				144 of 144	
File Read (1)				34 of 34	
File Write (1)				404 of 404	
File Read (2)				140 of 140	
File Write (2)				20508 of 20508	
Server				20508 of 20508	
Gauss Local Security Checks				20508 of 20508	
Windows Local Security Checks				145 of 145	
Windows Local Security Checks (0)				131 of 131	
FT_Groundcheck				90 of 90	
FT_Groundcheck (0)				100 of 100	
FT_Groundcheck (1)				65 of 65	
FT_Groundcheck (2)				60 of 60	
FT_Groundcheck (3)				60 of 60	
FT_Groundcheck (4)				136 of 136	
FT_Groundcheck (5)				173 of 173	
FT_Groundcheck (6)				329 of 329	
Magna Linux Local Security Checks				47 of 47	
Mikrosoft				904 of 904	
Microsoft Local Security Checks				904 of 904	
None				0 of 0	
Nmap NSC				154 of 154	
Open File				137 of 137	
Oracle Linux Local Security Checks				10000 of 10000	
Palo Alto PAN-OS Local Security Checks				40 of 40	
Policy				30 of 30	
Policy File Dealing				50 of 50	
Pat Selection				2 of 18	
Product inclusion				504 of 504	
Product deletion				10000 of 10000	
Root				11 of 11	
Run as Local Security Checks				1024 of 1024	
Remove file access				50 of 50	
Root problems				50 of 50	
Spear				7 of 7	
SSL and TLS				54 of 54	
TLS detection				300 of 300	
Upgrading				32 of 32	
Macosx Local Security Checks				564 of 564	
File Read (0)				14 of 14	
File Write (0)				3309 of 3209	
File Write (1)				26205 of 2625	
File Write (2)				14 of 14	
File Write (3)				50 of 50	
File Write (4)				303 of 303	
File Write (5)				179 of 179	
File Write (6)				1803 of 1803	
Windows				1803 of 1803	
Windows: Microsoft Building				1803 of 1803	
Total:	42	4452	10000	10000	10000 of 10000 in selected families

 **Credentials (2 of 2)**

Name	Type
admin (test)	smb (SNMP)
test1 (test)	up (username + password)

(Applied filter: rows<10 from1 sortname)

Blocklist operation: 0.88s

---

 **Schedule: schedule1**

Name	Comment	First Run	Next Run	Timezone	Period	Duration
schedule1	test	Thu Apr 20 14:25:00 2018 UTC	Fri Apr 21 14:25:00 2018 UTC	UTC	1 day	2 hours

 **Tasks using this Schedule (none)**

Name

 **User Tags (none)**

 **Permissions (none)**

Name	Description	Resource Ty

Produced on demand: 0.02s

# 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:8008	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.*

The screenshot shows the Arachni web interface. At the top, there is a navigation bar with the text "Arachni v1.5.1 - WebUI v0.5.12" and dropdown menus for "Scans", "Profiles", "Dispatchers", and "Users". The main content area has a white background with black text. It starts with a welcome message: "Welcome to Arachni's web interface," followed by a sub-instruction: "please skim through this page to get the information you need before you start wandering about." Below this, there is a section titled "Choosing the right database" with explanatory text. Further down, there is a section titled "Getting help" with links to "Documentation", "Reporting bugs", and "Asking for help". A note at the bottom states: "You can quickly access the above resources from any page of the interface via the links in the footer."

Arachni v1.5.1 - WebUI v0.5.12

Welcome to Arachni's web interface,  
please skim through this page to get the information you need before you start wandering about.

### Choosing the right database

By default, this interface uses an SQLite3 database and that allows for a configuration-free out-of-the-box experience. However, this setup is unsuitable for...  
If you plan on only having a few scans running at any given time then there shouldn't be any issue, if, however, you plan on running and managing multiple...  
*Unfortunately, you can't move your data between databases; thus, if you plan on evaluating Arachni using the default database, before moving to PostgreSQL*

### Getting help

Don't hesitate to ask for assistance if you run into issues or have any questions, but do use the right way to get in touch:

**Documentation**  
Cut and dry documentation, goes through all the available features and explains what everything does.

**Reporting bugs**  
If something exploded or you're seeing a scary error please do take some time to tell us about it so that we can fix it and have you back on your way.

**Asking for help**  
The support portal allows you to easily ask for assistance or clarifications. If you are unsure about how to do something, this is the right way to find out.

You can quickly access the above resources from any page of the interface via the links in the footer.

# Balayage de vulnérabilités Web

---

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

The screenshot shows the Arachni WebUI interface. At the top, there is a navigation bar with the text "Arachni v1.5.1 - WebUI v0.5.12" and dropdown menus for "Scans", "Profiles", "Dispatchers", and "Users". A blue button labeled "Administrator" is also visible. Below the navigation bar, the main content area has a heading "Start a scan" and a sub-instruction: "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." There are two input fields: one for the "Target URL" containing "http://192.168.10.253:80" and another for the "Profile" set to "Default (Global)". A "Description" text area is present with the placeholder "Description" and a note "You can use Markdown for text formatting.". A "Share with:" section includes a dropdown menu with "Regular User" selected.

# Balayage de vulnérabilités Web

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

The screenshot shows the Arachni v1.5.1 - WebUI v0.5.12 interface. The top navigation bar includes links for Groups, Scans, Profiles, Dispatchers, Users, and Administrate. The main content area is titled "Scans" and displays the following sections:

- Groups:** A section where users can create groups, with a message stating "You haven't created any groups." It includes fields for "(Required) Name" and "(Required) Description" and a "Share with:" dropdown for "Regular User".
- Active [3]:** A list of active scans. The first two entries are for "http://www.dev.webscanner.com" and "http://newapp.dev.webscanner.com", both using the "Default" profile, Direct type, and Scanning status. The third entry is for "http://mca.dev.webscanner.com". Each entry includes columns for URL, Profile, Type, Status, Issue count, Sitemap size, Running for, and Comments. To the right of each entry are four small colored squares (blue, orange, red, green) with icons.
- Finished [1]:** A list of finished scans. One entry is shown for "http://newapp.dev.webscanner.com" using the "Default" profile, Direct type, and Scanning status. The entry includes columns for URL, Profile, Type, Issue count, Started at, Finished at, and Comments. To the right of the entry are four small colored squares.
- Suspended [0]:** A section indicating there are no suspended scans.

# 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

Severity	Count
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)

Link
q
q
q
q
q
q
q
q



# 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**

```
[REDACTED]
```

**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_tracers();
_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_tracers();_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	0.09993378	request	[REDACTED]?

```
q=:window.top._arachni_js_namespace_taint_tracer.log_execution_flow_sink()
```



## 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 priorisées & 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  Check all  Uncheck all

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

- Code injection (code\_injection)
- Code injection (php\_input\_wrapper) (code\_injection\_php\_input\_wrapper)
- Code injection (timing) (code\_injection\_timing)
- CSRF (csrf)
- File inclusion (file\_inclusion)
- LDAPInjection (ldap\_injection)
- NoSQL injection (no\_sql\_injection)
- Blind NoSQL injection (differential analysis) (no\_sql\_injection\_differential)
- OS command injection (os\_cmd\_injection)
- OS command injection (timing) (os\_cmd\_injection\_timing)
- Path Traversal (path\_traversal)
- Response Splitting (response\_splitting)
- Remote File Inclusion (rfi)
- Session fixation (session\_fixation)
- Source code disclosure (source\_code\_disclosure)

**Passive** These checks will passively collect data

- Allowed methods (allowed\_methods)
- Backdoors (backdoors)
- Backup directories (backup\_directories)
- Backup files (backup\_files)
- CAPTCHA (captcha)
- Common administration interfaces (common\_admin\_interfaces)
- Common interests (common\_interests)
- Common interests (common\_interests)

HTTP: How the scanner will communicate with the web application

Http authentication username

Http authentication type  auto

Advanced options

Distribution  Scheduling

Start at  Recurring

hour/minute/day/month/year  Every: Minutes (1-59) Hours (1-23) Days (1-20) Months (1-12)  Use stamps of previous revisions:  
Instead of crawling   
in addition to crawling

Stop after  After: Finish time

hours/minutes/seconds  Suspend

Go!



...en continu !

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

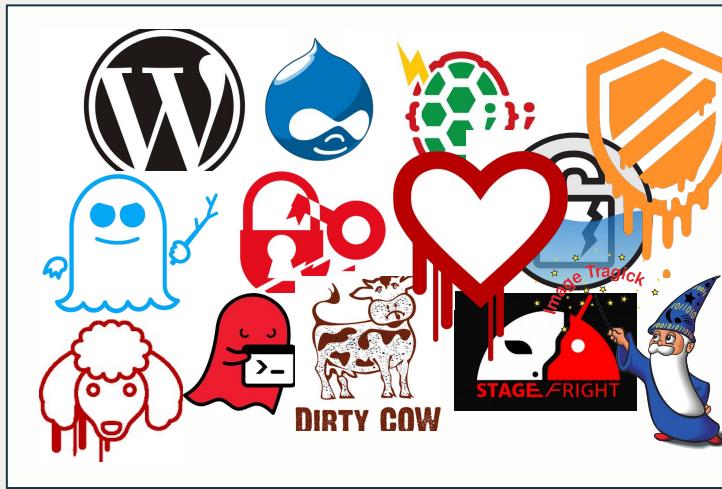
**Option 1:** Créer un balayage personnalisé dans OpenVAS pour balayer toutes les machines pour cette vulnérabilité.

**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":

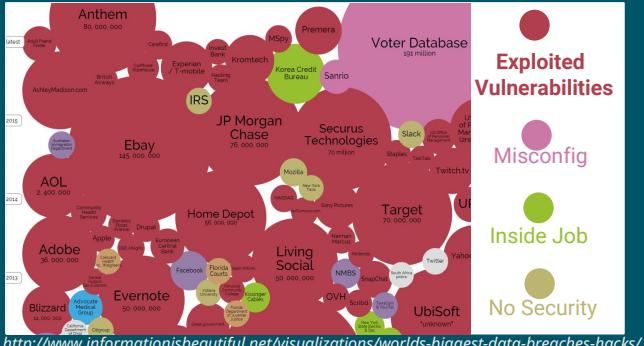
- Automatiser
- Automatiser
- Automatiser

# Pourquoi ?

# L'état de la cybersécurité actuel

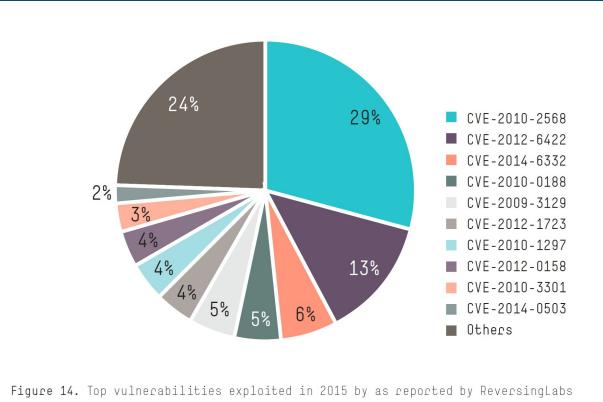
En 2017, le top 3 des sources de cyber attaques était encore:

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



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

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



Source: <https://snyk.io/blog/cwasp-top-10-breaches/>,  
<https://www.recordedfuture.com/rasputin-eac-breach/>, <http://www.nextgov.com/cio-briefing/2015/10/irs-cant-update-woefully-out-date-windows-servers-because-it-cant-find-some-them/122770/>, <https://www.veracode.co.uk/blog/2011/05/possible-playstation-network-attack-vectors>

## 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).

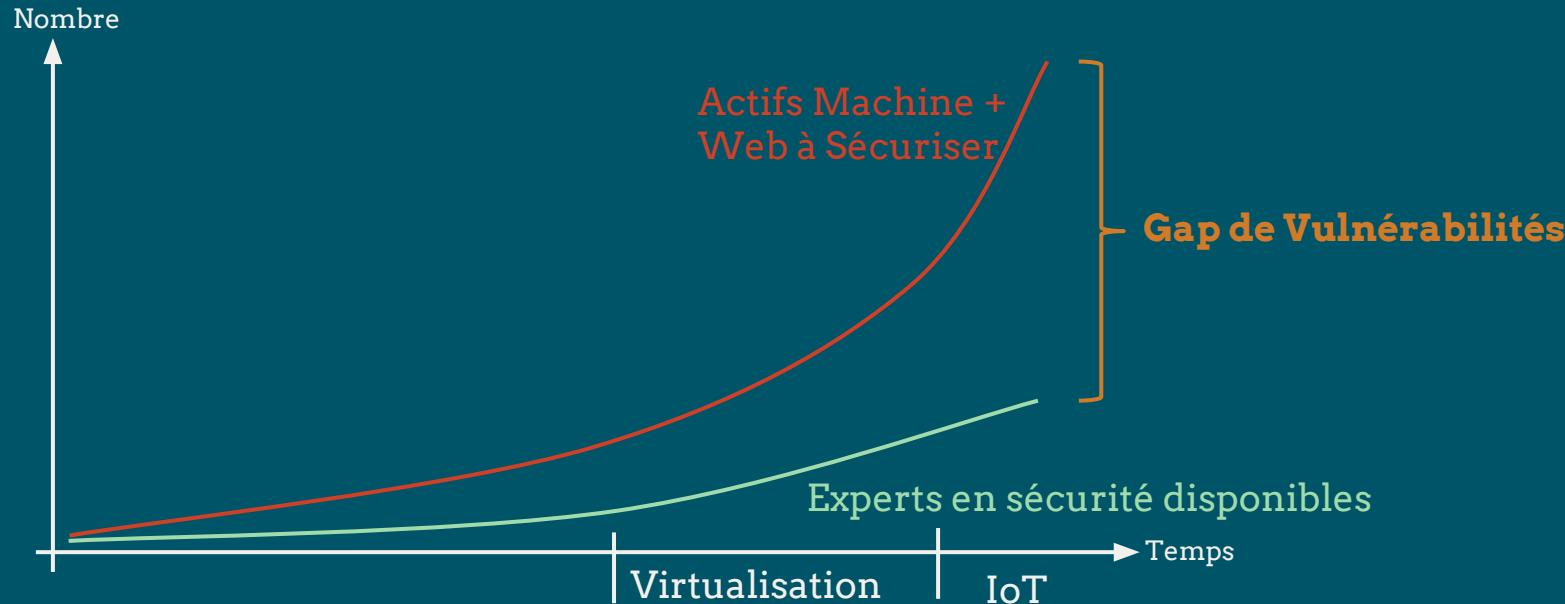
**"Vulnerability assessment is a standard component of most information security management and regulatory frameworks."**

**"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>

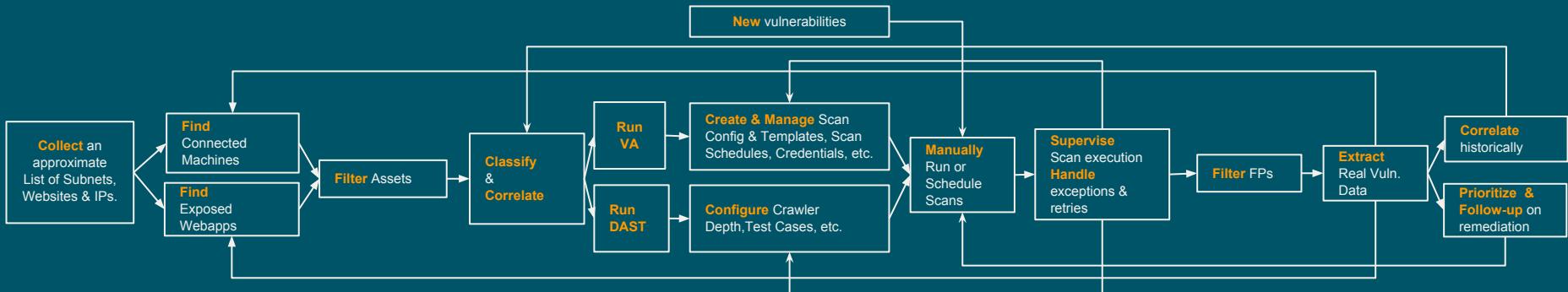
[2] <https://uk.sans.org/reading-room/whitepapers/analysts/reducing-attack-surface-sans%20%99-second-survey-continuous-monitoring-programs-37417>

[3] [http://ip.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox\\_Security\\_Vulnerability\\_Management\\_Survey.pdf](http://ip.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox_Security_Vulnerability_Management_Survey.pdf)

[4] <http://ip.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**.<sup>[3]</sup>
- La détection de vulnérabilité classique a un taux de **Faux-Positifs** de **50% à 90%** <sup>[1]</sup>
- Ce processus cause une accumulation de tâches répétitives et rébarbatives pour les experts<sup>[2]</sup>



[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://ip.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox\\_Security\\_Vulnerability\\_Management\\_Survey.pdf](http://ip.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox_Security_Vulnerability_Management_Survey.pdf)

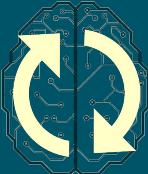
[3] <https://uk.sans.org/reading-room/whitepapers/analyst/reducing-attack-surface-sans%20%99-second-survey-continuous-monitoring-programs-37417>

# WARDEN

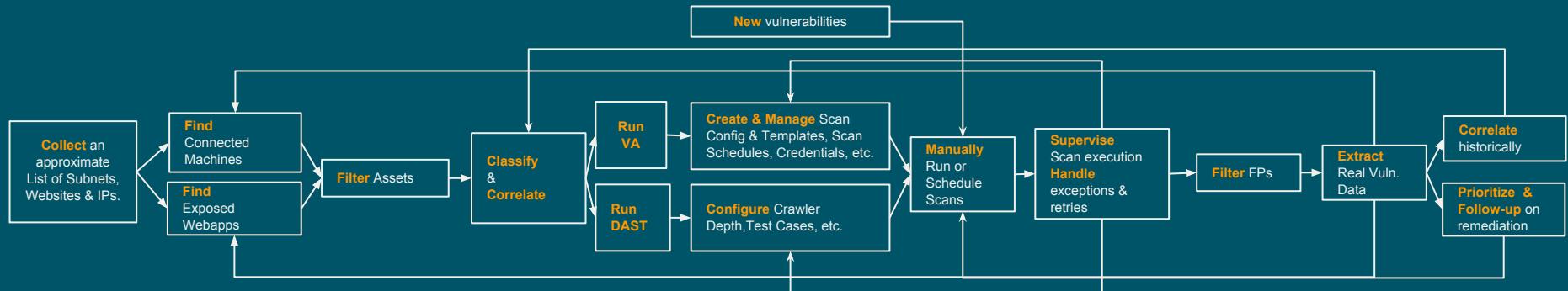
AI-DRIVEN VULNERABILITY ASSESSMENT

# Comment Warden automatise ce processus

## AI-DRIVEN

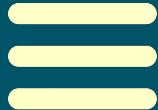


- **Système Expert** auto-évolutif conduisant la découverte et le balayage d'actifs
- **Apprentissage Machine** pour détection et classification des Faux-Positifs
- **Meta-Simulation de “pentest”** par l'AI pour pré-prioriser la remédiation



# 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