Découverte Réseau
(topologie et nature)

Aurélien Chivot - SRS 2003

13 mai 2002

Table des matières

Chapitre 1

Introduction

1.1 conventions et limites du sujet

La découverte réseau fait appel a de nombreux domaines techniques qui mériteraient des études dédiées. C'est d'ailleurs le cas pour bon nombre d'entre eux. Néanmoins, il est intéressant de pouvoir approcher un mécanisme de manière plus globale, et c'est l'objet de ce document. On verra ainsi une présentation de toute une gamme de techniques, chacune servant une cause spécifique mais toutes tendant vers le même but : la découverte réseau.

Pour plus de clarté, le sujet a été divisé en trois parties distinctes qui sont en générale les 3 étapes chronologiques parcourues. Dans chacune de ces phases, les techniques sont étudiées séparément, puis une conclusion résume la partie et donne des directions quant aux parades envisageables pour minimiser la quantité d'informations récupérables par un individu malveillant.

Ces parades contre la découverte réseau ne seront évoquées que brievement a titre de directives de recherche. En effet, celles-ci consistent en une application de chaque parade spécifique aux divers défauts d'un système qui permettent la récolte d'informations. Cela fait donc partie de l'étude spécifique des techniques abordées, et non de ce document.

On peut découvrir un réseau en y accèdent par Internet ou bien par accès téléphonique a distance. Les réseaux privés peuvent avoir des accès sur d'autres infrastructures comme par exemple le réseau européen transpac en X25. Ces infrastructures sont spécifiques et inaccessibles au particulier (a part les simples services minitel) et ne seront pas non plus abordées dans ce document.

1.2 c'est quoi la découverte réseau ?

La découverte réseau désigne l'acte de récolter toutes les informations possibles sur un réseau informatique, qu'il soit public ou prive. Ces informations qui sont surtout d'ordre technique (cartographie et topologie du réseau, nature des équipements et applications utilisées) nécessitent souvent de connaître d'autres informations d'ordre administratif (quelle(s) société(s) utilise(nt) ce réseau ? Le réseau est-il géré en interne ou bien fait-on appel a un sous-traitant ? Quelles sont les filiales de cette société ?). On va voir que c'est à partir de renseignements administratifs que commence souvent l'investigation...

1.3 motivations

En effet, la découverte réseau n'est quasiment entreprise que dans un but malveillant ou tout du moins illicite : Un pirate informatique cherche à s'introduire dans le système. Les motivations sont multiples, en allant du simple exploit " pour le fun " à l'espionnage industriel, en passant par le cyber-banditisme. C'est donc dans un but précis que le pirate cherchera à pénétrer le système, en ne connaissant parfois que le nom de l'entreprise ciblée ou d'un salarié.

Dans une optique opposée qui est celle de la sécurité informatique, on va donc s'approprier les mêmes motivations pour pouvoir protéger le système informatique. Ainsi, on voit que les simples tests d'intrusion ne sont qu'un moyen superficiel de protéger un réseau, et c'est à tout le système d'information qu'il faut s'intéresser pour établir une stratégie de sécurité efficace.

1.4 informations à obtenir

En aillant connaissance de toutes les caractéristiques d'un réseau ciblé, une faille est trouvée beaucoup plus facilement. Au-delà d'une simple faille, c'est une attaque chirurgicale et indétectable qui peut être mis en oeuvre, alors que cette action est souvent impossible pour une attaque directe et frontale du réseau. Voici un résumé des informations à obtenir dans le cadre de la découverte réseau.

Internet :

- noms de domaine
- blocs de réseau
- adresses IP spécifiques de systèmes accessibles par Internet
- services TCP et UDP exécutés sur chaque système identifié

- architecture système
- mécanisme de contrôle d'accès et listes de commande d'accès associées
- système de détection d'intrusion
- recensement du système (comptes utilisateurs et groupes, bannières, tables de

Intranet :

- Protocoles de réseau utilisés
- noms de domaines internes
- blocs de réseau
- adresse IP spécifiques de systèmes accessibles par Internet
- services TCP et UDP exécutés sur chaque système identifié
- architecture système
- mécanisme de contrôle d'accès et listes de commande d'accès associées
- système de détection d'intrusion
- recensement du système (comptes utilisateurs et groupes, bannières, tables de routage,...)

Accès a distance :

- Numéros de téléphone analogiques (RTC) / numériques (ISDN)
- Système d'accès a distance
- Mécanismes d'authentification

Extranet :

- Origine et destination de la connexion
- type de connexion
- mécanisme de contrôle d'accès

1.5 les différentes phases

Afin d'obtenir les informations ci-dessus, trois phases seront nécessaires :

- première phase : recuperation d'informations generales a propos du reseau et de la societe sous-jacente
- deuxième phase : etablissement de la topologie du reseau observe
- troisième phase : analyse et découverte du matériel et des applications utilisées

Chapitre 2

Première phase : information

2.1 introduction

Cerner l'organisation en établissement les limites de celles-ci est une phase préliminaire nécessaire du processus de découverte réseau. Les script-kiddies ne s'embêtent pas souvent de telles contraintes de ciblage, mais les individus les plus dangereux passent en général par cette étape, c'est pourquoi il est important de s'y intéresser. Pour apréhender le système visé dans sa globalité, il faut en maîtriser tous les tenants et aboutissants. On peut normalement obtenir une grande quantité d'informations par Internet directement, mais on verra que les vieilles méthodes peuvent aussi se révéler utiles !

2.2 champ d'activités

La première chose à faire consiste à parcourir le site web de l'organisation visée. On y glanera de nombreuses informations utiles ultérieurement. Par mis elles :

- l'implantation géographique (mono ou multi-sites, adresses)
- liens vers d'autres sites web liés ou partenaires
- informations sur le personnel :
  - noms et emails (comptes utilisateurs potentiels)
  - numéros de téléphone :

C'est à partir de ces numéros qu'on établira les plages numero de de téléphone à tester pour trouver d'éventuels accès a distance. Par mis les numéros possibles : numeros de poste interne, numero gratuit d'informations, numero de service hotline interne ou/et externe.
Outils :
- un navigateur web

2.3 domaine publique

En un mot : google.

Plus sérieusement, un moteur de recherche utilise de manière efficace permet de récupérer une mine d'informations. Parfois une société met en place une grosse politique de sécurité, fait passer des accords mutuels de non-divulgation... pour qu'au final des documents sensibles se retrouvent à la portée de tous sur un moteur de recherche !

Ce fut le cas de document secrets de l'armée américaine peut après que le moteur google soit capable de chercher les mots clef dans les documents Word et PDF !

Exemple d'utilisation avancée de moteurs de recherche :
- la recherche "host :www.cible.com mot" sur altavisa trouve le "mot" clef dans le domaine précise
- la recherche "link :www.cible.com cible" trouve tous les sites contenant le mot "cible" et qui ont en plus un lien pointant vers le domaine www.cible.com

Utilisation d'autres ressources publiques :
Parcours des bases de données IRC, usenet, a la recherche d'échanges relatifs à l'organisation visée. Par exemple, en cherchant "@cible.com" sur groups.google.com, on peut trouver un message du genre :

```
to: fr.comp.sys.routeurs
from: admin@cible.com
subject: a l'aide!

salut a tous!
je suis en galere, je possede un routeur modele
XXX de marque XXX et je ne sais pas comment
changer la configuration par defaut
svp aidez moi
merci

Mr admin
```

Cette situation est extrême est n'a que très peu de chance d'arriver, bien sur. Mais en étudiant les messages provenant des membres de la société visée, on peut obtenir des informations très utiles ultérieurement.

Outils :

- moteurs de recherches web/usenet : www.google.com, www.altavista.com, etc.
- utilitaires de meta-recherche (plusieurs moteurs) web/IRC/usenet : www.ferretsoft.com,

www.dogpile.com

2.4 informations administratives

Cette section concerne les sociétés cotées en bourse, c'est à dire en général les moyenne et grosses entreprises. Quand c'est le cas, il faut en général savoir ou se trouve la limite du réseau de l'organisation, étant donné que la société possède souvent des partenaires ou des filiales sur le même réseau.

On peut consulter librement la base de données EDGAR du SEC (Securities and Exchange Commission) en particulier les publications 10-Q et 10-K qui sont les plus intéressantes. En utilisant les mots clef "subsidiary" (filiale) et "subsequent events" (évènements postérieurs), il est possible de trouver les filiales et les sociétés nouvellement acquises de l'organisation concernée. Les fusions affaiblissent souvent les politiques de sécurité réseau, et un pirate peut utiliser le réseau d'une entité récente pour accéder au réseau principal ciblé plus facilement ou plus discrètement.

Attention : les noms de société qui sont trouves par ce biais sont différents de la société cible, bien qu'ayant un lien avec. Il faut les garder pour plus tard (notamment lors des requêtes whois - voir partie 2.2).
Outil :

– www.sec.gov

2.5 "oldskool"

La découverte réseau tire aussi parti des failles du système observe. Or, le maillon faible du système est souvent l'être humain. Récupérer des informations par ce biais porte souvent ses fruits.

Cette discipline appelée "social engineering" est moins populaire car elle demande des compétences humaines en plus des simples compétences techniques habituelles : il faut parvenir à entrer en contact avec une ou plusieurs personnes de l'organisation (par telephone, sur place) et en tirer le maximum d'information sans eveiller de soupcons. Les talents de négociateur et plus encore de manipulateur sont ici fortement utiles.

Souvent, la technique consiste à se faire passer pour une personne a qui on divulguera facilement des informations, soit par confiance ("bonjour, je suis le réparateur du téléphone, pouvez vous me renseigner.. etc.") soit par crainte ("bonjour, ici votre directeur informatique, nous effectuons une opération de maintenance, veuillez vérifier avec moi vos login/mot de passe...etc.").

Ces pratiques relèvent plus de l'espionnage classique. On utilisera si be-

soin les techniques de la vieille école comme les écoutes téléphoniques, la filature et prise de contact extérieure avec des personnes de l'organisation, la récupération des déchets de la société pour retrouver des factures, manuels d'installations, notes de services pouvant comporter des informations utiles (technique aussi appelée "trashing").

Cette section "oldskool" est ici a titre informatif, la découverte réseau étant menée la plupart du temps derrière un écran d'ordinateur !

Mais ces possibilité/risques existent réellement !! C'est même souvent la que le bas blesse, il ne faut donc pas oublier de les prendre en compte dans une stratégie de sécurité si on ne veut pas révéler d'information sensibles, notamment a propos du réseau informatique, pour ce qui concerne ce document.

outils :
- le matériel de l'apprenti espion

2.6 conclusion

Diverses méthodes existent pour récupérer des informations, mais aucune découverte que ce soit n'a encore été faites en ce qui concerne l'existence physique du réseau. Par contre, toutes les informations nécessaire a cette découvertes sont maintenant disponibles, et on va voir ultérieurement que cette phase préliminaire est loin d'être inutile !

En ce qui concerne la parade contre cette fuient d'information, elle consiste surtout à maîtriser le risque humain : ne pas poster n'importe quoi dans les newsgroups, ne pas reveler d'information sensible sur un media publique, et meme... ne pas jeter de papier sans les avoir detruits au prealable !! Une sensibilisation de tous les acteurs de la société est aussi une bonne parade contre ce risque. Par exemple, un séminaire commun pour rappeler les points respecter : politique de mots de passes difficiles à trouver, ne pas se connecter à Internet par modem depuis le milieu de l'entreprise, ne pas divulguer d'informations sans avoir la preuve de l'identité de l'interlocuteur, etc...

Chapitre 3

Deuxième phase : topologie

3.1 introduction

Cette première phase active de découverte réseau va consister à utiliser les outils standards de l'Internet pour cartographier le réseau visé. En effet, Internet n'est rien d'autre qu'une interconnexion de réseaux d'opérateurs, et il est basés sur des standards. On peut utiliser les outils simples comme whois, dons, ping et traceroute pour esquisser une première découverte réseau.

3.2 whois

Cet outil permet de se renseigner sur les noms de domaines associes à une organisation donnée. Il existe beaucoup d'organismes qui sont capables de donner ces renseignements. La liste est disponible a l'adresse suivante : http ://internic.net/alpha.html.
Plusieurs types de requêtes sont possibles :

- requête registar : affiches les informations specifiques au registar, nom de domaine et serveurs whois associes
- requête d'organisation : affiche toutes les informations a propos d'une organisation donnée
- requête de domaine : affiche toutes les informations relatives à un domaine donné
- requête de réseau : affiche affiche toutes les informations relatives à un reseau ou une ip donnée.
- requête d'utilisateur : affiche toutes les information concernant un utilisateur dans une organisation

Exemples : -

– la commande suivante permet d'obtenir la liste de tous les domaines commencent par "cible" :

```
evil$ whois "cible."@whois.super.net
[whois.super.net]
Whois server version 42
blabla banner

CIBLEHEHE.ORG
CIBLE1.COM
CIBLE.NET
CIBLETOTO.COM
CIBLE-MOI.COM
...
```

– la commande suivante affiche les infos du nom de domaine précis "cible.net" :

```
evil$ whois "cible.net"@whois.super.net
[whois.super.net]
Whois server version 42
blabla banner

Domain Name: CIBLE.NET
Registar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Refferal URL: www.networksolutions.com
Name Server: DNS1.CIBLE.NET
Name Server: DNS2.CIBLE.NET
```

On constate que network solutions et le registar de ce domaine, on peut donc effectuer des requêtes plus précises au serveur whois indiqué.

– commande cherchant les occurrences liées à l'entité recherchée

```
evil$ whois "name Cible Networks"@whois.networksolutions.com

Cible Networks (CMONOMN-DOM) UNDOMAINE.COM
Cible Networks (AUTRETRUC-DOM) TRUCSUPER.ORG
Cible Networks (CIBLE42-DOM) CIBLE.NET
...
```

Tous ces noms de domaine ne sont pas forcement utilises, ils peuvent être réservés pour éviter le squat ou tout simplement pour une utilisation ultérieure. Mais effectuons maintenant la requête principale :

```
cible$ whois cible.net@whois.networksolutions.com
[whois.networksolutions.com]
Registrant:
Cible Networks (CIBLE42-DOM)
42, rue des pigeons
75024 Paris

Domain Name : CIBLE.NET

Administrative Contact, Technical Contact, Zone Contact:
Roger Admin [admin reseau] sysop@CIBLE.NET
0643546587

Record last updated on 11-Sep-01
Record created on 11-Sep-00
Database last updated on 22-feb-02 13:42:27 EDT.
Domain severs in listed order:
DNS.CIBLE.NET 10.42.0.1
DNS2.CIBLE.NET 10.42.0.2
```

On a donc récupère des informations importantes a propos de :

- l'inscrit
- le nom de domaine
- le contact administratif
- les dates de création/mise à jour de l'enregistrement
- le(s) serveur(s) de domaine (DNS)

Grâce à ces informations récoltées ainsi qu'a d'autres informations obtenues en première partie (comme la localisation géographique par exemple), on peut obtenir les premier noeuds du réseau visé : les serveurs DNS.

Note : le serveur whois.arin.net donne les "net blocs" relatifs aux requêtes, c'est à dire les blocs réseau réservés pour un domaine donné.

```
evil$ whois"Cible Net."@whois.arin.net | grep NETBLK
Cible Networks (NETBLK)  10.42.0.0 - 10.64.127.255
```

Exemple de requête utilisateur :

```
evil$ whois "@cible.net"@whois.internic.net
Dupond, Roger (CS4567) rdupond@CIBLE.NET  0657829473
Tobin, Michel (RGT677) mtobin@CIBLE.NET 0145608539
...
```

outil :

- man whois

– www.networksolutions.com/en_US/help/whoishelp.html : syntaxe whois
– www.allwhois.com : meta-requete sur tous les whois, notament en dehors des US
– www.arin.net : whois contenant les blocs reseau

3.3 DNS - MX

Le serveur DNS permet de faire la correspondance entre les noms d'hôtes et les adresses IP. En cas de sécurité negligée, un serveur DNS donne des renseignements poussés sur la topologie du réseau visé.

L'une des erreurs de configuration les plus graves qu'un administrateur système puisse commettre est d'autoriser des utilisateurs Internet non validés à exécuter un transfert de zone DNS.

Un transfert de zone permet à un serveur maître secondaire de mettre à jour sa base de données de zone à partir du serveur maître principal. Cette opération permet d'exploiter des DNS redondants en cas de panne du serveur de noms principal. En règle générale, un transfert de zone DNS n'a besoin d'être exécuté que par des serveurs DNS maître de type secondaire. Toutefois, un grand nombre de serveurs DNS sont mal configurés et fournissent une copie de la zone à quiconque la demande. Fournir des informations d'adresses IP internes à un utilisateur non validé par Internet revient à fournir une copie i.e. carte complète du réseau interne de l'organisation.

Un moyen simple pour effectuer un transfert de zone consiste à utiliser le client nslookup qui est généralement fourni avec la plupart des installations UNIX ou NT.

Exemple pour récupérer une copie de zone du server DNS donné :

```
evil$ nslookup
Default Server: dns1.evil-isp.com
Address: 193.18.27.1
>> server 10.42.0.1
Default Server: [10.42.0.1]
Address: 10.42.0.1
>> set type=any
>> ls -d >> /tmp/output
```

Le fichier /tmp/output contient tous les enregistrements du DNS 10.42.0.1. Différents types d'informations sont disponibles pour chaque enregistrement, exploitable facilement avec des outils comme grep. La commande host souvent présente en environnement UNIX simplifie ce genre de processus, notamment la détermination des enregistrements Mail Exchange (MX).

Déterminer l'endroit où le courrier est géré est un excellent point de départ pour localiser le mur pare-feu de l'organisation cible. Dans un environnement commercial, le courrier est souvent géré sur le même système que le pare-feu, ou au moins sur le même réseau. Nous pouvons utiliser la commande host pour récolter encore plus d'informations.

```
evil$ host cible.net
cible.net has address 10.42.0.1
cible.net mail is handled (pri=20) by smtp-forward.cible.net
cible.net mail is handled (pri=10) by gate.cible.net
```

Outils :

- man nslookup
- host
- axfr : outil puissant de tra

3.4 traceroute

C'est avec la commande traceroute que commence la vraie cartographie du réseau. A l'origine, traceroute est un outil de diagnostic réseau, il est disponible avec la plupart des OS. Son fonctionnement est basé sur l'incrémentation du champ TTL d'un paquet IP. Un message TIME_EXCEEDED en ICMP est reçu pour chaque paquet, en indiquant par conséquent une étape du chemin qu'on cherche à tracer.

Examinons un exemple :

```
evil$ traceroute cible.net
traceroute to cible.net (10.42.0.1), 30 hops max, 40 byte packets
1 gate2 (192.168.0.1) 5.234ms 4.234ms 6.213ms
2 rtr1.evil-isp.net 193.128.0.4 12.241ms 234.123ms 12.123ms
3 rtr2.evil-isp.net 193.127.0.7 123.234ms 12.123ms 45.434ms
4 meta.operateur.net 10.27.3.1 213.234ms 12.123ms 35.354ms
5 gate.cible.net 10.42.0.1 12.123ms 35.234ms 345.345ms
```

On peut observer le trajet suivi par les paquets quittant le routeur (passerelle) et effectuant trois bonds (2-4) pour atteindre leur destination finale. Ces paquets passent ces différents tronçons sans être bloques. D'après les informations recueillies antérieurement, on sait que gate.cible.net correspond à l'enregistrement MX de cible.net. On peut en déduire que c'est bien un équipement actif, et que le routeur précédent situe la frontière du réseau. Ce routeur (numéro 4) pourrait être un firewall, mais toutes ces hypothèses ne sont que des pures spéculations.

L'exemple est d'autant plus simple que dans la réalité, en plus d'un chemin autrement plus long, il peut être bloqué à cause des ACL (listes de commandes d'accès). Il faut donc tracer tous les noeuds du réseau qu'on aura répertorié précédemment pour créer un premier schéma topologique. C'est ce schéma qu'on appelle les "voies d'accès".

L'utilisation des options de traceroute peut parfois s'avérer payante pour traverser des équipement de contrôle comme les firewall. En effet, traceroute peut utiliser des paramètres par défauts reconnaissables et bloqués par les administrateurs réseau. En utilisant l'option -p(n) avec n un numéro de port de départ (le port est incrémenté a chaque hop) ainsi que le switch -S qui permet de ne pas incrémenter les ports avec l'option -p, on peut passer outre certains filtres, qui laissent passer les requêtes DNS, par exemple (en utilisant -p23 -S).

Outils :

– man traceroute

3.5 bgp - snmp

La plupart des équipements d'infrastructure réseau offrent des outils de manutention. Ces outils permettent un monitoring du réseau tout entier facilement et depuis n'importe quel endroit. Ca facilite le travail de l'administrateur réseau, mais quelquefois les paramètres par défauts ne sont pas changé, et les informations sont à la portée du premier venu.

Le protocole BGP (Border Gateway Protocol) est de facto le protocole de routage sur Internet, c'est le langage utilisé par les routeurs pour communiquer le bon acheminement des paquets IP. En prenant connaissance de ces tables de routage, on prend connaissance tout simplement des réseaux liés a une organisation donnée. Il faut, pour que cette technique soit exploitable, que le réseau ciblé utilise aussi le protocole BGP. Pour savoir si c'est le cas, il faut chercher son numéro ASN, qui est en quelque sorte son identifiant BGP. On peut récupérer cette information en se logant en telnet sur un routeur public et en faisant avec une IP du réseau ciblé. Ensuite, on refait une requête de tous les réseaux dont le AS Path se termine par cet ASN, ce qui donne la liste des réseaux de l'organisation visée. Cette technique n'est néanmoins pas très développé car bon nombre d'organisations n'utilisent pas le langages de routage BGP (c'est d'ailleurs la seule parade pour éviter de rendre public ces informations sensibles)

SNMP signifie "Simple Network Management Protocol". Il a été conçu pour fournir le plus d'information possible aux logiciels de gestion de parc informatique.

En essayant les noms de communauté SNMP par défaut, on peut parfois accéder en lecture (souvent avec la chaîne "public") ou même en écriture (plus rare) au service SNMP d'un équipement (hub, switch, routeur). Si c'est le cas, c'est une quantité énorme d'information qui est disponible :

- informations sur le matériel (marque, model, version de l'OS, etc...)
- type de matériel réseau et protocoles utilises
- tables ARP
- services activés
- routes
- réseaux
- informations diverses sur le trafic, l'activité réseau

Outils :

- Outils solarwinds
- Outils de gestion SNMP

3.6 conclusion

Cette première partie de découverte active du réseau est assez méthodique. En utilisant les outils standards, on découvre souvent plus d'information qu'on pourrait croire. Mais la parade est assez simple : il suffit de bien configurer ses DNS et eventuellement de filtrer les paquets indesirables a l'entree du reseau. Malgré tout, c'est une étape incontournable de la découverte réseau car elle permet de dresser le diagramme des "voies d'accès", c'est à dire des routeurs disponibles de l'extérieur et de l'équipement actif qu'on rencontre à l'entrée du réseau (serveurs DNS, de messagerie au minimum). On connaît aussi les blocs d'IP du réseau et les noms de domaine de celui ci. Au mieux on aura beaucoup plus d'information grâce à un routeur lisible en SNMT !

Chapitre 4

Troisième phase : nature

4.1 introduction

La phase suivante consiste a scanner toutes ces plages d'IP pour repérer l'équipement actif et de compléter le schéma topologique du réseau observe.

Cette phase d'action est souvent celle qui comporte les premiers risques de détection. En effet, les moyens utilisés créent une forte activité réseau et se discernent facilement par mis le trafic habituel du réseau.

4.2 détection de l'équipement

4.2.1 équipement présent

Pour détecter les machines présentes sur un subnet, il faut utiliser un scanner d'IP. nmap est un excellent scanner, même si des techniques plus évoluées commencent à voir le jour. Le mécanisme est simple : on envoie un ping (ou simplement un paquet SYN pour les methodes plus subtiles) et si on recoit une reponse, il y a un equipement present.

```
evil$ nmap -sP -PT80 10.42.0.1/24
```

Cette commande va scanner les 255 machines du subnet et afficher les machines qui sont présentes. L'avantage de ce logiciel est qu'il permet de déterminer le degrés de discrétion d'un scan.

A titre informatif, hping est une version évoluée de ping qui permet grâce à des options utilisées a bon escient (voir le paragraphe précédent a propos de traceroute) de passer certains équipements filtrants.

Un autre type de reconnaissance de matériel actif consiste à utiliser des messages ICMP. icmpenum, élaboré par Simple Nomad, permet ce genre de chose facilement et surtout au travers d'équipement qui ne laissent pas passer

un nmap. La technique utilisée est l'envoi de paquets mal formés qui ne sont pas pris en compte par les filtres.

Le moyen le plus subtil de détecter une machine est encore le scan par témoin. Une machine n'ayant que peut d'activité est utilisée comme témoin par le biais de ses numéros de séquence TCP. S'ils sont suffisamment prédictibles, on peut spoofer cette machine pour envoyer des ping en TCP a la machine cible. Une étude du numéro de séquence TCP subséquent de la machine témoin indique si la machine cible a répondu.

4.2.2 Type d'équipement et services présents

La différence par rapport au point précédent, c'est qu'on ne scanne pas un ensemble de machines pour vérifier leur présence, mais un ensemble de ports et de tests sur une machine spécifique.

La présence d'un port ouvert laisse penser que le service associé est actif sur cette machine (en consultant la liste des "well known ports"). Par exemple si le port 21 est ouvert, le scanneur indiquera "ftp". Les tests permettent quant a eux de faire réagir la machine selon des critères bien précis afin de déterminer la plate-forme qui l'équipe. Cette technique est appelée fingerprinting. Elle a été largement développé par le développeur de nmap.

Nmap reste le meilleur outil pour déterminer ce qu'il y a sur une machine a distance. Au risque de me répéter, l'avantage de ce logiciel est qu'il permet de déterminer le degrés de discrétion d'un scan.

Notons aussi les outils standard de scan de port comme strobe (TCP) udp_scan (UDP) ou netcat (qui fait ça entre autre multitudes de services).

A défaut d'être très discret, on peut prendre des détours pour brouiller les pistes. Ainsi, on peut passer par un voire plusieurs serveurs proxy (en chaîne) pour scanner. Les serveurs proxy peuvent garder des logs de connexions, on peut donc essayer d'autres techniques comme le "bounce ftp scan" qui consiste à exploiter le protocole un peu laxiste de transfert de fichiers (FTP - file transfert protocol) pour scanner. (ces mêmes fonctionnalités qui sont utilisées pour faire du FXP i.e. échange de fichier entre serveurs ftp)

Bien entendu, Nmap prend en compte ce balayage avec l'option -b. Plusieurs conditions sont nécessaires : un répertoire sur le serveur FTP avec des permissions de lecture et d'écriture, la commande PORT doit être supportée par le serveur FTP. Mais un grand nombre de serveurs récents n'autorisent pas la mise en oeuvre de ce type d'activité nuisible.

Outils :

- ping
- nmap !!!! http ://www.insecure.org/nmap

– liste des well known ports : http ://www.iana.org/assignments/port-numbers
– hping, icmpenum, netcat...

sectionrecensement

Les renseignements que les intrus recueillent par recensement peuvent être classés en trois catégories :

– Les ressources réseaux partagées
– Les utilisateurs et groupes
– Les applications et bannières

4.2.3 Windows NT

Depuis la sortie de Windows 3.1, Microsoft propose en supplément un CD-ROM contenant des utilitaires d'administration réseaux NT : Le kit de ressources Windows NT. Ce kit, appelé NTRK (Windows NT Ressource Kit) contient une collection variée d'utilitaires puissants, par exemple des outils d'administration à distance non fournis dans la version du commerce NT.

Il y un néanmoins un inconvénient à toutes les commodités offertes par le NTRK. Un grand nombre de ces outils peuvent être utilisés par des intrus pour obtenir des informations précieuses, ce qui lui a valu d'être surnommé "The Windows NT Hacking Kit" (le kit de piratage Windows NT) dans certains milieux. Certains de ces outils sont disponibles gratuitement à l'adresse ftp : //ftp.microsoft.com/bussys/winnt/winnt-public/reskit/.

Windows NT présente un sérieux talon d'Achille dans les protocoles CIFS/SMB et NetBIOS, qui permettent de renvoyer des informations importantes via le port 139, même à des utilisateurs non identifiés. La première étape de l'accès à distance consiste à créer une connexion non authentifiée vers un système Windows NT, en utilisant une commande de connexion nulle :

Etablir une connexion avec la ressource partagée masquée de communication inter processus (IPC$) à l'adresse 192.168.202.33 en tant qu'utilisateur anonyme (/u :"") avec un mot de passe nul ("")

```
C:\>net use \\192.168.202.33\PC$ "" /u:""
```

En cas de succès, un canal est ouvert par le biais duquel on peut tenter d'exploiter les diverses techniques présentées dans cette section pour piller des informations à propos de la cible.

Recensement des ressources réseaux

La première opération qu'un pirate tentera sur un réseau Windows NT dont le terrain a déjà été repéré est d'essayer de déterminer ce qui s'y trouve. Nous commençons par présenter le recensement des ressources NetBIOS, puis

nous vous parlerons de recensement de services TCP/IP couramment proposé par les systèmes Windows NT.

Recensement NetBIOS

Les outils et techniques de sondage des réseaux NetBIOS sont disponibles : la plupart d'entre eux étant directement intégrés au système d'exploitation lui-même. Nous présentons ceux-ci en premier, puis passerons à quelques outils d'entreprises tierces.

Recensement des domaines Windows NT avec Net View

La commande net view est un excellent exemple d'outil de recensement intégré. C'est un utilitaire de ligne de commande NT extraordinairement simple qui permet de dresser le liste des domaines disponibles sur le réseau et de détailler ensuite toutes les machines d'un domaine. Voici la procédure à suivre pour recenser les domaines présents sur le réseau au moyen de net view.

Lister les domaines existants

```
C:\>net view /domain
Domain
----------------------
CORLEONE
BARZINI\_DOMAIN
BRAZZI
```

Lister les ordinateurs d'un domaine donné

```
C:\>net view /domain:brazzi
Server Name Remark
------------------------------------------------
\\VITO Get him an offer he can't refuse
\\MICHAEL Nothing personal
\\FREDO I'm smart
```

Envoi du tableau de noms NetBIOS avec nbtstat et nbtscan

Deux outils intégrés qui appellent le tableau de noms NetBIOS à partir d'un système distant.

```
c:\>nbtstat -A 192.168.202.33

Table de noms NetBIOS des ordinateurs distants

Nom  Type  État
------------------------------
MAT  <00> UNIQUE  Inscrit
RESO  <00> GROUP  Inscrit
```

```
MAT  <03> UNIQUE  Inscrit
MAT  <20> UNIQUE  Inscrit
RESO  <1E> GROUP  Inscrit

Adresse MAC = 00-50-FC-0B-88-D7
```

Comme indiqué, nbtstat extrait le non du serveur (MAT), le domaine dans lequel il se trouve (RESO), voici le tableau des correspondances de codes services NetBIOS :

Code Netbios	Ressource
nom de l'ordinateur [00]	Workstation Service
nom de domaine [00]	Domain Name
nom de l'ordinateur [03]	User Messenger Service
nom de l'utilisateur [03]	Workstation Messenger Service
nom de l'ordinateur [20]	Server Service
nom de domaine [1D]	Master Browser
nom de domaine [1E]	Browser Service Ellections
nom de domaine [1B]	Domain Master Browser

Les deux principaux inconvénients de nbtstat résident dans le fait qu'il est limité à un hôte unique et que ses résultats sont assez hermétiques. Ces deux problèmes sont résolus par l'outil gratuit nbtscan, disponible sur http ://www.inetcat.org/software/nbtscan.html Nbtscan est capable, au moyen de nbtstat, de traiter tout un réseau à la vitesse de l'éclair et de produire des résultats lisibles :

```
C:\nbtscan\_1\_0\_3>nbtscan 192.168.0.0/24
Doing NBT name scan for addresses from 134.214.170.0/24
IP address NetBIOS Name Server User MAC address
------------------------------------------------------------------------------
192.168.0.3 UMBERSUN <server> UMBERSUN 00-50-22-8c-eb-ab
192.168.0.11 JBTT <server> JBTT 00-e0-7d-74-41-82
192.168.0.14 AHX <server> AHX 00-50-fc-44-db-e0
192.168.0.16 RSI <server> \_\_VMWARE\_USER\_ 00-50-fc-0e-c1-67
192.168.0.21 SHB <server> ADMINISTRATEUR 52-54-05-e4-ac-29
192.168.0.22 SERAPHIN <server> SERAPHIN 00-20-e0-6a-14-e2
192.168.0.29 C605-B <server> OKPARANOID 00-50-fc-4d-a1-36
192.168.0.30 DANY <server> DQNY 00-48-54-6d-5d-0a
192.168.0.36 FJORD <server> JORDAN SANIAL 00-10-60-75-27-5f
192.168.0.38 SELBEN <server> SELBEN 00-05-5d-00-ff-e9
192.168.0.40 ZZZ <server> ZZZ 00-50-ba-65-2b-44
```

```
192.168.0.41 LOFT1 <server> AUDREY 00-d0-b7-48-26-ec
192.168.0.43 JARJOH <server> JARJOH 00-50-fc-46-83-aa
192.168.0.48 TARIK\_AZIZ <server> TARIK 00-50-fc-4c-6f-eb
192.168.0.49 PENTY2 <server> ADMINISTRATOR 00-01-02-9e-3e-67
192.168.0.55 ALEXALOISIO <server> JRAVEL 00-50-fc-24-a4-c5
```

On voit clairement que la connaissance de la plate-forme (Windows) et l'abus de certaines de ses failles (connexion nulle) ont permis d'avancer profondément dans la connaissance du réseau qu'on est en train d'observer !

Accessoirement, nbtscan est un bon moyen de détecter rapidement les machines Windows sur un réseau.

Recensement de ressources partagées NetBIOS avec Net View

Une fois qu'une connexion nulle est établie, nous pouvons aussi nous replier sur notre bon vieux net view pour recenser les ressources partagées des systèmes distants :

```
C:\>net view 192.168.0.9
Ressources partagées de 192.168.0.9
Nom Type Local Remarque
-----------------------------------------------
shared Disque to everyone
```

Outils très utile au recensement d'hôtes sous Windows :

- epdump de Microsoft (http ://www.ntshop.net), getmac et netdom (extraits du NTRK), netviewx (http ://www.ibt.ku.dk/jesper/Nttools/) : recensement d'informations de réseaux NT
- Enum, l'outil ultime du recensement (http ://www.cotse.com/tools/netbios.htm)

```
C:\>enum
usage: enum [switches] [hostname|ip]
-U: get userlist
-M: get machine list
-N: get namelist dump (different from -U|-M)
-S: get sharelist
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: be detailed, applies to -U and -S
-c: don't cancel sessions
-u: specify username to use (default "")
-p: specify password to use (default "")
-f: specify dictfile to use (wants -D)
```

Enum est capable d'automatiser l'établissement et l'interruption de connexions nulles. Il faut noter, en particulier, le commutateur de recensement de règle de mot de passe, -P, qui indique à des assaillants qu'ils peuvent deviner à distance les mots de passe des comptes utilisateurs (au moyen des commutateurs -D, -u et -f) et l'appliquer jusqu'à ce qu'ils en trouvent un de vulnérable.

Recensement via NetBIOS

Les ordinateurs Windows NT distribuent les informations utilisateur aussi aisément qu'ils révèlent les ressources partagées.

Nous avons déjà parlé de la capacité des utilitaires nbtstat et son homologue nbtscan à recenser les utilisateurs en renvoyant la table de noms NetBIOS. L'aspect intéressant de cette technique est qu'elle n'exige pas de connexion nulle.

Recensement des bannières et d'applications

Telnet et Netcat constituent les outils de base de la capture de bannière. Telnet a fait ses preuves en matière de recensement d'applications dans le domaine Windows NT.

Ce mécanisme fonctionne avec de nombreuses applications courantes qui répondent sur un port défini. (HTTP 80, FTP 21, SMTP 25)

Un outil de sondage plus précis, netcat, est disponible à l'adresse http ://www.atstake.com/rese

Connexion à un port TCP distant :

```
C:\netcat11>nc -v 192.168.0.9 80
mckinley [192.168.0.9] 80 (http) open

HTTP/1.1 400 Demande incorrecte
Server: Microsoft-IIS/5.0
Date: Thu, 28 Mar 2002 11:39:52 GMT
Content-Type: text/html
Content-Length: 80

<html><head><title>Error</title></head><body>Paramètre incorrect. </body></html>
```

Recensement du registre Windows NT

Un autre mécanisme de recensement d'information d'applications Windows NT implique le recueil de la base de registre Windows de la cible. La grande majorité des applications correctement installées laissent une forme ou une empreinte dans la base de registre.

Les deux outils les plus utilisés pour effectuer cette tâche sont regdmp de la boîte à outils NTRK et DumpSecde Somarsoft. Regdmp est un utilitaire assez fruste qui se contente de transférer la totalité de la base de registre vers la console.

Nous allons chercher de savoir quelles applications démarrent avec Windows

```
C:\>regdmp -m \\192.168.202.33 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\C

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SystemTray = SysTray.exe
BrowserWebCheck = loadwc.exe
```

DumpSec produit des sorties bien plus jolies, mais obtient globalement les mêmes résultats. Le rapport "Dump Services" recense tous les services et pilotes noyaux Win32 du système distant, qu'ils soient exécutés ou non (en faisant l'hypothèse que l'on dispose des autorisations d'accès appropriées). Une connexion nulle est nécessaire pour cette opération.

4.2.4 UNIX

La plupart des installations UNIX modernes reposent sur des fonctions de réseau TCP/IP standard et ne sont pas portées à livrer des informations aussi aisément que les systèmes Windows NT. Cela ne veut pas dire que UNIX est invulnérable mais les techniques qui donneront les meilleurs résultats dépendent de la manière dont est configuré le système.

Recensement des ressources partagées

Les meilleures sources d'information sur les réseaux UNIX restent les techniques TCP/IP de base présentées dans la partie deux. Toute fois, l'utilitaire UNIX showmount est un bon outil qui permet de creuser plus profondément.

```
Showmount -e 192.168.202.34
Export list for 192.168.202.34
/pub (everyone)
/var (everyone)
/usr user
```

Le commutateur -e fournit la liste d'exportation du serveur NFS. Mais NFS n'est plus le seul logiciel de partage de système de fichiers, en effet la suite logicielle Samba offre des services d'impression et des fichiers transparents aux clients SMB sous Windows NT. Samba est disponible sous http ://www.samba.org. Bien que la configuration par défaut de serveur Samba contienne quelques paramètres de sécurité de base, une erreur de configuration peut donner lieu au partage de données non protégées.

Parmi d'autres sources potentielles de renseignements portant sur les réseaux UNIX, on peut citer NIS. Le problème de NIS vient du fait que,

dès lors que vous connaissez le nom de domaine NIS d'un serveur, vous pouvez obtenir tous ses plans NIS en utilisant une simple requête RPC. Une attaque NIS classique comprend l'utilisation d'outils client NIS destinées à deviner le nom de domaine. Par ailleurs, un outil tel que pscan est capable d'extraire des renseignements intéressants au moyen de l'argument -n.

Recensement des utilisateurs

L'astuce la plus ancienne en matière de recensement d'utilisateurs est probablement l'outil UNIX finger. Un grand nombre d'outils d'attaque à base de scripts l'utilisent, et de nombreux administrateurs négligents laissent tourner finger sur des configurations où la sécurité est minimale. Le renseignement le plus dangereux fournit par finger est peut être la liste des utilisateurs connectés et des temps de repos. Cela peut donner une idée aux pirates de qui observe, et de son niveau de vigilance.

Une autre technique classique de recensement d'utilisateurs exploite le langage courant des messageries Internet, à savoir SMTP (Simple Mail Transfer Protocol). SMTP comprend deux commandes intéressantes :

- VRFY : confirme les noms des utilisateurs valides
- EXPN : signale les adresses de livraison effectives des alias des listes de publipostage

L'un des moyens les plus populaires pour s'emparer du fichier des mots de passe consiste à passer par le protocole TFTP (Trivial File Tranfer Protocol)

```
tftp 192.168.202.34
tftp>> connect 192.168.202.34
tftp>>get /etc/passwd /tmp/passwd.cracklater
tftp>>quit
```

Recensement des applications et bannières

Comme toutes les autres ressources de réseaux, les applications doivent disposer d'un moyen de communiquer les unes avec les autres par le réseau. L'un des protocoles les plus populaires assurant cette communication est RPC (Remote Procedure Call). Rpcinfo est l'équivalent à de finger pour le recensement d'applications RPC actives sur des sites distants et peut être mis en oeuvre sur des serveurs détectés comme étant à l'écoute du port 111 (rpcbind) ou 32771 (portmapper de Sun) à l'occasion de balayages antérieurs.

```
evil$ rpcinfo -p 192.168.202.34
Program vers proto port
100000 2 tcp 111 pcbind
100002 3 udp 712 rusersd
100003 2 udp 2049 nfs
100004 2 tcp 778 ypserv
```

On sait ainsi ce que cet hôte est en train d'exécuter : rusersd, NFS et NIS (ypserv est le serveur NIS). Dès lors, rusers, showmount -e et pscan -n vont générer des informations complémentaires. Une variante de rpcinfo qui peut être utilisée à partir de Windows NT est RPCdump (http ://www.atstake.com/research/tools/).

Une fois n'est pas coutume, nmap prend en compte les RPC et facilite et automatise le processus.

```
c:\>rpcdump 192.168.202.36
Program no. Name Version Protocol Port

(100000) portmapper 2 TCP 111
(100000) portmapper 2 UDP 222
(100024) status 1 UDP 32768
(100024) status 1 TCP 32768
```

4.3 scan téléphonique

Que ce soit pour des déplacements extérieurs ponctuels ou un postes fixe à distance, une organisation de moyenne ou grande taille disposent souvent d'un accès a distance direct par téléphone. Le but de cette section est d'évoquer les différentes façons de trouver ces accès pour les ajouter à la cartographie du réseau.

Mise en garde : contrairement a internet ou les ouverture de socket, scans et autres sont innoffensifs et ne genent personne sauf pour leur aspect de mauvaise augure, le reseau commuté est avant tout un reseau telephonique. Un scan de numéros de téléphone (dont on va voir l'utilité) peut semer la pagaille au sein d'une société si cela est fait durant les heures de bureau. Sur le plan juridique, il faut aussi faire la différence avec internet. Un scan IP ponctuel, même s'il n'est pas apprécié, n'occasionnera pas de suspension de ligne ou de poursuites judiciaires. Un scan de numéros de téléphones en pleine journée aura de fortes chances d'y conduire.

scan !

A l'aide des numéros de téléphone récupérés au début de l'opération, on va créer des plages de téléphone a scanner. Par exemple, si je récupère le numéro de téléphone suivant : 0800397397, on peut definir la plage suivante de 10000 numeros : 080039XXXX.

Le programme ira scanner les numéros 0800390001 a 0800399999.

Le résultat d'un tel scan donne pour chaque numéro le résultat obtenu :

- non attribué
- occupé
- voix humaine

– porteuse de fax
– porteuse de modem

La deuxième opération (qui peut être effectuée en batch directement en configurant les logiciels) consiste à essayer de détecter le système qui est derrière une porteuse de modem. Il peut s'agir (le plus souvent) d'un serveur d'accès réseau a distance.

Il peut s'agir aussi d'un autocommutateur privé (PABX). La ligne extérieure est souvent laissée activée à des fins d'assistance externe par le fabricant du PABX, mais c'est évidement risqué pour la société qui a acheté ce PABX. Cette détection du système opérant derrière une porteuse de modem suit en premier lieu le système des bannières et du fingerprinting : certains apareils s'annoncent en toutes lettres et facilitent la tache. Pour d'autre serveurs ou PABX, c'est en analysant le comportement a l'usage qu'on peut déterminer de quel appareil il s'agit (et même sans tenter l'intrusion).

Les script des logiciels d'exploitation de porteuse supporte en général la découverte d'un grand nombre d'équipement sur ligne téléphonique.

La deuxième ligne de résultat exploitable, c'est "voix humaine". En effet, cela annonce souvent une messagerie (puisque le scan est effectué en l'absence des utilisateurs). S'il s'agit d'une moyenne ou grande entreprise, il y a toutes les chances pour que ce résultat annonce un serveur de boites vocales. On peut récupérer un grand nombre d'informations si on réussit à deviner le mot de passe d'une ou plusieurs boites. Suivant le fonctionnement du serveur de boites vocale, on peut déterminer quel appareil il s'agit et essayer les mot de passe par défaut, ou les mots de passe bateau. L'attaque "brute force" est envisageables sur les boites vocales car le mot de passe est en général composé de 4 numéros, c'est à dire 10000 possibilité seulement. L'objectif de la manipulation est de récupérer toutes les informations qui intéressent directement la découverte réseau, c'est à dire les utilisateurs, ou bien par déduction d'autres informations. Cette section pourrait d'ailleurs faire partie de la premier phase de la découverte et qui consiste à récupérer un maximum d'information sur l'organisation proprement dite.

Outils :

– ToneLoc : le premier, le mythique et legendaire scanneur pour DOS
– THC-scan (http ://www.infowar.co.uk/thc) la releve
– Phonesweep (http ://sandstorm.net) Le meme genre de chose pour windows
– On consultera pour plus d'informations divers e-mags de phreaking i.e. piratage des systèmes téléphoniques, comme par exemple le regretté

cryptel

4.4 conclusion

Cette partie qui s'achève est la plus longue, pourtant les techniques abordée ne sont que survolées. Pour chacune d'elles on peut trouver des études complètes souvent disponibles sur internet. Ces techniques évoluent toujours avec le matériel et les applications, même si le principe reste souvent le même.

On a vu que durant cette dernière phase, les derniers éléments nécessaires a la récolte d'informations réseau sont normalement connus :

- éléments actifs du réseau (noeuds, machines utilisateurs, serveurs)
- réseau applicatif installe sur cette couche réseau
- réseau d'utilisateurs utilisant ce réseau applicatif

En reliant les diverses informations obtenues durant les 3 phases de rassemblement d'information, la découverte réseau est maximale.

Chapitre 5

Conclusion

La découverte réseau touche tous les domaines de l'informatique. Utilisée dans le cadre d'un audit de sécurité, cette technique longue et fastidieuse montre que le piratage, ce n'est pas seulement du subnet-scan-port-scan-vulerability-scan-exploit mais une analyse pragmatique de tout un réseau dans son ensemble. Une cartographie complète d'un réseau, si elle est faite sérieusement, ne laisse pas échapper de faille importante. Un jour, une entreprise de très grande envergure s'est fait pirater le coeur de son système alors qu'elle avait mis en place une stratégie de sécurité très rigide et très forte. Finalement, on s'est aperçu que la faute incombait à un utilisateur frustre de ces limitations de sa connexion Internet, et qui avait tout simplement connecte son ordinateur a sa ligne téléphonique pour jouer sur internet. Le pirate en avait profité pour entre dans la place forte en quelques techniques basique d'intrusions.

Comme quoi, la sécurité d'un système d'information ne se situe pas dans la rigidité absolue du réseau, mais dans la maîtrise de sa souplesse.

Comme l'homme est avant tout partie du système d'information qu'il utilise, la découverte de la topologie d'un réseau et la cartographie de celui ci doit intégrer pleinement cette variable humaine. C'est ce qui a été fait en intégrant la découverte du "réseau d'utilisateurs" au-dessus du réseau physique et applicatif proprement dit.

Point important à noter : Le sujet de la découverte réseau à été traite en majorité de manière "non intrusive", c'est à dire en utilisant les données a disposition sans essayer de pénétrer à l'intérieur du réseau immédiatement pour s'immiscer directement dans le l'organisation visée.

Il est évident que dans certains cas, la présence d'une faille et l'utilisation de celle ci par un individu mal intentionné peut aboutir à une cartographie immédiate et totale du réseau!!

Exemples :

– accès en écriture a tous les équipements SNMP.
– Une position "man in the middle"
– un accès utilisateur (ces deux derniers cas sont souvent liés)

Dans les cas ou un accès à l'intérieur du réseau est possible, la découverte du réseau est beaucoup plus aisée. C'est pourquoi la multiplication des systèmes et des utilisateurs ne peut aller que vers une facilitation du travail des pirates, de manière générale. L'apparition de nouveaux type de liaisons (surtout les liaisons sans fil : satellite, 802.11, bluetooth, ...) fait apparaître de nouvelles techniques de détection et de découverte réseaux.

Chapitre 6

Références Bibliographiques

"*Halte aux Hackers*" 3eme édition aux éditions OEM
Stuart McClure - Joel Scambray - George Kurtz

"*Les réseaux*" aux éditions Eyrolles
Guy Pujolle

Dossier sur le piratage - http ://www.z0rglub.com/piratage/imprimer.php
Patrick Legall

"*Discovering Internet Topology*"
R.Siamwalla, R.Sharma and S.Keshav
Cornell Network Research Group
Department of Computer Science
Cornell University, Ithaca, NY 14853

Online Network Tools : http ://tools-on.net
Alexander K. Yezhov

Homepage de nmap et source d'informations
http ://www.insecure.org

Grosse *source d'informations* et d'outils libres
http ://www.packetstormsecurity.org