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	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
4954b1093aa83613e0cfeb36492e468ca2d711526bb2a7911dfb82a7c66b486b
...
```

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

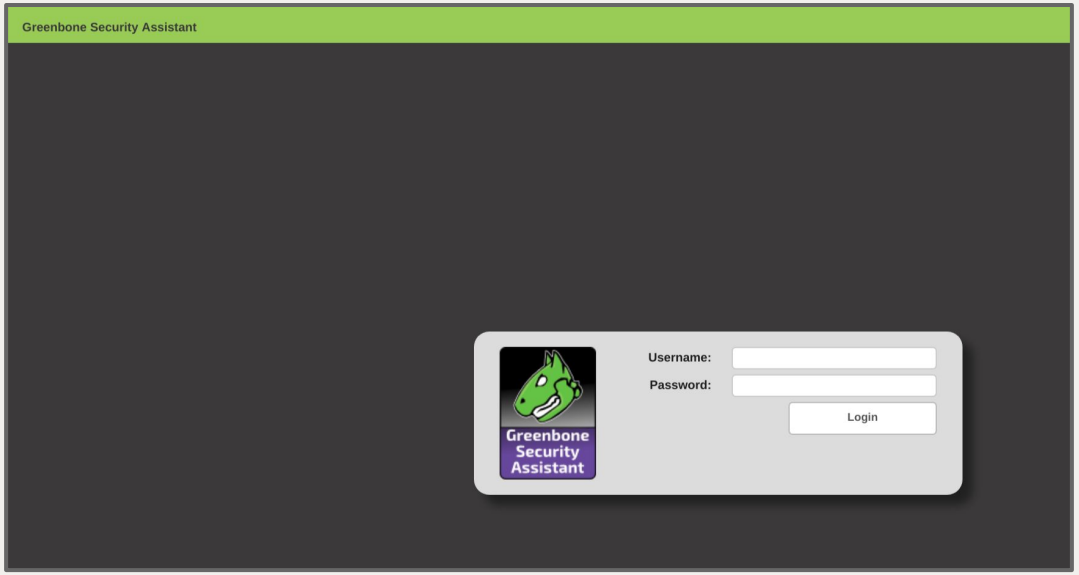
Point de départ: notre liste de machines internes et externes.

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

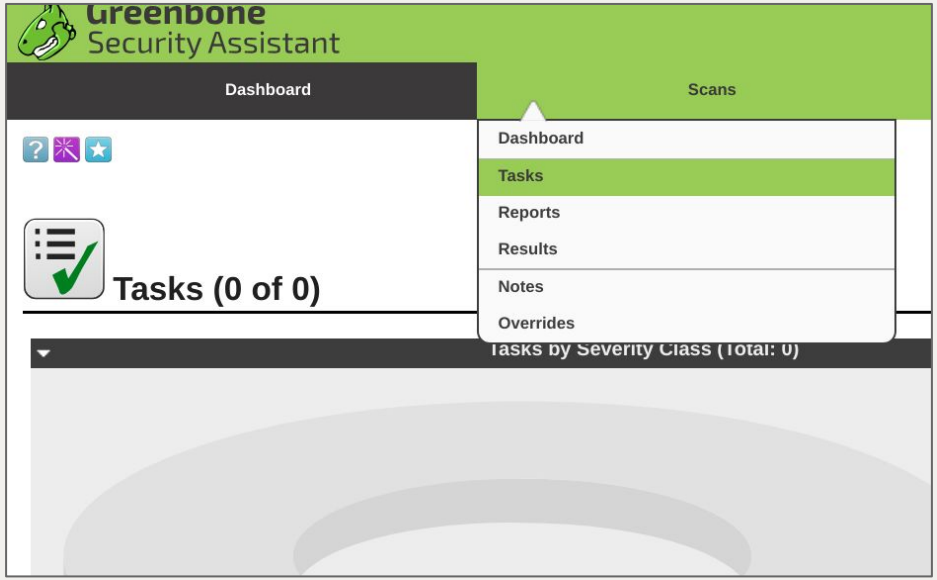
Exécuter de la détection de vulnérabilités (VA) sur les IPs trouvés ci-haut:

Outils disponibles
OpenVAS, Nessus, Retina CS free, nmap



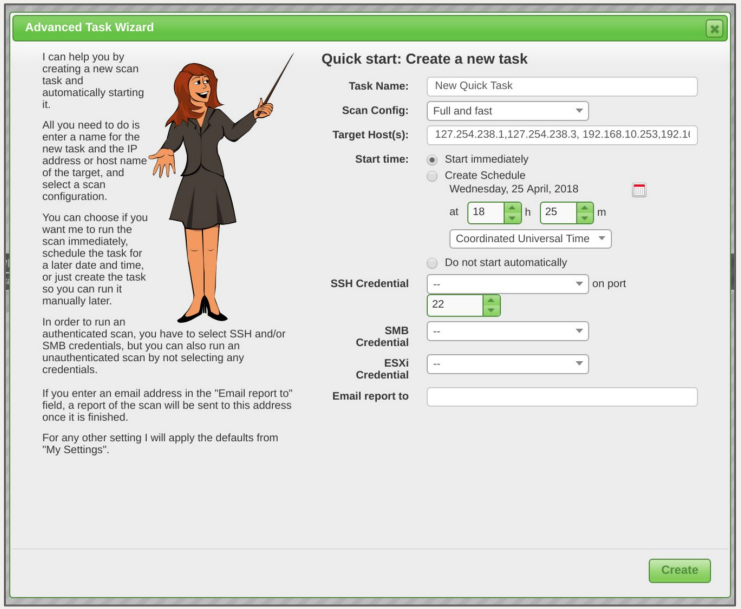
Balayage de vulnérabilité machine

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:

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	

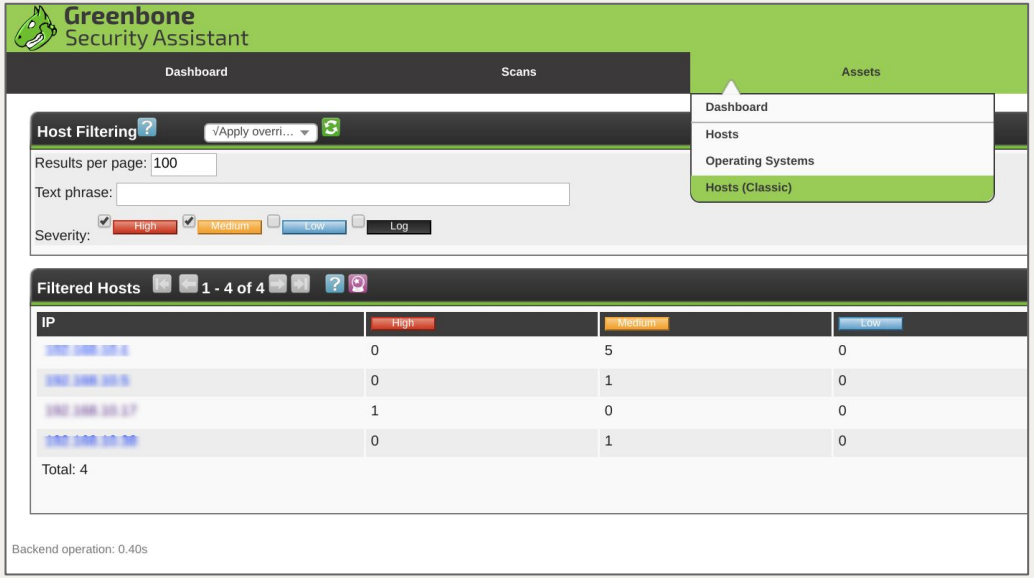
Filtrer les faux positifs

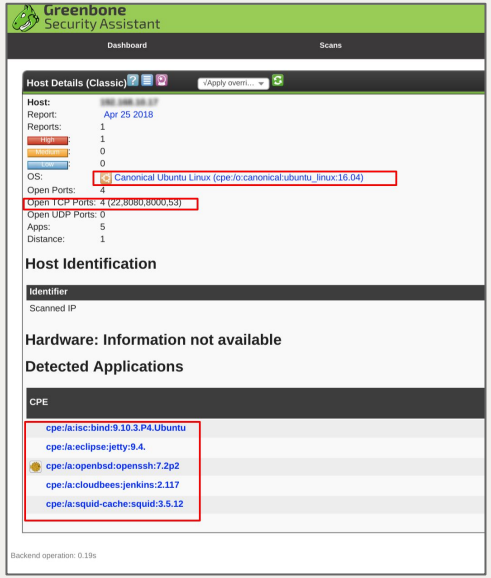
Pour chacune des vulnérabilités:

- ➔ 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.





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

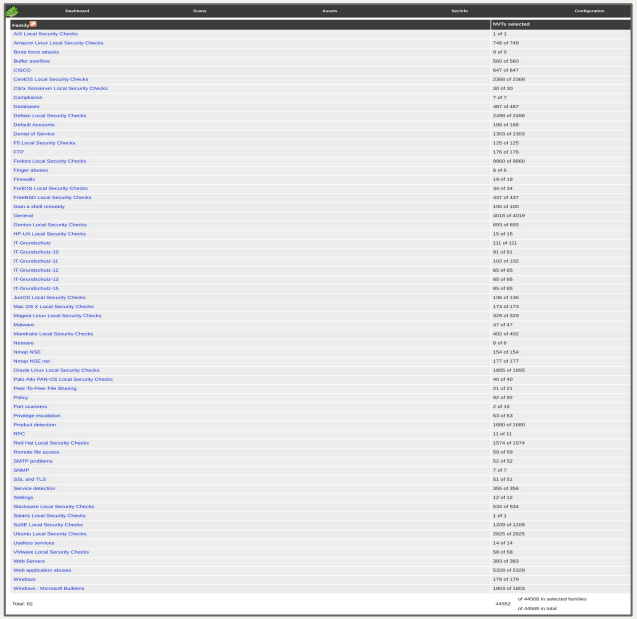
Extraire les données de vulnérabilité priorisées & initier la remédiation

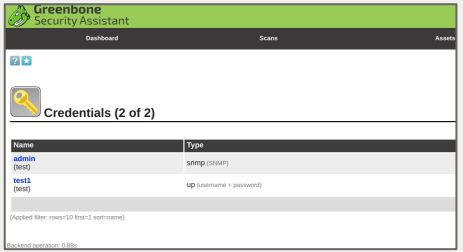
Récupérer l'information additionnelle sur les logiciels installés et combiner le tout dans notre chiffrier existant.

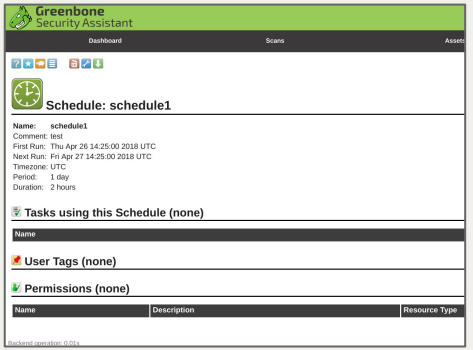
Machine	Vulnérabilité	Date découverte	Responsable résolution
127.254.238.1	OpenSSH Denial of Service And User Enumeration Vulnerabilities CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-10708	15 / 05 / 2018	Mr Untel 1 / email@compagnie.com
127.254.238.1	Apache HTTP Server 'mod_auth_digest' 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







Balayage de vulnérabilités Web

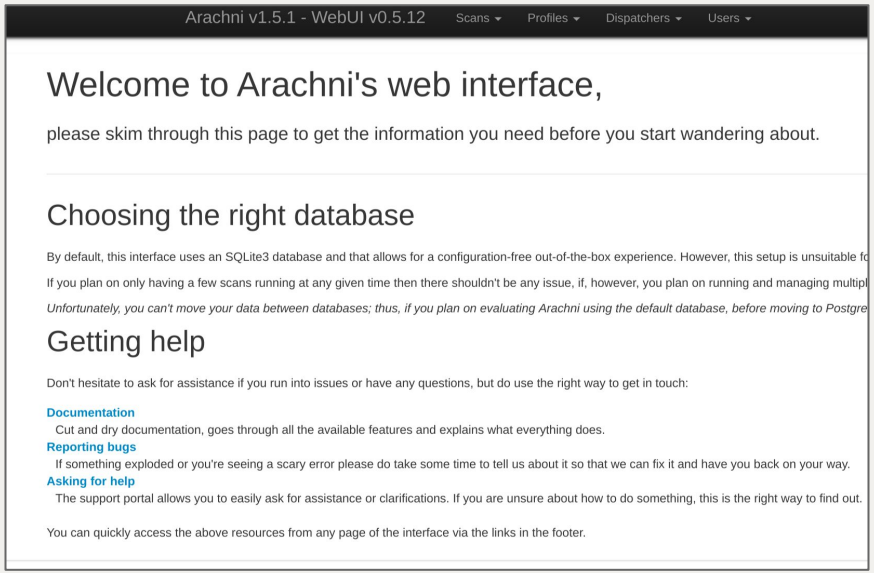
Point de départ: notre liste de sites Web internes et externes.

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

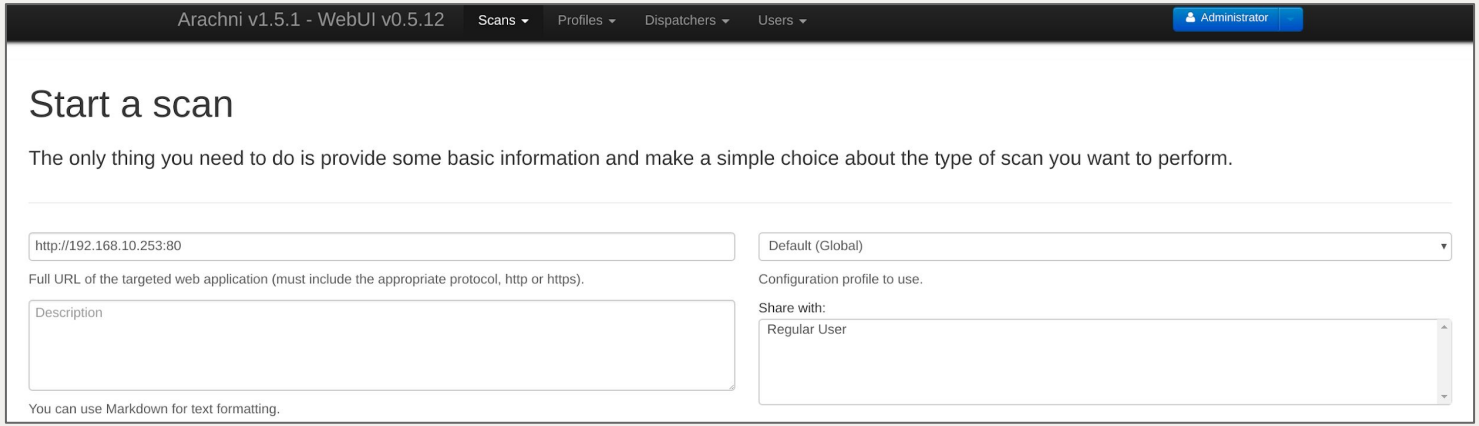
Exécuter de la détection de vulnérabilités (DAST) sur les sites Web ci-haut:

Outils disponibles
Arachni, ZAP, Burp, etc.



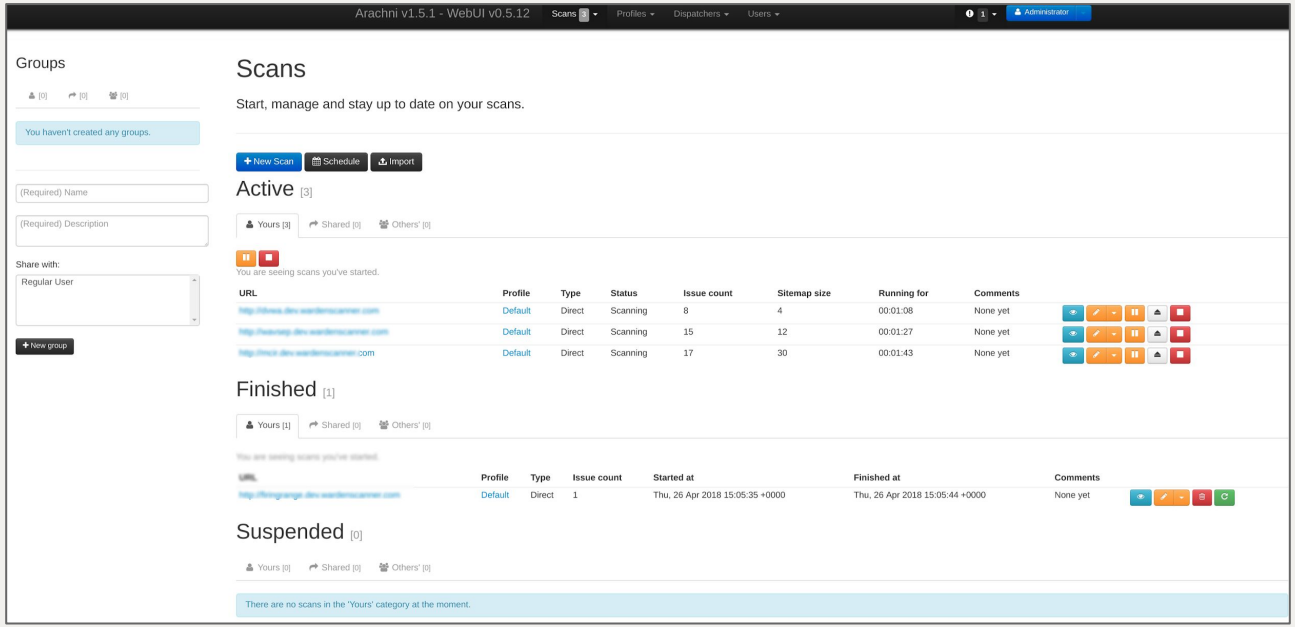
Balayage de vulnérabilités Web

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



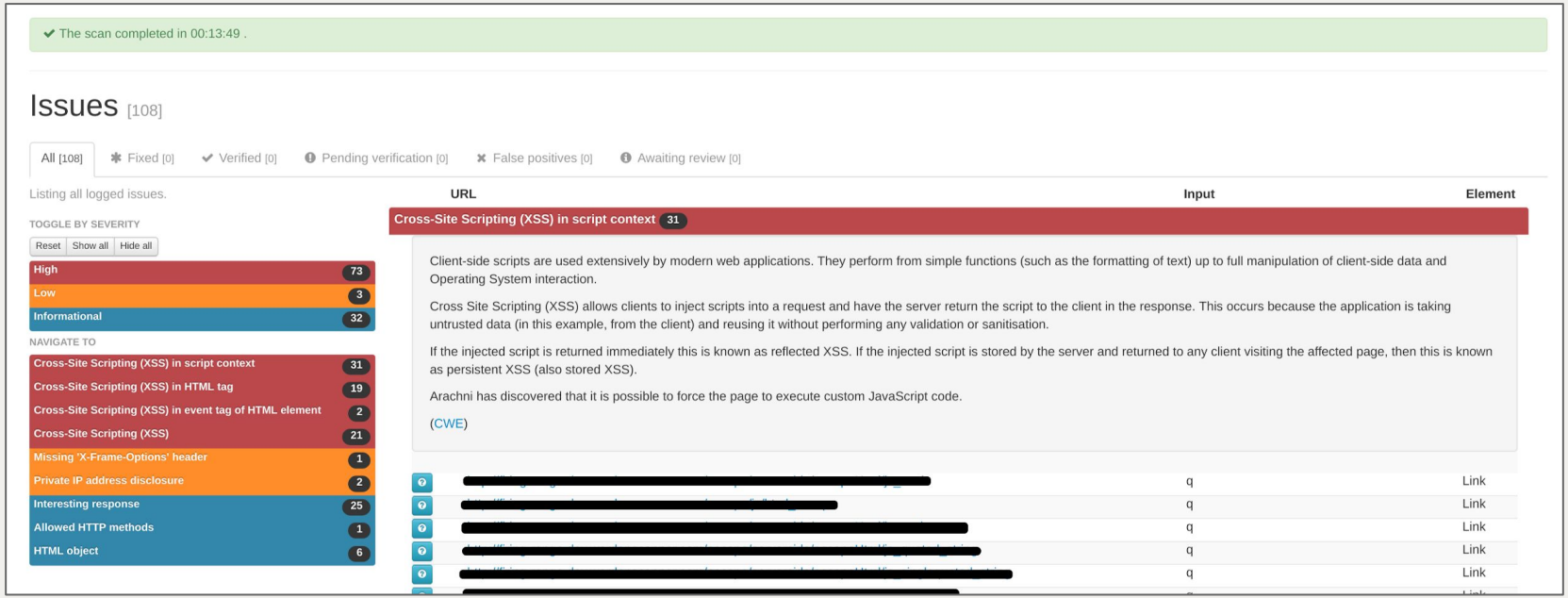
Balayage de vulnérabilités Web

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



Balayage de vulnérabilités Web

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



Filtrer les faux positifs

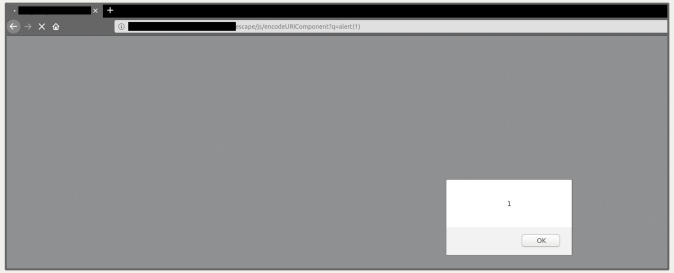
Pour chacune des vulnérabilités:

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

Filtrer les faux positifs

Pour chacune des vulnérabilités:

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



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)

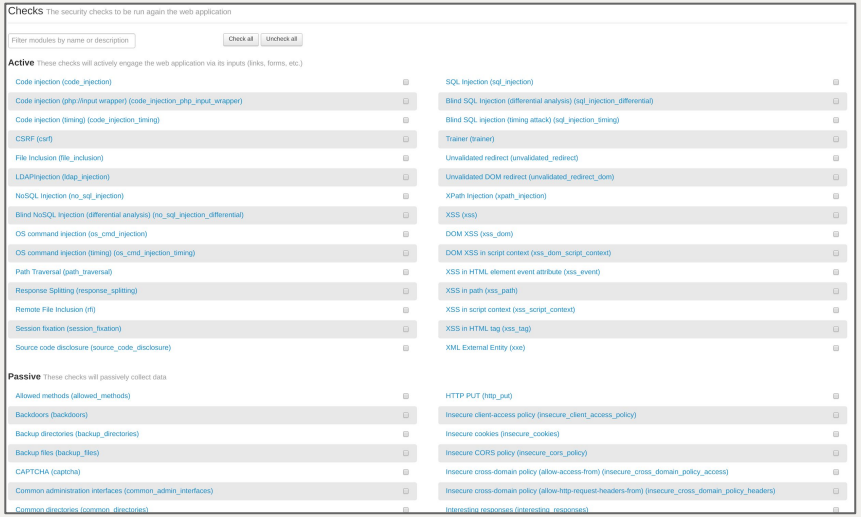
Extraire les données de vulnérabilité priorisées & initier la remédiation

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



...en continu !

Gérer les vulnérabilités "*Out-Of-Band*"

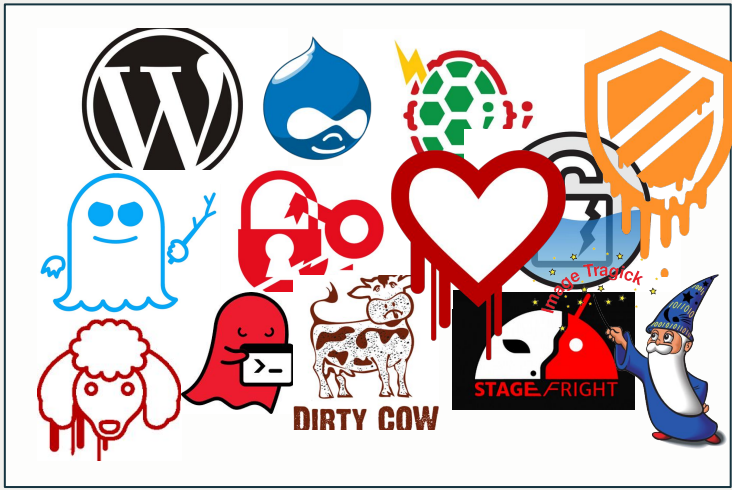
Option 1: Créer un balayage personnalisé dans OpenVAS pour balayer toutes les machines pour cette vulnérabilité.

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

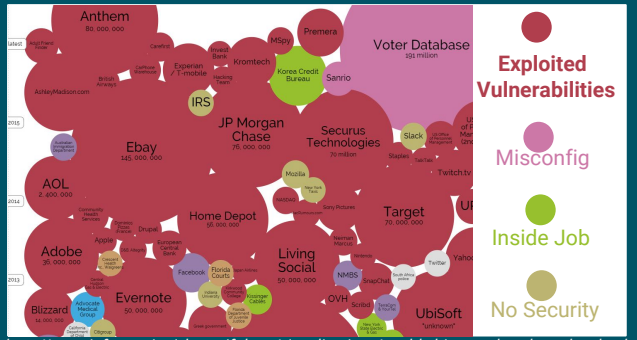
Pourquoi ?

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/

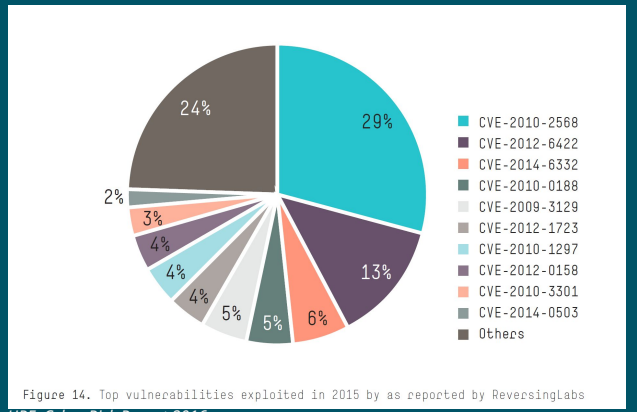


Figure 14. Top vulnerabilities exploited in 2015 by as reported by ReversingLabs

HPE Cyber Risk Report 2016

Source: https://snyk.io/blog/owasp-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

Gartner®

“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.”

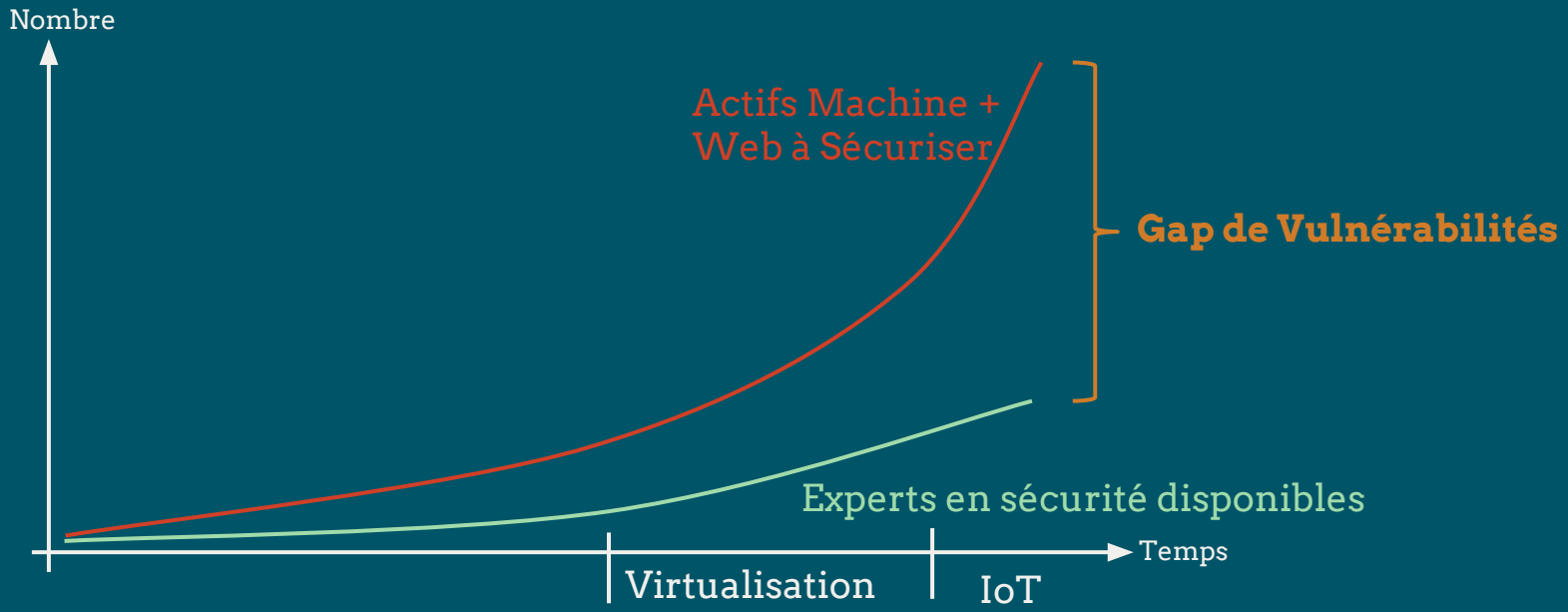
“99.99% of exploits are based on vulnerabilities that have already been known to security and IT professionals for at least one year”

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

Source: https://www.gartner.com/doc/reprints?id=1-3NIA3DF&ct=161208&st=sb & https://www.gartner.com/doc/3513217/predicts--threat-vulnerability-management

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

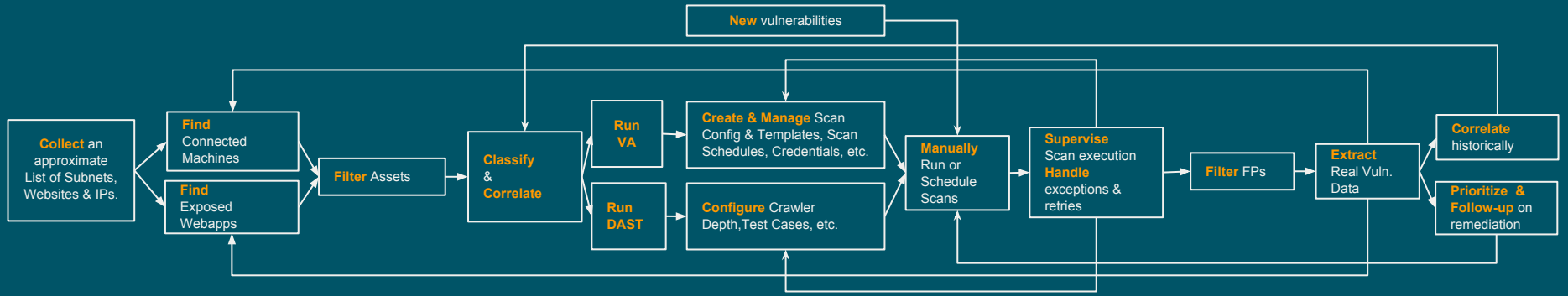
- **2M** d'experts seront manquants d'ici 2019 [1]
- Moins de 20% des compagnies balayent 100% de leurs actifs **critiques** [2]
- **70%** des compagnies **balayent moins de 50%** de leur réseau [3] sur une base mensuelle seulement[4]



[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%99-second-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://lp.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%99-second-survey-continuous-monitoring-programs-37417

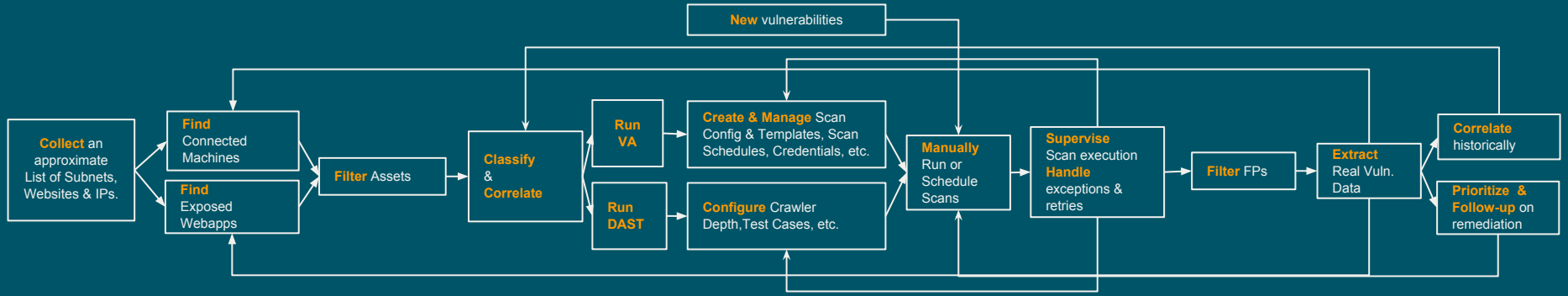
WARDEN

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