Réduction de la surface d'attaque d'un S.I.

Une approche pragmatique

OSSIR Paris ~ 12 juillet 2011

Saâd KADHI / saad.kadhi@hapsis.fr
HAPSIS

Contexte et Objectifs

Il était une fois...

- Multinationale présente sur les 5 continents
- Nombre important de filiales
- Différence de culture I.T., d'infrastructures, de budget, de géographie
- Ajustements locaux voire divergences avec les standards édictés

- A un bout du spectre, plusieurs îles et liens réseau de faible capacité
- Sollicités par màj antivirales et système
- Forte tendance au nomadisme

- A l'autre, filiales occidentales dotées d'une bande passante importante

- Datacenter dernier cri, suivi rigoureux dans la gestion des correctifs

- Certaines filiales sont hébergeurs de ressources IT avec centres de compétences, offres de service, etc.

- Monde interconnecté
- Fluidité de l'information, fluidité des attaques
- Dans un monde si hétérogène, comment améliorer le niveau de sécurité ?
- Approche par les vulnérabilités

- Un peu de réflexion à l'ère du tout, tout de suite et de la pensée compressée
- Nombre assez important de contraintes
- Penser service, ne pas penser produit

Surface d'attaque, vulnérabilités

...et homéopathie !

- ~~Surface d'attaque = tous les services réseau accessibles~~

- Surface d'attaque = somme des vulnérabilités connues et exploitables à distance

- N'inclut pas les vulnérabilités dites locales

- Supposition : attaquant disposant d'une connexion au réseau interne

- Comment estimer la surface d'attaque, vue du réseau interne ?
- Moteur de scan de vulnérabilités
- Mais encore ?

- *Horror stories*
- Qui dit scan de vulnérabilités dit dysfonctionnements système et applicatifs potentiels
- Comment réduire ce type de risques ?

- Pas de scan intrusif
- Charge réseau à estimer (technique du doigt mouillé ?)
- Ne pas surcharger les liens et les cibles
- Pas de garantie complète

Ceci dit, un attaquant ne vous garantit rien non plus quoique...

- Certaines piles TCP/IP sont fragiles
- Certains systèmes sont fragiles
- Certaines applications sont fragiles
- L'attaquant n'a pas de pitié
- Alors on fait quoi ?

- Saupoudrer quelques règles de filtrage réseau

- Confiner ces composants à la seule population qui en ait l'utilité

- Et si cette population est aussi nombreuse que celle de l'Inde ?

- Les faux négatifs sont difficiles à adresser
- Un moyen : une étude rétrospective
- (Rapidité de) prise en compte des vulnérabilités
- Fréquence de màj

Ce n'est pas une boule de Crystal

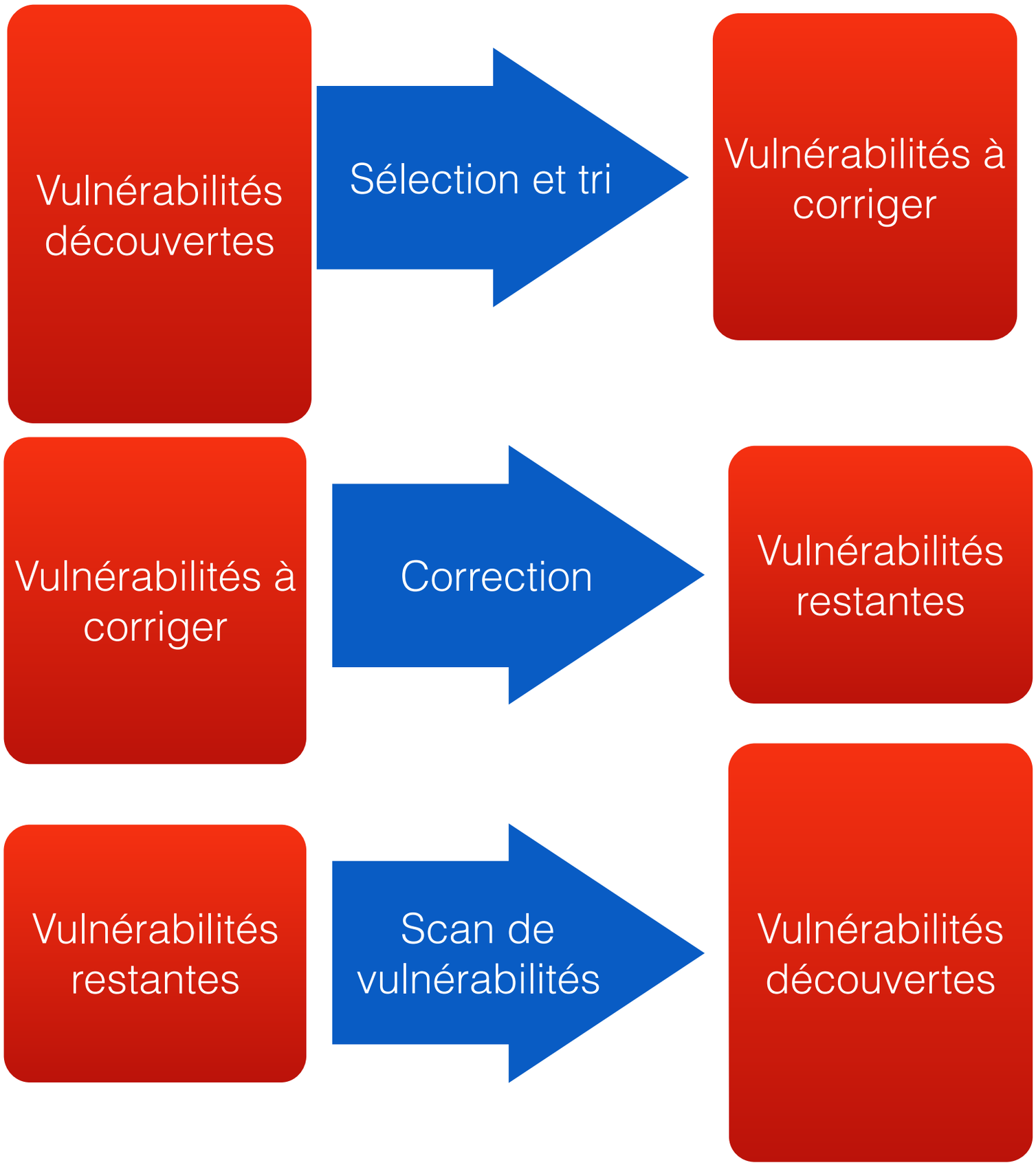
- Il y a pire, bien pire
- Les faux positifs
- Pierre et le Loup, le syndrome du lapin afghan,...
- Le taux de faux positifs a une influence directe sur la légitimité du service

- Que faire ?
- Mesure du taux de faux positifs
- Nécessite un ban de tests et des machines dont on connaît parfaitement les vulnérabilités
- Ou rechercher des études comparatives

Attention à la méthodologie et à l'indépendance

- Les vérifications authentifiées sont une autre piste
- Hum... Compte utilisateur créé sur tout le parc
- Comment les identifiants sont stockés dans le moteur de scan ?
- Quels risques induits par la présence de ce compte sur des machines à criticité différente ?

- Et si on sélectionnait soigneusement les actions d'amélioration ?
- Actions peu nombreuses pour être suivies d'effets
- Supportées par un processus itératif


Vulnérabilités découvertes
Sélection et tri
Vulnérabilités à corriger
Vulnérabilités à corriger
Correction
Vulnérabilités restantes
Vulnérabilités restantes
Scan de vulnérabilités
Vulnérabilités découvertes

- Le temps de vos interlocuteurs est précieux
- Ne le gaspillez pas
- Ne les dégoutez pas
- Mettez vous à leur place

- On scanne
- On ne garde que les vulnérabilités les plus critiques
- Failles à impact important et/ou facilement exploitables
- Taux de faux positifs quasi nul !

Du produit au service

Au-delà du scan bête et méchant

- Nessus
- Produit stable, éprouvé et performant
- Politique de scan flexible et facile à configurer
- Excellent support
- Vulnérabilités très bien documentées
- Rapports XML

- Un seul moteur peut scanner un nombre illimité d'IPs
- Licence *ProfessionalFeed* peu coûteuse
- Vulnérabilités très bien documentées
- Rapports XML

- Les filiales définissent elles-même les cibles
- Mais attention...
- L'utilisation du service est fortement recommandée par les normes de contrôle interne
- Le service est facturé, coût fixe inclut dans l'abonnement Télécom

- Une filiale peut tricher
- Liste très réduite de cibles avec un niveau de correctifs proche du paranormal
- D'où couplage très étroit avec la réponse à incidents
- Sans oublier des campagnes régulières de tests d'intrusion

- Listes soumises avec un formalisme très simple

- Cibles + destinataires des rapports

- Injectés sous forme de fichiers YAML

- Les filiales n'interagissent pas directement avec le service

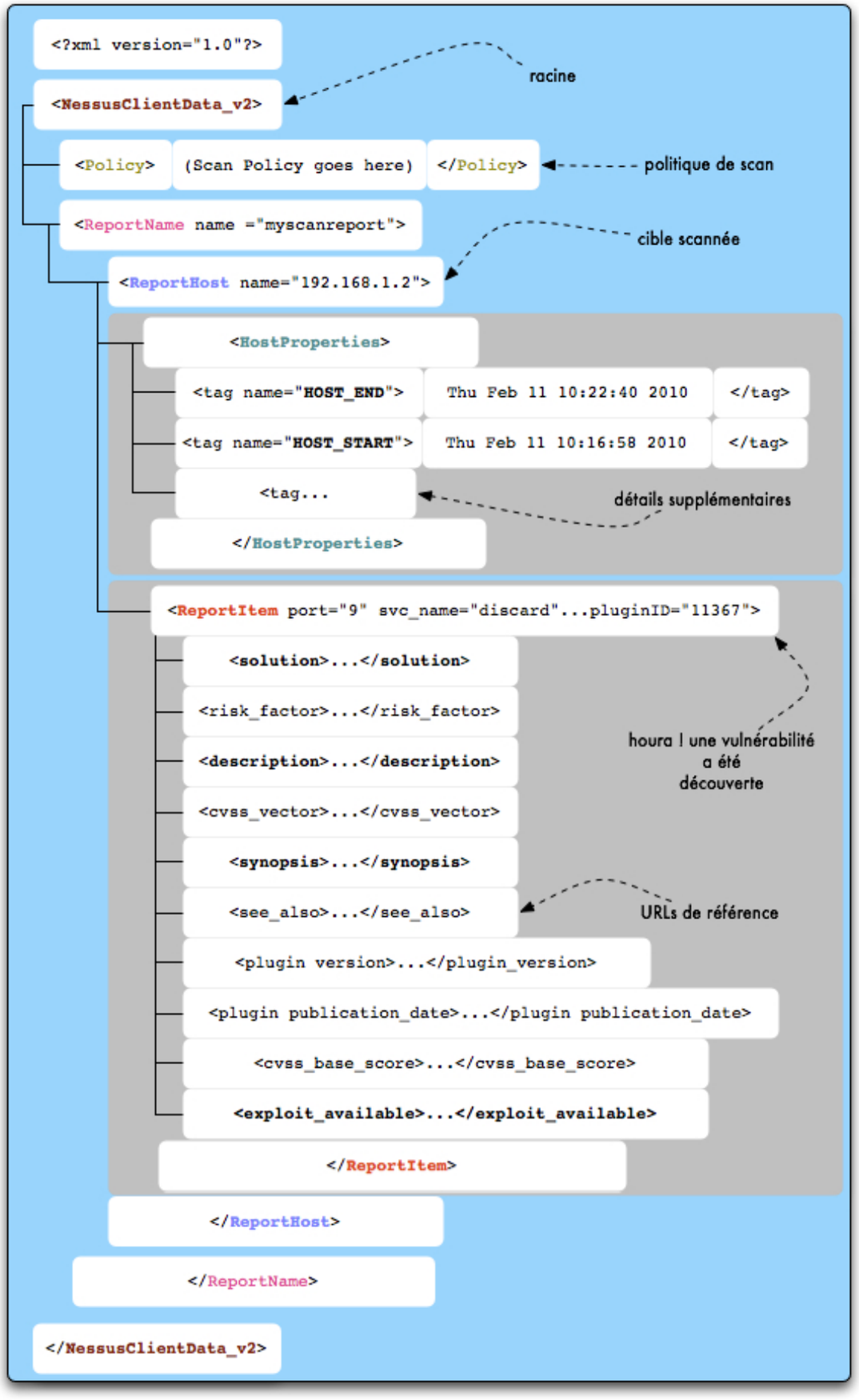
```yaml
# site_name: name of the site for which the scan will be conducted.
site_name: My Subsidiary

# site_contacts: list of contacts for site 'sitename'.
# Each contact is identified by:
# - first_name: the first name of the contact
# - last_name: the last name of the contact
# - email_addr: email address
# - ldap_user: LDAP username (for authentication purposes)
site_contacts:
  - first_name: John
    last_name: Smith
    email_addr: john.smith@mysubsidiary.inc
    ldap_user: jsmith
  - first_name: James
    last_name: Whoami
    email_addr: james.whoami@mysubsidiary.inc
    ldap_user: jwhoami

# targets: list of targets that need to be scanned.
targets:
  - 1.1.1.1
  - 1.1.1.2
  - 1.2.0.0/24
  - 1.3.0.5-1.3.0.34
```

- Interaction avec Nessus via API XML-RPC
- Requêtes HTTPS POST
- Réponses XML

- Scripts Ruby en CLI
- Gestion de scans
- Récupération des résultats
- Filtrage/tri et génération des rapports

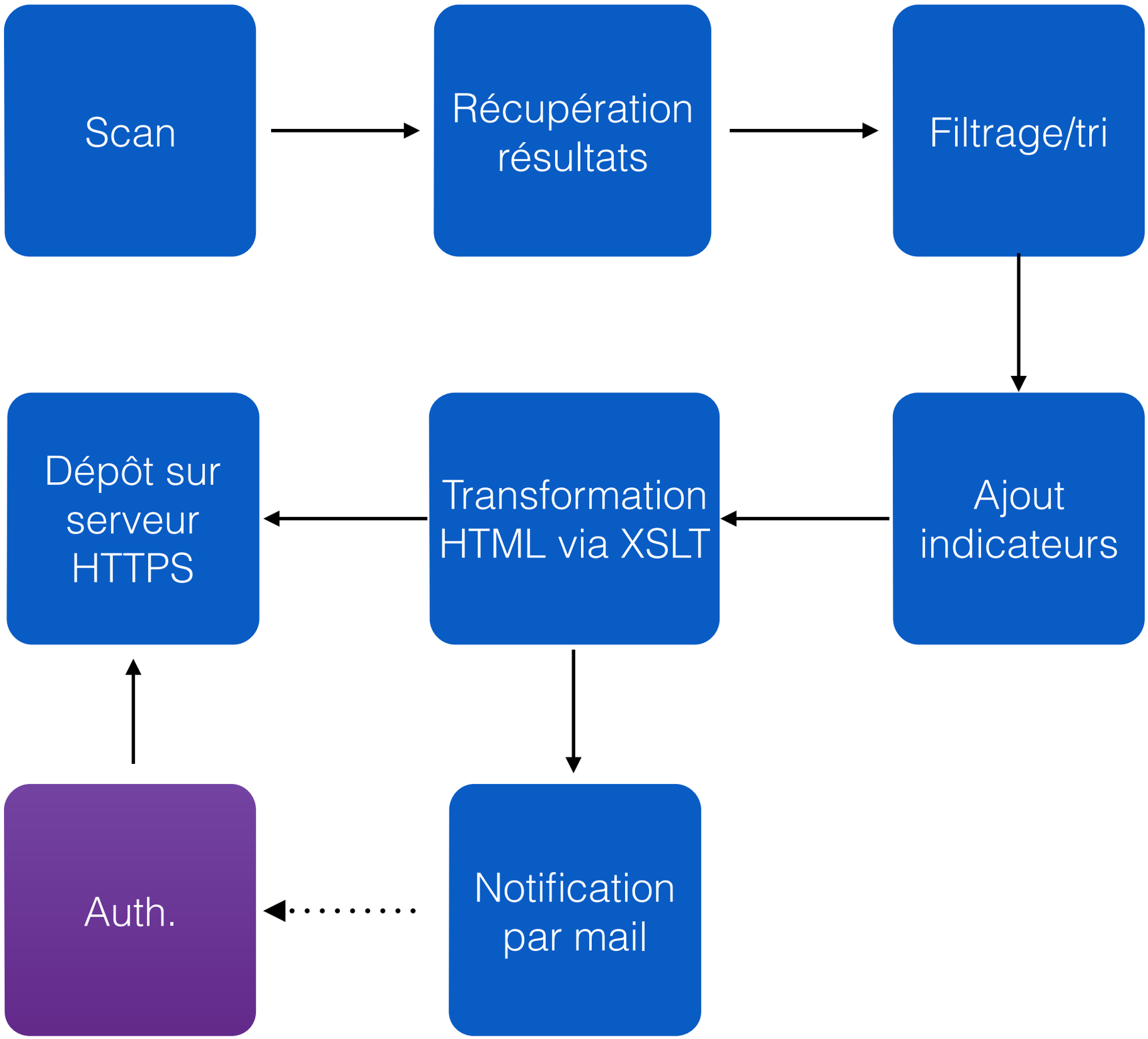

<?xml version="1.0"?>
racine
<NessusClientData_v2>
<Policy>
(Scan Policy goes here)
</Policy>
politique de scan
<ReportName name ="myscanreport">
cible scannée
<ReportHost name="192.168.1.2">
<HostProperties>
<tag name="HOST_END">
Thu Feb 11 10:22:40 2010
</tag>
<tag name="HOST_START">
Thu Feb 11 10:16:58 2010
</tag>
<tag...
détails supplémentaires
</HostProperties>
<ReportItem port="9" svc_name="discard"...pluginID="11367">
<solution>...</solution>
<risk_factor>...</risk_factor>
<description>...</description>
<cvss_vector>...</cvss_vector>
<synopsis>...</synopsis>
<see_also>...</see_also>
houra ! une vulnérabilité a été découverte
URLs de référence
<plugin version>...</plugin_version>
<plugin publication_date>...</plugin publication_date>
<cvss_base_score>...</cvss_base_score>
<exploit_available>...</exploit_available>
</ReportItem>
</ReportHost>
</ReportName>
</NessusClientData_v2>

- Enrichissement des résultats par des indicateurs

- Nb de cibles scannées, vulnérables

- Nb. total de vulnérabilités critiques

- % cibles non vulnérables sur la totalité des cibles scannées


Scan
Récupération résultats
Filtrage/tri
Ajout indicateurs
Transformation HTML via XSLT
Dépôt sur serveur HTTPS
Auth.
Notification par mail

logo goes here

Scan Results

CBU: My Subsidiary

The following report has been generated by my uber scan service, version 2.x.x. The scan engine is the award-winning Nessus scanner from Tenable Security Inc.

Please note that my uber scan service reports only on remotely-exploitable critical vulnerabilities.

company logo goes here

Local contact(s) at My Subsidiary:

- John Smith
- James Whoami

Enrollment Scope

Single Assets	16
Networks	0
IP Ranges	0

Overview

Metrics	Penultimate	Previous	Last
Scan Date	Wed Mar 23 23:58:35 2011	Sun Apr 24 23:25:17 2011	Mon May 23 09:58:47 2011
Scanned Assets	9	15	15
Vulnerable Assets	2	5	9
Critical Vulnerabilities	8	16	24
[redacted]**Score**	78%	67%	40%

Details

Asset IP Address	Asset DNS name	Critical Vulnerabilities
x.y.26.1	myvulnerableserver.mysubsidiary.inc	8
x.y.26.7	-	2
x.y.26.5	-	2
x.y.26.4	-	2

logo goes here

Scan Results

Asset: x.y.26.1, CBU: My Subsidiary

The following report has been generated by my uber scan service version 2.x.x. The scan engine is the award-winning Nessus scanner from Tenable Security Inc.

Please note that my uber scan service reports only on remotely-exploitable critical vulnerabilities.

company logo goes here

Local contact(s) at [redacted]

- John Smith
- James Whoami

Overview

Asset IP Address	x.y.26.1
Scan Start Date	Mon May 23 09:58:47 2011
Scan End Date	Mon May 23 10:04:19 2011
NetBIOS Name	MYVULNERABLESERVER
DNS Name	myvulnerableserver.mysubsidiary.inc
Operating System	Microsoft Windows Server 2003 Service Pack 2
MAC Address	FF:FF:64:fc:2f:ec
Critical Vulnerabilities	8

Critical Vulnerability List

Name	Nessus ID
HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities	46015
HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities	46677
HP System Management Homepage < 6.3 Multiple Vulnerabilities	53532
HP System Management Homepage < 6.2 Multiple Vulnerabilities	49272
HP System Management Homepage < 6.3 Multiple Vulnerabilities	53532
HP System Management Homepage < 6.2 Multiple Vulnerabilities	49272
HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities	46015
HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities	46677

HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities

Port
www (2381/tcp)

HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities

Port

www (2381/tcp)

Synopsis

The remote web server has multiple vulnerabilities.

Description

According to the web server banner, the version of HP System Management Homepage (SMH) running on the remote host is potentially affected by the following vulnerabilities : - Session renegotiations are not handled properly, which could be exploited to insert arbitrary plaintext by a man-in-the-middle. (CVE-2009-3555) - An unspecified vulnerability in version 2.0.18 of the Namazu component, used by the Windows version of SMH.

Solution

Upgrade to HP System Management Homepage 6.1.0.102 (Windows) / 6.1.0-103 (Linux) or later.

Additional Information

Product : HP System Management Homepage Version source : Server: CompaqHTTPServer/9.9 HP System Management Homepage/2.1.15.210 Installed version : 2.1.15.210 Fixed version : 6.1.0.102 (Windows) / 6.1.0-103 (Linux)

See Also

http://archives.neohapsis.com/archives/bugtraq/2010-05/0141.html
http://www.nessus.org/u?4e8707ba

Exploitability

true

Conclusion

A l'écoute des contraintes des utilisateurs

- Service actif depuis fin 2008
- Au début, deux filiales, une centaine de cibles
- Grande adhésion suscitée par la lisibilité et la simplicité des rapports

- Début 2011, plus de 4500 cibles dans une centaine de filiales

- Scan en moins de 24h

- Résultats très encourageants

- 80%+ de cibles non vulnérables dans la plupart des filiales

- Certes, la couverture de la surface d'attaque est partielle
- Vaut mieux être borgne qu'aveugle

- Améliorations à venir
- Moteur de scan de vulnérabilités Web
- Criticité métier par cible et prise en compte dans les indicateurs

- Toujours garder à l'esprit l'intérêt de vos interlocuteurs
- Adaptez-vous à leur façon de travailler et de penser

Hapsis

45 rue de la chaussée d'Antin
75009 Paris
FRANCE
Tél. : +33 (0)1 53 16 30 60 - Fax : +33 (0)1 53 16 30 62
Email : contact@hapsis.fr
Web : http://www.hapsis.fr/