SYNACKTIV
DIGITAL SECURITY

Techniques d'intrusion Windows

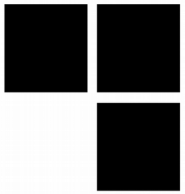
De l'accès anonyme au premier accès authentifié

10/12/2017 - Cours Université Rennes 1

Thibault Guittet – thibault.guittet@synacktiv.com

Accès « anonyme »

Mise en situation



Postulat

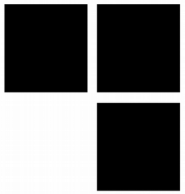
- Nous sommes connecté au réseau avec un équipement non affilié au domaine
  - Accès à une prise Ethernet brassée (intrusion physique)
  - Accès au VPN de l'entreprise (vol d'un compte d'accès valide)
  - Exploitation d'une *appliance* connectée au réseau de la cible mais hors domaine

Objectifs

- Comprendre l'architecture du SI dans lequel nous nous trouvons
- Émettre les premiers postulats sur la localisation de notre cible
- Élever ses privilèges de « anonyme » à « utilisateur authentifié »

Accès « anonyme »

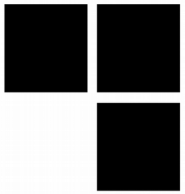
Mise en situation



- **Accès authentifié = obtention d'une identité sur le SI**
  - Compte utilisateur / de service local → Peu intéressant
    - A accès à une seule machine du réseau
    - Avec de la chance la machine en question héberge notre cible
    - Accès souvent obtenu après compromission d'un service (serveur web, etc.)
  - Compte utilisateur du domaine → Intéressant
    - A accès aux informations et services du domaine
    - A accès à des partages réseaux / machines sur le domaine
    - Accès souvent obtenu via des attaques par *phishing*
  - Administrateur local → Très intéressant
    - Permet la prise en main totale d'une machine
    - Accès souvent obtenu après compromission d'un service tiers (Tomcat, etc.)

Accès « anonyme »

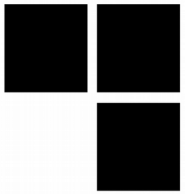
Mise en situation



- **Accès authentifié = obtention d'une identité sur le SI**
  - Administrateur dans le domaine (*helpdesk,* administrateur de l'infrastructure, etc.)
    - Compromission d'une partie du SI
    - Forte probabilité pour qu'il ait accès à la cible
    - Accès souvent récupéré après l'obtention d'un premier accès
  - Administrateur du domaine ou de l'entreprise
    - Compromission totale du SI
    - Forte probabilité pour qu'il ait accès à la cible
    - Accès souvent récupéré après l'obtention d'un premier accès

Accès « anonyme »

Démarche



Reconnaissance

- Se positionner dans le réseau (savoir où l'on se trouve)
- Comprendre l'architecture et l'organisation du système d'informations
- Localiser les actifs pertinents (serveurs, services, zones réseau, etc.)

Exploitation

- Accéder à un ordinateur du domaine
- Obtenir des identifiants de comptes (mots de passe, *hashes* ou tickets)
  - Compte de domaine
  - Compte d'administrateur

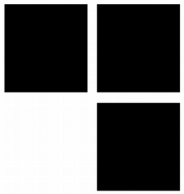
SYNACKTIV
DIGITAL SECURITY

Techniques d'intrusion Windows

Reconnaissance

Reconnaissance

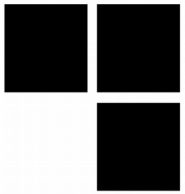
Méthodologie générale



- **Savoir où l'on est**
  - Dans quelle zone réseau ?
    - LAN utilisateur ? LAN serveur ?
- **Comprendre l'organisation du SI**
- **Localiser les actifs pertinents**
  - Services intéressants :
    - *Active Directory*
    - Partages de fichiers accessibles (SMB, FTP, NFS)
    - Bases de données (Oracle, SQL Server, etc.)
    - Services d'administration (TSE, SMB, WinRM, etc.)

Reconnaissance

Méthodologie de reconnaissance



Cartographie passive

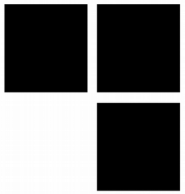
- Écoute réseau à l'aide de *sniffers* (*tcpdump, wireshark, tshark,* etc.)
- Lent mais très discret (aucun communication émanant de notre machine)
- Permet de dresser une cartographie du lien local uniquement

Cartographie active

- Utilisation des services réseau légitimes (DNS, RPC, etc.)
- Réalisation de scans réseau et scans de ports
- Efficace et relativement rapide mais bruyante :
  - Tout équipement réseau intermédiaire peut journaliser l'activité
  - Certains HIPS peuvent détecter les scans de ports et alerter l'utilisateur

Reconnaissance

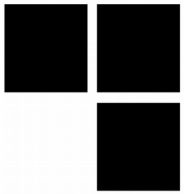
Cartographie passive



- **Écoute réseau des protocoles *broadcast***
  - ARP (requêtes *who-has*)
    - Permet d'évaluer le nombre de machine sur le LAN
    - Permet d'identifier le type des équipements via les adresses MAC
  - Résolution de noms de type *zeroconf*
    - Plusieurs types :
      - *LLMNR (Link-Local Multicast Name)*
      - NBNS (*NetBIOS Name System*)
      - mDNS (*multicast DNS*)
      - Browser Protocol
    - Permet d'obtenir des noms de machines, leur version et leurs rôles
    - Permet de connaître l'activité en cours sur les machines

Reconnaissance

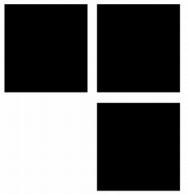
Cartographie active



- **Utilisation de services légitimes**
  - Session nulle sur les tubes RPC
  - Récupération d'informations via SMB
  - Résolution NetBIOS
  - Interrogations DNS
- **À privilégier avant toute attaque agressive (scan, etc.)**

Reconnaissance

Cartographie active / utilisation des sessions nulles



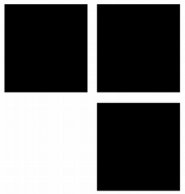
Accès RPC via une session nulle

- Sessions nulle ≃ accès non-authentifié : *rpcclient -U ‘ %’ <IP>*
- Permet d’effectuer anonymement des opérations RPC à distance
- Ne fonctionne plus par défaut depuis Windows NT 6.0 (Vista, 2008 et supérieur)
  - Parfois ré-activé pour des raisons de compatibilité
- Permet, suivant la configuration, d’accéder à certains tubes nommés :

Nom du tube	Rôle
SAMR	Gestion des comptes utilisateurs du système / domaine
LSARPC	Gestion des droits utilisateurs / informations sur les relations inter-domaine
SRVSVC	Informations sur le serveur / poste de travail (partages réseaux, sessions, ...)
WKSSVC	Informations sur le poste de travail (utilisateur connectés, nom de la machine, ...)

Reconnaissance

Cartographie active / utilisation des sessions nulles

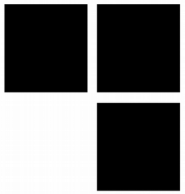


Informations intéressantes à récupérer

- Listing des partages réseaux : *netshareenumall*
- Accès au nom du domaine primaire et son SID : *lsaquery*
- Accès au rôle de la machine : *dsroledominfo*
- Accès à la politique de mot de passe du domaine : *querydominfo1*
- Accès à la politique de verrouillage des comptes : *querydominfo* 12
- Listing des utilisateurs du domaine : *enumdomusers*
- Listing des groupes du domaine : *enumdomgroups*
- Listing des groupes locaux : *enumalsgroups builtin*
- Listing des membres d'un groupe local : *queryaliasmem builtin 0x220* puis *lookupsids <SID>*
- Listing des membres d'un groupe du domaine : *querygroupmem 0x220* puis *lookupsids <SID>*
- etc

Reconnaissance

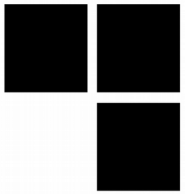
Cartographie active / utilisation des sessions nulles



- **Fortes restrictions depuis Windows 2003**
  - Énumération des utilisateurs interdite
  - Énumération des partages réseau interdite
  - Accès aux politiques de mot de passe et de verrouillage interdit
  - Accès aux informations de la machine interdit
- **Exploitation de la résolution des SID**
  - Fonctionnalité toujours accessible en session nulle
  - Fonctionne en 2 étapes :
    - Récupération du SID du domaine
    - Résolution de <*SID*>-<*RID*> par brute-force du RID

Reconnaissance

Cartographie active / utilisation des sessions nulles

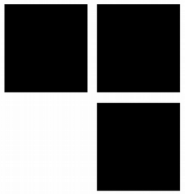


- **Session nulle inutile depuis Windows NT 6.0**
  - Énumération des utilisateurs interdite
  - **Résolution des SID interdites**
  - Énumération des partages réseau interdite
  - Accès aux politiques de mot de passe et de verrouillage interdit
  - Accès aux informations de la machine interdit
  - **Accès aux informations du domaine interdit**
- **La connaissance d'un compte permet d'accéder de nouveau à toutes ces fonctionnalités**

```
$ rpcclient -U '<login>%<password>' <IP>
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[krbtgt] rid:[0x1f6]
user:[userad1] rid:[0x451]
[...]
```

Reconnaissance

Cartographie active / session nulle sur SMB



SMB permet également les sessions nulles

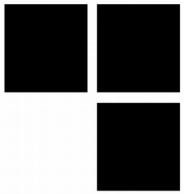
- Récupération de la version du système
  - Fuite de la version lors de la phase d'authentification
  - Exploitable même si les sessions nulles sont interdites
  - Située dans le paquet SMB *Setup Andx Response*

```
    8 1…  10.77.77.1          10.77.77.210         SMB       226 Session Setup AndX Request, NTLMSSP_NEGOTIATE
    9 1…  10.77.77.210        10.77.77.1           SMB       491 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

▸ Frame 9: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface 0
▸ Ethernet II, Src: RealtekU_e6:0d:37 (52:54:00:e6:0d:37), Dst: RealtekU_56:38:3f (52:54:00:56:38:3f)
▸ Internet Protocol Version 4, Src: 10.77.77.210, Dst: 10.77.77.1
▸ Transmission Control Protocol, Src Port: 445 (445), Dst Port: 58106 (58106), Seq: 210, Ack: 355, Len: 425
▸ NetBIOS Session Service
▾ SMB (Server Message Block Protocol)
  ▸ SMB Header
  ▾ Session Setup AndX Response (0x73)
      Word Count (WCT): 4
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 421
    ▸ Action: 0x0000
      Security Blob Length: 262
      Byte Count (BCC): 378
    ▸ Security Blob: a1820102308...6010401823702...
      Native OS: Windows 10 Enterprise N 10240
      Native LAN Manager: Windows 10 Enterprise N 6.3
```

Reconnaissance

Cartographie active / interrogations DNS



Tenter des résolutions inverses sur les IP connues

- Permet d'obtenir le nom de la machine associée à l'adresse IP
- Le nom reflète très souvent le rôle de la machine (*srvdb1, srvdata, wk1023*, etc.)
- Utilitaire *host* sous UNIX

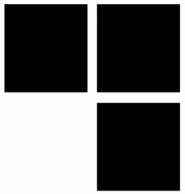
Tenter un transfert de zone

- Parfois autorisé en interne (même si désactivé par défaut)
- Permet d'obtenir la totalité des noms associés à une zone DNS

```
$ dig @<IP_DNS> axfr my.dns.zone
```

Reconnaissance

Cartographie active / interrogations DNS



Localiser les contrôleurs de domaine

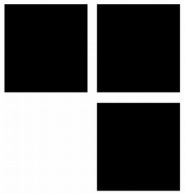
- Utilisation du mécanisme utilisé par les machines Windows pour trouver les AD
- Consiste à une résolution sur l'enregistrement SRV *_ldap._tcp.dc._msdcs.<domain>*

```
$ nslookup -type=SRV _ldap._tcp.dc._msdcs.corp.local
Server:  <DNS>
Address:  <DNS_IP>

_ldap._tcp.dc._msdcs.<domain>   SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = AD.corp.local
AD.corp.contoso.com        internet address = <AD_IP>
```

Reconnaissance

Cartographie active / NetBIOS Name Service (NBNS)



NetBIOS Name Service

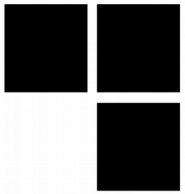
- Protocole historique utilisé par Microsoft pour la résolution de noms
- Utilise le port 137/UDP
- Similaire au protocole ARP
  - Réception d'une requête NBNS
  - Analyse de la requête (est-ce que cela me concerne ?)
  - Si oui, envoi de mon nom NetBIOS ou bien mon adresse IP
- Sous Linux, l'outil *ntbscan* peut être utilisé pour faire des requêtes NBNS *unicast*

```
$ nbtscan 192.168.122.0/24
Doing NBT name scan for addresses from 192.168.122.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.122.118  AD-01            <server>  <unknown>        52:54:00:e3:ad:8b
192.168.122.193  WKS-01           <server>  <unknown>        52:54:00:1c:a1:da
```

Reconnaissance

Cartographie active / scans de l'environnement



Identifier une machine Windows sur le réseau

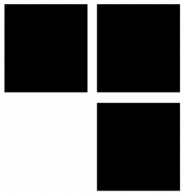
- Portmapper MS-RPC : 135/TCP
- Service NBNS : 137/TCP
- Services de transport NetBIOS : 138/UDP et 139/TCP
- SMB/CIFS : 445/TCP
- Terminal Server : 3389/TCP

Identifier le rôle d'une machine

- Contrôleur de domaine : 389/TCP (LDAP), 53/TCP (DNS), 88/TCP (KDC Kerberos)
- Serveur MS-SQL : 1433/TCP, 1434/UDP
- Serveur applicatif web : 80/TCP, 443/TCP, 8080/TCP, 8443/TCP, ...

Reconnaissance

Cartographie active / scans de l'environnement



Démarche

- Chercher les machines en fonctionnement et accessibles
  - Réaliser un *ping scan* (plus discret qu'un scan de ports)
  - Attention *nmap* réalise plus qu'un simple *ping* (scan des ports 80, etc.)

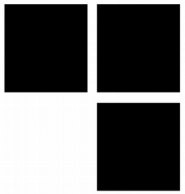
```
# nmap -vvv -sP 10.77.77.0/24
Nmap scan report for 10.77.77.80
Host is up, received arp-response (0.00062s latency).
MAC Address: 52:54:00:07:82:26 (QEMU virtual NIC)
[...]
Nmap scan report for 10.77.77.210
Host is up, received arp-response (0.00037s latency).
MAC Address: 52:54:00:E6:0D:37 (QEMU virtual NIC)
[...]
```

  - Une simple boucle permet de faire un véritable *ping scan* (plus lent)

- Chercher des services sur ces machines (scan de ports/services)

Reconnaissance

Cartographie active / scans de l'environnement

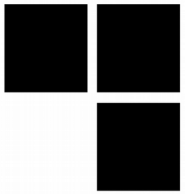


Autres outils de découverte souvent utilisés

- Masscan
  - Conçu pour scanner un faible nombre de ports sur une large plage d'adresses IP
  - Très rapide (attention aux dénis de service)
- Hping
  - Vérifier l'ouverture d'un port
- Traceroute, Firewalk
  - Découverte de la topologie du réseau
  - Découverte des équipements intermédiaires
- Netcat / openssl client
  - Pour ouvrir une *socket* brute vers un port afin de communiquer avec un service

Reconnaissance

Identifier les services intéressants



- **Services connus pour avoir des comptes par défaut**
  - MS-SQL (port 1433/TCP) :
    - sa:sa *ou* sa:<vide>
  - Oracle (port 1521/TCP)
  - Une quantité importante de services web en tous genres
    - admin:admin ou admin:password ...
- **Services ciblés par des exploits publiques**
  - Certaines versions de service peuvent être vulnérables
  - Il est important d'identifier les versions des services
    - Pour vérifier si des exploits publiques existent
- **Partages SMB accessibles en anonyme**