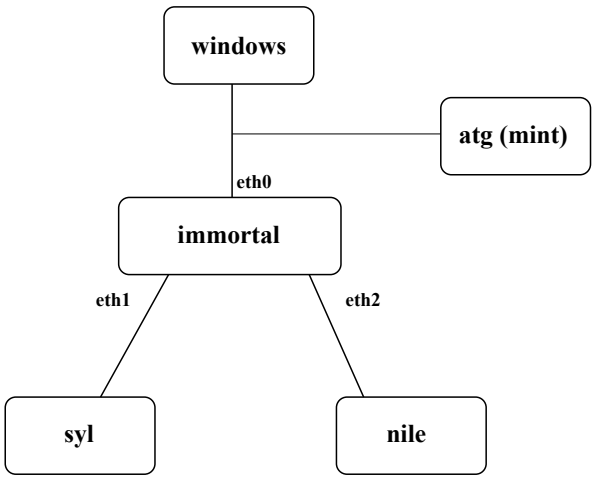
Université de Bordeaux — année 2019-2020

Master CSI/Master Info. — Sécurité des réseaux

TD - Est-il possible de faire des exploits ?

Le but de ce TP est de regarder un petit peu comment est ce qu'un attaquant peut faire pour lancer des exploits.



La topologie réseau présentée dans la figure ci-dessus correspond à celle obtenue en lançant le script La topologie réseau correspondante peut être obtenue en lançant le script de démarrage `/net/stockage/aguermou/SR/TP/4/qemunet.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initialte des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

```
cd /net/stockage/aguermou/SR/TP/4/; ./qemunet.sh -t topology -a archive_tp4.tgz
```

1. L'environnement `metasploit` est disponible sur toutes les machines linux. Il est accessible via le chemin `/opt/metasploit-framework/`. Cet environnement dispose d'un ensemble d'exploits et de shell-codes qu'il met à votre disposition. Bien entendu cet environnement est là avant tout pour valider la sécurité de votre système. Lancer la console `metasploit` avec la commande `msfconsole`. Un tutoriel illustrant l'utilisation de `metasploit` est disponible à l'URL suivante :
   `http://www.offensive-security.com/metasploit-unleashed/Introduction`.
2. Sur la machine windows un serveur TFTP fourni par *Allied Telesyn* et de version 1.9 est accessible. Ce serveur est connu pour avoir une vulnérabilité relative à la longueur du nom du fichier qu'on souhaite accéder. Essayer d'ouvrir un shell à distance à l'aide de `metasploit` sur la machine windows à partir de la machine attaquante. Il faut d'abord remarquer qu'il y a un exploit qui correspond à cette faille dans la liste des exploits fournis par `metasploit`. Ensuite, il suffit de configurer les paramètres de cet exploit pour que tout fonctionne.
3. À partir de maintenant, vous allez jouer le rôle du pirate. Un autre serveur (à définir) ayant une vulnérabilité connue tourne sur la machine windows. L'objectif de ce petit challenge est que vous puissiez exploiter la faille de ce dernier (en utilisant `metasploit`). Il vous est particulièrement demandé de motiver les choix que vous allez faire pour en arriver à l'exploitation de la faille.

4. Le navigateur `firefox` disponible sur la machine windows est vulnérable à une attaque de type buffer overflow. Vous devez donc essayer d'exploiter cette faille pour prendre le contrôle de la machine lorsque le navigateur visite votre site malveillant.
5. Nous allons maintenant utiliser un document `libreoffice` utilisant des macros pour lancer un `meterpreter` sur la machine victime lorsque l'utilisateur ouvre le document en question. Pour ce faire, il faut créer le document en utilisant l'exploit suivant.

```
Module options (exploit/multi/misc/openoffice_document_macro):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   BODY                       no        The message for the document body
   FILENAME                   yes       The OpoenOffice Text document name
   SRVHOST                    yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT   5555             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                    no        The URI to use for this exploit (default is random)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Apache OpenOffice on Linux/OSX (Python)
```