

Dans le cadre de **SECURIDAY 2009**

SECURINETS



Présente

Atelier : Collecte de malwares avec un Honeypot

Formateurs: 1. Boussaid Henda

2. Mkacher Mahdi

3. Msallem Emna

4. Tbourbi Hamdi

1. Présentation :

Un honeypot (en français pot de miel) est un ordinateur ou un programme volontairement vulnérable destiné à attirer et à piéger les pirates informatiques.

Le but de cet atelier est d'utiliser un honeypot afin de surveiller le réseau pour collecter des informations sur les différents bots qui circulent dans le réseau. Ensuite, analyser ces informations pour pouvoir découvrir les défaillances du réseau à protéger et les motivations des pirates.

On compte deux types de honeypots qui ont des buts et des fonctionnalités bien distinctes :

- ✓ Les honeypots à faible interaction.
- ✓ Les honeypots à forte interaction.

1. Honeypots à faible interaction :

Ils sont les plus simples de la famille des honeypots. Leur but est de récolter un maximum d'informations tout en offrant un minimum de privilèges aux pirates. Ils permettent de limiter les risques au maximum. Contrairement à un honeypot à forte interaction, il ne fait que simuler ces services et ne les possède pas réellement. Ils ne peuvent donc pas être exploités par les malwares pour se déployer.

2. Honeypots à forte interaction :

Ce type de honeypots peut être considéré comme le côté extrême du sujet puisqu'il repose sur le principe de l'accès à de véritables services sur une machine du réseau plus ou moins sécurisée.

→ Les risques sont beaucoup plus importants que pour les honeypots à faible interaction. Il apparaît donc nécessaire de sécuriser au maximum l'architecture du réseau pour que l'attaquant ne puisse pas rebondir et s'en prendre à d'autres machines.

3. Outils utilisés :

2.1 Nepenthes

Nepenthes est un honeypot à faible interaction s'exécutant côté serveur sous Linux et simulant des services (réseau) Windows vulnérables. Il collecte des malwares étant faits pour s'exécuter dans un environnement Windows (car il simule des services Windows).

Nepenthes est disponible dans ce lien : <http://nepenthes.carnivore.it/>

3.2 Amun

Amun est aussi un honeypot à faible interaction. Il est basé sur XML et Python, ce qui lui rend facile à étendre.

Amun est disponible dans ce lien : <http://amunhoney.sourceforge.net/>

3.3 Surfnetids

C'est un logiciel qui est composé par plusieurs parties nous allons dans notre atelier exploiter une partie de surfnetids qui est le logging server.

L'exploitation du logging server est constituée de 2 parties, la base de données et une interface web.

La base de données est utilisée pour stocker les informations de l'analyse du pot de miel. Cette information est présentée aux utilisateurs dans une interface web qui assure le suivi de l'état du capteur d'informations.

4. Installation et configuration :

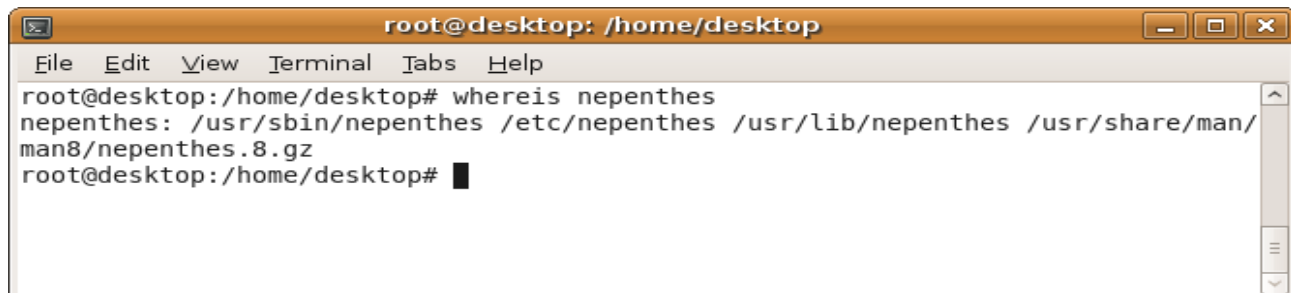
3.1 Nepenthes :

Afin d'installer Nepenthes, on commence par exécuter la commande :

```
# apt-get install nepenthes
```

Cette commande va nous installer le paquet Nepenthes et tous les autres paquets nécessaires.

On peut par la suite vérifier que Nepenthes est bien installé comme suit :



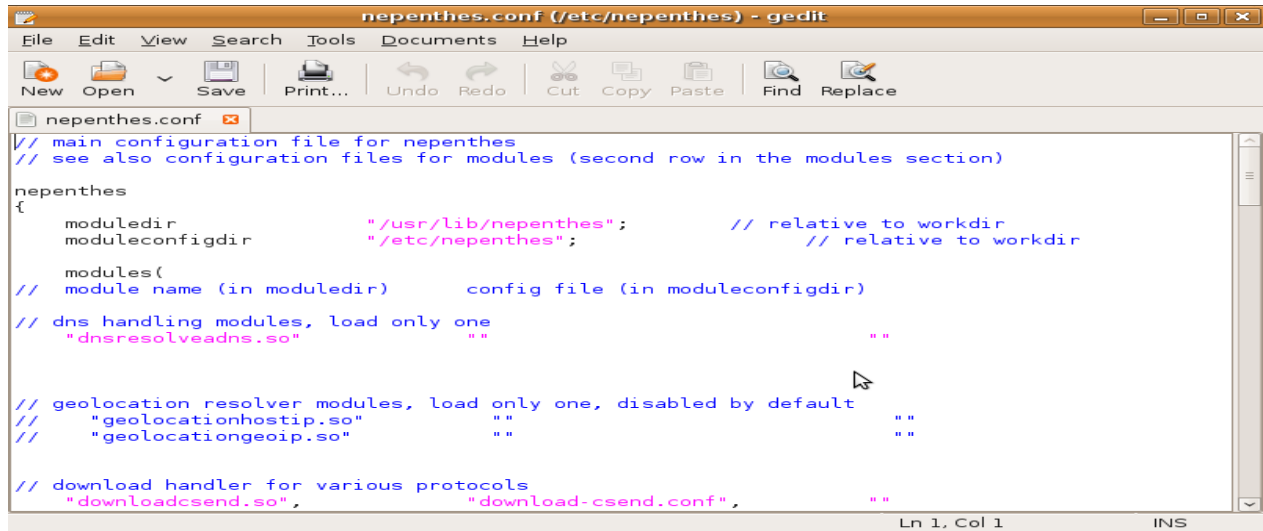
```
root@desktop: /home/desktop
File Edit View Terminal Tabs Help
root@desktop:/home/desktop# whereis nepenthes
nepenthes: /usr/sbin/nepenthes /etc/nepenthes /usr/lib/nepenthes /usr/share/man/
man8/nepenthes.8.gz
root@desktop:/home/desktop#
```

Parmi les avantages de Nepenthes c'est qu'il suffit de l'installer et il va commencer la

S E C U R I N E T S

Club de la sécurité informatique
I N S A T

collecte. En effet, il ne nécessite pas une configuration bien spécifique. Le fichier de configuration par défaut est suffisant.



```
nependthes.conf (/etc/nependthes) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
nependthes.conf
// main configuration file for nependthes
// see also configuration files for modules (second row in the modules section)
nependthes
{
    moduledir                "/usr/lib/nependthes";        // relative to workdir
    moduleconfigdir         "/etc/nependthes";          // relative to workdir

    modules(
// module name (in moduledir)      config file (in moduleconfigdir)
// dns handling modules, load only one
    "dnsresolveadns.so"          ""
    ""

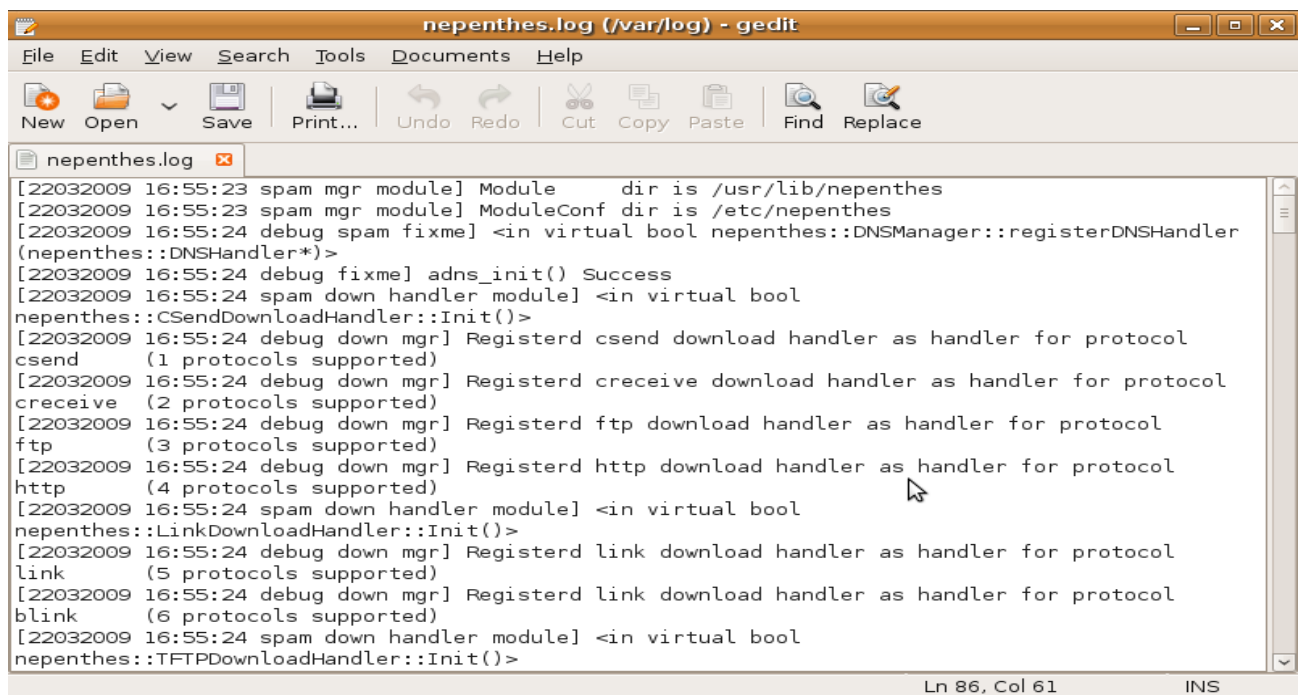
// geolocation resolver modules, load only one, disabled by default
// "geolocationhostip.so"        ""
// "geolocationgeoip.so"        ""

// download handler for various protocols
    "downloadcsend.so",          "download-csend.conf",    ""
    )
}
Ln 1, Col 1      INS
```

Après la collecte, les informations sont enregistrées dans des fichiers log. Pour y accéder on tape :

```
# gedit /var/log/nependthes.log
```

Voici ci-dessous un exemple de fichier log :



```
nependthes.log (/var/log) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
nependthes.log
[22032009 16:55:23 spam mgr module] Module      dir is /usr/lib/nependthes
[22032009 16:55:23 spam mgr module] ModuleConf dir is /etc/nependthes
[22032009 16:55:24 debug spam fixme] <in virtual bool nependthes::DNSManager::registerDNSHandler
(nependthes::DNSHandler*)>
[22032009 16:55:24 debug fixme] adns_init() Success
[22032009 16:55:24 spam down handler module] <in virtual bool
nependthes::CSendDownloadHandler::Init()>
[22032009 16:55:24 debug down mgr] Registered csend download handler as handler for protocol
csend
(1 protocols supported)
[22032009 16:55:24 debug down mgr] Registered creceive download handler as handler for protocol
creceive
(2 protocols supported)
[22032009 16:55:24 debug down mgr] Registered ftp download handler as handler for protocol
ftp
(3 protocols supported)
[22032009 16:55:24 debug down mgr] Registered http download handler as handler for protocol
http
(4 protocols supported)
[22032009 16:55:24 spam down handler module] <in virtual bool
nependthes::LinkDownloadHandler::Init()>
[22032009 16:55:24 debug down mgr] Registered link download handler as handler for protocol
link
(5 protocols supported)
[22032009 16:55:24 debug down mgr] Registered link download handler as handler for protocol
blink
(6 protocols supported)
[22032009 16:55:24 spam down handler module] <in virtual bool
nependthes::TFTPDownloadHandler::Init()>
Ln 86, Col 61      INS
```

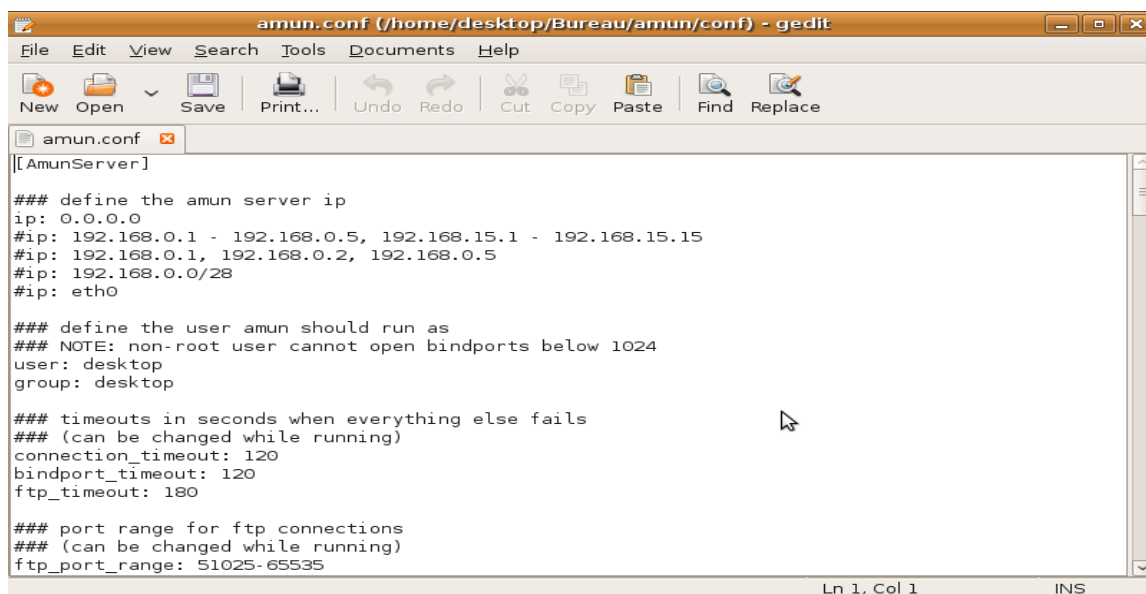
4.2 Amun

Afin d'installer Amun, il suffit de télécharger la dernière version du fichier tar à partir du site déjà spécifier en dessus (<http://amunhoney.sourceforge.net/>).

Ensuite, il y a d'autres paquets nécessaires qu'on peut télécharger à partir du gestionnaire de paquets synaptic. Les paquets sont les suivants : Python 2.4 ; Python Psyc (disponible dans <http://psyco.sourceforge.net/>);MySQLdb ; psycopg2 .

Par la suite on doit modifier la configuration en éditant le fichier « amun.conf ».

Dans ce fichier on peut modifier l'adresse ip du serveur (Rq : mettre cette adresse « 0.0.0.0 » si on veut que Amun reste en écoute sur toutes les interfaces),le nom d'utilisateur, le groupe, le timeout et plusieurs autres informations.



```
[AmunServer]
### define the amun server ip
ip: 0.0.0.0
#ip: 192.168.0.1 - 192.168.0.5, 192.168.15.1 - 192.168.15.15
#ip: 192.168.0.1, 192.168.0.2, 192.168.0.5
#ip: 192.168.0.0/28
#ip: eth0

### define the user amun should run as
### NOTE: non-root user cannot open bindports below 1024
user: desktop
group: desktop

### timeouts in seconds when everything else fails
### (can be changed while running)
connection_timeout: 120
bindport_timeout: 120
ftp_timeout: 180

### port range for ftp connections
### (can be changed while running)
ftp_port_range: 51025-65535
```

Puis pour lancer Amun on tape la commande suivante :

```
#!/amun_server.py
```

Amun va donc rester en écoute et collecter des informations sur les bots. Ces informations seront enregistrées dans les fichiers log se trouvant dans «le dossier « logs »».

4.3 Surfnetids :

Pour installer le logging server on doit utiliser ubuntu 6.06 (dapper) car les dépôts php4 et postgresql8.1 sont toujours valable. Pour installer le serveur on tape dans la ligne de commande :

1.étape :

```
apt-get install postgresql-8.1 libclass-dbi-pg-perl perl php4 libapache2-mod-php4  
libfreetype6 libpq4 php4-common php4-gd php4-pgsql apache2 libphp-phplot libmime-lite-  
perl libgnupg-perl libmail-pop3client-perl libio-socket-ssl-perl sudo libapache2-mod-auth-  
pgsql libmime-perl sendmail xalan
```

2.étape :

```
svn checkout http://svn.ids.surfnet.nl/surfids/logserver/tags/stable-2.00.03/  
/tmp/surfnetids/logserver/
```

```
cd /tmp/surfnetids/logserver/
```

3.étape :

```
./install_log.pl
```

Pour la configuration, Les fichiers sont localisés dans : `/etc/surfnetids/surfnetids-log.conf`. (Rq : on doit ajouter dans les fichiers de configuration le login et le mot de passe de la base de données qu'on a déjà créer).

5. Comparaison entre Nepenthes et Amun

Nepenthes	Amun
Honeypot à faible interaction.	Honeypot à faible interaction.
Collecte automatique de malwares tel que les bots.	Collecte de malwares se propageant de façon autonome sur le réseau.
Emulation des vulnérabilités connues.	Emulation des vulnérabilités des services réseaux connues.
Extraction d'informations à partir du payload d'exploit puis téléchargement des malwares essayant d'exploiter les vulnérabilités du réseau.	Téléchargement de payload malicieux afin de les analyser.
Implémenté en c++.	Implémenté en python et basé sur XML donc sa maintenance et son extension de modules

	sont plus faciles.
Contient les modules suivants : <ul style="list-style-type: none">● Modules de vulnérabilités qui émulent des services existants comportant des vulnérabilités.● Modules d'analyse du contenu envoyé par les modules de vulnérabilités.● Modules de récupération, qui utilisent les informations reçues par les modules d'analyse afin de télécharger le malware.● Modules de chargement qui s'occupent de stocker le malware.● Modules de génération de log qui enregistrent toutes les informations concernant l'émulation.	Contient les modules suivants : <ul style="list-style-type: none">● Modules de vulnérabilités.● Modules d'analyse du contenu des payload.● Modules de récupération.● Modules de téléchargement des malwares.● Soumission, des malwares à analyser, vers des sandbox.● Modules de génération de fichiers log.

Conclusion

Le honeypot aussi récent Amun, a suivi une approche similaire à Nepenthes dans la mesure où il fait la collecte des malwares par émulation des services réseaux vulnérables puis le téléchargement des payload malicieux afin de les analyser.

La différence principale entre Nepenthes et Amun est que ce dernier est implémenté en python ce qui facilite son extension et sa maintenance.

Amun est apparu début 2008, par contre nepenthes existe depuis l'année 2005 et il a été testé par pas mal de personne et a prouvé son efficacité.