

Sécurité des Systèmes d'Information

Audit et test d'intrusion

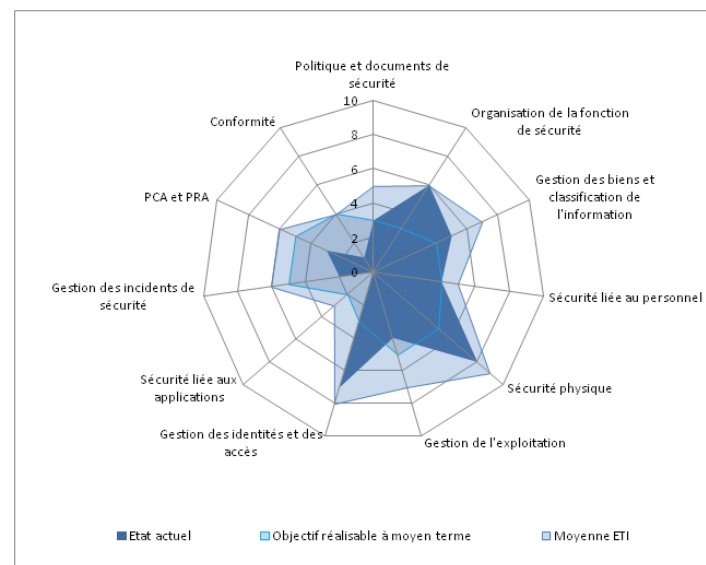
Sommaire

- Définition et exemples
- Types d'audit de sécurité
- Test d'intrusion
- Phases du test d'intrusion
- Organisation d'audit



Audit de sécurité

- ▶ Vue à un instant t de tout ou partie du SI
- ▶ Permet de comparer l'état du SI à un référentiel
- ▶ Moyen d'éprouver et de s'assurer du niveau de sécurité de son système d'information
- ▶ Met en évidence les forces mais surtout les faiblesses et vulnérabilités du système d'information
- ▶ Ses conclusions permettent d'identifier des axes d'amélioration et de contribuer à l'élévation de son niveau de sécurité



Audit

► Le référentiel est généralement constitué de :

- La **politique** de sécurité du système d'information (PSSI)
- La **base documentaire** du SI
- Les **réglementations** propre à l'entreprise
- Les **documents de référence** dans le domaine de la sécurité informatique (OWASP, CIS, guides de hardening, etc)



Politique, organisation, gouvernance

Organisation de la sécurité des systèmes d'information

Objectif 1 : organisation de la SSI. Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

Organisation SSI

ORG-SSI : organisation SSI. Une organisation dédiée à la SSI est déployée à tous les niveaux de l'État, au sein de chaque ministère et au sein de chaque entité suivant les principes de l'IGI 1300. Cette organisation, établie selon les directives du haut fonctionnaire de défense et de sécurité (HFDS), définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

Acteurs SSI

ORG-ACT-SSI : identification des acteurs SSI. L'organisation SSI de l'État s'appuie sur des acteurs SSI clairement identifiés, à tous les niveaux d'organisation de l'État. Les acteurs responsables en matière de SSI pour la protection du secret de la défense désignés dans l'IGI 1300, et les agents chargés de les assister dans cette mission, sont responsables de la mise en application générale de la politique SSI de l'État. Ils sont référencés dans un annuaire interministériel. Cette chaîne fonctionnelle s'appuie, pour chaque ministère, sur le HFDS, assisté par un fonctionnaire de sécurité des systèmes d'information (FSSI).

Responsabilités internes

ORG-RSSI : désignation du responsable SSI. Chaque autorité qualifiée en sécurité des systèmes d'information (AQSSI) s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargé(s) de l'assister dans le pilotage et la gestion de la SSI. Des « correspondants locaux SSI » peuvent être désignés, le cas échéant, afin de constituer un relais du RSSI. Le RSSI d'une entité fait valider les mesures d'application de la PSSI par l'autorité qualifiée et veille à leur application. Des dénominations alternatives des fonctions citées ci-dessus peuvent être utilisées si nécessaire.

ORG-RESP : formalisation des responsabilités. Une note d'organisation fixe la répartition au sein de chaque entité et au niveau local des responsabilités et rôles en matière de SSI. Cette note sera, le plus souvent, proposée par le RSSI et validée par l'autorité qualifiée.

Source : [PSSIE](#)

ISO 19011

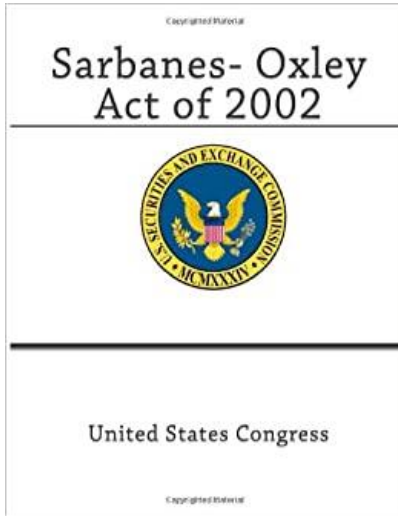
- L'ISO 19011:2011 fournit des lignes directrices sur l'audit de systèmes de management



- Cette norme présente :

- Les principes de management d'un audit
- Les compétences attendues d'un auditeur et d'un responsable d'audit
- Les différentes étapes à mener au cours d'un audit
 - ✓ Déclenchement de l'audit (objectifs, critères, constitution de l'équipe)
 - ✓ Revue documentaire
 - ✓ Audit sur site (plan et constats d'audit, conduite de réunions)
 - ✓ Préparation du rapport d'audit (contenu du rapport et diffusion)
 - ✓ Clôture de l'audit (conservation ou destruction des documents)
 - ✓ Suivi d'audit

Exemple d'audit : l'audit SOX



► La loi Sarbanes-Oxley (SOX) de 2002 établit des normes strictes pour toutes les entreprises cotées aux États-Unis

- Suite aux scandales financiers d'Enron, WorldCom et Tyco, entre autres
- Protéger les actionnaires et le grand public contre les erreurs comptables et les pratiques frauduleuses
- Améliorer l'exactitude des informations financières fournies par les entreprises

► Contrôles de communication de l'information pour garantir une communication financière exacte

- Analyse des objets de l'AD (utilisateur, groupe, ordinateur, OU, GPO)
- Création/modification d'utilisateur et de groupe
- Rapports sur la connexion et les actions par un utilisateur
- Création/modification/suppression de fichier ou d'autorisation sur les fichiers de données financières

Exemple d'audit : l'audit PCI-DSS

- ▶ **La réglementation PCI-DSS s'applique à toute entité qui stocke, traite et/ou transmet les données de carte de paiement**
 - Couvre les aspects techniques et opérationnels des systèmes qui gèrent ces données
 - Spécifie 6 objectifs de contrôle (sécurisation réseau, protection des données du titulaire, gestion des vulnérabilités, contrôle d'accès, surveillance des accès, sensibilisation des utilisateurs à la PSSI)

- ▶ **Type de contrôles réalisés sur les systèmes :**



- Accès à distance (activité de connexion RDP, d'authentification RADIUS)
- Traçabilité des actions administrateurs (modifications de stratégies du domaine, modifications des droits sur les fichiers, etc.)
- Accès aux données (audit des connexion/déconnexion réussies/échouées)

Activités d'audit

► Dans le domaine de la sécurité des systèmes d'information, différentes activités d'audit peuvent être effectuées :

- Audit d'architecture
- Audit de configuration
- Audit de code source
- Audit organisationnel
- Test d'intrusion



Audit d'architecture

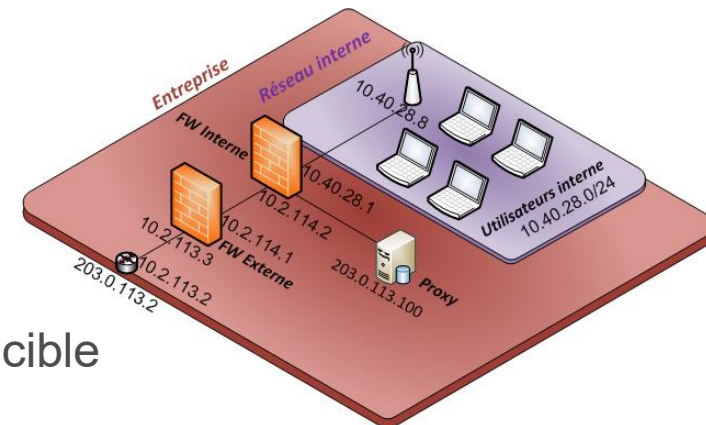
- Vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des matériel et logiciels

- Evaluation des aspects tels que :
 - ✓ la pertinence des choix technologiques
 - ✓ l'organisation des flux de données
 - ✓ le dimensionnement et la robustesse



- L'audit d'architecture peut se baser sur les documents suivants

- Schémas d'architectures de niveau 2 et 3 du modèle OSI
- Matrices de flux
- Documents d'architecture technique liés à la cible



Audit d'architecture

- ▶ **L'auditeur énumère les points positifs et axes d'améliorations**

- ▶ **Il peut détailler des propositions techniques :**
 - Schéma d'architecture
 - Diagramme fonctionnels ou de flux
 - Cartographie
 - Spécifications
 - Cahier des charges

- ▶ **Résultats classiques :**
 - Conseils sur la segmentation
 - Evaluation de propositions techniques

Audit de configuration

- ▶ **Vérification de la conformité des éléments d'une infrastructure par rapport aux référentiels internes et par rapport à l'état de l'art en matière de sécurité (normes, guides de configuration, etc...)**
 - Ces infrastructures peuvent être :
 - ✓ des équipements réseau,
 - ✓ des systèmes d'exploitation (serveur ou poste de travail),
 - ✓ des applications
 - ✓ des produits de sécurité

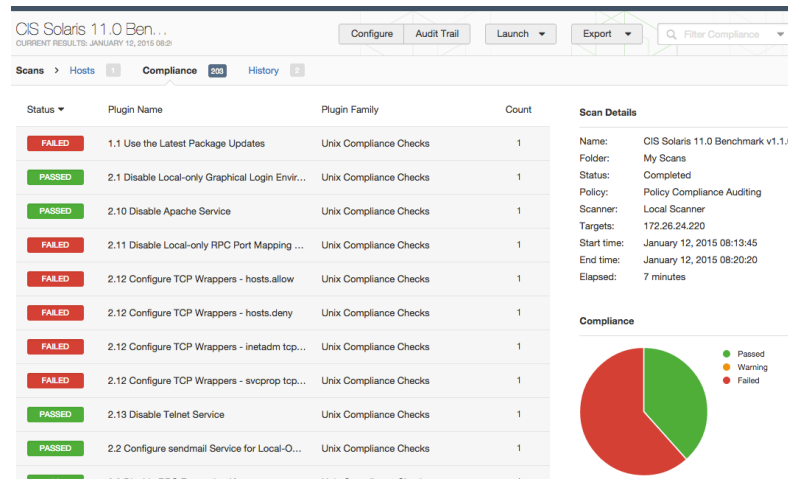
- ▶ **L'audit de configuration, contrairement aux tests d'intrusion, est non invasif**
 - Ne nécessite l'installation d'aucun logiciel sur les systèmes à auditer et peut donc être parfaitement mené sur des **systèmes en production**, sans risque de perte de données ou de service

Audit de configuration

► Les éléments de configuration peuvent être récupérés:

- Automatisement / à l'aide d'outils pour les composants courants (Windows, Linux, Apache, etc.)
- Manuellement sous la forme de fichiers de configuration ou de captures d'écran

► Du fait des accès privilégiés nécessaires pour la récupération des éléments, celle-ci est généralement effectuée par l'audité ou du moins sous son contrôle



Audit de configuration

► Les recommandations portent sur :

- Les mécanismes d'authentification (robustesse des dispositifs...)
- Les mécanismes cryptographiques utilisés
- Les règles de filtrage réseau (entrée, sortie, routage, NAT...)
- Les bonnes pratiques en matière de segmentation (VLAN...)
- Les bonnes pratiques de durcissement des systèmes d'exploitation, des configurations des serveurs applicatifs et des services d'infrastructure

```
# Relations d'ordre utilisées :  
# - ECDHE > DHE > chiffrement RSA ;  
# - GCM > CBC ;  
# - AES256 > AES128 > CAMELLIA256 > CAMELLIA128 ;  
# - SHA384 > SHA256 ;  
# - ECDSA > RSA.  
#  
# Avec le support actuel et futur prévu, en branche 1.0.2:  
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:  
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-  
AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-  
AES128-SHA256:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:  
ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:DHE-RSA-AES256  
-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128  
-SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:  
CAMELLIA128-SHA256
```

Source : [Guide TLS](#)

Audit de code source

► Consiste en l'analyse :

- de tout ou partie **du code source**
- des conditions de compilation d'une application

► Objectif :

- **Découvrir des vulnérabilités**, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité

► Le code est audité sous deux aspects :

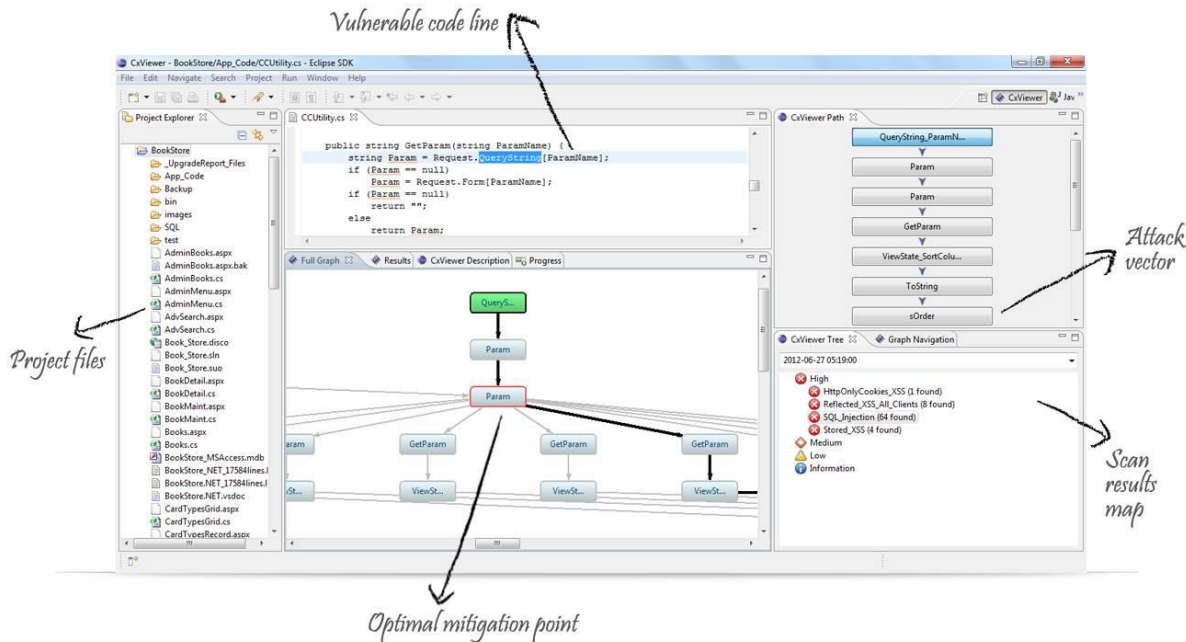
- L'aspect technique : validation du respect des **bonnes pratiques de développement** associées à la production de code et spécifiques aux langages employés
- L'aspect fonctionnel : il s'agit de valider la **bonne implémentation des fonctionnalités** et le respect des bonnes pratiques associées, indépendantes des langages employés

Audit de code source

- L'audit de code source permet de détecter un grand nombre de vulnérabilités à la source, et est plus complet qu'un test d'intrusion (applicatif)

- Outils automatisés: Checkmarx, SonarQube

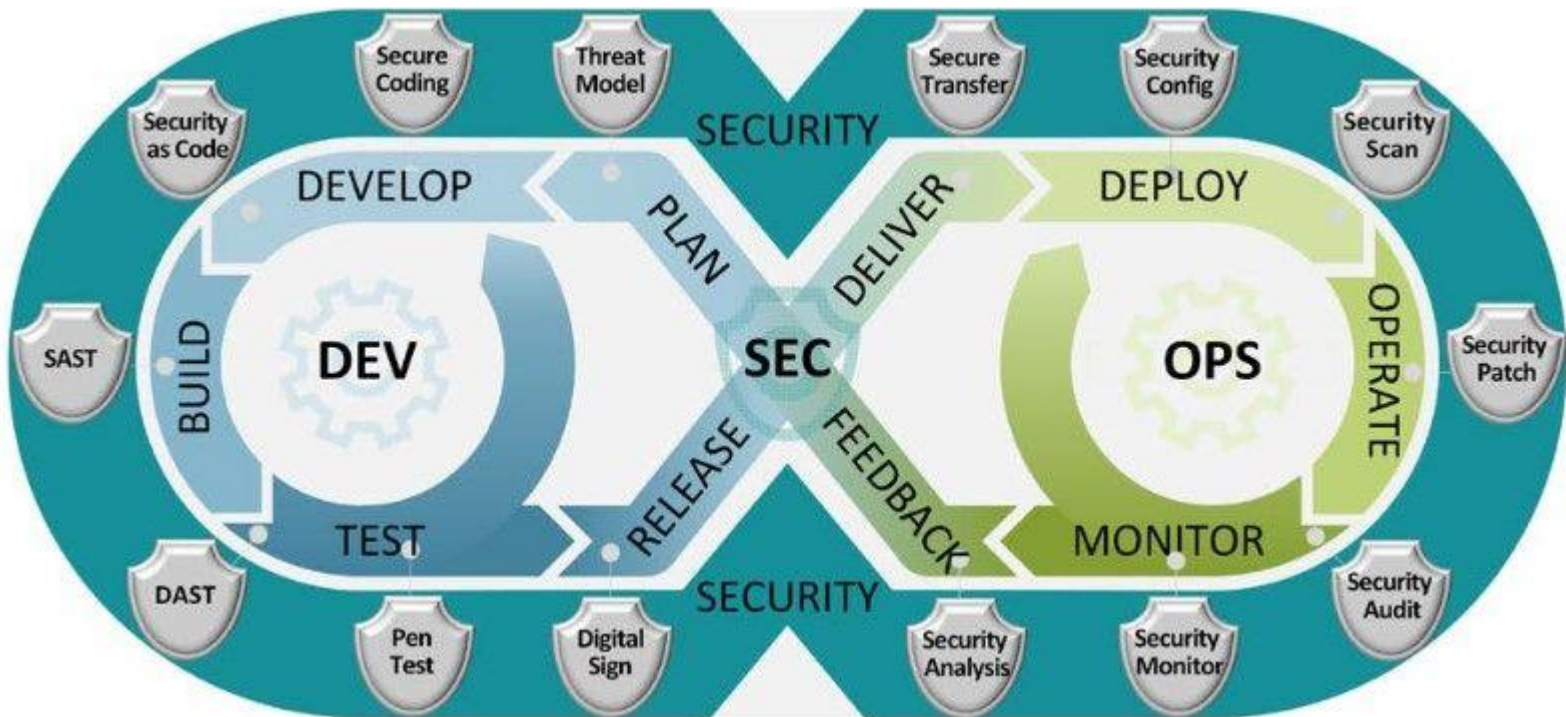
- Nécessite malgré tout un traitement des résultats car présence de faux positifs et liste des vulnérabilités potentielles peu présentable



DevSecOps

► Intégration de la sécurité au cycle de vie complet des applications

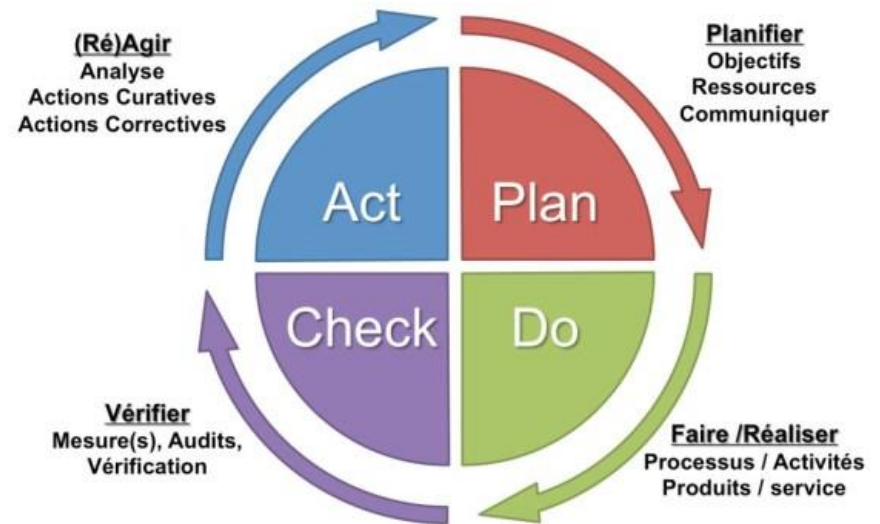
- Intégration de la sécurité dans les cycles de développement rapides et fréquents



Source : https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583

Audit organisationnel

- L'audit de l'organisation de la sécurité vise à s'assurer que les politiques et procédures de sécurité définies par l'audité pour assurer le maintien en conditions opérationnelles et de sécurité :
 - Sont **conformes** au besoin de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur (ISO 27K, etc.)
 - **Complètent** correctement les **mesures techniques** mises en place
 - Sont efficacement mises en pratique



Roue de Deming

Compétences

► Compétences organisationnelles nécessaires pour la réalisation d'audit :

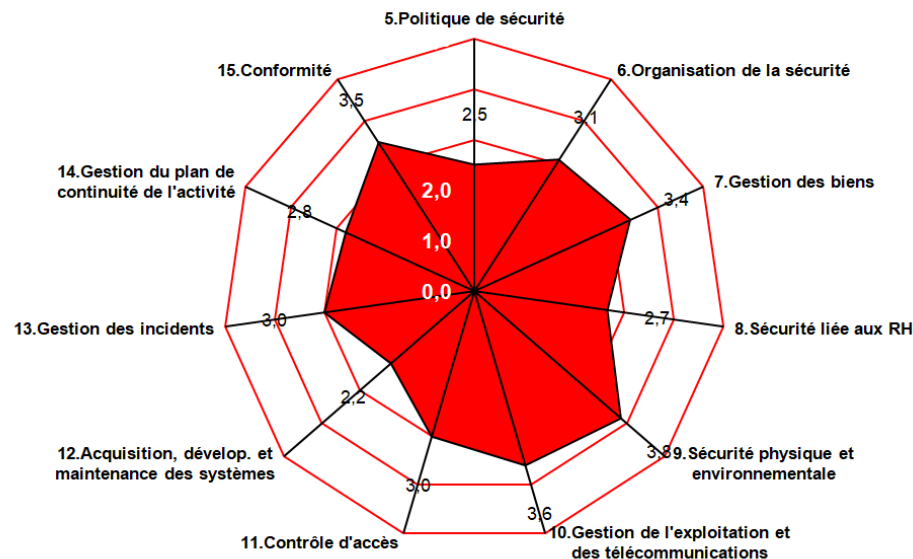
- Maîtrise du cadre normatif :
 - ✓ Les normes ISO 27001, ISO 27002, ISO 22301, etc.
 - ✓ Les textes réglementaires relatifs à la SSI (RGS, LPM, etc.)
- Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
 - ✓ Analyse des risques
 - ✓ Politique de sécurité des SI
 - ✓ Gestion de l'exploitation et de l'administration du SI
 - ✓ Contrôle d'accès logique au SI
 - ✓ Développement et maintenance des applications
 - ✓ Gestion des incidents
 - ✓ Gestion du plan de continuité de l'activité
 - ✓ Sécurité physique



Audit organisationnel

Exemples

- Vérification de l'existence d'une politique de sécurité approuvée par la direction (contrôle 5.1.1 de l'ISO 27002)
- Vérification du réexamen de la politique de façon régulière (contrôle 5.1.2 de l'ISO 27002)
- Vérifier que tous les biens sont clairement identifiés et présents dans un inventaire (contrôle 7.1.1 de l'ISO 27002)
- ...



Test d'intrusion

► Principe :

- Découvrir des **vulnérabilités** sur le système d'information audité
- Vérifier leur **exploitabilité et leur impact**, dans les **conditions réelles** d'une attaque sur le système d'information
- **Sensibiliser** le management, le personnel IT et les utilisateurs



► Les vulnérabilités testées peuvent également avoir été identifiées au cours d'autres activités d'audit

► Peut être réalisée soit :

- Depuis l'**extérieur** du système d'information audité (notamment depuis Internet ou le réseau interconnecté d'un tiers)
- Depuis l'**intérieur**

Test d'intrusion

► Un test d'intrusion seul n'a pas vocation à être exhaustif

- Activité qui doit être effectuée en complément d'autres activités d'audit afin d'en améliorer l'efficacité ou de **démontrer la faisabilité** de l'exploitation des failles et vulnérabilités découvertes à des fins de sensibilisation

► Les scanners de vulnérabilité automatisés (Qualys, Nessus, OpenVAS, Nikto, etc.), ne représentent pas à eux seuls une activité de test d'intrusion



Test d'intrusion

► Types de tests d'intrusion :

- Black Box (boîte noire) : l'auditeur ne dispose **d'aucune information** à part le nom de la cible. Seules les adresses IP et les URL associées à la cible auditée sont généralement fournies
- Grey Box (boîte grise) : l'auditeur dispose des connaissances d'un **utilisateur standard** du système d'information et un compte sur le système ou l'application à auditer. Les identifiants peuvent appartenir à des **profils d'utilisateurs** différents afin de tester des niveaux de **privilèges distincts**
- White Box (boîte blanche) : l'auditeur dispose du maximum d'informations techniques (dossier d'architecture, fichiers de configuration des systèmes, code source, identifiants, etc). Ils ont également accès à des contacts techniques liés à la cible



► Il est possible d'effectuer les trois types de façon séquentielle pour un même test d'intrusion

Red team

► Objectif

- Se mettre dans la peau d'un attaquant cherchant à s'introduire, **par tous les moyens nécessaire**, dans le SI de la cible
- **Tester la robustesse** d'un SI en combinant des vecteurs d'attaque variés et en **rebondissant** sur des cibles indirectes pour effectuer une **action nuisible réaliste**

► Moyens

- Accès physique
- Accès distant via exploitation de vulnérabilités techniques
- Recherche d'identifiants de connexion aux portails de la cible
- Ingénierie sociale sur les collaborateurs pour un accès à un poste du réseau interne



Objectifs détaillés du test d'intrusion

► Les objectifs peuvent varier selon les contextes :

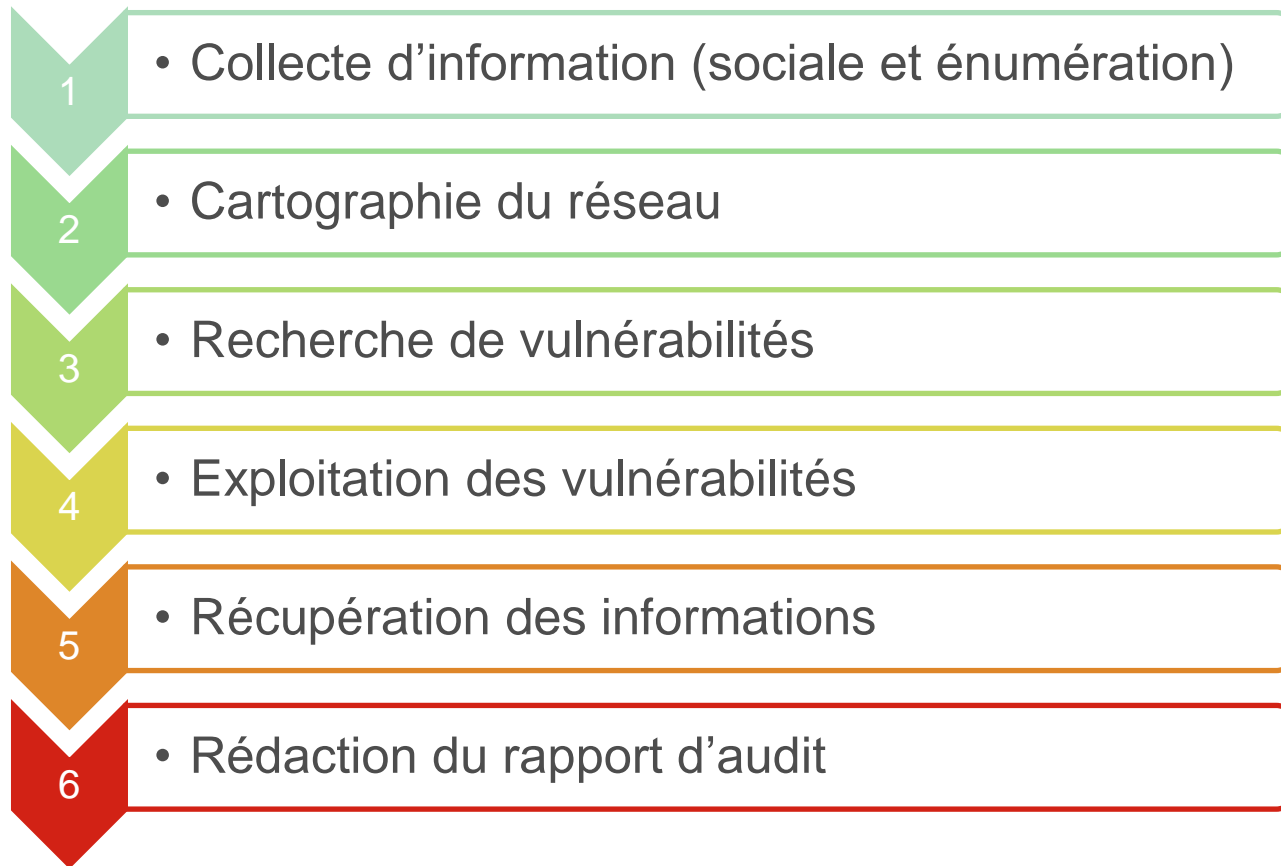
- **Lister un ensemble d'informations**, trouvées d'une manière ou d'une autre, et qui peuvent être sensibles ou critiques
- Dresser une **liste des vulnérabilités** ou faiblesses du système de sécurité pouvant être exploitées
- Tester l'efficacité des systèmes de **détection d'intrusion** et la **réactivité** de l'équipe de sécurité, et parfois des utilisateurs (social engineering)
- Démontrer qu'un attaquant potentiel est **en capacité de trouver des vulnérabilités et de les exploiter** pour s'introduire dans le système d'information
- Effectuer un **reporting** et une présentation finale de son avancement et de ses découvertes au client
- Donner des pistes et **conseiller sur les méthodes de résolution** et de correction des vulnérabilités découvertes

Objectifs

- ▶ En revanche, certains objectifs **ne peuvent pas être satisfaits** :
 - **Avoir l'assurance** qu'un environnement informatique **est sécurisé**
 - ✓ Manque de connaissance ou de moyens
 - ✓ **Condition d'évaluation** ne permettant pas de mettre en évidence certaines vulnérabilités
 - ✓ Vulnérabilités pouvant apparaître dans des briques logicielles ou des modifications de paramétrage de sécurité
 - Identifier **exhaustivement** les vulnérabilités de sécurité d'un environnement
 - ✓ L'auditeur identifie rarement d'autres vulnérabilités que celles utilisées pour prendre le contrôle d'un système (alors qu'il peut en exister plusieurs)
 - ✓ Le test d'intrusion ne permet pas de détecter des vulnérabilités dans les couches de protection **au-delà de la première couche** présentant un niveau de sécurité suffisant
 - ✓ Ne se limite qu'aux **faiblesses de sécurité techniques** et non d'ordre organisationnel ou procédural

Déroulement d'un test d'intrusion

► Phases du test d'intrusion



Méthodologie de collecte d'information

► Méthode de collecte :

- Ingénierie sociale
- Collecte d'information **passive** de type OSINT (Open Source INTelligence : exploitation des informations issues de sources ouvertes)
- Collecte d'information **active** :
 - ✓ Scan et cartographie du réseau dans le périmètre des actions définies lors du cadrage de l'audit
 - ✓ Détection des failles et vulnérabilités des cibles
 - ✓ Analyse des données collectées et définition des vecteurs d'attaque
 - ✓ Test sur les cibles

Collecte d'information

► Collecte d'information à partir des sources suivantes :

- **Moteur de recherche** : permet de récupérer les documents publics d'une cible – par exemple un communiqué de presse décrivant la refonte de l'architecture...
- Service **Whois** : permet d'obtenir des informations sur le propriétaire d'un nom de domaine ou d'une plage d'IP
- Enumération **DNS** : permet de lister les machines d'un domaine
- **Prise d'empreinte** : permet de connaître les versions et les types de serveurs de la cible afin de déterminer les vulnérabilités connues
- **Moteur de recherche de vulnérabilité** (Shodan, Censys) : permet de trouver des serveurs vulnérables en fonction de leurs réponses

Service Whois

- Exemple de commande whois (sous linux) :

```
domain: ece.fr
status: ACTIVE
epstatus: active
hold: NO
holder-c: OED5-FRNIC
admin-c: CTC104973-FRNIC
tech-c: CTC104974-FRNIC
registrar: GANDI
Expiry Date: 2023-04-08T09:06:32Z
created: 1994-12-31T23:00:00Z
last-update: 2022-10-14T20:25:07.663482Z
source: FRNIC

nsserver: ns-138-c.gandi.net
nsserver: ns-247-b.gandi.net
nsserver: ns-51-a.gandi.net
source: FRNIC
```

- Renseignements sur le contact du domaine :

```
nic-hdl: OED5-FRNIC
type: ORGANIZATION
contact: Organisation et Developpement
address: Organisation et Developpement
address: 43 quai de grenelle
address: 75015 PARIS
country: FR
phone: +33.147207582
```

Enumération DNS

- Nslookup permet de rechercher des informations dans le Domain Name System (DNS) qui associe noms de domaine et adresses IP

- Natif sous Windows

```
C:\Users\          >nslookup ece.fr 8.8.8.8
Serveur :   dns.google
Address:    8.8.8.8
```

```
Réponse ne faisant pas autorité :
Nom :      ece.fr
Address:   217.70.184.55
```

- Host permet d'afficher les redirections DNS

- Utilitaire libre UNIX

```
L$ host ece.fr
ece.fr has address 217.70.184.55
ece.fr mail is handled by 0 ece-fr.mail.protection.outlook.com.
```

Enumération DNS

- Objectif : lister l'ensemble des machines d'un domaine pour définir les cibles

- Dnsenum permet d'effectuer un brute force sur la recherche de sous-domaines avec la commande suivante :

✓ `dnsenum -f dns.txt -o ece.xml ece.fr`
(permet de faire un brute force sur les sous-domaines en utilisant le fichier dns.txt et renvoie les résultats sous format XML)

— ece.fr —

Host's addresses:

ece.fr.	10611	IN	A	217.70.184.55
---------	-------	----	---	---------------

Name Servers:

ns-51-a.gandi.net.	600	IN	A	173.246.100.52
ns-138-c.gandi.net.	600	IN	A	217.70.187.139
ns-247-b.gandi.net.	600	IN	A	213.167.230.248

Mail (MX) Servers:

ece-fr.mail.protection.outlook.com.	10	IN	A	104.47.1.36
ece-fr.mail.protection.outlook.com.	10	IN	A	104.47.0.36

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for ece.fr on ns-51-a.gandi.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for ece.fr on ns-138-c.gandi.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for ece.fr on ns-247-b.gandi.net ...
AXFR record query failed: NOTAUTH

Brute forcing with /usr/share/dnsenum/dns.txt:

intranet.ece.fr.	300	IN	CNAME	waf01.inseecu.net.
waf01.inseecu.net.	300	IN	CNAME	inseecwaf01.westeurope.cloudapp.azure.com.
inseecwaf01.westeurope.cloudapp.azure.com.	10	IN	A	51.144.185.40

Moteurs de recherche

► Objectif : permet de trouver des serveurs vulnérables en fonction des en-têtes de réponse

➤ Exemple : serveurs FTP autorisant l'accès anonyme :



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.




TOTAL RESULTS	
97,502	
TOP COUNTRIES	
United States	27,933
China	8,638
Japan	7,216
Korea, Republic of	6,885
Germany	4,525
More...	
TOP PORTS	
21	96,901
2121	562
221	34
14147	4
22	1
More...	
TOP ORGANIZATIONS	
EGiHosting	6,096
DigitalOcean, LLC	6,038
Korea Telecom	2,929

View Report View on Map	
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor	
 NICNET, INDIA India, New Delhi	220 (vsFTPD 3.0.2) 230 Login successful. 214-The following commands are recognized. ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD MODE NLST NOOP OPTS PASS PASV PORT PHD QUIT REIN REST RETR RMD RINFR RINFO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCMD XMKD...
 TELEFONICA DE ESPANA Spain, Madrid	220 FTP server ready, 1 active clients of 1 simultaneous clients allowed. 230 User login successful. 214-HELP: To see the help of a command use HELP command Commands with help available: ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV HELP LIST M...
 Taiwan Fixed Network CO.,LTD. Taiwan, Taichung	220 (vsFTPD 1.2.2) 230 Login successful. 214-The following commands are recognized. ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD MODE NLST NOOP OPTS PASS PASV PORT PHD QUIT REIN REST RETR RMD RINFR RINFO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCMD XMKD...
 EGiHosting United States, San Jose	220 (vsFTPD 2.2.2) 230 Login successful. 214-The following commands are recognized. ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD MODE NLST NOOP OPTS PASS PASV PORT PHD QUIT REIN REST RETR RMD RINFR RINFO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCMD XMKD...

Moteurs de recherche

- Permet de compléter la cartographie du réseau accessible depuis l'extérieur

 **Censys**

ece.fr

Quick Filters

For all fields, see [Data Definitions](#)

Tag:

- 367 CT
- 366 DV
- 356 Google CT
- 356 Leaf
- 310 Expired

☒ More

Issuer:

- 323 Let's Encrypt
- 21 Gandi
- 10 DigiCert Inc
- 4 cPanel, Inc.
- 2 GoDaddy.com, Inc.

☒ More

Certificates

Page: 1/17 Results: 412 Time: 1066ms

- [CN=www.boutique.alumni-ece.fr](#)
 - R3
 - 2021-08-20 – 2021-11-18
 - alumni-ece.fr, boutique.alumni-ece.fr, www.alumni-ece.fr, www.boutique.alumni-ece.fr, ...
- [CN=www.boutique.alumni-ece.fr](#)
 - R3
 - 2021-08-20 – 2021-11-18
 - alumni-ece.fr, boutique.alumni-ece.fr, www.alumni-ece.fr, www.boutique.alumni-ece.fr, ...
- [CN=vpe-ece.fr](#)
 - R3
 - 2021-10-18 – 2022-01-16
 - vpe-ece.fr, www.vpe-ece.fr

Prise d'empreinte

- La façon la plus simple de déterminer le type et la version d'un serveur est de vérifier ses en-têtes :

```
$ nc 203.0.113.1 80  
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Expires: Sun, 20 Jun 2021 01:41:33 GMT  
Date: Sat, 19 Jun 2021 01:41:33 GMT  
Content-Type: text/HTML  
Accept-Ranges: bytes  
Last-Modified: Mon, 24 May 2021 15:32:21 GMT  
ETag: b0aac0542e25c31: 89d  
Content-Length: 7369
```

Prise d'empreinte

► Cependant, l'en-tête de réponse peut être masqué

- Dans ce cas, il est possible de vérifier l'ordre des en-têtes HTTP ou encore le comportement à la suite d'une requête malformée

```
$ nc iis.example.com 80  
GET / HTTP/3.0
```

```
HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Content-Location:  
http://iis.example.com/Default.htm  
Date: Fri, 11 Jun 2021 20:14:02 GMT  
Content-Type: text/HTML  
Accept-Ranges: bytes  
Last-Modified: Fri, 11 Jun 2021 20:14:02 GMT  
ETag: W/e0d362a4c335be1: ae1  
Content-Length: 133
```

Réponse d'un IIS 5.0

```
$ nc apache.example.com 80  
GET / HTTP/3.0
```

```
HTTP/1.1 400 Bad Request  
Date: Fri, 11 Jun 2021 17:12: 37  
GMT  
Server: Apache/1.3.23  
Connection: close  
Transfer: chunked  
Content-Type: text/HTML;  
charset=iso-8859-1
```

Réponse d'un Apache 1.3.23

Prise d'empreinte

► Détermination d'utilisation de ports non standards

- Utilisation d'un scanner de port (par exemple Nmap)
- La reconnaissance de service se fait avec l'option `-sV`
- La commande suivante permet d'effectuer un scan TCP (`-sT`) de tous les ports ouverts sur l'IP cible et de déterminer quels sont les services (`-PN` évite le ping) :

```
nmap -PN -sT -sV -p0-65535 192.168.1.100
```

```
PORT STATE SERVICE VERSION
```

```
22/tcp open  ssh OpenSSH 3.5p1 (protocol 1.99)
```

```
80/tcp open  http Apache httpd 2.0.40 ((Red Hat Linux))
```

```
443/tcp open  ssl OpenSSL
```

Identification des frameworks

- ▶ L'identification d'un CMS change le cours du test d'intrusion car elle permet :
 - D'identifier les vulnérabilités connues d'une version
 - De connaître la structure des fichiers du CMS
 - De connaître les mauvaises configurations spécifiques au CMS
 - De se servir de la **capitalisation** effectuée lors d'un précédent test sur le même framework

- ▶ Elle s'effectue par l'analyse :
 - Des en-têtes HTTP et des cookies (CakePHP, django)
 - Du code source HTML (Powered by, %nom_du_framework%)
 - Des fichiers et dossiers spécifiques (URL spécifiques ou comparaison des condensats de fichiers de configuration)

Exploitation de vulnérabilités

► Une fois la cartographie effectuée, les éléments suivants peuvent être testés :

- Gestion du déploiement et de la configuration (interfaces d'admin, HSTS, informations sensibles)
- Gestion des identités (création d'utilisateur, énumération de comptes, droits d'accès des comptes de test)
- Authentification (mots de passe par défaut, processus de déconnexion, contournement d'authentification, réinitialisation de mot de passe)
- Autorisations (inclusion de fichiers, escalade de privilège)
- Gestion des sessions (timeout, fixation de session, CSRF)

Exploitation de vulnérabilités

- Validation des entrées (XSS, SQLi, injection de code, overflows)
- Gestion des erreurs (analyse des codes d'erreur et des stacktraces)
- Cryptographie (algorithmes faibles, envoi d'information sensibles non chiffrées)
- Logique métier (validation des données métier, capacité à forger des requêtes, vérifications d'intégrité, upload de fichiers malveillants)
- Côté client (exécution de javascript, injection d'HTML, manipulation de ressources côté client, clickjacking)

► **Pour plus d'information, voir la méthodologie de test de l'OWASP (Open Web Application Security Project)**



Rapport d'audit

- ▶ **Le rapport d'audit doit être découpé en deux grandes parties :**

- La synthèse
- Le descriptif technique



- ▶ **La synthèse doit comprendre les éléments suivants :**

- Rappel du périmètre, des objectifs et des résultats globaux
- Une classification globale du risque liée aux enjeux métiers
- Un résumé des recommandations afin qu'un décideur puisse comprendre les tâches nécessaires pour réduire les risques identifiés
- Une feuille de route indiquant les actions à entreprendre le plus rapidement en fonction de l'impact potentiel

Rapport d'audit

- ▶ **Le descriptif technique doit comprendre une description détaillée des éléments suivants :**
 - Le périmètre
 - La collecte d'information (permet de montrer à l'audité l'étendue des informations publiques disponibles)
 - L'évaluation des vulnérabilités potentielles (scanner, version d'un logiciel) et leurs classifications
 - Les activités d'exploitation et l'impact réel des vulnérabilités (niveau d'accès obtenu)
 - Les suggestions de correction des vulnérabilités



Organisation d'audit

► Actions du commanditaire d'audit :

- Définition du **périmètre de l'audit** basée sur une analyse des risques métier
- Adapter la durée de l'audit en fonction :
 - ✓ Du périmètre d'audit et de sa complexité
 - ✓ Des exigences de sécurité attendues du système d'information audité
- Réaliser un échantillonnage (afin de réduire le coût de l'audit) :
 - ✓ Pour les audits de configuration, auditer les **serveurs les plus sensibles** : Active Directory, serveurs de fichiers, applicatifs, d'infrastructure (DNS, SMTP, etc.)
 - ✓ Pour un audit de code source, auditer les **parties sensibles du code source** : gestion des authentifications, gestion des contrôles d'accès, accès aux bases de données, contrôle des saisies utilisateur...
- Réaliser les tests d'intrusions sur un **environnement de test** (ou de pré-production) afin d'éviter les conséquences liées aux éventuels dysfonctionnements sur la production à condition que l'environnement soit **similaire à celui de production**

Organisation d'audit

- Les audits d'architecture, de configuration, de code source et organisationnels doivent être réalisés en **production**
- Définir les **modalités de réalisation** des activités d'audit (horaires des interventions, autorisations, etc.)
- **Sauvegarder** les données avant l'audit



- Obtenir une **décharge signée** du client et des sous-traitants de celui-ci (hébergeurs, CDN, prestataires SaaS, etc.) pour ne pas être soumis à l'article 323-1 du code pénal (accès ou maintien frauduleux dans un STAD)
- Faire signer un **NDA** (Nondisclosure agreement – Accord de confidentialité) aux auditeurs