H4ck 1n TN

De la collecte d'informations à l'extraction

Valentin Giannini

Ceten – TELECOM Nancy

January 14, 2016

Préambule

- Ce document est donné à titre indicatif
- L'utilisation des outils n'est pas développée, pour l'utilisation utilisez man ou google (RTFM)
- La liste des outils n'est pas exhaustive, il y a sûrement beaucoup d'autres outils
- Ce document se base sur le livre "Les bases du hacking" de Patrick Engebretson des éditions Pearson.

Quésako

Définition

Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique. La méthode consiste à se faire passer pour un hacker et de voir tout ce qui n'est pas sécurisé afin d'appliquer des correctifs.

Quésako

Définition

Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique. La méthode consiste à se faire passer pour un hacker et de voir tout ce qui n'est pas sécurisé afin d'appliquer des correctifs.

Différents types

- WhiteBox
- GreyBox
- BlackBox
- Red Team

Droit

Autorisation

Pour faire un test d'intrusion vous devez obligatoirement avoir un contrat spécifiant ce que vous avez le droit de faire. Vous devez spécifier le périmètre de votre test, les sites/machines visées, utilisation de rootkit, ...

HackInTN

Pour ce qui est du Pentest à l'école, il est seulement autorisé d'en faire sur le serveur du club via le VPN. Vous ne devez en aucun cas faire de scans sur le réseau de l'école.

Droit

Autorisation

Pour faire un test d'intrusion vous devez obligatoirement avoir un contrat spécifiant ce que vous avez le droit de faire. Vous devez spécifier le périmètre de votre test, les sites/machines visées, utilisation de rootkit, ...

HackInTN

Pour ce qui est du Pentest à l'école, il est seulement autorisé d'en faire sur le serveur du club via le VPN. Vous ne devez en aucun cas faire de scans sur le réseau de l'école (et de vos voisins).

Droit

Autorisation

Pour faire un test d'intrusion vous devez obligatoirement avoir un contrat spécifiant ce que vous avez le droit de faire. Vous devez spécifier le périmètre de votre test, les sites/machines visées, utilisation de rootkit, ...

HackInTN

Pour ce qui est du Pentest à l'école, il est seulement autorisé d'en faire sur le serveur du club via le VPN. Vous ne devez en aucun cas faire de scans sur le réseau de l'école (et de vos voisins (et de tout le reste)).

Déroulement

- Reconnaissance
- Scan
- Exploitation
- Post Exploitation

But

Récupération d'informations sur

- Le personnel
- La société
- La structure interne
- Les machines
- Les services

Collecte d'informations

HTTrack

- Clone d'un site web
- Examiner le site
- Collecte de numéros, e-mails, ...

Collecte d'informations

Google Dorking,...

- Indexe tout et n'importe quoi
- Opérateurs → nom:terme
  → site, intitle, allintitle, inurl, filetype, cache, ...
- Exemple : inurl:admin site:telecomnancy.eu

Collecte d'informations

The Harvester

- Récupération de sous domaines et e-mails
- Trouver des schémas de génération d'e-mails
- Choix de la source d'information

Whois, Netcraft, Hosts

Whois

- Informations sur le propriétaire du domaine
- Informations de localisation

Whois, Netcraft, Hosts

NetCraft

- Moteur de recherche
- Informations supplémentaires
  $\rightarrow$ IP, OS, versions, DNS? ...

Whois, Netcraft, Hosts

Hosts

- Récupération d'adresse IP
  (Modèle OSI : couche 3)

DNS

DNS

- Premières cibles
- Plan du réseau
- Mal protégés/configurés

DNS

NSlookup

- Obtenir des enregistrements
- Exemple :

  $ nslookup
  > serveur X.X.X.X
  > set type=any
  > domaine.com
  Server : Y.Y.Y.Y
  Address : Y.Y.Y.Y#53
- *(Modèle OSI : couche 3)*

DNS

dig

- Extraire de l'information
- Transfert de zone
- Exemple : dig @X.X.X.X domaine.com -t AXFR
- Limites → Fierce
- *(Modèle OSI : couche 3)*

Messagerie

Messagerie

- Serveurs internes
- Messages automatiques
- Messages d'erreurs
  $\rightarrow$ Envoie de .bat, .exe, ...

Social Engineering

En attendant une futur présentation

- Utiliser la naïveté des personnes
- Utiliser l'usurpation d'identité
- Jouer un rôle avec les cibles
- Et plus encore...

Etat actuel

- Liste d'URL
- Liste d'adresses IP
- Liste d'adresses e-mail
- Version des équipements accessibles directement

But

Use cases

- Lister les machines d'un réseau
- Lister les ports ouverts d'une machine
- Lister les programmes/versions d'une machine
- Lister les vulnérabilités d'une machine

Ping

Ping

- Un bon début
- Peu voyant ... mais peu fiable

Ping

Ping

- Un bon début
- Peu voyant ... mais peu fiable

Fping

- Découverte rapide d'un réseau
- Même problème que ping

Ping

Ping

- Un bon début
- Peu voyant ... mais peu fiable

Fping

- Découverte rapide d'un réseau
- Même problème que ping

Hping

- ICMP + TCP + UDP
- vérification de l'état d'une connexion
- On se rapproche

Scan de ports

Principe

- Découvrir les ports ouverts d'une machine
  $\rightarrow$ *(Modèle OSI : couche 4)*
- Détection des services
- Fabriquer une base de connaissances

Scan de ports

Nmap

- Simple d'utilisation
- Plusieurs type de scan
  $\rightarrow$ TCP Connect, SYN, NULL, XMAS, UDP, ...
- Configurable à souhait

Scan de ports

Nmap Scripting Engine

- Récupérer des bannières
- Connaître l'OS, les versions des programmes, ...
- Tests de vulnérabilités basiques

Scans de vulnérabilités

Vulnérabilités

- Fonctionnalité cachée non voulue
- Dépend des versions
- Présent sur un OS, un service ou un programme
  $\rightarrow$ *(Modèle OSI : couche 7)*
- Permet un accès illégitime avec un certain niveau de privilèges
- CVE

Scans de vulnérabilités

Outils

- Nessus
- Nexpose
- OpenVAS
- Nmap Scripting Engine

Etat actuel

- Liste de machines
- Liste de ports
- Liste d'OS, services, programmes, ...
- Liste de vulnérabilités

But

- Obtenir un accès sur la cible
- Collecter des mots de passe
- Ecouter le réseau

Mot de passe

Medusa

- Trouver des mots de passe
- Compatible avec beaucoup de services
- Utilisation sur le système cible
- Ne pas sous estimer l'intelligence des humains :P

John

- Craquer des mots de passe
- Utilisation en local

Metasploit

Présentation

- Framework écrit en Ruby
- Open Source mais pas trop
- Participatif
- Connu

Metasploit

Utilisation

- Recherche de modules
- Configuration des modules
- Choix du payload
- Possibilité de scripting
- Bonus
  → Scans de ports, lien avec des programmes exterieurs, ...

Réseau

A venir (Amember)

- SSH
- DoS / DDoS
- Sniffing
- MITM (ARP spoofing
- TCP Hijacking et IP spoofing
- Wi-Fi
- Rogue AP
- IP over DNS

Etat actuel

- Une liste d'utilisateurs/mots de passe
- Un accès distant sur des machines

But

- Installer une porte dérobée
- Garder un shell distant disponible même après un patch
- Exfiltration de données
- Pivoter

Netcat et autres

Principes

- Mettre en place une connexion
- Simple d'utilisation
- Cryptcat pour une liaison chiffrée

Cas d'utilisations

- Simple connexion
- Envoie de fichiers
- Scan de ports
- Serveur web léger

Rootkit

Définition

Un rootkit est un ensemble de techniques mises en oeuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible

Principes

- Se cacher dans un fichier
- Se cacher dans un processus
- Keylogger
- ...

Meterpreter

Un couteau suisse

- Manipulation de fichier
- Manipulation d'utilisateurs
- Exécution de programme
- KeyLogger
- Migration dans des processus
- Gestion des processus
- Pivoter
- ...

Etat actuel

- Accès à toute la machine
- Machine de pivot pour recommencer sur un réseau privé
- La fin du pentest, ou presque

Comment faire une synthèse

Déroulement

- URL, IP, e-mail
- Machines, Ports, Services, OS
- Exploits
- Liens établis
- Données récupérées

Comment faire une synthèse

Résultat

- Donner la liste des machines accessibles depuis internet
- Donner la liste des services accessibles
- Donner la liste des vulnérabilités
- Conseiller des patchs, mises à jours, ...
- Sensibiliser les employés
- ...

Conclusion

- Un acte majeur en audit de sécurité
- Un domaine très large
- Utilisation de nombreux outils
- Demande de nombreuses connaissances

À vous de jouer

- Installer des VM sur vos PC
- Utiliser les VM du club
- Apprenez en davantage sur les différentes parties

Conclusion

- Un acte majeur en audit de sécurité
- Un domaine très large
- Utilisation de nombreux outils
- Demande de nombreuses connaissances

À vous de jouer

- Installer des VM sur vos PC
- Utiliser les VM du club
- Apprenez en davantage sur les différentes parties
- Éclatez vous :D

Merci de votre attention.