Techniques et outils de piratage

Reconnaissance : Énumération

Comprendre les attaques pour mieux se défendre

Mohamed Mejri

Université Laval

October 13, 2016

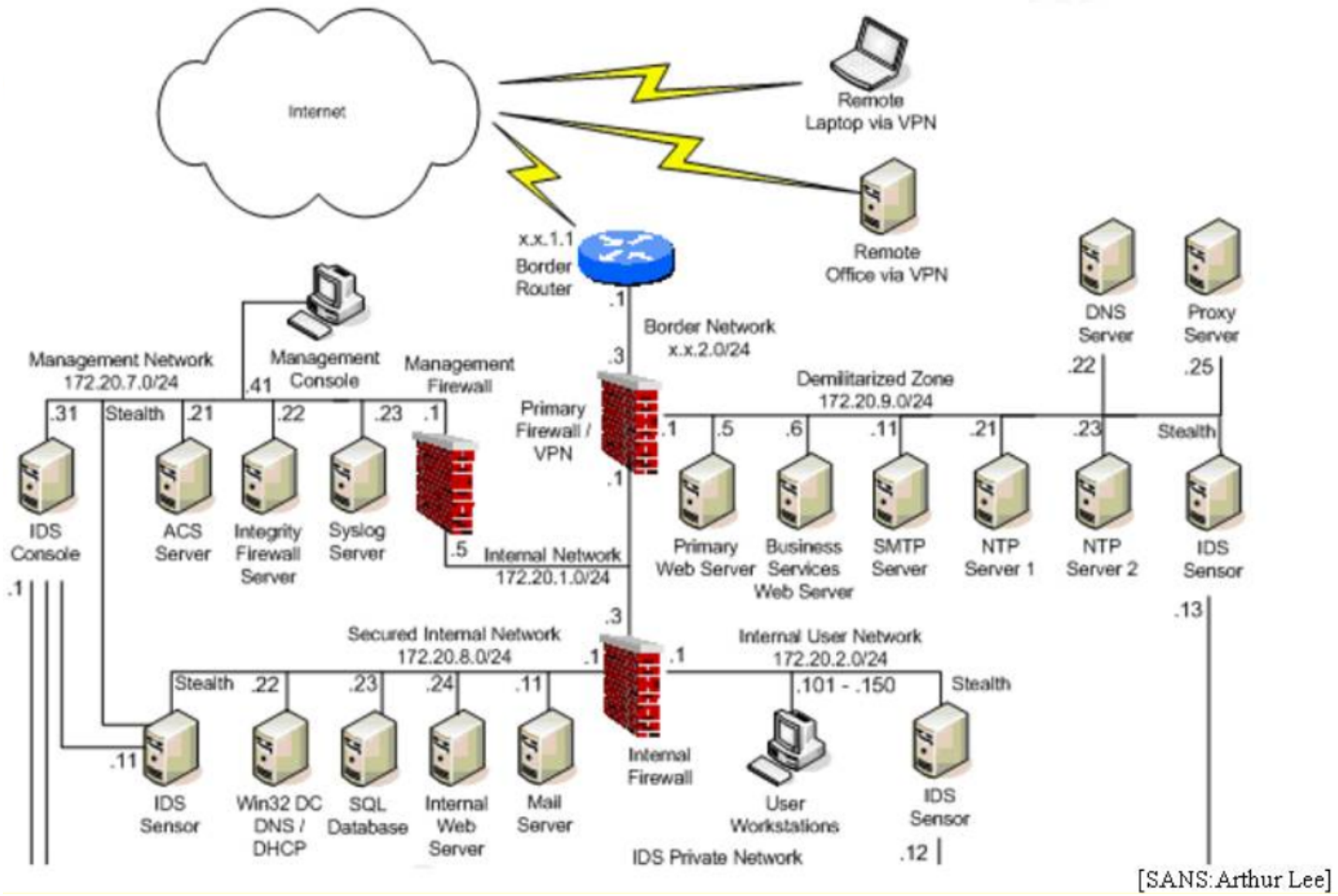
Plan

Introduction

- Le scanning permet de déterminer les machines actives et les ports actifs et le systèmes d'exploitation
- L'énumération pousse l'enquête sur les ports ouverts pour déterminer les noms des services actifs, leurs versions, les noms des utilisateurs ayant accès à ces services, leurs rôles, leurs groupes, les noms des machines, leurs rôles, les versions de système d'exploitation, les partages, les politiques de mots de passe, etc.
- L'énumération est généralement plus intrusive que le scan : plus de connexions actives et de requêtes directes
- Cette activité est généralement détectée et elle est souvent enregistrée dans les fichiers logs de la cible
- Elle est généralement fortement liée au système d'exploitation de la cible
- Elle nécessite une bonne maitrise des services pour pouvoir leur soutirer le maximum d'informations
- Au lieu de se contenter d'ouvrir une connexion, on va aussi faire appel aux commandes du protocole lié au service

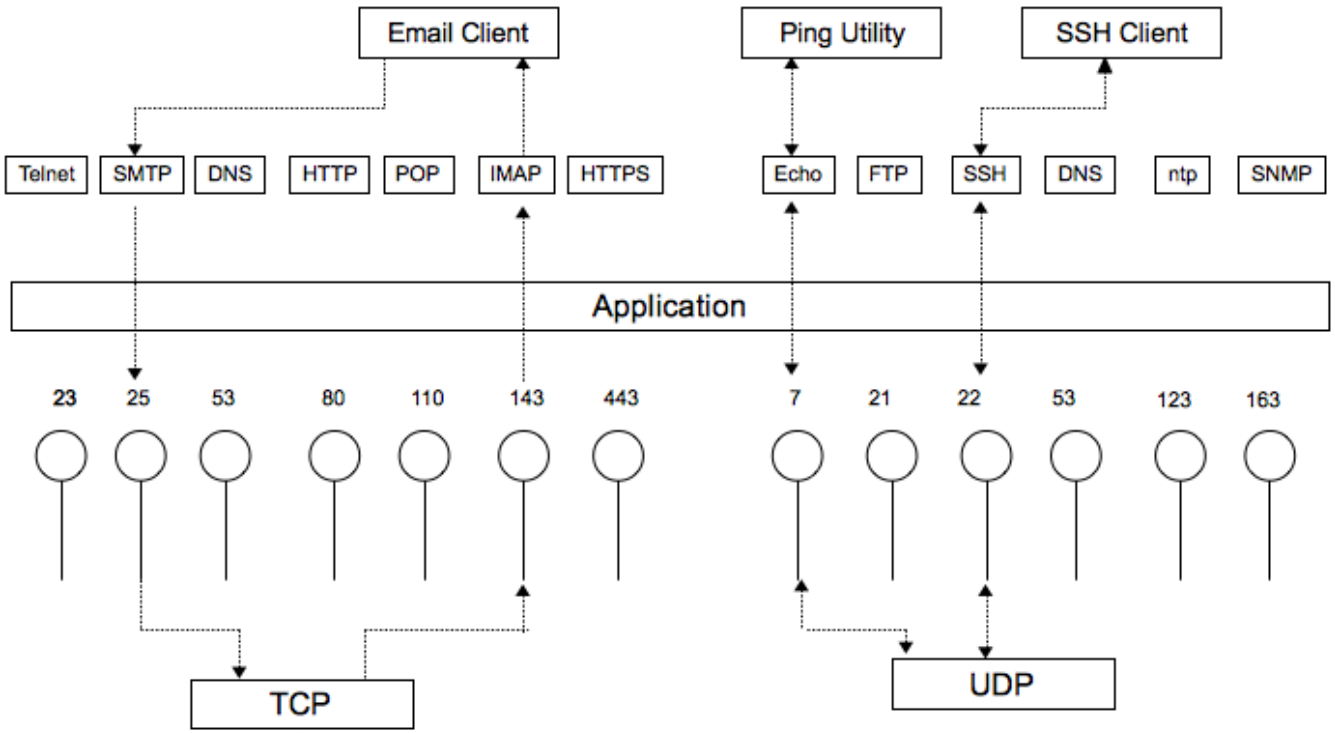
Introduction

Quelques services classiques



Introduction

Quelques services classiques et leurs ports associés



Introduction

Objectifs :

Déterminer, entre autres, les

- noms des utilisateurs (User ID)/groupe/politiques de mots de passe : très utile pour des attaques par dictionnaire.
- noms des machines et leurs rôles : certaines machines ont des rôles critiques comme les contrôleurs de domaines.
- ressources réseau : les routeurs, les concentrateurs, protocoles de routage, etc. Un concentrateur nous permet de sniffer le réseau.
- ressources partagées et mal configurées : par exemple des fichiers partagés d'une manière non sécuritaire
- services (service vs port), les applications et leurs versions : vieilles versions de logiciels connus par des failles de sécurité : par exemple un serveur web avec une faille de débordement de tampon à distance.
- fichiers d'audit : certains fichiers log donnent beaucoup d'informations sur les applications installées comme leurs versions.

Analyse de bannières

- Il s'agit de "faire parler" une application distante et d'analyser ses sorties
- C'est la technique la plus fondamentale dans l'étape d'énumération.
- Elle est très informative.
- Beaucoup d'outils de scan supportent cette fonctionnalité

Remarque : Avec "`nmap`" et "`namp -sV`" on risque d'avoir deux résultats différents

- `nmap` se base sur le numéro du port pour donner le nom de service
- `namp -sV` se base sur l'analyse de bannières pour trouver le nom et la version du service
- Puisqu'on peut faire tourner n'importe quel service sur n'importe quel port, donc `namp -sV` est plus fiable

Analyse de bannières

telnet et *netcat*

- `telnet` est un service implanté dans la quasi-totalité des systèmes d'exploitation
- L'idée est simple :
  - ouvrir une connexion Telnet avec le serveur cible sur un port choisi
  - puis, taper plusieurs fois sur `ENTER`

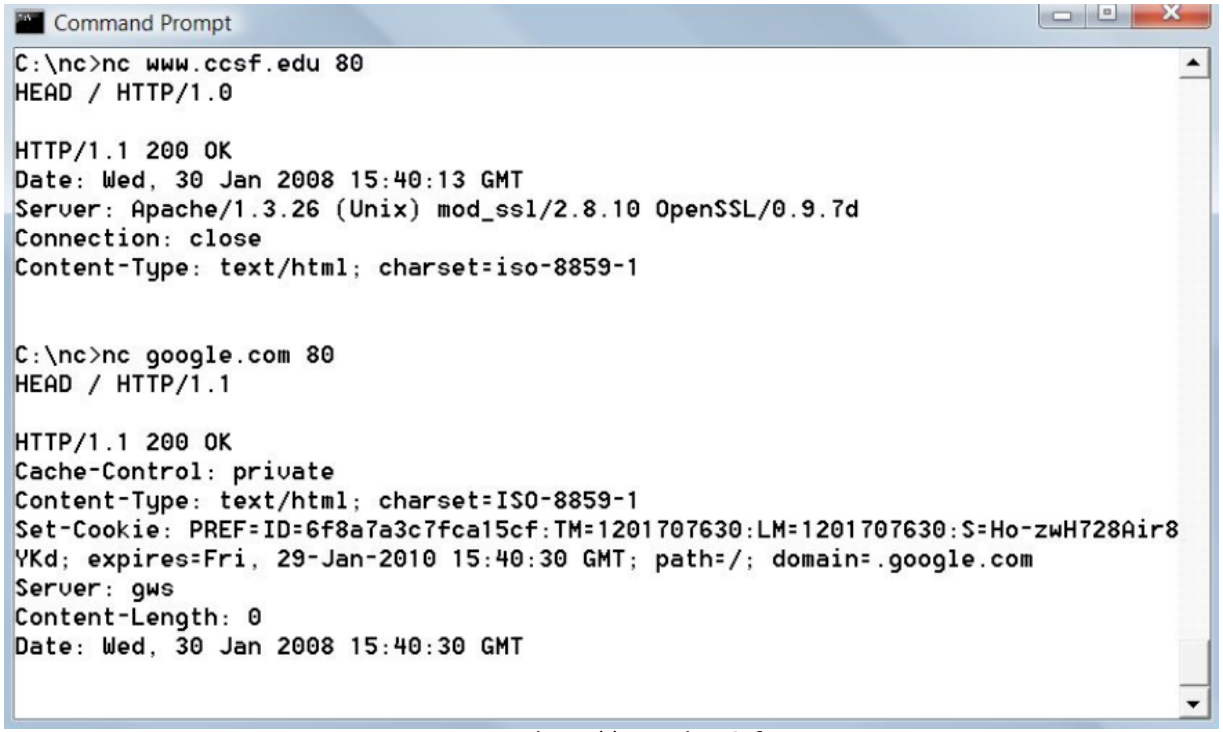
```
C:\> telnet www.exemple.com 80

HTTP/1.1 400 Bad request
Server:  Microsoft-IIS/5.0
Date:  Tue, 10 Jul 2009 23:10:19 GMT
Content-Type:  text/html
Content-Lenght:  87

<html><head><title> Error</title>
</head><body>The parameter is incorrect.  </body>
</html>
```

  - connaitre n'importe quel exploit contre Microsoft-IIS/5.0 permet de lancer une attaque!

Analyse de bannières

telnet et *netcat*

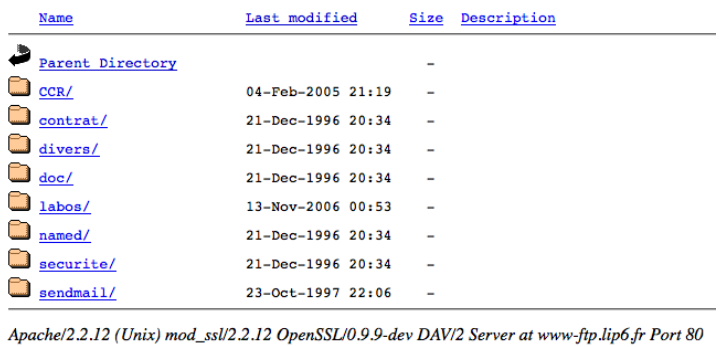
- L'idée fonctionne avec la plupart des applications ayant des ports standards : HTTP 80, SMTP 25, FTP 21
- `netcat` est un outil flexible et puissant qui peut faire le travail



source : http://samsclass.info

Énumération de FTP (port TCP 21)

- FTP (File Transfert Protocol) est aujourd'hui obsolète (mot de passe en claire), mais son énumération est souvent rentable
- Plusieurs serveurs web utilisent encore FTP pour télécharger des contenus web. Cela ouvre également le chemin pour placer des codes exécutables malicieux.
- Plusieurs serveurs FTP sont disponibles sur Internet pour partager des fichiers. Chercher (google) : "Index of ftp://"



Name	Last modified	Size	Description
Parent Directory		-	
CCR/	04-Feb-2005 21:19	-	
contrat/	21-Dec-1996 20:34	-	
divers/	21-Dec-1996 20:34	-	
doc/	21-Dec-1996 20:34	-	
labos/	13-Nov-2006 00:53	-	
named/	21-Dec-1996 20:34	-	
securite/	21-Dec-1996 20:34	-	
sendmail/	23-Oct-1997 22:06	-	

Apache/2.2.12 (Unix) mod_ssl/2.2.12 OpenSSL/0.9.9-dev DAV/2 Server at www-ftp.lip6.fr Port 80

- **Énumération :** Déterminer la version des services, des noms d'utilisateurs valides, voir si la connexion anonyme est permise, voir quels sont les répertoires accessibles en lecture et écriture, récupérer des fichiers, placer des fichiers, etc.

Énumération de SMTP (TCP 25 (sans chiffrement)/TCP 587 (avec chiffrement)/ TCP 465 (SSL))

- SMTP (Simple Mail Transport Protocol) : permet de transférer des courriels vers des serveurs de messagerie électronique.

```
telnet smtp.xxxx.xxxx 25
Connected to smtp.xxxx.xxxx.
220 smtp.xxxx.xxxx SMTP Ready
EHLO client
250-smtp.xxxx.xxxx
250-PIPELINING
250 8BITMIME
MAIL FROM: <auteur@yyyy.yyyy>
250 Sender ok
RCPT TO: <destinataire@xxxx.xxxx>
250 Recipient ok.
DATA
354 Enter mail, end with "." on a line by itself
Subject: Test
.
250 Ok
QUIT
221 Closing connection
Connection closed by foreign host.
```

source : http://fr.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Énumération de SMTP (TCP 25)

- **Énumération :** trouver le nom et la version du service, chercher des adresses courriel valides, vérifier si le serveur fait le relais de messages, trouver le nom et la version de l'antivirus utilisé par le serveur (aide à envoyer des courriels infectés), etc.
- **Nom et version de l'antivirus :** Une des chose à faire et d'envoyer un fichier exécutable non malicieux (ex. calc.exe) en espérant que le serveur nous retourne un message qui dit que ce genre de fichier n'est pas accepté tout en indiquant le nom et la version du l'antivirus utilisé dans le serveur.
- **Remarque :** Un site où vous pouvez tester si un d'un antivirus peut détecter votre code malicieux : www.virustotal.com

Énumération de SMTP (TCP 25)

- **Énumération de comptes :** Envoyer des courriels à une liste de noms prise d'un dictionnaire et voir la réaction du serveur. Ces deux commandes peuvent être utiles:
  - `VRFY` : permet de confirmer si un nom est valide
  - `EXPN` : révèle les adresses de livraisons des aléas et des listes de diffusions

```
------------------------------------------------------------

            Example of Verifying a User Name

   Either

      S: VRFY Smith
      R: 250 Fred Smith <Smith@USC-ISIF.ARPA>

   Or

      S: VRFY Smith
      R: 251 User not local; will forward to <Smith@USC-ISIQ.ARPA>

   Or

      S: VRFY Jones
      R: 550 String does not match anything.

   Or

      S: VRFY Jones
      R: 551 User not local; please try <Jones@USC-ISIQ.ARPA>

   Or

      S: VRFY Gourzenkyinplatz
      R: 553 User ambiguous.

                        Example 3

------------------------------------------------------------
```

source : http://james.apache.org/server/rfclist/smtp/rfc0821.txt

- Pour accélérer le travail, l'outil *vrfy.pl* prend en entrée un fichier qui contient le nom de serveur et une liste de noms à vérifier et retourne les noms valides

Énumération de SMTP (TCP 25)

- **Relai :** Vérifier si un serveur SMTP fait le relai
  Exemple : Envoyer *spam_me@hotmail.com* à travers *mail.example.org*

Réponse positive	Réponse négative
$ telnet mail.example.org 25 Trying 192.168.0.25... Connected to 192.168.0.25. Escape character is '^]'. 220 mail.example.org Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready at Sun, 5 Oct 2003 18:50:59 +0100 **HELO** 250 mail.example.org Hello [192.168.0.1] **MAIL FROM: spammer@spam.com** 250 2.1.0 spammer@spam.com....Sender OK **RCPT TO: spam_me@hotmail.com** 250 2.1.5 *spam_me@hotmail.com* **DATA** 354 Start mail input; end with <CRLF>.<CRLF> **This is a spam test!** . 250 2.6.0 <MAIL7jFOR3rfWX300000001@mail.example.org> Queued mail for delivery **QUIT** *source : Network Security Assessment (livre)*	**RCPT TO: spam_me@hotmail.com** 550 5.7.1 Unable to relay for spam_me@hotmail.com

- Si le relai est permis, un pirate peut se passer pour n'importe qu'elle employer (boss) pour envoyer des courriels à d'autres personnes
- Si votre serveur SMTP devient un générateur de SPAM, il y a un grand risque de voir votre serveur courriel dans des listes noires. Vos clients ne recevront pas vos courriels
- Il y a même un risque d'avoir tout votre réseau dans des listes noires

Énumération de SMTP (TCP 25)

Voir la possibilité d'avoir un MITM pour SMTP: analyser le domaine du serveur du courriels et voir les erreurs probables: oublier un point, deux "m" deux "t", un "s", une tiré, etc.

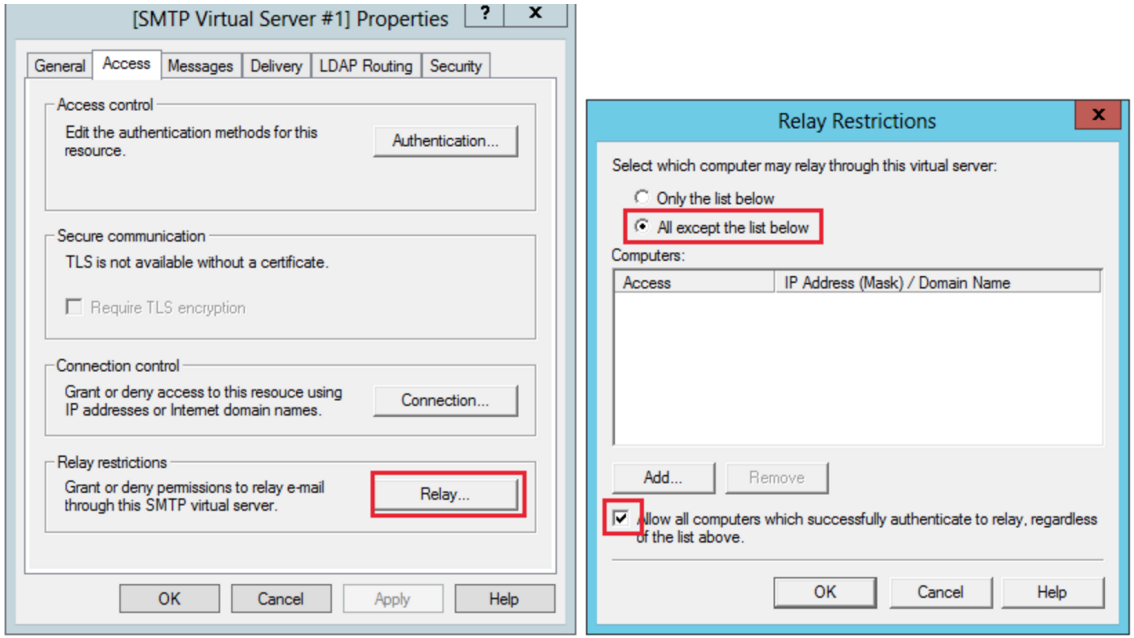
Exemple

- voir si les adresses courriel sont associées à un sous domaine. Exemple : bob@email.test.com, bob@uk.test.com
- Plus tard durant la phase d'attaque, on peut cibler les utilisateurs qui oublient le premier point : bob@emailtest.com, bob@uktest.com
  - acheter ses domaines d'erreurs (exemple emailtest.com, uktest.com)
  - installer un serveur courriel pour ces sous domaines
  - configurer le serveur smtp pour que tout message reçu sera relayer à la bonne adresse tout en changer l'adresse source avec le faut domaine pour recevoir la réponse et la relayer de nouveau
  - c'est un MITM pour le SMTP
  - le principe est applicable pour d'autres services (http, dns, etc.)

Énumération de SMTP (TCP 25)

Contre mesures

- Désactiver les commandes VRFY et EXPN ou les restreindre à des utilisateurs authentifiés
- Désactiver le relai



source :

http://business.plumchoice.com//techtips/wp-content/uploads/2013/11/13-1127_5.png

Énumération de DNS (TCP/UDP 53)

- L'emplacements de services importants peuvent être découverts via des enregistrements de type SRV

```
[root$] dig @192.168.152.10 exemple.org axfr
; «» DiG 9.3.2 «» @192.168.152.10 exemple.org axfr
;(1 server found)
;; global options:  printcmd
  exemple.org    86400    IN    SOA    corp-de.exemple.org admin
  exemple.org    86400    IN    A      192.168.152.10
  exemple.org    86400    IN    NS     corp-de.exemple.org
...
  _kerberos._tcp    86400    IN    SRV    0 100 88 corp-de.exemple.org
  _ldap._tcp        86400    IN    SRV    0 100 389 corp-de.exmple.org
;; Query time:  500 msec
;; SERVER: 192.168.152.10#53(192.168.152.10)
;; WHEN: Tue Sep 5 02:57:55 2009
;; XFR size:  42 records (message 1)
```

Énumération de DNS (TCP/UDP 53)

- BIND (serveur DNS pour UNIX) contient un enregistrement de la classe "CHOAS" donnant sa version dans une ligne commençant par `version.bind`

```
[root$] dig @192.168.112.17 version.bind txt choas
; «» DiG 9.3.2 «» @192.168.112.17 version.bind txt choas
;; ANSWER SECTION:
  VERSION.BIND    0S    CHAOS    TXT    "8.2.4"
```

Vulnerability	CVE reference	BIND versions affected
SIG overflow	CVE-2002-1219	4.9.5–4.9.10, 8.1, 8.2–8.2.6, and 8.3–8.3.3
NXDOMAIN overflow	CVE-2002-1220	8.2–8.2.6 and 8.3–8.3.3
libresolv overflow	CVE-2002-0029	4.9.2–4.9.10
OpenSSL overflow	CVE-2002-0656	9.1.0 and 9.2.x if built with SSL
libbind overflow	CVE-2002-0651	4–4.9.9, 8–8.2.6, 8.3.0–8.3.2, and 9.2.0
TSIG overflow	CVE-2001-0010	8.2, 8.2.1, 8.2.2 patch levels 1–7, and 8.2.3 beta releases
`nslookupcomplain( )` format string bug	CVE-2001-0013	4.9.3–4.9.5 patch level 1, 4.9.6, and 4.9.7
NXT record overflow	CVE-1999-0833	8.2, 8.2 patch level 1, and 8.2.1

source : Network Security Assesment (livre)

- Vérifier si le serveur DNS est ouvert au public et déterminer son meilleur tau d'amplification (utile pour lutter contre les DDOS)

Énumération de TFTP (TCP/UDP 69)

- TFTP (Trivial File Transport Protocol) : Un transfert de fichier simple, mais complètement non sécuritaire (ni chiffrement ni authentification)
- Il faut connaître à priori les noms de fichiers à télécharger ainsi que leurs emplacements
- Permet à un pirate de récupérer des fichiers importants comme `/etc/passwd`

```
[root$ ] tftp 192.168.112.17
tftp>connect to 192.168.112.17
ftp> get /etc/passwd
ftp> quit
```

- Utilisé aussi par des administrateurs pour configurer des équipements réseaux (switch, routeur, concentrateur VPN, etc.) en les considérant comme des serveurs TFTP
- Un attaquant peut, entre autres, aller chercher des fichiers importants (running-config, startup-config, .config, config, run) sur ces équipements

Énumération de HTTP (TCP 80)

- Quel serveur est utilisé et quelle est sa version?
- Le site fait-il appel à des bases de données?
- Le site web est statique ou dynamique?
- Quelles sont les variables utilisées?
- Est-ce qu'il y a des formulaires et quels sont leurs champs?
- Le serveur envoie t-il des cookies?
- Le site fait-il appel à du JavaScript?
- Quelles sont les pages qui demandent une authentification?
- Quelles sont les pages qui permettent de créer un compte ou de modifier un mot de passe?
- Est ce que le site permet de déposer des messages ou des fichiers?
- Quelles sont les adresses courriel qui se trouvent sur le site web?
- Etc.

Énumération de SNMP (UDP 161/162)

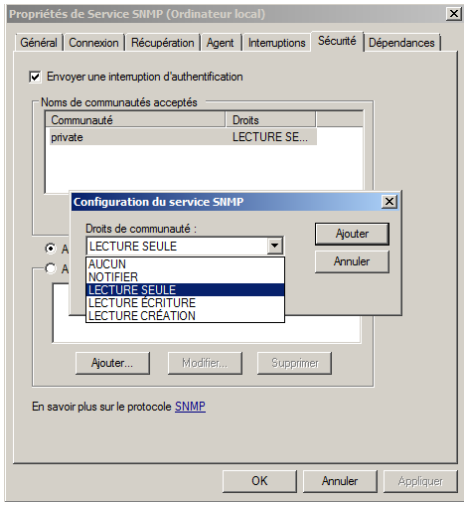
- SNMP (Simple Network Management Protocol) : les motivations de la création de ce protocole sont :
  - Nécessité d'avoir un protocole permettant de remonter des informations sur les activités des différentes ressources du réseau : serveurs, routeurs, switchs, PC, etc.
  - Nécessité de pouvoir envoyer des informations (e.g. de configuration) à différentes ressources du réseau
- Pour ce faire, SNMP offre 3 opérations simples :
  - GET (161): Permet à la station d'administration de retirer les valeurs d'un objet de la station administrée.
  - SET (161): Permet à la station d'administration d'affecter des valeurs à un objet dans la station administrée.
  - TRAP (162): Permet à une station administrée d'envoyer des notifications à la station d'administration pour les événements significatifs. Une composante d'un système d'alarme peut l'utiliser pour envoyer des TRAP suite à certains événements

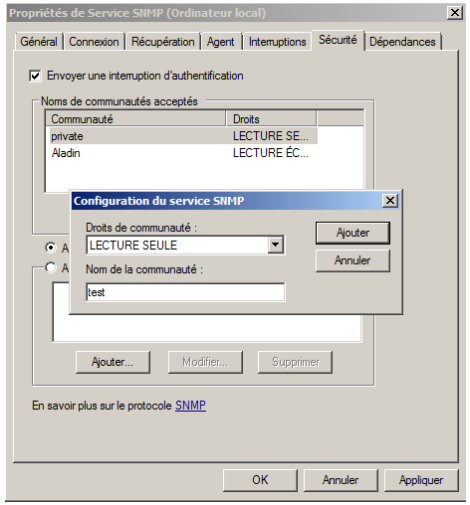
Énumération de SNMP (UDP 161/162)

- Les objets administrés sont une abstraction des ressources physiques (interfaces, équipements, etc.) et logiques (connexions TCP, paquets IP, etc.).
- Les données des objets administrés sont stockées dans une base de données appelée MIB (Management Information Base) : un arbre ayant une structure standardisée (ressemble à la structure des registres sous Windows)
- Chaque nœud contrôlé dans le système maintient un MIB
- Parmi les données disponibles via l'énumération SMNP :
  - les services actifs,
  - les noms des utilisateurs (*username*)
  - les domaines des utilisateurs
  - des informations sur le partage
  - les processus en cours d'exécution
  - des adresses IP

Énumération de SNMP (UDP 161/162)

- SNMP V1 (1980) : faible sécurité : communauté (mot de passe) circule en clair. Communautés par défaut : *private* (read/write) et *public* (read)

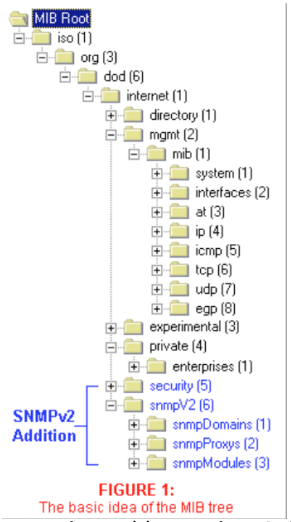




- SNMP V2(1993) : amélioration de la version 1 (performance, sécurité), mais la sécurisé est complexe; (non adopté)
- SNMP V2C(1996) : même chose que la version 2, mais une sécurité simplifié (utilisation de communauté comme la version 1)
- SNMP V3(1999) : Renforcement de la sécurisé (authentification + chiffrement) de la version 2;

Énumération de SNMP (UDP 161/162)

- Chaque donnée dans le MIB a une adresse (Object IDentifier : OID) : en mode texte ou en mode numérique (comme @IP vs nom de domaine)
  - .iso.org.dod.internet.mgmt.mib-2.system.sysDescr en mode texte ;
  - .1.3.6.1.2.1.1.1 en mode numérique.



source : http://samsclass.info

- Des outils comme `snmputil`, *snmpget* ou *snmpwalk* permettent d'accéder aux objets d'un MIB

Énumération de SNMP (UDP 161/162)

- snmputil

```
C:\>snmputil get 127.0.0.1 public  .1.3.6.1.4.1.311.1.7.3.1.6.0
```

  - `127.0.0.1` : l'@ IP de la cible
  - `public` : mot de passe
  - `.1.3.6.1.4.1.311.1.7.3.1.6.0` : OID (Object Identifier) qui est l'adresse de l'information demandée dans le MIB.

- snmpset : modifier le contenu d'un objet

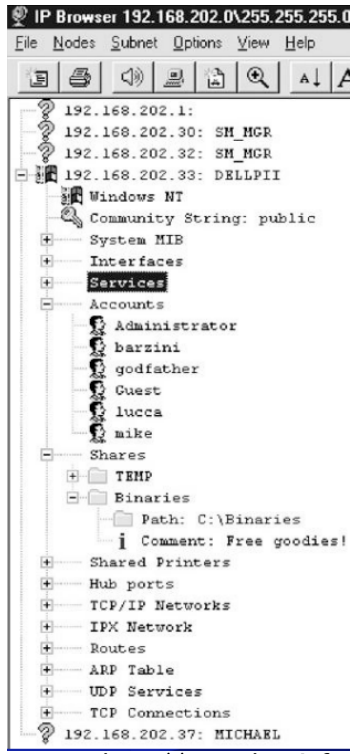
```
snmpset [options...] <hostname> {<community>} [<objectID> <type> <value> ...]
```

- snmpwalk : afficher les valeurs des objets d'un sous arbre au complet de la base MIB à partir d'un nœud donné

```
snmpwalk [options...] <hostname> {<community>} [<objectID>]
```

Énumération de SNMP (UDP 161/162)

- Ils existent des outils intéressants avec interfaces graphiques :
  - SolarWinds



source : http://samsclass.info

Énumération de SNMP (UDP 161/162)

- Quelques vulnérabilités spécifiques

CVE reference	Date	Notes
CVE-2007-1257	28/02/2007	Cisco Catalyst 6000, 6500, and 7600, and IOS 12.2 *Network Analysis Module* (NAM) SNMP spoofing vulnerability
CVE-2006-5583	12/12/2006	Microsoft Windows 2000 SP4, XP SP2, and 2003 SP1 SNMP buffer overflow resulting in command execution
CVE-2006-5382	25/10/2006	3Com SS3 4400 switch SNMP information disclosure
CVE-2006-4950	20/09/2006	Cisco IOS 12.2-12.4 hard-coded DOCSIS community string device compromise
CVE-2005-2988	15/09/2006	HP JetDirect information disclosure
CVE-2005-1179	15/04/2005	Xerox MicroServer SNMP authentication bypass
CVE-2005-0834	18/03/2005	Multiple Belkin 54G wireless router SNMP vulnerabilities
CVE-2004-0616	22/06/2004	BT Voyager wireless ADSL router default community string and administrative password compromise
CVE-2004-0312	17/02/2004	Linksys WAP55AG 1.07 SNMP compromise
CVE-2004-0311	16/02/2004	APC SmartSlot 3.21 and prior default SNMP community string device compromise
CVE-2002-1048	16/09/2002	HP JetDirect password disclosure over SNMP
CVE-2004-1775	16/06/2002	Cisco IOS 12.0 and 12.1 VACM device configuration compromise
CVE-2002-0013	12/02/2002	Multiple vulnerabilities in SNMPv1 request handling
CVE-2001-0236	15/03/2001	Solaris SNMP to DMI mapper daemon (`snmpXdmid`) buffer overflow

(Source : Network Security Assessment)

- Des exploits liés à ces vulnérabilités sont disponibles à : http://www.packetstormsecurity.org

Énumération des services réseaux Windows

Windows serveur 2000, 2003, 2008, 2012 : un système d'exploitation avec plusieurs services prêts à installer et faciles à configurer

- Contrôleur de domaine + Active Directory
- Serveur DNS
- Serveur DHCP
- Serveur VPN
- Serveur SNMP
- Serveur de Courriel (Exchange Server)
- Serveur Web (Microsoft IIS)
- Serveur SQL
- Un pare-feux (ISA)
- Etc.

Énumération de services réseaux Windows TCP 135, UDP 135, UDP 137, UDP 138, TCP 139, TCP, 593, TCP 445, UDP 5535)

Port	Service
TCP 135	Microsoft RPC Endpoint Mapper sur TCP
UDP135	Microsoft RPC Endpoint Mapper sur UDP
UDP137	NetBIOS Name services (nbns)
UDP138	Service Datagramme (nbdgm)
UDP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP 445	SMB over TCP
TCP 593	Microsoft RPC Endpoint Mapper sur HTTP
UDP 5355	Link Local Multicast Name Resolution (LLMNR)

Résolution de noms chez Windows

Dans l'ordre, on a

- Domain Name System (DNS)
  - DNS Resolver Cache (Host File : ajouté automatiquement au cache au démarrage et après toute modification)
  - DNS Server
- Link Local Multicast Name Resolution (LLMNR, port 5355/udp) : utilisé à partir de Windows Vista (Vista, Wndoiws 7, Server 2008)
  - LLMNR cache
  - Multicast (FF02::1:3) (224.0.0.252)
- NetBIOS : utilise WINS Server, LMHost File et Broadcast dépendamment de la configuration de la machine
  - Broadcast (b-node) : utilise le Broadcast seulement
  - Point-to-point (p-node) : utilise le serveur WINS
  - Mixed (m-node) : Brodcast ensuite WINS
  - Hybrid (h-node) : WINS ensuite Brodcast

Énumération des services réseaux Windows (TCP 135, UDP 135, UDP 137, UDP 138, TCP 139, TCP, 593, TCP 445, UDP 5535)

Link Local Multicast Name Resolution (LLMNR, port 5355/udp)

- Installer un serveur DNS et le gérer n'est ni à la portée de tout le monde ni approprié pour toutes les situations
- Installer un serveur WINS : n'est pas toujours pratique et ne supporte que le IPv4
- Pour un réseau ad hoc, on a besoin d'une solution simple (*plug and play*), dynamique (les machines et leurs noms peuvent changer constamment) qu'on peut rapidement mettre en place
- Idée : Via une adresse Mutilcast, on envoie des requêtes de résolution de noms
- La machine qui a le nom en question répond
- Pour permettre à une machine de s'inscrire à ce service, il faut activer l'option "Network Discovery"

Énumération des services réseaux Windows : noms NetBIOS, (UDP 137, UDP 138)

Les noms NetBIOS (en cours de disparation) : Quoi

- Un nom NetBIOS contient 16 caractères
  - 15 premiers caractères identifient le nom d'une machine, le nom d'un groupe, le nom d'un domaine, etc.
  - le numéro 16 identifie le rôle de la machine, les services qu'elle héberge, etc.
    - <nom_machine> <00>, type U (Unique) : identifie une machine
    - <nom_domaine> <00>, type G (Groupe) : identifie un groupe ou un domaine
    - <nom_machine><20>, partage smb
    - <nom_machine><06>, serveur d'accès distant (RAS)
    - <nom_domaine><1C>, la machine qui envoi ce type d'information est un Contrôleur du domaine "nom_domaine"
    - <nom_domaine><1D>, serveur WINS pour "nom_domaine"
    - <nom_machine><03>, utilisateur connecté localement
    - Etc.

Énumération des services réseaux Windows : noms NetBIOS, (UDP 137, UDP 138)

Noms NetBIOS : Énumération

- Objectif : Connaitre les noms des domaines, les noms des machines, les utilisateurs connectés sur une machine <03>, les partages, les rôles des machines et les autres services, etc.
- Outils : nbtstat, net config, net view, etc.
  - *nbtstat* : gestion de noms NetBios locaux (option -n) et à distance (option -a, -A)

```
C:\Users\momej>nbtstat -n

Connexion au réseau local:
Adresse IP du noeud : [192.168.1.10] ID d'étendue : []

              Table nom local NetBIOS

    Nom                    Type         Statut
---------------------------------------------
    WIN-RN11D4F8JJU<00>  UNIQUE       Inscrit
    WORKGROUP      <00>  Groupe       Inscrit
    WIN-RN11D4F8JJU<20>  UNIQUE       Inscrit
```

```
C:\Users\momej>nbtstat -A 192.168.1.4

Connexion au réseau local:
Adresse IP du noeud : [192.168.1.10] ID d'étendue : []

    Table de noms NetBIOS des ordinateurs distants

    Nom                    Type         État
---------------------------------------------
    USAGER-CROENK8M<00>  UNIQUE       Inscrit
    USAGER-CROENK8M<20>  UNIQUE       Inscrit
    MSHOME         <00>  Groupe       Inscrit
    MSHOME         <1E>  Groupe       Inscrit
    MSHOME         <1D>  UNIQUE       Inscrit
    ..__MSBROWSE__.<01>  Groupe       Inscrit
    USAGER-CROENK8M<03>  UNIQUE       Inscrit
    ADMINISTRATEUR <03>  UNIQUE       Inscrit

    Adresse MAC = 00-0C-29-74-91-20
```

Énumération des services réseaux Windows : noms NetBIOS, (UDP 137, UDP 138)

Noms NetBIOS : Énumération

- *net view* : énumérer un domaine et les machines dans un domaine

Énumération des services réseaux Windows : SMB (TCP 139/445)

SMB : Concept

- Protocole client-serveur : client accède à des ressources mises à sa disposition par le serveur
- Partages :
  - Partage de fichiers
  - Partage d'imprimantes
  - Partage spécial : IPC$
- SMB est orienté session
- SMB est accessible via des APIs
- Une session SMB commence toujours par une authentification en utilisant des protocoles tels que NTLM et Kerberos V

Énumération des services réseaux Windows : SMB (TCP 139/445)

SMB : en pratique

- Client SMB
  - Commande **net use** pour l'établissement d'une session SMB
- Serveur SMB
  - Commande **net share** : gestion des partages (voir les partages actifs, ajout, suppression)
  - Commande **net sessions** : gestion de sessions SMB (énumération, suppression)
  - Commande **net files** : gestion des ressources partagées (énumération, suppression)

Énumération des services réseaux Windows : SMB (TCP 139/445)

SMB : en pratique

```
C:\Documents and Settings\Administrateur>net use \\192.168.1.10
Le mot de passe ou nom d'utilisateur n'est pas valide pour \\192.168.1.10.

Entrez le nom d'utilisateur de '192.168.1.10': fred
Entrez le mot de passe de 192.168.1.10 :
La commande s'est terminée correctement.
```

```
C:\Users\MeHome>net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
D$           D:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
Users        C:\Users
The command completed successfully.
```

```
Command Prompt

C:\tools>net sessions
Computer                User name            Client Type        Opens Idle time

-------------------------------------------------------------------------------
\\192.168.1.25          ADMINISTRATOR        Windows 2002 Serv      0 00:02:06
\\192.168.1.28          ADMINISTRATOR        Windows 2002 Serv      0 00:01:49
The command completed successfully.
```

Énumération des services réseaux Windows : SMB (TCP 139/445)

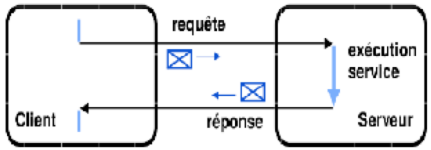
SMB : Sécurité

- Problème le plus connu :
  - Session SMB nulle (null session): récupération d'informations (partages, utilisateurs, groupes, registres, etc.) de façon anonyme
    ```
    C:\>net use \\132.181.11.3\IPC$ "" /u:""
    ```
- Autres :
  - MS02-045: Unchecked Buffer in Network Share Provider Can Lead to Denial of Service
  - MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified
  - MS03-049 - Buffer Overrun in the Workstation Service Could Allow Code Execution

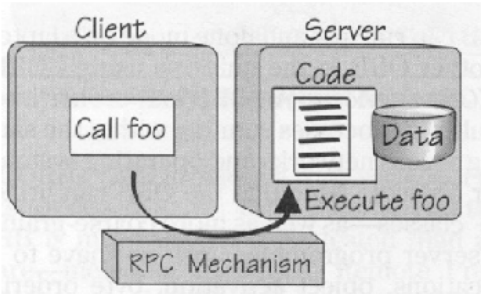
Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : concept

- RPC (Remote Procedure Call) : permet d'appeler des fonctions et services distants (on envoie les données et on récupère les résultats)
- Se concentrer sur l'essentiel lors d'un appel d'une fonctions et laisser les détails (gérer des sockets, ouvrir de connexions, formatage de données, etc.) à une couche intermédiaire (RPC)



Source : Krakowiak



- MSRPC est une mise en œuvre du standard DCE RPC par Microsoft

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : concept (terminologie)

- Opération : Procédure
- Interface : groupe d'opérations
- Service : fournit des interfaces
- Endpoint : Où se trouve le service
- Endpoind map : liste de Endpoint
- Endpoint mapper : Le serveur dans lequel se trouve le Endpoint map

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : exemple

Opérations Task

- Ajouter une tâche

  JobAdd
- Retirer une tâche

  JobDell
- Voir les tâches planifiées

  JobEnum
- Avoir de l'information sur une tâche

  JobGetInfo

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

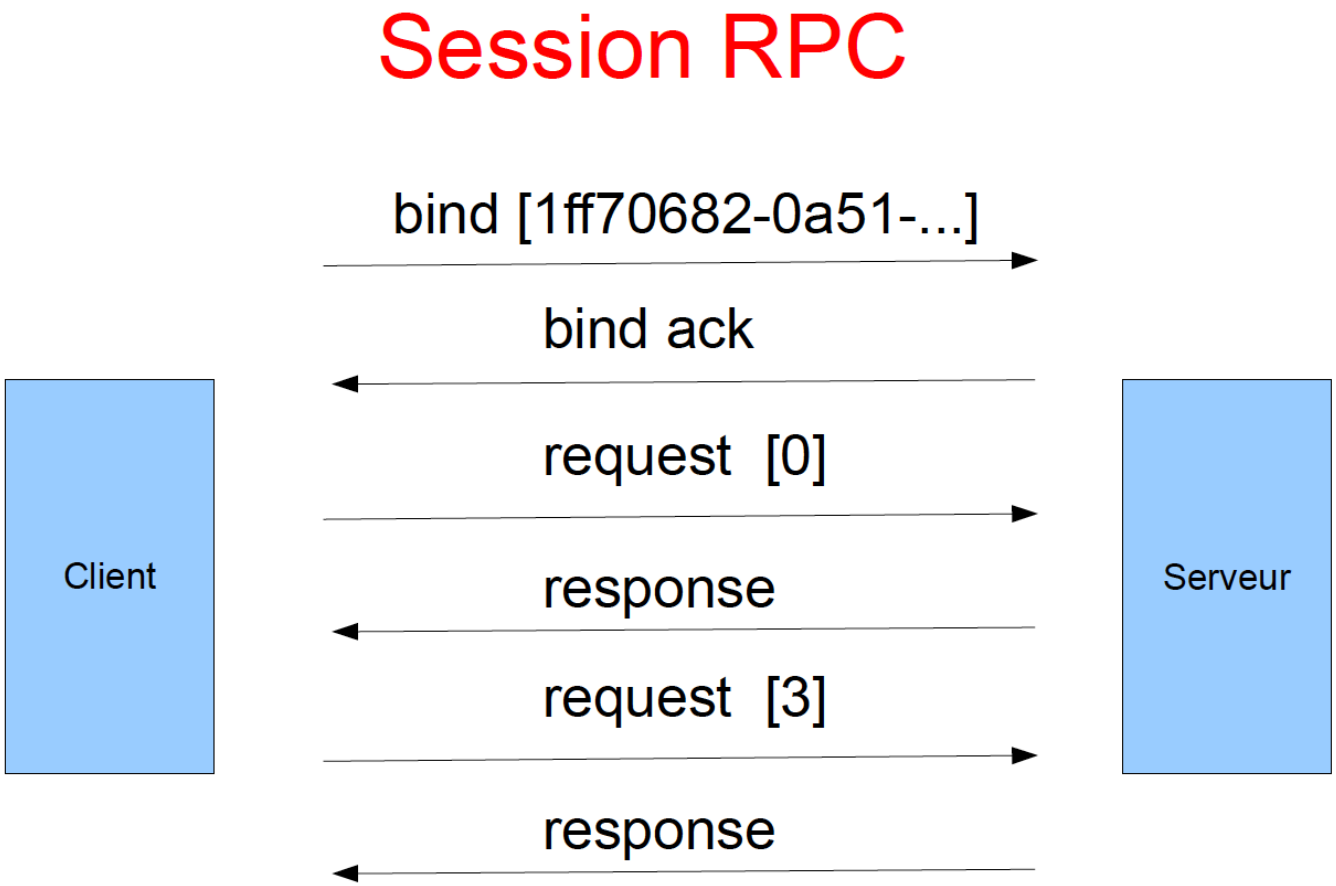
MSRPC : exemple

Task

- Operation: JobAdd, JobDell, JobEnum, JobGetInfo
- Op. No: 0, 1, 2, 3
- Interface: Task
- Interface ID: 1ff70682-0a51-30e8-076d-740be8cee98b
- Service: Task Scheduler
- Endpoint: nmacn_ip_tcp:192.168.0.101[1025]

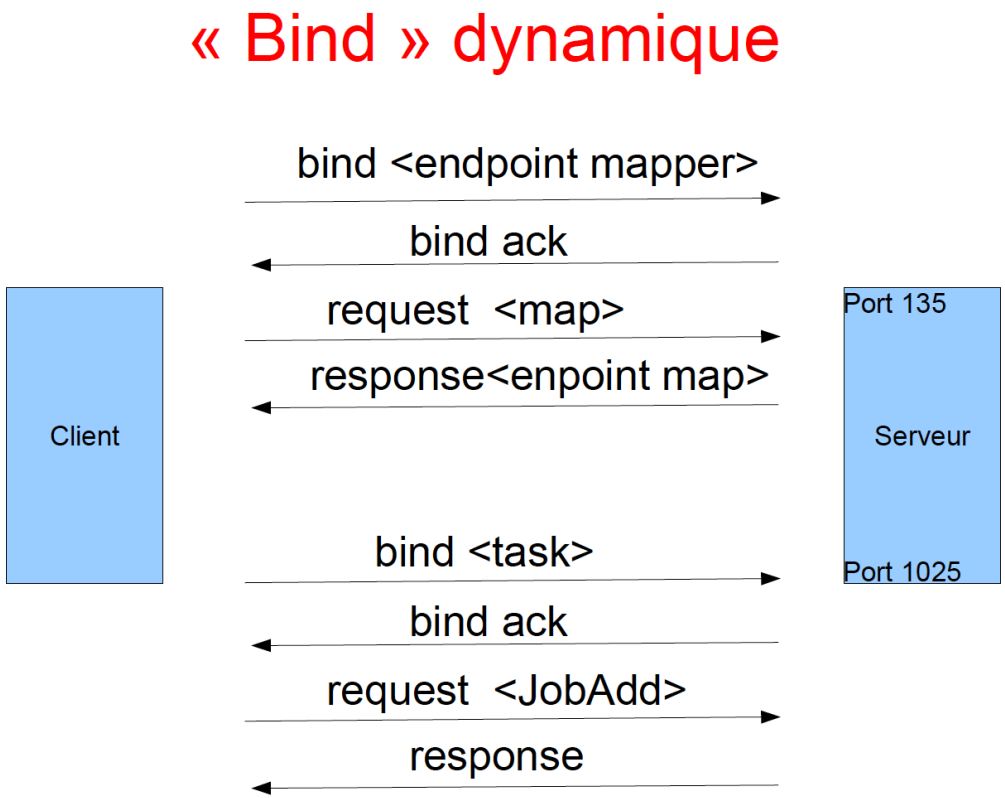
Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : exemple



Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : exemple



Le Endpoint mapper peut être disponible sur différents ports : TCP 135, UDP 135, TCP 593 (sur HTTP) où le tube \pipe\epmapper

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : concept

- Un service RPC peut être accessible via plusieurs protocoles de transport TCP, UDP, SMB, etc.
- DCE RPC sur TCP/IP utilise des ports TCP/IP
- DCE RPC sur SMB utilise des tubes nommés
- Les protocoles de transport utilisés par un service RPC se trouvent dans un "*endpoint*" ayant le format suivant :
  `endpoint("ncacn_ip_tcp:132.203.5.12[2046]'')` : indique qu'il y a un service qui écoute sur le port TCP 2046 du *endpoind* 132.203.5.12
  - ncacn_np: SMB Named Pipes transport
  - ncacn_ip_tcp: RPC sur TCP 135
  - ncacn_ip_udp: RPC sur UDP 135
  - ncalrpc: Local interprocess communication
  - ncacn_http: RPC sur HTTP (via un serveur IIS)
  - ncadg_ip_udp, ncacn_at_dsp, ncacn_nb_ipx, ncacn_dnet_nsp, etc.

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : En pratique

- Utilisés pour d'administration distante des machines Windows (comme le service SNMP)
- Les services accessibles à distance sont accessibles via des noms des tubes
- Exemple de noms de tubes: **eventlog** , **winreg** et **svcctl** pour la consultation à distance, respectivement, des journaux, la base de registres et des services Windows
- L'authentification se fait au niveau SMB (pas d'authentification au niveau DCE RPC)
- Possibilité d'utiliser une session SMB nulle pour récupérer des informations pertinentes concernant les tubes nommés **lsarpc** (LSA Windows), samr (SAM), **wkssvc** (service workstation), **srvsvc** (service serveur), etc.

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : Énumération

- Déterminer les adresses des machines et les ports sur lesquels il y a des services RPC
- Déterminer les noms et les IFID (interface ID) de ces services
- Identifié les IFID connues par des vulnérabilités
- Chercher s'il y a un service LSA (cela permettrait via une attaque par dictionnaire de récupérer des informations sur les utilisateurs et leurs mots de passe (hachage))
- Chercher s'il y a un service Task Scheduler (cela permettrait d'exécuter des commandes liées à la gestion de processus)
- Chercher s'il y a un service Server (cela permettrait d'activer de nouveaux services)
- **Outils :** epdump, rpctools, RpcScan, SuperScan, etc.

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : Énumération (Informations retournées par `rpcdump`)

- IFID (identifiant de l'interface) et version (version majeur.mineur)
- UUID : identifiant du type d'objet géré par l'interface (UUID:). Une interface peut gérer plusieurs types d'objets répartis sur plusieurs "Endpoint" :
  - UUID nul (00000000-0000-0000-0000-000000000000) : l'interface gère toutes les requêtes ne précisant pas un type d'objets
  - UUID non nul : l'interface répondue seulement aux requêtes liées au type d'objet identifié par UUID
- Binding (attache) : sous forme de "protocoles:point_de_terminaison"
- Annotation: identification significative du service

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : Exemple d'énumération

```
C:\> epdump 192.168.189.1
binding is 'ncacn_ip_tcp:192.168.189.1'
int 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc v1.0
binding 00000000-000000000000@ncadg_ip_udp:192.168.0.1[1028]
annot 'Messenger Service'
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
binding 00000000-000000000000@ncacn_ip_tcp:62.232.8.1[1025]
annot ''
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
binding 00000000-000000000000@ncacn_ip_tcp:192.168.170.1[1025]
annot ''
int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0
binding 00000000-000000000000@ncacn_ip_tcp:192.168.0.1[1025]
annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
binding 00000000-000000000000@ncacn_ip_tcp:62.232.8.1[1025]
annot ''
int 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0
binding 00000000-000000000000@ncacn_ip_tcp:192.168.170.1[1025]
annot ''
int 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc v1.0
binding 00000000-000000000000@ncacn_np:\\\\WEBSERV[\\PIPE\\ntsvcs]
annot 'Messenger Service'
int 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc v1.0
binding 00000000-000000000000@ncadg_ip_udp:192.168.170.1[1028]
annot 'Messenger Service'
no more entries
```

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : Exemple d'énumération

L'exemple précédent montre que :

- Il y a des services RPC sur les machines suivantes :
  62.232.8.1[TCP,1025]
  192.168.0.1[TCP,1025]
  192.168.170.1[UDP, 1028]
- Le nom NetBios de la machine locale est : `WEBSERV`
- Le service "Messenger Service" tourne sur :
  Le tube `ntsvcs` de `WEBSERV`
  Le port UDP 1028 de la machine 192.168.170.1
  Le port UDP 1028 de la machine 192.168.0.1
- Les IFID (interface ID) sont :
  5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc v1.0
  1ff70682-0a51-30e8-076d-740be8cee98b v1.0
  378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

MSRPC : Exemples de IFIDs

IFID	Service comments
50abc2a4-574d-40b3-9d66-ee4fd5fba076	DNS
45f52c28-7f9f-101a-b52b-08002b2efabe	WINS
12345778-1234-abcd-ef00-0123456789ab	LSA interface
12345778-1234-abcd-ef00-0123456789ac	SAMR interface
906b0ce0-c70b-1067-b317-00dd010662da	MSDTC
3f99b900-4d87-101b-99b7-aa0004007f07	MS SQL Server
1ff70682-0a51-30e8-076d-740be8cee98b	MS Task Scheduler
378e52b0-c0a9-11cf-822d-00aa0051e40f	MS Task Scheduler
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc	Messenger Service
6bffd098-a112-3610-9833-46c3f874532d	TCP/IP Services (*tcpsvcs.exe*)
5b821720-f63b-11d0-aad2-00c04fc324db	TCP/IP Services (*tcpsvcs.exe*)
fdb3a030-065f-11d1-bb9b-00a024ea5525	Message Queuing (*mqsvc.exe*)
bfa951d1-2f0e-11d3-bfd1-00c04fa3490a	IIS Admin Service (*inetinfo.exe*)
8cfb5d70-31a4-11cf-a7d8-00805f48a135	SMTP, NNTP and IIS (*inetinfo.exe*)

Énumération des services réseaux Windows : MSRPC, Microsoft RPC Endpoint Mapper, (TCP 135, UDP 135, TCP 593)

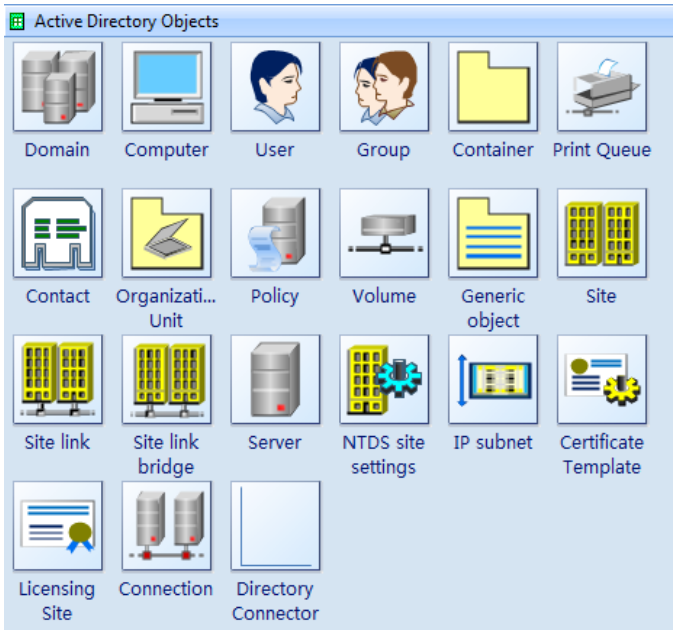
MSRPC : Exemple de problèmes de sécurité : Plusieurs problèmes liés à l'implantation des services (débordement de tampons, etc.).

Bulletin	Module	Identifiant de l'interface	Fonction
MS05-051	MsDtc	906b0ce0-c70b-1067-b317-00dd010662da	BuildContextW
MS05-043	Spoolss	12345678-1234-abcd-ef00-0123456789ab	AddPrinterExW
MS05-046	NwWks	e67ab081-9844-3521-9d32-834f038001c0	NwrGetUser NwrGetUser
MS05-039	UmPnpMgr	8d9f4e40-a03d-11ce-8f69-08003e30051b	PNP_Detect ResourceConflict
MS05-017	Msmq	fdb3a030-065f-11d1-bb9b-00a024ea5525	QMDeleteObject
MS05-010	Lls	342cfd40-3c6c-11ce-	LlsReplication
		a893-08002b2e9c6d	RequestW
MS04-011	Lsarpc	3919286a-b10c-11d0-9ba8-00c04fd92ef5	LsarClear AuditLog
MS03-039	epmapper	000001a0-0000-0000-c000-000000000046	RemoteGet ClassObject
MS03-026	epmapper	4d9f4ab8-7d1c-11cf-861e-0020af6e7c57	Remote Activation

Source (article) Dissection des RPC Microsoft
Nicolas Pouvesle and Kostya Kortchinsky

Énumération de Windows Active Directory LDAP (TCP/UDP 389 et 3268)

- Active Directory : Un annuaire (une base de données) qui nous permet de décrire des objets (utilisateurs, ordinateur, fichiers, imprimantes, etc.), de les structurer (groupe, unité d'organisation, domaine) et de définir leurs droits d'accès. Le protocole LDAP est utilisé pour accéder et manipuler ces informations à distance



source : http://www.edrawsoft.com/Active-Directory.php

Énumération de Windows Active Directory LDAP (TCP/UDP 389 et 3268)

- AD (Active Directory) est riche en information : les utilisateurs, les contrôleurs des domaines Windows, etc.
- Sans un accès sécurisé (accès Anonyme), l'énumération est possible

```
$ ldapsearch -h 192.168.0.65

# Nick Baskett, Trustmatta
dn: CN=Nick Baskett,O=Trustmatta
mail: nick.baskett@trustmatta.com
givenname: Nick
sn: Baskett
cn: Nick Baskett, nick
uid: nick
maildomain: trustmatta

# Andrew Done, Trustmatta\2C andrew
dn: CN=Andrew Done,O=Trustmatta\, andrew
mail: andrew.done@trustmatta.com
givenname: Andrew
sn: Done
uid: andrew
maildomain: trustmatta
```

- Avec un outil comme *hydra* ou *bf_ldap* on peut faire des attaques "force brute" ou par dictionnaire sur LDAP
- Si le domaine est compatible avec des anciennes versions de Windows, telles que Win NT, alors n'importe qui dans le domaine peut énumérer le répertoire

Connaître les rôles de utilisateurs à partir de leurs SID sous Windows

- Deux outils importants : `user2sid` et `sid2user`
  - Chaque utilisateur ou objet a un Security Identifier (SID)
  - Un SID a le format suivant : S-1-21-12-7623811015-3361044348-030300820-1011
    - S - La chaîne de caractères est un SID.
    - 1 - Le niveau de révision
    - 21 - Identificateur de l'autorité (locale, mondiale, etc.)
    - 12–7623811015-3361044348-030300820 - Identificateur de domaine ou d'ordinateur
    - 1011 – Un identificateur relatif (RID : Relative ID)
  - RID=500 pour un administrateur, 501 pour un *invité*. Le RID du premier compte est 1000, du deuxième 1001, etc.
    Exemple de résultats

Name	SID
Administrator	S-1-5-21-1180699209-877415012-3182924384-500
Guest	S-1-5-21-1180699209-877415012-3182924384-501
Alice	S-1-5-21-1180699209-877415012-3182924384-1001
Tom	S-1-5-21-1180699209-877415012-3182924384-1002
Bob	S-1-5-21-1180699209-877415012-3182924384-1003

Énumération des équipements et des protocoles réseau

Équipements réseau:

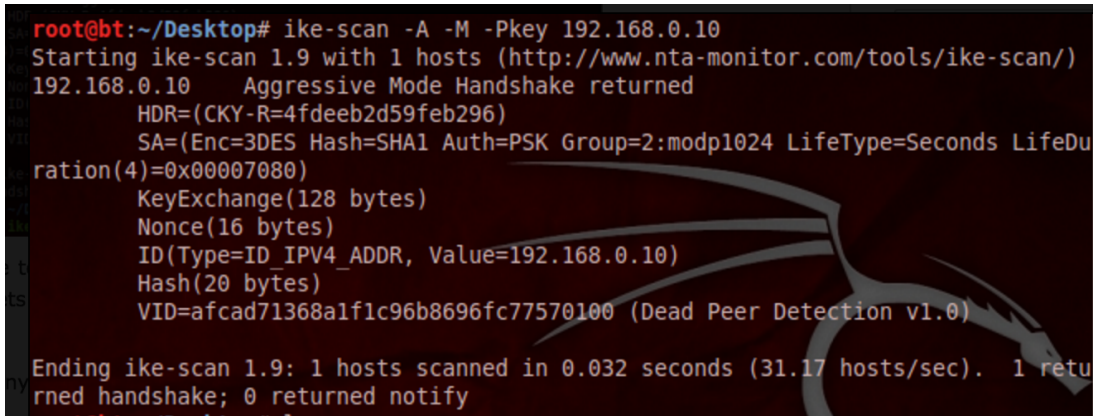
- **Traceroute** : permet de connaitre les nœuds qui nous séparent de la cible. Le dernier nœud est généralement un routeur.
- **DNS** : parfois, le rôle d'un équipement apparait dans son nom DNS (exemple *router.redhat.com*). Les enregistrements de type HINFO.
- **Nmap** : avec l'option -O peut dévoiler des équipements réseau

- **SNMP**: peut donner le type d'un équipement.
- **Ports tcp/udp** : RIP (udp/520) , BGP (tcp et udp/179). D'autres protocoles utilisent leurs numéros de protocoles (comme tcp (6) et udp (17)) IGRP (9), EIGRP (88), OSPF (89).

Énumération des équipements et des protocoles réseau

Équipements réseau:

- **ike-scan** : cherche les équipement VPN qui utilise Internet Key Exchange (IKE). Quand un équipement VPN est configuré pour utiliser "aggressive mode", il ouvre la porte à des attaques sur le Pre-Shared Key (PSK)



Énumération des équipements et des protocoles réseau

Protocoles réseau:

- **ASS (Autonomous System Scanner)** : Il fait des collectes actives et passives des protocoles de routages utilisés dans un réseau : OSPF, IGRP, EIGRP, RIP, HSRP, DHCP, ICMP. Un outil comme IRPAS (Internet Routing Attack Suite) permet plus tard de se faire passer pour un routeur et injecter des routes (ouvre la porte à MITM), spoofer des paquets, etc.

Énumération d'autres service

- Énumération de Novell NetWare, TCP 524 et IPX
- Énumération de UNIX RPC, TCP/UDP 111 et 32771
- Énumération de rwho (UDP 513) et rusers (RPC Program 100002)
- Énumération de NIS, RPC Program 100004
- Énumération de SQL Resolution Service, UDP 1434
- Énumération de NFS, TCP/UDP 2049
- Etc.