

# Introduction à l'audit sécurité & pentest

Ludovic

Eschard



# Qui suis-je ?

Ludovic Eschard

Manager Audit Sécurité chez **Orange France**



# I. Introduction à l'audit



# Objectifs de l'audit

- Appréhender les risques sécuritaires de l'entreprise
- Évaluer la conformité de l'existant par rapport à un référentiel (norme)
- Connaître son environnement et les points critiques
- Estimer la valeur des risques
- Dans tous les cas, **identifier les vulnérabilités avant que d'autres ne le fassent**





# I.1 Quelques concepts

## Audit

Processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits. Pour les besoins du référentiel, un audit est constitué d'un sous-ensemble des activités d'audit de la sécurité d'un système d'information décrites au chapitre II et des recommandations assorties.

## Auditeur

Personne réalisant un audit.

## Audité

Organisme(s) responsable(s) de tout ou partie du système d'information audité. Le commanditaire peut être l'audité.

# Commanditaire

Entité faisant appel au service d'audit de la sécurité des systèmes d'information.

# Constats d'Audit

Résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

# Critère

Ensemble des référentiels, guides, procédures ou exigences applicables à la sécurité du système d'information audité.



# Périmètre

Environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel l'audit est effectué.

# Preuves d'audit

Enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et sont vérifiables.

# Rapport d'audit

Document de synthèse élaboré par l'équipe d'audit et remis au commanditaire à l'issue de l'audit. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

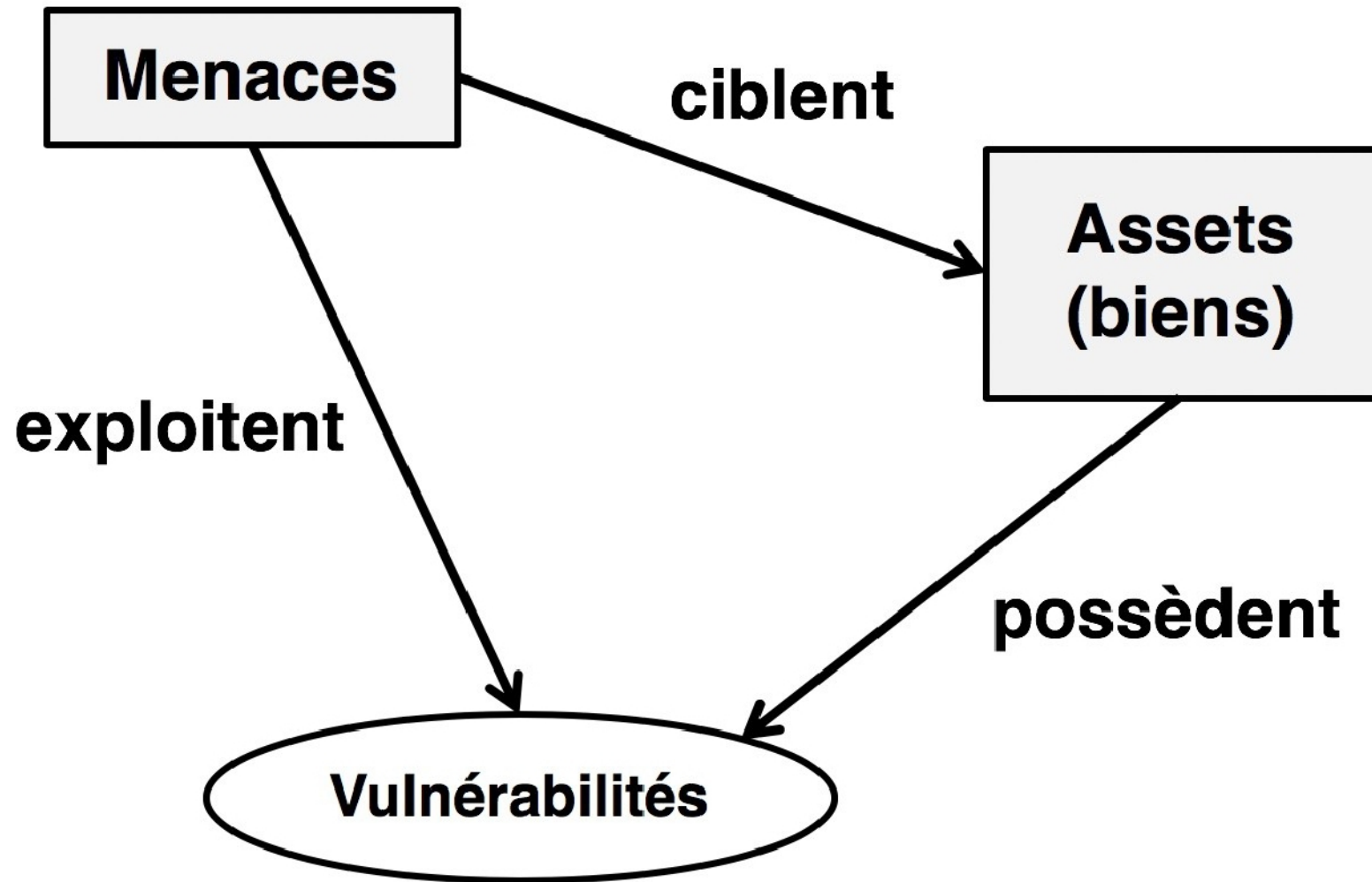
# Vulnérabilité

Faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces. **La vulnérabilité est propre à un bien.**

# Menace

Un danger potentiel pour le système. Un agent de menace est un élément pouvant décider de lancer une attaque. **La menace est un facteur externe et indépendante du bien**





# Estimation du risque

**Risque = Probabilité x Impact**

ou bien, avec le bon terme : **Risque = Vraisemblance x Impact**

Impact	1	2	3	4
Probabilité				
1	Faible	Faible	Moyen	Elevé
2	Faible	Moyen	Elevé	Elevé
3	Faible	Moyen	Elevé	Très Elevé
4	Moyen	Moyen	Très Elevé	Très Elevé





# Rémédiation

Recommandation formulée pour réduire le risque. La recommandation n'est pas toujours applicable directement car la réduction du risque nécessite une solution discutée avec les concepteurs.

# Classification selon le niveau de connaissances

- - Black box -> (presque) aucune information

White box -> Toute information (interne) disponible

Grey box -> Un entre deux pertinent pour gagner du temps et limiter les risque de loupé



# Déroulement de l'audit

1. Définition de la demande d'audit
2. Préparation de l'audit
  - Planification
  - Récupération des éléments logistiques (accès, comptes, ...)
  - Récupération de la documentation
3. Réunion de pré-lancement / kickoff
4. **Période de test**
5. Rédaction du rapport d'audit
6. Restitution d'audit
7. (option) suivi des recommandations

Normalisé dans **ISO 19011**, qui est prise en compte pour la certification PASSI\* de l'ANSSI.

[\*]: Prestataires d'audit de la sécurité des systèmes d'information



# Types d'audit

- Audit "papier" / d'architecture
- Audit de conformité
- Audit de code
- Audit de configuration
- Test d'intrusion / pentest
- Red Team





# Red team / Blue team

## Red team

**Auditeurs** red team ayant pour mission de tester la sécurité d'un périmètre.

## Blue team

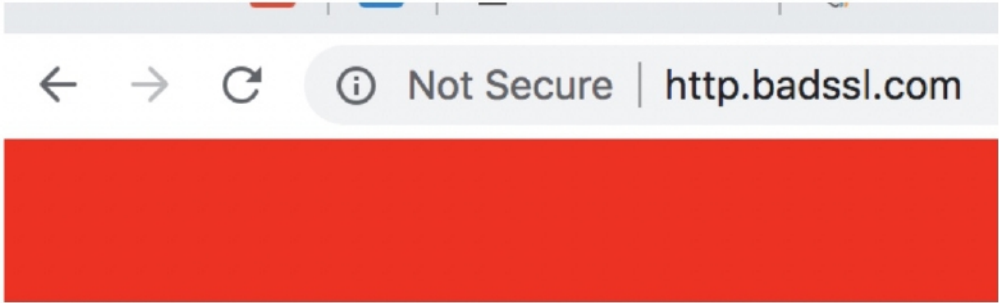
**Équipes de défense** : analystes SOC, exploitant sécurité, architectes sécurité.

=> **Objectif** : Le but est que le résultat de chaque audit améliore la défense : blue team



# Constat d'audit

## Constat C-01

Titre	Absence de HTTPS pour la connexion vers le site
Description	Les informations transmises entre le navigateur des visiteurs et le site web ne sont pas chiffrées. Une interception de celles-ci sont possible notamment en Wi-Fi mode open (hotspot).
Preuve	 A screenshot of a web browser's address bar. It shows navigation icons (back, forward, refresh) on the left. In the center, there is an information icon (i) followed by the text 'Not Secure   http.badssl.com'. Below the address bar, a large red rectangular area is visible, likely representing a security warning or error message from the browser.
Estimation du risque	Impact : 3/4 Vraisemblance : 2/4 Sévérité : Haute
Recommandation	Mettre en place HTTPS en obtenant un certificat auprès d'un autorité de certification (Letsencrypt est gratuit pour cet usage)



## II. Reconnaissance

Après la phase de préparation souvent non-technique (planification, obtention de documentation, obtention d'accès), la phase de reconnaissance est la **première phase technique d'un audit**.

- Permet de mieux connaître le périmètre
- Permet de déterminer les tests et cheminement de l'audit
- Donne parfois immédiatement les premiers constats d'audit

# II.1 Recherche en sources ouvertes (OSINT)

- OSINT : Open Source Intelligence

=> Obtenir des renseignements sur le périmètre à partir d'informations librement accessible.

◦  
**Librement** signifie :

- Exposé sur Internet
- Publié dans les médias
- Présent dans les annuaires
- Indexé dans les moteurs de recherche
- Accessible sur les serveurs DNS





Première et plus grande source d'OSINT !

- Permet (souvent) de trouver :
  - Qui est le fournisseur de la solution ? Dans quel pays se situe l'entreprise ?

=> Avez-vous déjà tapé votre nom "Prénom Nom" dans Google et consulté la 2ème page ?





# Google Dorks / Google Hacking

•  
•  
Utilisation des mots clés :

- `inurl:` - filtre un mot clé dans l'URL
- `intitle:` - filtre un mot clé dans le champ titre de la page HTML
- `site:` - filtre selon l'URL
- `filetype:` - filtre selon l'extension de fichier

**Tous ces filtres peuvent être inversés avec le caractère "-"**

## Exemple de Google dorks

```
dump filetype:sql -site:github.com
```

```
"-----BEGIN PRIVATE KEY-----" filetype:pem`
```

```
intitle:"index of" database`
```

# Shodan.io / Censys.io

- Moteur de recherche indexant ports ouverts, bannières de services, certificats HTTPS,
- Permet d'identifier des interfaces web d'administration, webcam, FTP,

## Exemples

- mots clés : webcam, axis, netgear  
protocols: "3306/mysql"



# DNS

- Le protocole DNS permet de faire la résolution *Nom de domaine* -> *Adresse IP*, mais pas que.
- Il définit / indexe également :
  - 
  - les serveurs de mail
  - les sous-domaines (dont éventuellement certains non-destinés au public)  
quels sont les serveurs DNS secondaire (gérés par l'organisation cible)

## Outils utilisés

- host, dig, nslookup, whois

(déjà présents, ou installable rapidement sous Linux)



# Exemple de reconnaissance DNS : Outil

host

```
host -t ANY esigelec.fr
esigelec.fr mail is handled by 80 mail.esigelec.fr.
esigelec.fr mail is handled by 5 b-mx1.relay.syrhano.net. mail
esigelec.fr is handled by 5 a-mx1.relay.syrhano.net.
esigelec.fr descriptive text "v=spf1 mx a ptr a:spf.protection.outlook.com -all"
esigelec.fr descriptive text "MS=ms67762688"
esigelec.fr descriptive text "2G18uOfJqV5H+DS4y/cmVyHRKk3CsG74H6AJVnCmXegFTYMUQMicfQrg+yLAyn9oMnKucAx8O
esigelec.fr has address 193.52.189.36
esigelec.fr has SOA record esigelec.esigelec.fr. postmaster.esigelec.esigelec.fr. 2018092514 21600 3600
esigelec.fr name server esigelec.esigelec.fr. name server ns.crihan.fr.
esigelec.fr
```





# Exemple de reconnaissance DNS : Outil

## whois

**whois esigelec.fr**

[...]

**nserver:** esigelec.esigelec.fr [193.52.189.2]

**nserver:** ns.crihan.fr

[...]

**contact:** Ecole Superieure d'Ingenieur en Genie Electrique

**address:** avenue Galilee

**address:** 76800 Saint Etienne du Rouvray

**country:** FR

**phone:** +33 2 32 91 58 58

**e-mail:** tech@esigelec.fr

**registrar:** GIP RENATER

:

[...]

**contact:** Christophe Berquez

**address:** ESIGELEC

**address:** avenue Galilee

**address:** 76800 Saint Etienne du Rouvray

**address:** FR

**country:** +33 2 32 91 59 53

**phone:** christophe.berquez@esigelec.fr

**e-mail:**

[...]



# Exemple de reconnaissance DNS : Outil whois

whois est aussi utilisable pour savoir à quel hébergeur ou opérateur appartient une adresse IP.

Par exemple :

```
whois 198.27.92.1

NetRange:      198.27.64.0 - 198.27.127.255
CIDR:          198.27.64.0/18
NetName:       OVH-ARIN-4
NetHandle:     NET-198-27-64-0-1
Parent:        NET198 (NET-198-0-0-0-0)
NetType:       Direct Allocation
:              AS16276
OriginAS:      OVH Hosting, Inc. (HO-2)
Organization:  2012-08-28 2013-
RegDate:       10-21
Updated:       https://rdap.arin.net/registry/ip/198.27.64.0
Ref:
```

198.27.92.1 est une IP gérée par l'hébergeur OVH.



## 2.2 Scan réseau

### Scan Nmap

- Outil de scan réseau de référence. Installable facilement sous Linux.

### Avantages

- Multi-protocoles (TCP, UDP, SCTP)  
Nombreux scripts ajoutés (par ex: listing des mécanismes crypto proposés par HTTPS)

### Inconvénients

- Par défaut, "bruyant" et facilement détectable. (des options existent pour le rendre plus furtif)



# nmap, utilisation

- Par défaut nmap réalise un **SYN scan**. C'est à dire, qu'il envoie des messages TCP **SYN** et se base sur l'éventuelle réponse **SYN ACK** de la cible pour déterminer si les ports sont ouverts. Dans tous les cas, nmap ne termine pas les connexions : il n'envoie pas de **ACK** final.

Scan simple :

```
nmap localhost
```

Scan seulement de ports TCP 80, 443 et 22 :

```
nmap google.com -p 80,443,22
```

Scan des ports UDP (par défaut seul TCP est scanné) :

```
nmap localhost -sU
```





# III Audit de configuration



# TP audit de configuration

- Quelle est la version du noyau Linux ?

```
uname -a
```

- Quels sont les services en écoute ?

```
netstat -ltnp
```

- Quels sont les packages installés ?

```
dpkg -l | less
```

- Quelle est la configuration du firewall iptables ?

```
iptables-save  
iptables -L
```



# TP audit de configuration (suite)

- Quelle est la configuration `sudoers` ?

```
cat /etc/sudoers
```

- Quels processus sont exécutés ?

```
ps -edf ps faux
```

# Cassage de mot de passe avec l'outil

john

```
cd /tmp  
cp /etc/shadow /tmp/shadow
```

```
john /tmp/shadow
```

Quel *hash* venez-vous de "casser" ?





# I.V Tests d'intrusion

## Objectifs

- **Se positioner et agir (presque) comme un attaquant afin d'identifier des vulnérabilités**
- Avoir une approche "offensive" (tout en restant bienveillant) pour venir en complément d'un audit de configuration
- **Partir d'un point d'entrée** (URL, prise réseau, Wi-Fi, application mobile) et tenter de compromettre le périmètre jusqu'aux ressources sensibles (données utilisateurs, mots de passes, etc.).

# TP Tests d'intrusion

## DVWA

Apprendre à exploiter les vulnérabilités du **Top 10 de l'OWASP**

## CTF7

Cas (presque) réel.



**Merci !**

