

De l'insécurité des Intranets

Par Stéphane Aubert

– Hervé Schauer Consultants –

Introduction

L'activité du Cabinet Hervé Schauer Consultants, spécialisé en sécurité informatique depuis plus de 10 années, nous permet des visites fréquentes chez de nombreuses grandes sociétés. Ces visites sont généralement des prestations techniques d'audit et de conseil. Nous bénéficions ainsi d'une vision d'ensemble de l'état de la sécurité des réseaux informatiques au sein de la plupart des grands comptes français, dans des domaines aussi variés que les télécommunications, le milieu bancaire, la défense ou l'industrie.

En 1996, le Clusif (Club de la sécurité des systèmes d'information français) publiait que 62% des causes de perte de données informatiques provenaient d'origine malveillante. Dans un rapport d'enquête sur la sécurité des systèmes d'information Ernst & Young annonçait, en 1997, que 68% des entreprises françaises exprimaient la crainte d'une attaque interne et 46% celle d'une attaque externe. L'accroissement massif des réseaux IP locaux, dits Intranets, dans les sociétés françaises, ne nous laisse pas envisager une diminution du pourcentage des tentatives d'attaques internes, initiées depuis le réseau Intranet.

Thomas Harris dans son roman "Le silence des agneaux" exprimait l'idée que nous convoitons principalement ce qui nous est proche. Les sociétés françaises, de plus en plus consommatrices de réseaux informatiques locaux, ont besoin d'être mises en garde et correctement conseillées. Elles doivent prendre conscience des risques introduits par l'utilisation d'un réseau intranet global et ouvert à toute l'entreprise, un réseau trop souvent non maîtrisé.

Nous nous proposons, dans un premier temps, d'illustrer combien il est simple d'effectuer des actes malveillants sur un réseau Intranet peu ou mal sécurisé. Nous présenterons ensuite les différentes prestations techniques pouvant aider une société à appréhender les différents problèmes de sécurité présents sur son réseau. Nous concluons enfin sur les perspectives techniques, en terme de sécurité, des réseaux Intranet.

description des attaques

Ce chapitre est entièrement dédié à la démystification des attaques pouvant être mises en place sur un réseau Intranet. Nous avons trop souvent constaté que certains décideurs ou membres du service sécurité n'ont pas conscience de la facilité de mise en place d'attaque sur leur propre Intranet.

En France, la sécurité informatique est encore trop épistolaire et théorique. En revanche,

les attaques, et tout particulièrement les intrusions, sont techniques. En sécurité informatique, plus que dans d'autres domaines, les différents protagonistes ne peuvent plus ignorer la technique. Il est temps de se protéger efficacement contre le vol, la falsification ou la destruction de données situées sur les ordinateurs connectés entre eux par le réseau Intranet. Il est important aussi de s'assurer que le service rendu par le réseau, service devenu généralement indispensable, n'est pas altérable sur demande.

La nature d'un réseau Intranet est la même que celle du réseau Internet, les problèmes de sécurité sont similaires. Toutefois, les attaques sur réseau Intranet sont beaucoup plus dangereuses de part la proximité de l'attaquant. L'écoute de réseau, par exemple, n'est possible sans gros moyens que sur un réseau local. Elle est assimilable à des écoutes téléphoniques et réalisable simplement : nous allons le détailler, sous Windows NT ou Unix grâce à des programmes nommés "*sniffers*". Ces simples *sniffers* entre les mains d'une personne malveillante peuvent porter aujourd'hui un préjudice considérable à une société, un organisme ou une administration.

Le rôle d'Internet dans le nombre d'attaques des réseaux Intranet est important. Les différentes méthodes d'attaques sur Internet s'appliquent, de part la nature commune (TCP/IP), aux réseaux Intranet. Mais Internet joue aussi parfaitement son rôle de diffuseur d'information en permettant à tout le monde de se connecter sur des sites de piratage. Une personne malveillante préparera ainsi ses attaques, en toute discrétion, depuis son domicile.

Pour tuer le mythe du pirate super technicien génial, nous ne citons et ne détaillons ici que des outils (des programmes) disponibles sur Internet. Des programmes que chaque service sécurité se doit de connaître, d'étudier et, dans la plupart des cas, d'utiliser. La liste de toutes les adresses des serveurs Web relatifs à ces programmes est donnée en annexe.

Le 13 août 1998 on pouvait lire dans le San Francisco Chronicle que "en utilisant un programme appelé John The Ripper, qui peut être téléchargé sur Internet, un pirate "high-tech" a obtenu des mots de passe non seulement à l'université de Berkeley mais aussi dans des universités ou entreprises autour du monde. Le pirate a décodé environ 48000 mots de passe dans une liste de 186000 mots de passe chiffrés."

Dans le monde informatique du 2 février 1999 on peut lire que, "un certain John The Ripper, opérant depuis l'Europe, a subtilisé, grâce à un logiciel de recherche, 180000 mots de passe dans plusieurs universités américaines".

John The Ripper est simplement un programme qui permet de retrouver les mots de passe en clair lorsqu'on possède un fichier de mots de passe chiffrés (laissez moi ne pas employer le mot crypté qui ne veut pas dire grand chose). Vous pouvez télécharger ce programme à l'adresse <http://www.false.com/security/john/index.html>.

Le système d'exploitation que nous employons pour ce genre de prestations est principalement un système Unix issu du logiciel libre comme Linux ou FreeBSD. Ces deux systèmes ont été choisis pour des raisons de performance et de souplesse, ils peuvent aussi être installés avec les programmes cités sur une disquette de démarrage

pour ordinateurs de type PC. Cette manipulation permet de transformer temporairement un ordinateur de bureau en sonde d'écoute de réseau, par exemple, avec une seule disquette, sans laisser aucune trace. Il est important de ne pas oublier que Microsoft Windows (95, 98 ou NT) est aussi utilisable pour ce genre d'actions.

Écoutes de réseau

Très peu d'Intranets sont aujourd'hui protégés contre les écoutes de réseau. Sur l'Intranet sont amenées à transiter des informations comme des données comptables, des données sensibles liées aux applications métiers de l'entreprise, le courrier électronique, les mots de passe (indirectement les mots de passe Windows NT), etc.

L'écoute du réseau est locale. L'écoute d'un sous-réseau distant, sur l'Intranet ou sur Internet, n'est généralement réalisable que par la prise de contrôle totale d'une machine à distance, soit un piratage.

Le *sniffer* nommé linsniffer est un petit programme de 240 lignes qui permet, par écoute du réseau, de capturer et d'afficher en clair les mots de passe des utilisateurs qui utilisent les protocoles POP3, IMAP, FTP, telnet et rlogin. POP3 et IMAP sont utilisés quotidiennement pour, par exemple, transférer depuis un poste sous Windows son courrier électronique reçu par le serveur de l'entreprise. FTP peut être utilisé par des utilisateurs ou des applications pour transférer des fichiers. Telnet et rlogin sont principalement utilisés pour se connecter de manière interactive non sécurisée sur un serveur.

L'exécution de ce programme fournit le résultat suivant (directement dans le fichier texte "tcp.log") lorsque l'utilisateur Pierre sur la machine VENUS lit son mail sur la machine MAIL via le protocole POP3 (110/tcp) :

```
Résultat de la commande : linsniffer
venus.hsc.fr => mail.hsc.fr [110]
USER pierre
PASS 123soleil
STAT
QUIT
```

Le mot de passe de cet utilisateur sur le serveur MAIL est 123soleil, il permettra de lire le courrier électronique à la place de son réel possesseur et donnera souvent la possibilité de se connecter à la place de l'utilisateur sur le serveur.

Ce *sniffer* permet, en écoutant les connexions telnet, de capturer aussi simplement les mots de passe des routeurs lorsque ceux-ci sont configurés depuis les postes des administrateurs. Prendre le contrôle des routeurs revient à prendre le contrôle du réseau.

Lorsque vous êtes sur un Intranet protégé par une passerelle de sécurité d'accès à Internet (en langage marketing : un firewall) et que cette passerelle vous demande un mot de passe pour vous identifier, ce mot de passe circule en clair (sans chiffrement) sur le réseau. Lorsque vous accédez à des informations sensibles sur votre serveur Intranet et que vous devez vous identifier avec votre mot de passe, il circule en clair sur le réseau. Le *sniffer* web_sniff est spécialisé dans l'écoute de requêtes HTTP, le protocole utilisé

pour visiter, sans chiffrement, les sites Web. Il permet de connaître les adresses des pages visitées et d'afficher les mots de passe utilisés soit pour sortir sur Internet soit pour accéder à des informations sensibles sur Intranet.

```
Résultat de la commande : web_sniff -v
[x.x.x.x] [3648] => [y.y.y.y] [3128]
GET http://rufus.chenil.int/ HTTP/1.0
...
User-Agent: Mozilla/4.5b2 [en] (X11; I; Linux 2.0.34 i586)
...
-----[ USER = pierre      PASS = 123soleil ]-----
```

Le mot de passe ne circule pas en clair dans le cas d'un réseau utilisant uniquement Windows NT ou dans le cas de l'utilisation du protocole HTTPS (HTTP avec chiffrement). Toutefois, dans le cas de Windows NT un programme de cassage de mots de passe NT fonctionne très bien, il se nomme L0phtCrack. Toujours dans ce cas, il est important de savoir que même avec Windows NT dernière version, les pages visitées circulent en clair sur le réseau et peuvent être entièrement capturées avec le *sniffer* sniffit. Dans le cas de l'utilisation du protocole chiffré HTTPS (limité en France à RC4 et 40 bits), les pages Web visitées peuvent être capturées chiffrées (avec sniffit) et décodées, avec par exemple, deux programmes client/serveur : master.c et slave.c (<http://pauillac.inria.fr/~doligez/ssl/press-conf.html>).

Le programme L0phtcrack, disponible sur Internet, a été détaillé dans une présentation de Denis Ducamp (<http://www.ossir.org/ftp/supports/99/motdepasse/crackNT/>) au sein du groupe Sécurité Windows NT de l'Ossir (Observatoire de la Sécurité des Systèmes d'Information & des Réseaux). Cet outil écoute les protocoles Microsoft sur le réseau pour capturer des empreintes chiffrées non réversibles de mot de passe NT et essaye par essais successifs de retrouver les mots de passe correspondants. Cet outil peut, dans certaines entreprises, trouver jusqu'à 80% des mots de passe des utilisateurs en moins d'une journée.

La disponibilité de tous ces outils d'écoute de réseau, comme snmpsniff qui permet d'obtenir les communautés SNMP et administrer de nombreux équipements réseaux, met en danger de manière évidente les réseaux Intranets non sécurisés.

Découverte de réseau

La découverte du réseau consiste à trouver des information sur ce réseau comme les adresses IP des machines connectées, l'emplacement logique des routeurs, des serveurs de nom (DNS), des serveurs Web, des serveurs de courriers électroniques, des serveurs sensibles (applications métiers, comptabilité, stations des directeurs).

Il y a deux méthodes pour découvrir le réseau. L'une est passive discrète mais peu exhaustive. L'autre est active, plus voyante, mais très complète. La méthode passive est fondée sur l'écoute de réseau avec un sniffer comme tcpdump. Cette méthode permet de visualiser ce qui circule sur le réseau (flux Web, flux DNS, flux de courrier électronique) et de découvrir les clients et les serveurs pour chaque type d'application.

```
Une ligne de résultat de la commande : tcpdump -q dst port domain
qui sélectionne sur le réseau les requêtes DNS :
14:55:09.998063 pluton.hsc.fr.1319 > ns.hsc.fr.domain: udp 30
```

```
14:55:46.605247 neptune.hsc.fr.2657 > ns.hsc.fr.domain: udp 41
Le serveur ns.hsc.fr est très certainement, dans cet exemple, un serveur DNS.
```

Remarquons que l'écriture d'un sniffer est aujourd'hui possible en langage perl. Voici un exemple écrit pour l'occasion qui permet de découvrir des serveurs Web :

```
#!/usr/local/bin/perl -w
use Net::RawIP;
use Socket;

$a = new Net::RawIP;
$pcap=$a->pcapinit("eth0","proto \\tcp and dst port 80",1500,30);
loop $pcap,-1,\&dumpit,\@a;

sub dumpit {
    $a->bset(substr($_[2],14));
    ($ipsrc,$ipdst,$source,$dest,$data) = $a->get({ ip=>[qw(saddr
daddr)],tcp=>[qw(data source dest)]});

    print "Flux tcp/80 from ",inet_ntoa(pack("N",$ipsrc)),"[$source] to ",
        inet_ntoa(pack("N",$ipdst))"\n";
# print $data,"\n" if($data =~ /^Proxy-authorization:/);
};
```

Résultat obtenu avec ce *sniffer* (13 lignes de langage Perl) :

```
Flux tcp/80 from 192.168.2.65[1689] to 192.168.1.50
Flux tcp/80 from 192.168.2.52[1312] to 192.168.1.50
Flux tcp/80 from 192.168.1.100[1725] to 192.168.1.50

Le serveur ayant l'adresse IP 192.168.1.50 héberge très certainement un
serveur Web.
```

La découverte active est fondée sur des techniques de *scan*. Un des outils gratuits les plus connu est le programme Satan qui a beaucoup vieilli. Un des outils les plus performants (et gratuit) aujourd'hui pour effectuer le *scan* d'un réseau s'appelle Nmap. Il possède de nombreuses options de fonctionnement, il peut envoyer des paquets ICMP-echo-request (Ping) pour découvrir toutes les machines accessibles sur un réseau (même distant). Il peut aussi faire la même chose, lorsque ICMP est bloqué par les routeurs, avec des paquets TCP de type ACK et attendre les paquets de type Reset correspondants. Il est surtout capable d'établir rapidement la liste des ports TCP ou UDP accessibles sur toutes les machines de l'Intranet.

```
Résultat de la commande : nmap -O shootme.test.fr

Interesting ports on shootme.test.fr (192.168.1.77):
Port      State    Protocol  Service
21        open    tcp       ftp
22        open    tcp       ssh
42        open    tcp       nameserver
53        open    tcp       domain
80        open    tcp       http
139       open    tcp       netbios-ssn
1723      open    tcp       pptp

Remote operating system guess: Windows NT4 / Win95 / Win98
```

Attaque d'applications métiers

Les applications métiers que nous rencontrons sont très souvent vulnérables. Nous découvrons des débordements de *buffer*, des programmes CGI ou ASP mal programmés, des flux SQLNET écoutables, des DNS vulnérables, des comptes de test sans mot de passe, etc.

Il est souvent possible d'écouter des écrans Xwindow ou de visualiser des fichiers sur des partitions NFS ou SMB exportées à tout le monde. De nombreux serveurs Unix et Windows NT non mis à jour et mal configurés sont aujourd'hui encore en fonctionnement, tous sont souvent facilement "piratables". La sécurité des applications et des données qu'ils hébergent est alors hypothétique.

Dénis de service

Les attaques par déni de service sont des interruptions pures et simples de service via le réseau, comme : arrêter un serveur web à distance sans en avoir a priori le droit, faire redémarrer un routeur, saturer un réseau ou faire s'arrêter inopinément le poste de travail d'un collaborateur.

Un programme est disponible pour chacune de ces attaques, il y a même souvent plusieurs versions pour un même programme. Les programmes qui exploitent des vulnérabilités des couches logicielles au niveau du réseau portent les noms : land, teardrop, newtear, syndrop, targa, sping, bonk, boink, brkill, oshare, nestea, snork, etc.

Ces programmes sont simples d'utilisation : la seule information à fournir est, pour la plupart, le nom ou l'adresse IP de la machine distante. Un des plus dévastateurs sur un réseau de Windows NT SP3 est très certainement syndrop. Il envoie deux fragments IP qui se ré-assemblent l'un dans l'autre. Ceci arrête le système instantanément, la seule action possible est de redémarrer la machine en appuyant sur le bouton marche/arrêt. Si cette attaque est lancée contre des centaines de Windows NT SP3 sur un Intranet ayant des ramifications internationales, il faudra impérativement redémarrer, par une intervention humaine locale, toutes les machines. Qui peut se permettre de négliger ce genre d'attaque ?

D'autres vulnérabilités sont exploitables : elles sont présentes au sein même d'applications (commerciales ou non) comme, pour la gestion des courriers électroniques, Sendmail, Microsoft Exchange ou le MTA de Lotus Domino. L'outil utilisé pour démontrer ces attaques est souvent un simple telnet ou le programme à tout faire netcat.

D'autres attaques par dénis de service sont possibles en détournant le fonctionnement des protocoles réseaux au niveau IP, ICMP ou TCP. Les programmes smuf et fraggle permettent d'inonder (de saturer) des réseaux avec des paquets en jouant avec les adresses broadcast. Le programme icmp permet de générer de faux messages de contrôle comme icmp-redirect ou icmp-source-quench. Le programme synk4 permet d'envoyer des centaines de demandes de connexions TCP à une machine pour la rendre aveugle.

La liste est longue, les nuisances peuvent porter de grands préjudices.

Utilisation de ressources

L'utilisation illicite de ces ressources par un employé, un stagiaire ou un tiers, n'est

jamais bien accueillie. Il est important de savoir qu'il est de plus en plus simple d'installer des programmes sur une machine qui vont permettre à une personne de se reconnecter ultérieurement. Ceci est faisable même à travers un firewall : le programme rwwwshell, écrit en perl, est prévu pour cela. Il fonctionne sous Unix et sous Windows NT (après une petite modification) et permet à un employé, par exemple, d'exécuter des commandes sur son poste de travail (au sein d'une entreprise) depuis son accès Internet à domicile. Ce programme utilise des techniques d'encapsulation de protocole, dans ce cas il insère des commandes dans des requêtes et des réponses Web (protocole HTTP).

Ce genre de procédé est de plus en plus développé, le programme wosp encapsule des commandes dans un flux DNS, loki fait la même chose avec des paquets Ping.

Sur les machines Windows l'utilisation de ressources a fait beaucoup de bruit lors de la sortie des programmes BackOrifice et Netbus qui une fois installé permette à une ou plusieurs personnes de contrôler entièrement la machine Windows à distance.

Nous avons démontré lors d'une prestation, qu'il est possible d'encapsuler (d'imbriquer) différents types de protocoles, comme la mise en oeuvre de SSH sur PPP sur DNS.

tests d'intrusion et audits

En France, la terne image du consultant réalisant des audits plus ou moins techniques n'est pas très rassurante, ni en terme de budget ni en terme de résultat. Toutefois, en s'éloignant des "supermarchés du conseil", il est encore possible de travailler avec des consultants, artisans de la sécurité, compétents et aimant le travail bien fait.

Le véritable consultant en sécurité a, aujourd'hui, un rôle très important en France pour sensibiliser, informer et conseiller les sociétés, les organisations ou les administrations.

A l'origine de la sensibilisation de l'ensemble du personnel à la sécurité, se trouve toujours une personne interne. Cette personne doit obtenir le budget pour un projet sécurité et convaincre en peu de temps sa hiérarchie de l'existence de problèmes réels et souvent graves, de sécurité sur l'Intranet. Les prestations alors demandées aux consultants sont souvent de nature intrusive, soit un test d'intrusion externe (depuis Internet) soit un audit intrusif interne pour illustrer les attaques réalisables (ou non) depuis l'intérieur.

Le résultat de ce genre de prestation ne peut, et donc ne doit, pas être un rapport "barbare" délivré par un logiciel de détection automatique de vulnérabilités. La stratégie humaine est indispensable dans l'analyse des résultats, elle conduit souvent à la modification du scénario initial de la tentative d'intrusion après analyse des premiers résultats. Les outils présentés au paragraphe précédent automatisent certaines phases des audits intrusifs mais l'essentiel du résultat est dans l'interprétation des données obtenues et dans leur présentation aux principaux protagonistes.

Pour le client le plus grand danger d'un test d'intrusion est d'ignorer le niveau de compétence technique de son fournisseur. Toutefois, si la prestation est correctement

réalisée elle peut jouer un rôle important dans le processus de sensibilisation des décideurs, des administrateurs ou des utilisateurs.

Toutes les sociétés (dans la quasi totalité) ont déployé un réseau Intranet en un temps record avec comme seule préoccupation : le bon fonctionnement des télécommunications. Le résultat obtenu est un réseau ouvert et très fonctionnel où tous les ordinateurs peuvent communiquer entre eux. Ce résultat est à l'antipode d'un réseau sécurisé.

Lorsque la sensibilisation est en bonne voie, le niveau de sécurité du réseau doit être évalué pour déterminer le plan d'éventuelles actions. L'audit technique, proche des administrateurs et des machines, est alors la meilleure solution. Il permet la rédaction de documents de travail qui détaillent l'existant, mettent à jour les problèmes rencontrés et proposent des solutions en adéquation avec les besoins réels de l'entreprise. La pérennité du bon niveau de sécurité dépendra de la compétence des consultants mais aussi de leur volonté à informer et à former (transfert de compétences) les personnes amenées à gérer la sécurité du réseau. Ces prestations d'audit, de conseil et de formation permettent à l'entreprise de comprendre ses problèmes de sécurité et de donner les moyens nécessaires au service sécurité. La sécurité est un métier difficile qui ne doit plus être laissé à la charge des services communication. Le responsable de la sécurité doit être indépendant du directeur informatique et dépendre directement de la direction générale de l'entreprise.

conclusion

Les services sécurité des entreprises et organismes français, s'ils ont généralement affiné leur sécurité vis-à-vis d'Internet, n'ont pas encore sérieusement travaillé la sécurité de leur réseau Intranet. Rares sont ceux qui ont réussi le cloisonnement de leur réseau Intranet permettant, par exemple, d'interdire techniquement (dans chaque routeur du réseau) aux stagiaires d'accéder aux sous-réseaux de la direction ou de la comptabilité. Nombreux, par contre, sont ceux qui s'embrouillent dans la rédaction de mesures et de contre-mesures.

Aucun chef d'entreprise français ne peut se permettre aujourd'hui ne continuer à négliger la sécurité de ses réseaux en clamant qu'elle est inutile et en affirmant que tous les systèmes informatiques sont pénétrables dès lors que l'on peut engager le bon "serrurier".

La sécurité informatique, principalement dans le domaine des réseaux, fait des progrès considérables en permanence, la législation française change aussi. L'application des techniques traditionnelles comme la gestion des flux IP, l'authentification des utilisateurs la protection contre les écoutes réseau, etc., et l'utilisation de techniques plus nouvelles comme la détection d'intrusion ou le chiffrement (SSH, PGP et bientôt IPsec) vont permettre aux entreprises de se protéger convenablement. La sécurité est et restera relativement binaire, elle permet de ne prendre que les risques résiduels identifiés plutôt que de prendre des risques réels inconnus.