

Une approche pragmatique de la mise en œuvre de politiques de sécurité

Guillaume Rousse,
Denis Joiret,
Bertrand Wallrich



Journées Réseau 2013



Plan

- 1 Problème
- 2 Réponse
 - Démarche
 - Aspects techniques
 - Aspects humains
- 3 Conclusions

Contexte simple

Cumul des fonctions

Répartition de l'ensemble des fonctions au sein d'un groupe unique

Avantages

- forte cohésion
- fort partage des valeurs et de l'expertise

Inconvénient

- passage à l'échelle

Contexte simple

Cumul des fonctions

Répartition de l'ensemble des fonctions au sein d'un groupe unique

Avantages

- forte cohésion
- fort partage des valeurs et de l'expertise

Inconvénient

- passage à l'échelle

Contexte simple

Cumul des fonctions

Répartition de l'ensemble des fonctions au sein d'un groupe unique

Avantages

- forte cohésion
- fort partage des valeurs et de l'expertise

Inconvénient

- passage à l'échelle

Séparation des rôles

Ceux qui spécifient

- RSSI : PSSI
- experts sécurité : audits et préconisations

Ceux qui réalisent

- ingénieurs : conception et déploiement
- exploitants : gestion quotidienne

Conséquences

- dilution de l'expertise
- différence dans les priorités

Séparation des rôles

Ceux qui spécifient

- RSSI : PSSI
- experts sécurité : audits et préconisations

Ceux qui réalisent

- ingénieurs : conception et déploiement
- exploitants : gestion quotidienne

Conséquences

- dilution de l'expertise
- différence dans les priorités

Séparation des rôles

Ceux qui spécifient

- RSSI : PSSI
- experts sécurité : audits et préconisations

Ceux qui réalisent

- ingénieurs : conception et déploiement
- exploitants : gestion quotidienne

Conséquences

- dilution de l'expertise
- différence dans les priorités

Résultat

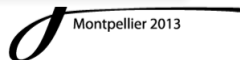
Constat

Écart grandissant entre :

- la spécification : ce qu'il faudrait faire
- la réalité : ce qui est effectivement en place

Besoin

- mesurer l'écart
- réduire cet écart



Plan

- 1 Problème
- 2 Réponse
 - Démarche
 - Aspects techniques
 - Aspects humains
- 3 Conclusions

De l'outil au service

Outils disponibles

- nmap : scanner de port
- openvas : scanner de vulnérabilité générique
- nessus : scanner de vulnérabilité générique
- nikto : scanner de vulnérabilité web
- ...

Mise en place progressive d'un service

- 1 mise à disposition
- 2 intégration
- 3 industrialisation

De l'outil au service

Outils disponibles

- nmap : scanner de port
- openvas : scanner de vulnérabilité générique
- nessus : scanner de vulnérabilité générique
- nikto : scanner de vulnérabilité web
- ...

Mise en place progressive d'un service

- 1 mise à disposition
- 2 intégration
- 3 industrialisation

Mise à disposition

Principe

Simple déploiement centralisé d'un ou plusieurs outils

Limites

- classification des risques établie par l'outil
- sélection des priorités faite par l'utilisateur

Conséquences

- processus faiblement maîtrisé
- peu de lien avec la PSSI

Mise à disposition

Principe

Simple déploiement centralisé d'un ou plusieurs outils

Limites

- classification des risques établie par l'outil
- sélection des priorités faite par l'utilisateur

Conséquences

- processus faiblement maîtrisé
- peu de lien avec la PSSI

Mise à disposition

Principe

Simple déploiement centralisé d'un ou plusieurs outils

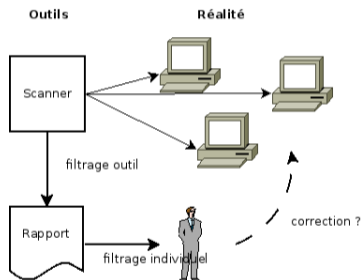
Limites

- classification des risques établie par l'outil
- sélection des priorités faite par l'utilisateur

Conséquences

- processus faiblement maîtrisé
- peu de lien avec la PSSI

Mise à disposition : schéma



Intégration

Principe

Piloter les outils à partir des spécifications

Exemples

- référentiel des ressources :
 - liste de réseaux : ce qu'il faut tester
- PSSI :
 - politique de test : comment tester
 - politique de conformité : ce qu'il faut trouver

Conséquences

- processus fortement maîtrisé

Intégration

Principe

Piloter les outils à partir des spécifications

Exemples

- référentiel des ressources :
 - liste de réseaux : ce qu'il faut tester
- PSSI :
 - politique de test : comment tester
 - politique de conformité : ce qu'il faut trouver

Conséquences

- processus fortement maîtrisé

Intégration

Principe

Piloter les outils à partir des spécifications

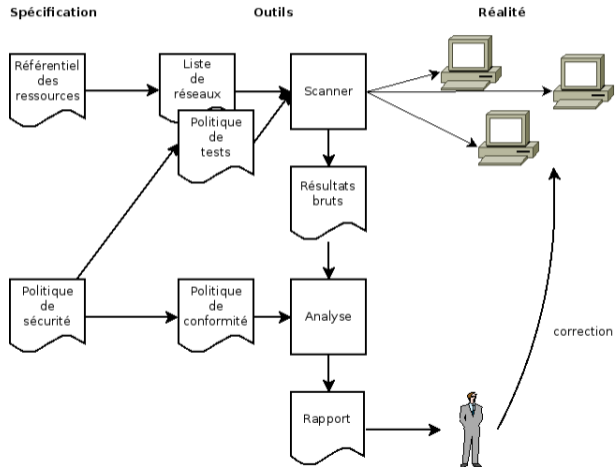
Exemples

- référentiel des ressources :
 - liste de réseaux : ce qu'il faut tester
- PSSI :
 - politique de test : comment tester
 - politique de conformité : ce qu'il faut trouver

Conséquences

- processus fortement maîtrisé

Intégration : schéma



Industrialisation

Principes

- automatisation
- historisation des résultats

Conséquences

- suivi des évolutions dans le temps
- pilotage du changement

Industrialisation

Principes

- automatisation
- historisation des résultats

Conséquences

- suivi des évolutions dans le temps
- pilotage du changement

Plan

- 1 Problème
- 2 Réponse
 - Démarche
 - **Aspects techniques**
 - Aspects humains
- 3 Conclusions

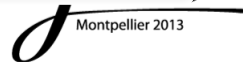
Outils

Sources de données

- Nessus
- Nmap

Assemblage

- Perl
- XML-RPC
- YAML



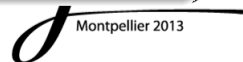
Outils

Sources de données

- Nessus
- Nmap

Assemblage

- Perl
- XML-RPC
- YAML



Liste de réseaux

Exemple

```
128.93.128.0/24:  
  description: production  
  class: fermé  
  subclass: services internes  
128.93.162.0/23:  
  description: dmz  
  class: ouvert  
  subclass: services externes
```

Politique de conformité

Pas de service accessible depuis l'extérieur sur les réseaux de postes de travail

```
accessibility:  
  indicators:  
    open_hosts:  
      name: machines accessibles  
      description: nombre de machines avec au moins un port accessible
```

Pas d'authentification HTTP sur une connexion non sécurisée

```
conformity:  
  indicators:  
    http_conf_auth_http:  
      name: authentifications HTTP en clair  
      description: nombre de serveurs web autorisant des authentifications  
                  en clair  
      nessus_id: 34850
```

Politique de conformité

Pas de service accessible depuis l'extérieur sur les réseaux de postes de travail

```
accessibility:  
  indicators:  
    open_hosts:  
      name: machines accessibles  
      description: nombre de machines avec au moins un port accessible
```

Pas d'authentification HTTP sur une connexion non sécurisée

```
conformity:  
  indicators:  
    http_conf_auth_http:  
      name: authentifications HTTP en clair  
      description: nombre de serveurs web autorisant des authentifications  
                   en clair  
      nessus_id: 34850
```

Réglages

Objectifs

- minimiser la durée
- minimiser l'impact
- maximaliser les résultats produits

Leviers

- réduire la plage des ports et les catégories de test
- limiter la bande passante utilisée
- afficher les horaires de test



Réglages

Objectifs

- minimiser la durée
- minimiser l'impact
- maximaliser les résultats produits

Leviers

- réduire la plage des ports et les catégories de test
- limiter la bande passante utilisée
- afficher les horaires de test

Rapport synthétique : vue d'ensemble

Scan de réseaux pour sesi - Mozilla Firefox

file:///home/guillaume/Téléchargements/index.html

Scan de réseaux pour sesi

plage	nom	classe	sous-classe	accessibilité	vulnérabilité	conformité
129.94.129.0/24	production	fermé	services internes	OK	OK	OK
129.94.131.0/24	administration	fermé	administration	OK	OK	OK
129.94.143.0/24	numérique	fermé		OK	OK	OK
129.94.145.0/24	tma	fermé		OK	OK	OK
129.94.163.0/23	dmz	ouvert	services externes	OK	OK	KO
129.94.185.0/24	vpn-ng roc	fermé		OK	OK	OK
193.94.123.64/27	bbnat2	fermé	interco	OK	OK	OK
193.94.123.66/27	bbnat1	fermé	interco	OK	OK	OK
194.52.194.0/25	qualification	fermé		OK	OK	OK
194.52.194.128/25	dmz	ouvert	services externes	OK	OK	KO
194.52.197.0/25	ressources	fermé		OK	OK	OK

Page générée le 12/11/2013 à 11:14:44

Rapport synthétique : vue d'un réseau

Scan pour le réseaux 129.94.163.0/23 - Mozilla Firefox

file:///home/guillaume/Téléchargements/128.93.162.0_23.html

129.94.163.0/23

Information

description: dmz
classe: ouvert
sous-classe: services externes

Résultats synthétiques

- ▶ Horaires
- ▶ Accessibilité OK
- ▶ Vulnérabilité OK
- ▼ Conformité **KO: 13 erreur(s)**

indicateur	valeur	résultat actuel détails	historique		
			03/11	27/10	20/10
certificats SSL émanant d'une autorité inconnue	0		0	0	0
certificats SSL auto-signés	0		0	0	0
certificats SSL expirés	0		0	0	0
utilisations du protocole SSLv2	0		0	0	0
utilisations de suites cryptographiques anonymes	3	▶ • 129.94.163.28:443	3	3	3
utilisations de suites cryptographiques faibles	2	▶ • 129.94.163.28:443	2	2	2
utilisations de suites cryptographiques moyennes	3	▶ • 129.94.163.4:443	3	3	3
disponibilité des méthodes TRACE/TRACK	2	▶ • 129.94.163.62:80	2	2	4
vulnérabilités RANGE	0		0	0	0
authentifications HTTP en clair	1	▶ • 129.94.163.62:80	1	1	2
authentifications par formulaire en clair	2	▶ • 129.94.163.25:80	3	3	3
bannière trop détaillées	0		0	0	0
authentification par mot de passe	0		0	0	0
utilisation du protocole SSHv1.0	0		0	0	0

res

Montpellier 2013

Plan

- 1 Problème
- 2 Réponse
 - Démarche
 - Aspects techniques
 - Aspects humains
- 3 Conclusions

De la détection à la correction

Principe

Détecter, c'est bien, faire corriger, c'est mieux

Stratégies utilisées

- présenter la démarche
- chercher l'adhésion
- faciliter la correction

De la détection à la correction

Principe

Détecter, c'est bien, faire corriger, c'est mieux

Stratégies utilisées

- présenter la démarche
- chercher l'adhésion
- faciliter la correction

Présenter la démarche

Expliquer

- différence entre conformité et vulnérabilité

Justifier

- la PSSI constitue la règle
- l'outil ne fait que vérifier son application

Présenter la démarche

Expliquer

- différence entre conformité et vulnérabilité

Justifier

- la PSSI constitue la règle
- l'outil ne fait que vérifier son application

Chercher l'adhésion

Objectif

Passer d'une contrainte imposée à un service apprécié

Faire évoluer l'outil

- adapter aux besoins supplémentaires
- déléguer la gestion et le suivi

Chercher l'adhésion

Objectif

Passer d'une contrainte imposée à un service apprécié

Faire évoluer l'outil

- adapter aux besoins supplémentaires
- déléguer la gestion et le suivi

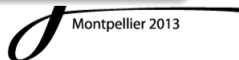
Faciliter la correction

Améliorer la forme des rapports

- cibler sur un interlocuteur
- adapter au niveau technique de l'interlocuteur
- focaliser sur l'essentiel

Simplifier l'aspect technique

- commencer par les problèmes simples
- fournir des solutions techniques possibles



Plan

- 1 Problème
- 2 Réponse
 - Démarche
 - Aspects techniques
 - Aspects humains
- 3 Conclusions

Limites techniques actuelles

Constat

- les applications web constituent la vulnérabilité majeure
- elles n'apparaissent pas dans nos résultats actuels

Améliorations possibles

- compléter les données sources : recenser les noms, en plus des adresses
- compléter les outils utilisés : ajouter un scanner web, en plus de nessus

Limites techniques actuelles

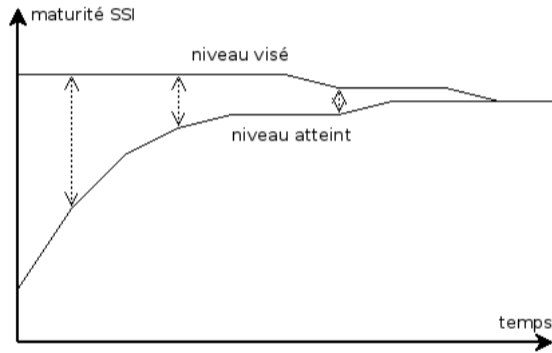
Constat

- les applications web constituent la vulnérabilité majeure
- elles n'apparaissent pas dans nos résultats actuels

Améliorations possibles

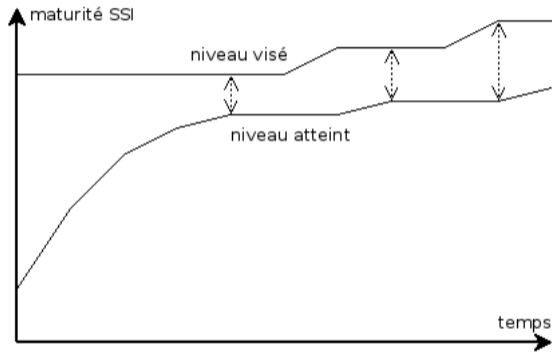
- compléter les données sources : recenser les noms, en plus des adresses
- compléter les outils utilisés : ajouter un scanner web, en plus de nessus

Stratégie pragmatique



Objectif : réduire l'écart entre l'objectif et la réalité

Stratégie cynique



Objectif : atteindre l'objectif initial