UE INF-2211
« Administration système/réseau »

Sujet de TP n°6 : sécurisation (très partielle) des réseaux *uranus* et *saturne*

Informations préliminaires

L'objectif de cette séance de TP est de mettre en œuvre quelques mesures élémentaires visant à sécuriser (jusqu'à un certain point) les réseaux *saturne* et *uranus* que vous administrez. Attention : les « mesures de sécurité » prises ici le sont à titre d'exemple. N'en déduisez pas que de telles mesures s'appliquent à n'importe quelle infrastructure et suffisent à la sécuriser. En matière de sécurité, chaque système informatique est un cas particulier...

1 Interception de couples login/password sur sessions telnet

Le protocole TELNET (RFC 854, mai 1983) est l'un des tout premiers protocoles permettant d'ouvrir une console sur une machine distante pour y exécuter des commandes. Il a été développé à une époque où la sécurité des transmissions n'était pas un souci majeur, et n'utilise donc aucun système de chiffrement. TELNET a peu à peu été remplacé par des solutions alternatives plus sûres telles que SSH. Cependant, beaucoup de systèmes embarqués (e.g., caméras IP, capteurs, actionneurs, commutateurs, routeurs, etc.) peuvent encore être administrés à distance via une session TELNET, ce qui peut souvent constituer une faille de sécurité majeure sur de tels équipements.

Pour illustrer cette faiblesse de TELNET, vous allez :

- installer les programmes client et serveur implémentant TELNET (i.e., paquets *telnet* et *telnetd*) sur les machines d'*uranus* et de *saturne ;*
- vérifier qu'avec la commande *telnet* vous pouvez à présent vous connecter d'une machine à l'autre (y compris d'*uranus* vers *saturne* et inversement), en passant par une phase d'authentification ;
- utiliser un outil de capture de trafic tel que *tshark* ou *wireshark* pour intercepter le trafic correspondant à l'ouverture d'une session TELNET, et vérifier que vous pouvez notamment intercepter les identifiants (i.e., *login/password)* de l'appelant ;
- effectuer de même la capture du trafic TELNET au niveau d'un goulôt d'étranglement du réseau (par exemple les machines qui desservent la liaison point-à-point *ophelia-phoebe*), et vérifier ainsi qu'un routeur est un équipement privilégié pour la capture de trafic.

Ayant constaté les faiblesses de TELNET en matière de confidentialité, reprenez les expériences précédentes en utilisant cette fois le protocole SSH (RFC 4252, janvier 2006). Vous devriez constater qu'une simple capture de trafic ne permet pas de découvrir aisément les identifiants de l'appelant, ni d'observer les commandes exécutées dans une session SSH.

2 Audit de machine ou de réseau

La commande *nmap* (contenue dans le paquet du même nom) permet « d'explorer » une machine ou un réseau (i.e., ensemble de machines), en déterminant pour chaque machine si elle est active ou inactive, et quels sont les ports ouverts sur cette machine.

Dans son utilisation la plus simple, *nmap* permet de dresser rapidement un inventaire des services déployés sur chacune des machines d'un réseau. C'est donc un outil extrêmement utile pour l'administrateur désirant s'assurer que son réseau a bien les caractéristiques désirées.

Toutefois *nmap* implémente également des algorithmes permettant par exemple de fonctionner en mode « furtif » *(stealth mode)* afin d'échapper aux systèmes de détection d'intrusion (IDS), et permettant d'exploiter certaines failles de sécurité connues. De ce point de vue, la finalité réelle de *nmap* est ambiguë, puisque cette commande est tout aussi utile à l'administrateur qu'à l'intrus potentiel.

Installez le paquet *nmap* sur votre machine, et utilisez la commande pour recenser les ports ouverts sur quelques machines de la salle CyberLab (y compris *phobos* et l'un des Raspberry Pi). Notez que le jeu d'options de cette commande est particulièrement riche, et faites-en l'expérience.

Vous pouvez également utiliser *nmap* pour examiner une machine située hors de la salle CyberLab (voire hors de l'UBS), mais vous devriez constater que le diagnostic ne vous annoncera que fort peu de ports ouverts sur cette machine. Normal : en tant que pare-feu, *phobos* ne laisse sortir que peu de choses vers l'extérieur de la salle (principalement ICMP et SSH).

3 Contrôle fin des services actifs

NB : Les opérations demandées dans cette section ne nécessitent pas d'utiliser la commande iptables*. L'objectif est de réaliser dans un premier temps une configuration fine des services déployés, pas d'installer un système pare-feu.*

3.1 Contrôle fin des montages NFS

Le serveur NFS de votre réseau exporte pour l'instant le répertoire des *homedirs* des utilisateurs. Faites en sorte qu'il exporte en outre deux répertoires supplémentaires baptisés *forum* et *shared*. Le répertoire *forum* devra pouvoir être monté en lecture seule depuis n'importe quelle machine de l'un ou l'autre des réseaux *saturne* et *uranus*. Le répertoire *shared* devra quant à lui pouvoir être monté en lecture/écriture, mais seulement depuis les machines du réseau local (i.e., *saturne* **ou** *uranus*, donc), l'accès à ce répertoire étant impossible depuis l'autre réseau local ainsi, bien sûr, que depuis le « monde extérieur ».

3.2 Contrôle fin de l'accès au service NIS

Le serveur NIS desservant votre réseau local ne doit répondre qu'aux requêtes émanant du même réseau.

3.3 Restriction d'accès à certains utilisateurs

Identifiez dans votre population de Gaulois quelques individus « dignes de confiance », et faites en sorte que seuls ces utilisateurs puissent se connecter par *ssh* sur la machine hébergeant le serveur NFS du réseau local.

Remarque : De manière générale, la connexion sur un serveur ne devrait être possible que pour quelques utilisateurs privilégiés, seuls habilités à accéder au serveur pour ensuite y faire un su root*. L'accès direct au compte root (par* ssh root@hostname*) devrait quant à lui être impossible. Toutefois, pour des raisons pratiques nous laisserons cet accès possible dans le cadre des séances de TP.*

4 Configuration de systèmes pare-feu (avec *iptables*)

4.1 Mascarade sur adresses IP dynamiques

La machine *phobos* ne perçoit plus des réseaux *uranus* et *saturne* que les machines *cordelia* et *titan*. Ses tables de routage ne contiennent que les adresses de ces deux machines.

Pour que du trafic provenant de l'une quelconque des machines d'*uranus* (resp. *saturne)* puisse être accepté et traité par *phobos*, le trafic doit transiter par *cordelia* (resp. *titan*), qui se comporte en tant que routeur pare-feu pour le réseau *uranus* (resp. *saturne*), avec fonction de mascarade activée. En d'autre

termes *cordelia* doit faire *croire* à *phobos* que tout le trafic provenant d'*uranus* émane en fait de *cordelia* elle-même. La machine *titan* fait de même pour le trafic provenant de *saturne*.

4.2 Filtrage du trafic initié localement

Pour des raisons de sécurité, il est souhaitable que les utilisateurs Gaulois ne puissent exploiter qu'un ensemble choisi de protocoles lorsqu'ils accèdent à Internet via *phobos*. Faites donc en sorte de restreindre le trafic routé par *cordelia* et *titan* afin que seuls les protocoles ICMP, SSH, NTP, et DNS soient autorisés pour le trafic initié par une machine située dans le réseau local considéré.

4.3 Filtrage du trafic transitant entre *saturne* et *uranus*

Bien que les réseaux *saturne* et *uranus* représentent des réseaux locaux qui « se font mutuellement confiance » (jusqu'à un certain point en tout cas), il est souhaitable de filtrer les paquets IP transitant par la liaison point-à-point *ophelia-phoebe* afin de ne laisser passer à travers cette liaison que le trafic réellement utile. À vous de déterminer quel est ce trafic « utile », et de configurer le filtrage sur *ophelia* et *phoebe* en conséquence.

4.4 NAT sur adresses IP statiques

L'attribution dynamique d'adresses IP par un fournisseur d'accès ne permet pas aux machines de ses « clients » d'être aisément identifiables, donc accessibles, depuis l'extérieur de leur propre réseau. Nous allons à présent considérer que les routeurs *cordelia* et *titan* se sont vus attribuer statiquement (c'est-à-dire une fois pour toutes) les adresses 192.168.3.10 et 192.168.3.20 (respectivement) par le fournisseur d'accès dont *phobos* constitue le point de présence.

— Le mécanisme de mascarade mis en œuvre précédemment doit être remplacé par un mécanisme de NAT, qui se prête mieux à la manipulation d'adresses statiques.

— Les routeurs *cordelia* et *titan* étant à présent accessibles depuis le monde extérieur, il faut à présent limiter le trafic entrant en provenance d'Internet. Faites donc en sorte que *cordelia* et *titand* n'acceptent aucun trafic entrant, et relaient en revanche le trafic SSH entrant (et ce type de trafic seulement) vers les machines *portia* et *pandore* respectivement.