DE LA RECHERCHE À L'INDUSTRIE

Master 2 SeCReTS

Sécurité windows

Scénarios d'intrusion,
Faiblesses et contre-mesures

www.cea.fr

19 février 2019

Sommaire

Généralités

Constat et retour :

- *Phishing*
- Scans réseaux
- Presse
- Environnement personnel
- Annonces régulières de vulnérabilités
- Méconnaissance du niveau réel de vulnérabilité (et des fonctions de sécurité)
- Attaque à grande échelle *vs* ciblage

Assume breach

Considérer systématiquement qu'un attaquant finira par trouver un point d'entrée.

- Il a le temps et les moyens :
  - niveau 0 à ∞
  - personne solitaire à structure étatique
  - compromission pérenne et progressive dans le temps
- Il suffit d'un problème :
  - utilisateur maladroit
  - machine oubliée

$\rightarrow$ Il faut rendre la tâche de l'attaquant le plus difficile possible et faciliter sa détection

Sommaire

Menace externe

- *Phishing*
  - A grande échelle
  - Ciblé et personnalisé (importance des informations publiques disponibles)
  - Avec ou sans pièces jointes
- Exploitation de vulnérabilité :
  - Pièces jointe : doc, docx, pdf
  - Lien web vers du contenu malveillant (flash ?)
- Ou pas :
  - Maladresse / méconnaissance de l'utilisateur

Menace interne

- Employé ou sous-traitant
- Attaque à l'insu du salarié
  - Clef USB / Téléphone personnel / Ordinateur portable (*BYOD*)
  - *Social Engineering*
  - Naïveté de l'utilisateur

→ Même situation que le cas précédent sauf que l'attaquant à déjà un pied sur le réseau

Objectif de l'attaquant

- Menace interne ou externe, la démarche se rejoint.
- L'objectif est d'avoir une exécution de code au niveau **utilisateur**, et si possible d'avoir un canal de contrôle / commande (CC)

Fingerprint distant (en avance de phase)

- *user-agent*
- en-têtes en général

Cartographie passive (après la 1re exécution)

- Étude de la configuration de la machine :
  - Utilisateurs
  - Processus
  - *Filesystems*
  - Périphériques
  - Programmes installés

Cartographie passive

- Plan d'adressage
- Environnement (proxy ?)
- Netstat
- Services en écoute
- Table ARP

- Écoute sur le réseau ?

Découverte de l'environnement

- Énumération :
  - Des comptes
  - Des groupes
  - Des Mails (ciblage plus précis ?)
- Ping scan
- Requêtes netbios (*nbtstat* / *nbtscan*)
- Scan réseau (en plusieurs étapes)
- *traceroute*

Accès aux données de façon légitime (droits sur les partages)

- En anonyme
- Avec les *crédentials* de l'utilisateur
- Depuis de nouveaux serveurs
- Accès à des sauvegardes
- Fichiers de configuration avec mot de passe en clair
- Rebond USB ?

- Boot live ? TPM ?
- Accès physique au disque de la machine ?

Identification des **services d'intérêt** :

- Pour les informations qu'ils peuvent contenir
- Pour les vulnérabilités qu'ils peuvent présenter
- Pour les rôles qu'ils peuvent porter (poste d'admin par exemple)

Divers outils

- DNS (énumération, transfert de tables, *_srv*)
- *masscan*
- scripts *nmap*
- outils linux classiques : *smbclient, ldapsearch, rpc net, kinit*
- certificats ssl
- *nbtscan, smbenum, enum4linux*

Détection : rejoint le thème plus général de la détection d'intrusion

- Surveillance des échanges avec l'extérieur, pièces jointes, anti-spam et des flux internes
- Surveillance des journaux d'événements
  - Collecte de logs (*nxlog, winlogbeat, event forwarder*)
  - Politique de logs et de rétention adaptée
- Détection par signature et comportementale
  - Antivirus à jour
  - Ids avec jeu de règles à jour
- Sensibilisation des utilisateurs

→ Cours de détection d'intrusion

Contre-mesures

- Segmentation réseau (architecture)
- Filtrage
- Fermeture des accès anonymes
  - Session invité
  - Partage samba
  - Serveurs web
  - LDAP anonyme

Sommaire

Élévation de privilèges locaux

Exploitation de vulnérabilité non corrigée

- Délai d'application d'une mise à jour = période d'exposition
- Redémarrage nécessaire dans certains cas
- Systèmes obsolètes

Faiblesses de configuration

- Utilisateur déjà admin
- Permissions sur des exécutables (exécutés en SYSTEM)
- Services qui tournent en SYSTEM
- Scripts de démarrage
- Privilèges de DEBUG / chargement de driver
- Vulnérabilité de configuration d'un service (unquoted path)

Élévation de privilèges

Le cas idéal : exploitation de vulnérabilité à distance

- MS08-067 (conficker)
- MS14-068 (kerberos)
- MS17-010 (wannacry)

Autres cas triviaux

- Mots de passe sur des partages (*.txt)
- Backup des DCs en lecture pour tout le monde

Élévation de privilèges à distance

Attaques sur les services ayant des possibilités d'exécution de code

- MS-SQL : xpcmdshell
- Oracle : exécutions de procédures stockées Java
- Tomcat : déploiement d'une JSP maison
- Jboss : même idée
- Applications web, inclusion de code
- Applications lourdes, injection de commande SQL, etc.

Avec de la chance

Compte de service trop privilégié, admin de domaine

Segmentation système et réseau (encore...)

- Principe du moindre privilège
- ACL des flux strictement nécessaires

Patch management

- WSUS (patchs os + applicatifs microsoft)
- SCCM

Contre-mesures

Minimiser les points d'entrée

- Ne pas laisser de configuration par défaut (toujours se poser la question)
- Fermeture des consoles d'administration, changement des mots de passe
- Réseau de déploiement à part
- Identifier les applicatifs à risques (vulnérabilités récurrentes, *insecure by design*)

- Se méfier des produits tout packagés : boites noires

Contre-mesures

Audits / scans périodiques

- Outils de gestion de configuration
- Outils d'inventaire / mises à jours
- Audit des permissions d'accès sur les fichiers / partages

- Nmap et scripts nse
- Nessus (possibilité de scans authentifiés)
- OpenVAS

Contre-mesures locales

Filtrage réseau

- Pare-feu local, jeu de règles plaqué par GPO
- *Private VLAN* pour les stations

Contre-mesures applicatives et traçabilité

- Blocage des périphériques USB
- Applocker
- WER
- Suivi de processus
- Sysmon
- ... Analyse de logs

Applocker

Principe

- *Whitelist* des emplacements où il est possible de lancer des exécutables et scripts
- Gestion par PATH, Signature, hash
- Mode audit (logs)
- Efficace contre une menace automatique

Inconvénients

- Gestion qui peut être lourde suivant la taille du parc et son ancienneté
- Bypass possible

→ Applocker ne fait pas tout, mais augmente sensiblement le niveau de sécurité

WER & Sysmon

WER

- Permet de récupérer les *coredumps* de crash d'applications

  $\rightarrow$ détection de l'utilisation d'un exploit ?

Sysmon

- Permet de logguer plus finement
- Arguments des process et scripts
- Lancement d'application depuis d'autres applications (outlook, ie)
- Accès réseaux associés aux processus
- Accès à la base de registre (filtre sur le chemin)

Sommaire

Dumps de mots de passe

Comptes locaux

- reg save
- samdump

Comptes du domaine

- Utilisation des shadow copies
- ntdsutil
- dcsync

LM/NTLM

LM

- Alphabet Simplifié
- *Padding* a la fin pour compléter les 14 caractères
- Découpé en 2 mots de passe distincts de 7
- DES

- Encore activé sur les 2003, à bannir

LM/NTLM

- Réutilisation possible du hash LM si présent
- Importance de vider l'historique des mots de passe LM

NTLM

- Pas de sel
- john - - rules=NT
- PassTheHash

PassTheHash

- Pas besoin de retrouver le mot de passe
- Le hash suffit à s'authentifier
- Pas de notion de timestamp

- pth-net, pth-rpcclient, pth-smbclient, pth-winexe, pth-wmic
- Contraintes de rétro-compatibilité,
- L'accent est mit sur la protection du hash, en attendant...

Identification des chemins de contrôle dans l'AD

- ANSSI : ad-control-path
- Empire : module bloodhound

→ ciblage des comptes

Mouvement latéral

While not Admin de domaine :

1. Réutilisation de *crédentials* sur d'autres machines accessibles à distance
   - mot de passe
   - pass the hash
   - john
2. Vol d'autres authentifiants
   - mimikatz
   - keylogger
3. Scan réseau
4. Réutilisation des authentifiants sur un ensemble potentiellement plus important de machines
5. IF NOT Admin de domaine, GOTO étape 1 (généralement pas besoin de beaucoup d'itérations)

Pérennisation

Pérennisation de l'accès

- Positionnement de *backdoors* triviales (sethc par exemple)
- Récupération de l'ensemble des empreintes de mot de passe (notamment pour les comptes privilégiés), attention aux réutilisations
- Golden ticket / Silver ticket
- (Alternate Data Stream)

Exfiltration des données

- Communication avec un CC
- USB avec partition cachée

Administration en silos

- Limiter la portée d'une compromission à un périmètre
- Sanctuariser les systèmes donnant accès à l'ensemble du SI (AD, Exchange)

Outils à limiter ou proscrire

Objectif : limiter l'exposition des comptes, avoir des pratiques homogènes permettant de distinguer admin / attaquant.

- Éviter l'authentification explicite qui laissent les mots de passe en clair en mémoire
- Privilégier l'authentification implicite, l'utilisation de kerberos

Sommaire

Identifier les informations fiables

- Tout peut avoir été modifié par l'attaquant
- En quoi avoir confiance ?
- Envergure de la compromission ?
- L'attaquant est-il toujours la ?

L'importance de la centralisation des informations

- Logs
- Process tracking
- Sysmon
- Flux réseaux
- ELK / splunk

→ Ces informations doivent être séquestrées dans une zone sûre

Dump ram en live

- win32dd, DumpIt.exe
- virsh dump –memory-only
- VBoxManage debugvm dumpvmcore

Volatility

- volatility -f dump –profile=Win7SP0x64 clipboard
- pslist, hashdump, dumpregistry, cachedump, dumpfiles

Fichiers

- Strings
- evt
- Ruches
- fls / sleuthkit

Autoruns

- Liste les programmes configurés pour s'exécuter pendant le lancement ou la connexion du système
- plus complet que msconfig
- *Whitelist* des entrées signées Microsoft
- client console : autorunsc

Autres pistes

- Historique usb : (setupapi.log, HKLM/SYSTEM/CurrentControlSet/Enum/USBSTORE, USBDeview)
- cache de navigation
- NTUSER.dat
  - Recherches
  - Lancement comptabilité
  - *RunMRU*
  - *RecentDocs*
  - *Typed URL*
  - *UserAssist*
  - *ShellBag*
- *regripper*

Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Bruyères-le-Châtel | 91297 Arpajon Cedex
T. +33 (0)1 69 26 40 00 | F. +33 (0)1 69 26 40 00
Établissement public à caractère industriel et commercial
RCS Paris B 775 685 019