Université Sorbonne Paris Nord
Département réseaux et Télécommunications

Parcours: Cybersécurité

TRAVAUX PRATIQUES (TPS) SUR LA SUPERVISION DE SÉCURITÉ

BUT3 Cybersécurité

Superviseur:

Dr. Mohamed Amine Ouamri
Université Sorbonne Paris Nord

Travaux pratiques – année universitaire 2025/2026

1 Observation d'Internet et Analyse Malware

Objectif

Dans ce TP, vous allez réaliser une observation d'Internet comprenant, dans un premier temps, un test de connectivité et une analyse des itinéraires. Ensuite, vous vous familiariserez avec les concepts de site web compromis, d'exploit kit (kit d'exploitation) et de communication **C&C** (Command and Control). L'objectif de cet exercice est de comprendre la chaîne d'infection, c'est-à-dire les différentes étapes conduisant à l'infection. Dans ce laboratoire, vous utiliserez principalement **Wireshark** pour examiner le trafic généré par un échantillon de logiciel malveillant une pratique courante chez les analystes en renseignement sur les menaces.

Avant-propos

Lisez cet énoncé en entier afin de ne pas vous lancer dans des manipulations et configurations inutiles ; regardez notamment combien de temps est consacré à chaque partie. Notez que durant la séance, vous serez constamment évalué.

Les manipulations à exécuter sont indiquées de cette manière. ✋
Les questions auxquelles il vous est demandé de répondre sont indiquées de cette manière. ✎

1.1 Test de la connectivité et analyse des itinéraires

✋ Examinons le site WWW de l'université de Californie à Berkeley, dont le nom DNS est `www.berkeley.edu`. Lancez une capture Wireshark et testez la connectivité entre votre station et ce site grâce à l'utilitaire Ping afin de répondre aux questions ci-dessous.

✎ Quel est le protocole utilisé par Ping? Filtrez la capture Wireshark sur le protocole en question et expliquez sommairement le fonctionnement de Ping. Quelle est l'adresse IP du site web de Berkeley qu'utilise Ping ? Quel est le temps aller-retour entre votre machine et le site de Berkeley ?

✎ On veut connaître le nombre de routeurs entre votre machine et le site web d'IIJ, un fournisseur d'accès à Internet japonais : `www.iij.ad.Jp`. Pour cela, trouvez la plus petite valeur de N à partir de laquelle la commande ping -t N www.iij.ad.jp s'exécute correctement. Déduisez-en le nombre de routeurs traversés entre votre machine et www.iij.ad.jp.

✋ A partir de la capture Wireshark d'une commande Ping vers `www.iij.ad.jp`, retrouvez la valeur du champ TTL d'un paquet IP contenant une réponse ICMP (echo reply) reçue par votre machine.

✎ Déduisez-en le nombre de routeurs traversés par ce paquet, et comparez le résultat obtenu à celui de la question précédente.

✋ Les paquets de test émis par Ping sont transmis par un ensemble de routeurs à travers le réseau. Vous pouvez mesurer le délai d'acheminement d'un paquet vers les routeurs intermédiaires à l'aide de l'utilitaire traceroute. Utilisez traceroute pour déterminer le nombre de routeurs traversés lors d'une communication entre

votre machine et un serveur de votre choix

✎ Dans ce cas, comment pouvons-nous conclure sur la connexion entre votre machine et ce serveur?

✎ Lancez une capture Wireshark, puis lancez traceroute pour déterminer le nombre de routeurs entre votre station et `intranet.u-ga.fr`.

✎ Déterminez à partir de votre capture les protocoles intervenant dans le fonctionnement de traceroute et expliquer le principe de fonctionnement de chacun. Pour un TTL donné, combien de paquets sont émis ?

✋ En utilisant Wireshark, il arrive d'observer des paquets émis par traceroute avec un TTL supérieur au nombre de routeurs traversés (destination incluse) depuis votre machine.

✎ Qu'est-ce que cela vous apprend sur le fonctionnement de traceroute ?

✋ En utilisant la commande traceroute -f 10 host, contraindre traceroute à n'afficher la route entre votre machine et le site web `www.slac.stanford.edu` qu'à partir du routeur numéro 5.

✋ Servez-vous de wireshark pour examiner les requêtes DNS lancées lors de la consultation d'un serveur de noms. Il est possible de filtrer l'affichage dans wireshark pour ne visualiser que les échanges DNS à l'aide du filtre "dns". Ne tenez pas compte des échanges MDNS, qui ne relèvent pas du champ d'application de ce TP.

✎ Trouvez l'adresse IPv4 et IPv6 de lipn.univ-paris13.fr en utilisant dig ou nslookup.

✎ Quels sont les serveurs de courrier du domaine univ-paris13.fr ? Appartiennent-ils au domaine univ-paris13.fr ?

✋ Exécutez les commandes suivantes pour obtenir le nom DNS associé à l'adresse IP 128.59.21.231 (DNS inverse)

✎ Que pouvez-vous dire sur le protocole de transport du DNS ? Quel est le numéro de port utilisé par l'application DNS ?

✋ Lancez une capture Wireshark (vous pouvez filtrer pour n'observer que les échanges utilisant le protocole HTTP), puis accédez à la page web `http://evasion.imag.fr/`via votre navigateur, en utilisant le protocole HTTP (pas de HTTPS pour l'instant).

✎ Repérez dans Wireshark les échanges de PDU au niveau du protocole HTTP, en utilisant le filtre http. Utilisez la fonctionnalité de suivi de flux (clic droit sur une trame ensuite suivre et Flux TCP) pour lire l'ensemble du flux TCP qui a servi à télécharger la page HTML. Repérez-y les 3 sections principales de cet échange : en-têtes de la requête, en-têtes de la réponse, corps de la réponse.

✋ Nous allons maintenant essayer d'imiter un serveur HTTP, en répondant nous-même à des requêtes. Pour cela, nous allons ouvrir une connexion TCP en mode listen : c'est une connexion côté serveur, qui attend qu'un client se connecte à elle.

✎ À l'aide de nc-l -p 8080, trouvez comment démarrer nc en mode listen avec le port source 8080.

✋ Lancez nc de cette façon-là dans votre terminal. Votre terminal s'arrête et attend la connexion d'un client (c'est normal).

✋ Ouvrez l'URL `http://localhost:8080` dans un navigateur. Observez la requête reçue par nc.

✎ Composez une réponse HTTP correcte simple (vous devrez peut-être finir

votre réponse par Control-D ou Control-C). Vous pouvez vous aider en regardant avec Wireshark ce qu'un serveur web vous répond lorsque vous lui faites une requête depuis votre navigateur. Vérifiez que le navigateur affiche correctement votre page.

Attention

N'oubliez pas la ligne vide (deux retours à la ligne consécutifs) entre l'en-tête et le corps de votre réponse.

1.2 Analyse de l'infection par des logiciels malveillants

Dans ce laboratoire, vous utiliserez principalement Wireshark pour examiner le trafic généré par un échantillon de logiciel malveillant, ce qui est une pratique courante chez les analystes de renseignements sur les menaces. La Figure 1 illustre l'écosystème d'un kit d'exploitation typique. La première étape se produit lorsque des utilisateurs légitimes visitent un site web totalement inoffensif (légitime) mais compromis (piraté). Ils ne savent pas que le site a été compromis. Par conséquent, ils visitent le site web comme n'importe quel autre site web bénin qu'ils visitent tous les jours. À l'intérieur du site web compromis, il y a une iframe (balise HTML) qui a été injectée par les attaquants pour lancer leur attaque. La balise iframe n'est pas malveillante en soi, mais elle redirige les utilisateurs vers une autre page appelée page d'atterrissage. La redirection peut se produire plusieurs fois vers plusieurs pages d'atterrissage (en fonction de la complexité du vecteur d'attaque). La page d'atterrissage est chargée de prendre l'empreinte des navigateurs des utilisateurs, c'est-à-dire de spécifier la chaîne User-Agent, les plugins installés et les extensions sur les navigateurs de la victime. Après avoir établi le profil de l'appareil de l'utilisateur à la recherche d'une éventuelle extension ou d'un plugin vulnérable, ou de tout type de vulnérabilité dans le navigateur lui-même, la page d'atterrissage redirige les utilisateurs vers le serveur du malfaiteur, qui renvoie la charge utile à la victime.

La charge utile s'exécute sur l'appareil de la victime, puis (la plupart du temps), elle télécharge le véritable fichier malveillant sur l'ordinateur de la victime et l'exécute. C'est le rôle des kits d'exploitation dans la chaîne d'infection des logiciels malveillants. Bien que le processus semble très simple, il n'en est rien. Les kits d'exploitation sont très insaisissables. Il est difficile de les attraper en raison des nombreuses techniques de défense qu'ils utilisent. Par exemple, certains kits d'exploitation ne transmettent le véritable code malveillant qu'aux victimes de certains pays. Certains kits d'exploitation ne transmettent les données qu'une seule fois par adresse IP (par exemple, si vous envoyez deux requêtes avec une adresse IP, la deuxième requête ne recevra rien).

Le Fichier pcap fournie contient le trafic d'un ordinateur Windows infecté par un logiciel malveillant. Le scénario est basé sur l'image ci-dessus. À partir du fichier fourni relevez les informations suivantes:

- Quelles sont la date et l'heure de l'infection ?
- Quelle est l'adresse MAC de l'ordinateur Windows infecté ?
- Quelle est l'adresse IP de l'ordinateur Windows infecté ?
- Quel est le nom d'hôte de l'ordinateur Windows infecté ?

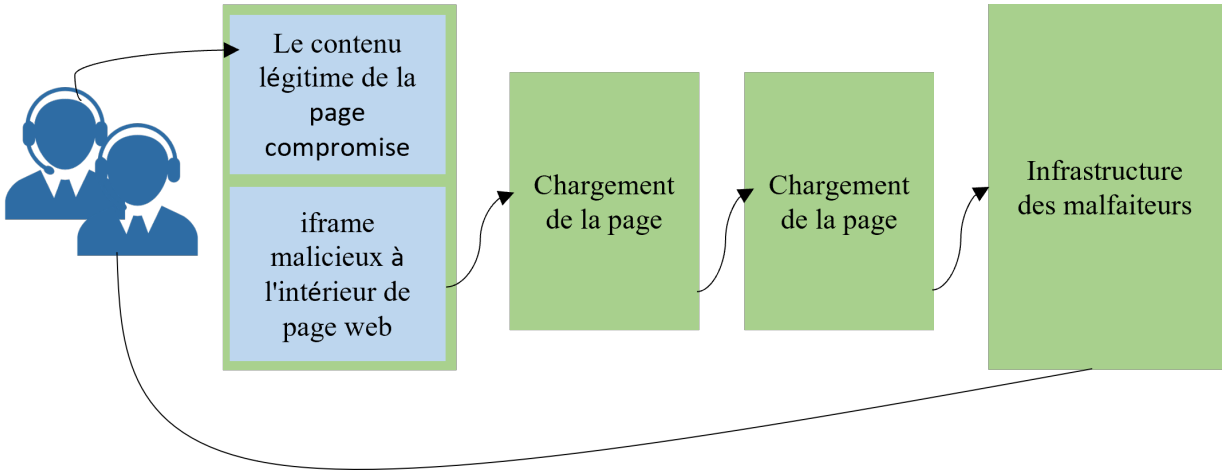


Figure 1: L'écosystème des kits d'exploitation.

✎ Quel kit d'exploitation a été utilisé pour infecter l'ordinateur de l'utilisateur ?

✎ Avant que l'ordinateur Windows ne soit infecté, qu'est-ce que l'utilisateur a recherché sur Bing?, Quel site web compromis a déclenché la chaîne d'événements de l'infection ?

✎ Quels sont les indicateurs de compromission (IOC) du pcap ?

2 Analyse des Logs HTTP avec GoAccess

Objectif

Le TP a pour but de fournir une analyse des Logs http en utilisant le Framework open source Goaccess. C'est un analyseur de journaux spécialement développé pour analyser les journaux des serveurs Web et particulièrement bien adapté pour l'analyse des logs d'Apache. Il propose une analyse en temps réel et la génération d'un rapport en HTML. Deux parties sont étudiées dans ce laboratoire, la première consiste à analyser à froid en analysant un fichier Logs contenant plusieurs milliers d'événements et avoir un aperçu des sollicitations du serveur en question. La deuxième partie consiste à analyser en temps réelle un site web fonctionnant avec apache sur notre machine de manière à avoir du contenu à analyser.

Avant-propos

Lisez cet énoncé en entier afin de ne pas vous lancer dans des manipulations et configurations inutiles ; regardez notamment combien de temps est consacré à chaque partie. Notez que durant la séance, vous serez constamment évalué.

Les manipulations à exécuter sont indiquées de cette manière. ✋ Les questions auxquelles il vous est demandé de répondre sont indiquées de cette manière. ✎

2.1 Installation de Goaccess

GoAccess permet de surveiller les journaux des serveurs web en temps réel via un tableau de bord en ligne de commande, facilitant l'analyse rapide des mesures de trafic. L'application s'exécute entièrement dans un terminal, avec des statistiques organisées en panneaux distincts sur un tableau de bord interactif. Il est également possible de générer des rapports de trafic aux formats HTML, JSON et CSV.

En tant qu'utilisateur root, exécutez les étapes suivantes :

Commande à exécuter

✋ `echo "deb http://deb.goaccess.io/ $(lsb_release -cs) main" | sudo tee -a /etc/apt/sources.list.d/goaccess.list`

Commande à exécuter

✋ `wget -O - https://deb.goaccess.io/gnugpg.key | sudo apt-key --keyring /etc/apt/trusted.gpg.d/goaccess.gpg add -`
✋ `sudo apt-get update`
✋ `sudo apt-get install goaccess`

✎ En vous servant de Google expliquez brièvement la fonctionnalité de Goaccess. Avant de commencer l'analyse, décompressé le fichier archive.zip fournit durant la séance du TP. Les journaux des serveurs Web contiennent des informations sur

tous les événements enregistrés. Ils contiennent de nombreuses informations sur les visiteurs du site web, leur comportement, les robots d'indexation qui accèdent au site, des informations commerciales, des questions de sécurité, etc.

2.2 Analyse des Logs à froid

Nous souhaitons analyser le fichier de log access.log du serveur Web facilement et visualiser le nombre de requêtes arrivant sur ce serveur afin d'avoir un nombre précis de visiteurs. L'objectif est de visualiser depuis un portail Web ou en mode terminal Linux le trafic HTTP entrant sur le serveur en question.

Comme le fichier access.log est volumineux, nous allons filtrer afin d'afficher les données d'une seul journée en exécutant la commande suivante:

Commande à exécuter

```
head -n 1000000 access.log | docker run --rm -i -e
LANG=$LANG allinurl/goaccess -a -o html --log-format COMBINED
- > report.html
```

Vérifier que votre report.html a été bien créé ? Expliquer la syntaxe de la commande head ?

Ouvrir le fichier repodrt.html avec le navigateur Google-chrome ? Donner la commande appliquée ?

Visualiser le tableau de bord généré afin d'analyser les données du site

Rechercher les informations qui vous intéressent en priorité à savoir le nombre de requête valide et échouer, les adresses IP, les noms des sites. . . .etc.

2.3 Création d'un site et analyse en temps réelle

Dans cette section, vous allez créer un site appache qui servira de test pour Goaccess. Pour rappel, apache propose deux types de configuration, les sites virtuels, qui sont déclarés dans /etc/apache2/sites-available et les alias, qui sont déclarés dans /etc/apache2/conf-available. Ces répertoires contiennent tous les sites et alias. Cependant, tous ces sites et alias ne sont pas actifs. Pour savoir quels éléments le sont réellement le contenu des dossiers suivants les sites virtuels actifs sont visibles dans /etc/apache2/sites-enabled et les alias actifs sont visibles dans /etc/apache2/conf-enabled.

Créez maintenant deux sites qui vous servirons de test pour GoAccess. Dans le dossier /etc/apache2/sites-available, créez un fichier 002-sitetest.conf.

Ensuite dans /var/www et comme illustré ci-dessus, créez un dossier nommé sitetest avec un fichier index.php dont le contenu est :

Vérifier le bon fonctionnement de votre site et l'affichage des logs dans votre fichier .Log

À partir de votre fichier .Log récupéré L'adresse IP du client, la date et l'heure de la requête http, la requête http (GET), le code statuts renvoyé par le serveur apache, la taille de l'objet retourné.

Afin de remplir les logs, créer une page test.html avec comme contenu une image. Demander à vos camarade de faire plusieurs test et notamment provoqué des erreurs en appelant Test.html

```
<VirtualHost *:80>
        ServerName serveur.domVMID.net
        ServerAdmin admin@domVMID.net
        DocumentRoot /var/www/sitetest
        DirectoryIndex index.php

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/sitetest.log combined

        <Directory /var/www/sitetest>
                Options -Indexes +FollowSymlinks
                AllowOverride All
                Require all granted
        </Directory>

</VirtualHost>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Figure 2: Enter Caption

```
<?php
phpinfo();
?>
```

Figure 3: Commande à réaliser

✎ Avec le Framework Goaccess (s'il est bien installé) vous pouvez voir en temps réelle les adresses IP, le nombre de visiteurs, le nombre de pages... etc. Utiliser la commande suivante :

Commande à exécuter

☞ `goaccess /var/log/apache2/sitetest.log`

⚠ Attention

NB. Faite plusieurs requête pour observer le bon fonctionnement en temps réelle. En effet, vous le verrait apparaitre immédiatement des informations sur votre Framework.

✎ Refaite la manipulation de la partie 1 et obtenez un rapport avec des graphiques (Tableau de bord) de toutes les informations sur votre site

3 Analyse des logiciels malveillants (Malware).

Objectif

Une machine virtuelle Windows (VM) est l'un des outils les plus importants pour analyser les logiciels malveillants. Une VM permet de déboguer les logiciels malveillants sans craindre d'infecter l'hôte. Si la VM est infectée, il est possible de revenir rapidement à un instantané propre pour poursuivre l'analyse. Les logiciels malveillants peuvent souvent détecter qu'ils sont exécutés à l'intérieur de la VM et n'affichent aucun comportement (ils restent dormants). Par exemple, les logiciels malveillants peuvent vérifier si l'environnement est réaliste, en particulier la quantité de mémoire vive et le nombre de cœurs de la machine Windows. La configuration recommandée pour votre machine Windows est de 2 cœurs et de 4 à 8 Go. Toutefois, vous pouvez également affecter moins de ressources à votre machine. Dans cette session, vous installerez et configurerez une VM Windows 7 gratuite sur votre machine hôte à l'aide de VirtualBox et d'INetSim, une suite logicielle permettant de simuler des services Internet courants dans un environnement de laboratoire, par exemple pour analyser le comportement du réseau d'échantillons de logiciels malveillants inconnus. Après avoir configuré le laboratoire, vous analyserez le comportement réseau d'un échantillon de logiciel malveillant fourni.

Avant-propos

Lisez cet énoncé en entier afin de ne pas vous lancer dans des manipulations et configurations inutiles ; regardez notamment combien de temps est consacré à chaque partie. Notez que durant la séance, vous serez constamment évalué.

Les manipulations à exécuter sont indiquées de cette manière. ✋ **Les questions auxquelles il vous est demandé de répondre sont indiquées de cette manière.** ✎

3.1 Installation de VirtualBox

✋ Installation de VirtualBox. Si vous souhaitez installer VirtualBox sur votre machine hôte (de préférence un système d'exploitation Linux), rendez-vous sur la page de téléchargement de VirtualBox https://www.virtualbox.org/wiki/Downloads et choisissez le programme d'installation correspondant à votre système d'exploitation. Téléchargez et exécutez le programme d'installation et suivez les instructions d'installation. Si vous ne parvenez pas à installer VirtualBox sur votre système d'exploitation Linux, demandez de l'aide à Google.

✋ Installation d'une VM Windows gratuite. Pour télécharger les VM gratuites, rendez-vous sur la page de téléchargement des VM de Microsoft à l'adresse suivante : https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/.

✋ Téléchargez le fichier `.zip` et décompressez-le sur votre hôte. Le dossier `zip` doit contenir un fichier `.ova`. Ensuite, ouvrez VirtualBox et sélectionnez **File ensuite Import Appliance**. Sélectionnez le chemin d'accès au fichier `.ova` que

vous venez de décompresser et cliquez sur **Continuer**. Il vous sera alors demandé de sélectionner les paramètres de l'appliance. Si possible, augmentez le nombre de CPU à 2. Enfin, cliquez sur **Import** pour importer la VM. Cette opération peut prendre un certain temps. Une fois la VM importée, vous devez prendre un *instantané* avant de la mettre sous tension.

3.2 Installation d'Inetsim

✋ INetSim. Visitez le site https://www.inetsim.org pour télécharger INetSim. Il y a plusieurs façons de télécharger le logiciel, il suffit de suivre les instructions fournies sur le site web. Notez que le logiciel doit être installé sur votre machine hôte (de préférence sous Linux).

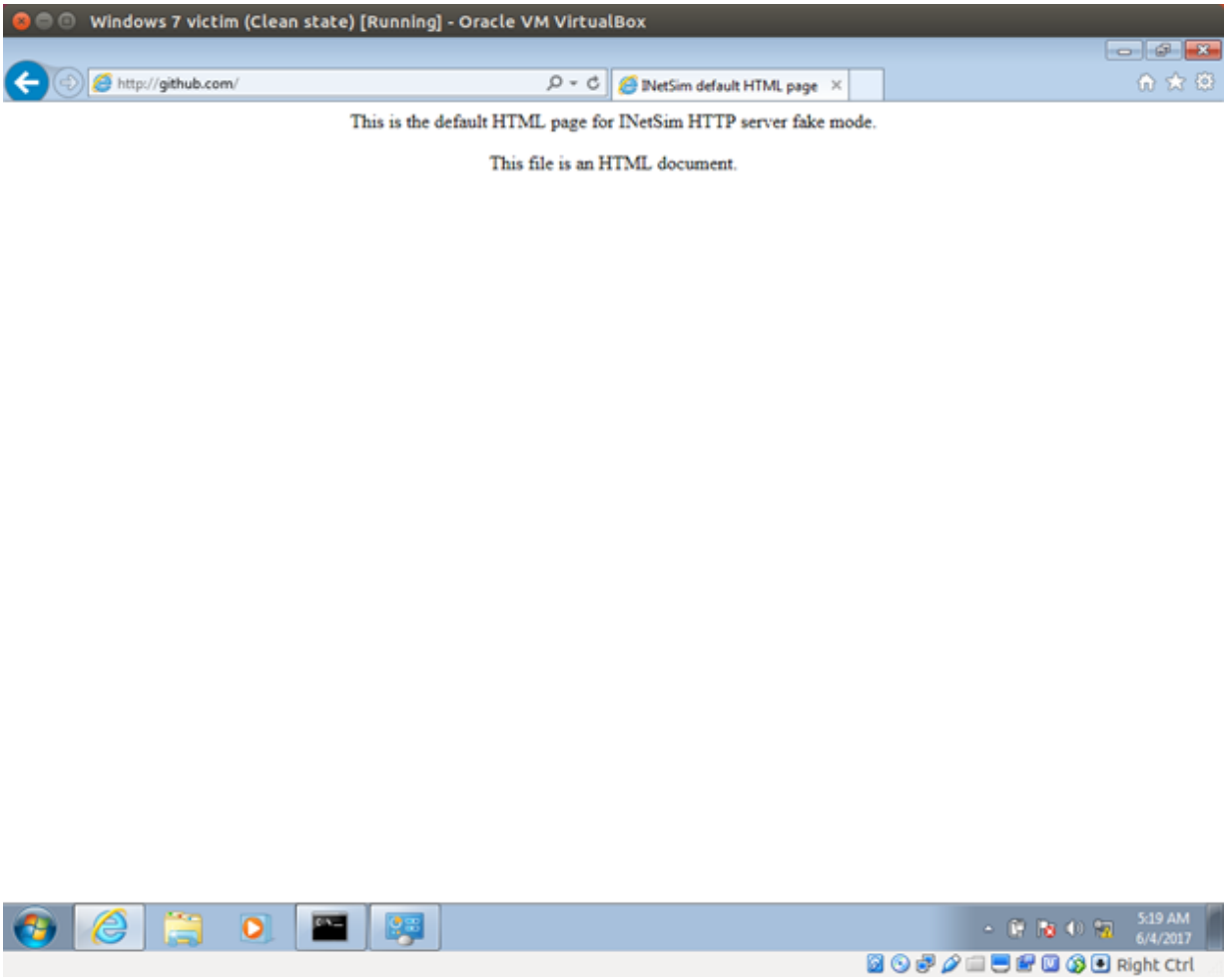
✋ Cliquez avec le bouton droit de la souris sur l'icône du réseau dans la barre des tâches (ou allez dans le menu **Démarrer- Panneau de configuration- Réseau et Internet- Centre de réseau et de partage**), puis cliquez sur **Connexion au réseau local -Propriétés**. Sélectionnez **Protocole Internet Version 4** et cliquez sur le bouton **Propriétés**. Nous allons maintenant configurer l'adresse IP de votre machine victime, sa passerelle par défaut et un serveur DNS. Dans votre machine hôte Linux, vérifiez les interfaces disponibles en utilisant, par exemple, la commande `ifconfig` et identifiez l'adresse IP assignée à votre VirtualBox. Utilisez-la comme passerelle par défaut sur votre machine victime. Ensuite, assignez une IP statique sur votre machine victime appartenant au même réseau local et configurez le serveur DNS (appartenant également au même réseau local). Vérifiez la connectivité et faites un *snapshot* de votre VM.

✋ Comme indiqué précédemment, **INetSim** permet d'émuler une large gamme de services Internet standards, notamment `DNS`, `HTTP(S)`, `SMTP`, etc. Il possède un fichier de configuration par défaut : `/etc/inetsim/inetsim.conf`, qui est très bien documenté. Il est également livré avec un répertoire de données : `/var/lib/inetsim`, contenant divers fichiers par défaut, par exemple un modèle de page web. Pour les besoins de ce laboratoire, configurez uniquement les services suivants: DNS,HTTP, HTTPS, ICMP.

✋ Maintenant, lançons INetSim. Allumez votre VM victime, ouvrez le navigateur Internet Explorer et naviguez sur le site web configuré (par exemple, http://www.liglab.fr). Tout le trafic doit être redirigé vers INetSim et un site web par défaut doit s'afficher, par exemple :

✋ À un moment donné, vous voudrez évidemment transférer des fichiers de la machine hôte vers la machine victime (dans notre cas, Windows VM) ; nous mettrons en place un partage de fichiers pour y parvenir. Éteignez votre VM. Dans la VirtualBox qui exécute la machine victime, allez dans Devices -Shared Folders- Shared folders settings (Périphériques- Dossiers partagés -Paramètres des dossiers partagés). Créez un nouveau dossier partagé, choisissez le dossier local de votre système d'exploitation hôte auquel il doit être associé et choisissez un nom. Cochez la case pour qu'il soit permanent, monté automatiquement et en lecture seule (s'il n'est pas en lecture seule, les logiciels malveillants peuvent essayer d'écrire/chiffrer le consentement du répertoire partagé). S'il n'est pas monté automatiquement, montez le dossier partagé sur la machine hôte (demandez à Google). Faites un autre instantané.

✋ Exécutez Wireshark sur la machine hôte et assurez-vous que vous écoutez sur l'interface vbox. Exécutez nslookup, ping, et visitez des sites web prédéfinis


Windows 7 victim (Clean state) [Running] - Oracle VM VirtualBox
http://github.com/
INetSim default HTML page
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
5:19 AM
6/4/2017
Right Ctrl

sur votre machine victime (par exemple http://www.liglab.fr).

3.3 Analyse du Malware

✋ Vous êtes maintenant prêt à analyser des échantillons de logiciels malveillants. Téléchargez des échantillons de logiciels malveillants à partir de https://bazaar.abuse.ch/browse (pass : 'infected') ainsi que des échantillons de logiciels malveillants sélectionnés à partir de (samples.tar.gz). Décompressez le fichier, puis décompressez chacun des 10 échantillons et déplacez-les dans le dossier partagé afin de pouvoir y accéder dans votre machine victime virtuelle. Chacun des échantillons est protégé par un mot de passe (pass : 'infected'). Afin d'exécuter les échantillons à partir de samples.tar.gz, vous devez changer les extensions de fichiers en '.exe' pour les rendre exécutables. Lancez Wireshark sur votre machine hôte et exécutez chaque échantillon pendant au moins 5 minutes. Il se peut qu'ils aient un comportement ou qu'ils restent dormants. Notez que vous êtes en sécurité. INetSim n'autorisera aucune transmission de trafic vers l'Internet. Analysez le fichier pcap et déterminez les domaines et les adresses IP auxquels les logiciels malveillants tentent de se connecter (et pourquoi ?). Mettez à jour le fichier de configuration d'INetSim avec les noms de domaine et les hôtes auxquels les logiciels malveillants tentent de se connecter. Par exemple, le logiciel malveillant peut essayer de résoudre un nom de domaine "dns.example.com", qui peut être un serveur DNS géré par l'attaquant.

4 Mise en œuvre d'un environnement virtuel pour l'étude des attaques DDoS et leur mitigation

Objectif

Une attaque par déni de service distribué (DDoS) vise à submerger un réseau, un service ou un serveur avec un trafic excessif provenant de multiples sources, le rendant indisponible pour les utilisateurs légitimes. La détection et la réponse à ce type d'attaque sont essentielles pour garantir la disponibilité et la performance des services en ligne. Ce TP vous apprend à détecter et à répondre à une attaque DDoS en utilisant différents outils et techniques.

Avant-propos

Lisez cet énoncé en entier afin de ne pas vous lancer dans des manipulations et configurations inutiles ; regardez notamment combien de temps est consacré à chaque partie. Notez que durant la séance, vous serez constamment évalué.

Connaissances de base en réseaux
— Maîtrise de la ligne de commande Linux
— Connaissances des protocoles HTTP, TCP/IP, etc.
— Ordinateur avec au moins 8 Go de RAM et 20 Go d'espace disque libre.
— Logiciel de virtualisation (VirtualBox, VMware, etc.)

Configuration du laboratoire

Machines virtuelles :

- VM1 : Machine attaquante (Kali Linux)
- VM2 : Machine victime (Ubuntu Server)
- VM3 : Machine de surveillance et réponse (Ubuntu Desktop)

Réseau :

- Créer un réseau virtuel commun entre toutes les VMs
- Attribuer des adresses IP statiques

Outils : Wireshark, tcpdump, DDoSify, Snort, fail2ban, netstat

Tâches à réaliser

Tâche 1 : Simulation d'une attaque DDoS

Installation de DDoSify

```
sudo apt-get update
sudo apt-get install ddosify
```

Lancer l'attaque

```
ddosify -t http://¡IP-Victime¿ -n 1000 -c 100
```

Résultat attendu : le serveur web devient lent ou non réactif.

Tâche 2 : Capture du trafic réseau

Installer Wireshark et tcpdump

```
sudo apt-get update
sudo apt-get install wireshark tcpdump
```

Capturer le trafic réseau

```
sudo tcpdump -i eth0 -w ddos-attack.pcap
```

Résultat attendu : un fichier `ddos-attack.pcap` est généré.

Tâche 3 : Analyse du trafic avec Wireshark

Ouvrir le fichier dans Wireshark

```
wireshark ddos-attack.pcap
```

Résultat attendu : identification des adresses IP responsables du trafic excessif.

Tâche 4 : Détection de l'attaque avec Snort

Installer Snort

```
sudo apt-get update
sudo apt-get install snort
```

Configurer le fichier `/etc/snort/snort.conf` pour inclure des règles de détection DDoS.

Lancer Snort en mode IDS

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Résultat attendu : alertes en console signalant un trafic suspect.

Tâche 5 : Mitigation avec fail2ban

Installer fail2ban

```
sudo apt-get update
sudo apt-get install fail2ban
```

Configurer le fichier `jail.local` avec le contenu suivant :

```
[http-get-dos]
enabled = true
port = http,https
filter = http-get-dos
logpath = /var/log/apache2/access.log
maxretry = 300
findtime = 300
bantime = 3600
```

Redémarrer fail2ban

```
sudo systemctl restart fail2ban
```

Résultat attendu : les adresses IP malveillantes sont automatiquement bannies.