TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

I. Honeypot

Honeypot adalah suatu cara untuk menjebak atau menangkal usaha-usaha penggunaan yang tidak memiliki otoritas dalam sebuah sistem informasi. Honeypot merupakan pengalih perhatian hacker, agar ia seolah-olah berhasil menjebol dan mengambil data dari sebuah jaringan, padahal sesungguhnya data tersebut tidak penting dan lokasi tersebut sudah terisolir.

II. Klasifikasi Honeypot

1. Low Intercation Honeypot

Low Interaction Honeypot merupakan honeypot dengan tingkat interaksi rendah, yaitu honeypot yang didesain untuk mengemulasikan service seperti pada server yang asli. Penyerang hanya mampu memeriksa dan terkoneksi ke satu atau beberapa port.

Kelebihan:

- Mudah di install, dikonfigurasi, deployed, dan dimaintain
- Mampu mengemulasi suatu layanan seperti http, ftp, telnet, dan sebagainya.
- Difungsikan untuk deteksi serangan, khususnya pada proses scanning atau percobaan.

Kekurangan:

- Layanan yang di berikan hanya berupa emulasi, sehingga penyerang tidak dapat berinteraksi secara penuh dengan layanan yang diberikan atau sistem operasinya secara langsung
- Informasi yang bisa kita dapatkan dari penyerang sangat minim.
- Apabila serangan dilakukan oleh "real person" bukan "automated tools" mungkin akan segera menyadari bahwa yang sedang dihadapi merupakan mesin honeypot, karena keterbatasan layanan yang bisa diakses.

2. High Interaction Honeypot

High Interaction Honeypot terdapat sistem operasi dimana penyerang dapat berinteraksi langsung dan tidak ada batasan yang membatasi interaksi tersebut. Menghilangkan batasan-batasan tersebut menyebabkan tingkat risiko yang dihadapi semakin tinggi karena penyerang dapat memiliki akses root.

Pada saat yang sama, kemungkinan pengumpulan informasi semakin meningkat dikarenakan kemungkinan serangan yang tinggi. Dikarenakan penyerang dapat berinteraksi secara penuh dengan sistem operasi apabila si penyerang telah mendapat akses root.

Kelebihan:

- Penyerang berinteraksi langsung dengan sistem yang nyata termasuk diantaranya sistem operasi, network, hingga layanan yang diberikan seperti web service, ssh service, mail service, dan lain-lain.
- Umumnya dibangun suatu sistem khusus dengan topologi yang telah dipersiapkan.
- Sistem tersebut biasanya terdiri dari berbagai macam implementasi dari teknologi keamanan yang banyak digunakan untuk melindungi suatu sistem, seperti firewall, IDS/IPS, router, dan lain-lain.
- Target serangan berupa sistem operasi sebenarnya yang siap untuk berinteraksi secara langsung dengan penyerang.

Kekurangan:

- Perencanaan dan implementasi sistem jauh lebih rumit dan dibutuhkan banyak pertimbangan.
- High-interaction honeypot bersifat tidak efisien karena membutuhkan pengawasan berkala.
- Apabila telah diambil alih oleh penyerang maka honeypot tersebut dapat menjadi ancaman bagi jaringan yang ada.

III. Kippo

Kippo adalah media interaksi honeypot SSH yang buat menggunakan bahasa Python. Kippo digunakan untuk mencatat serangan brute force dan keseluruhan interaksi shell yang dilakukan oleh seorang penyerang.

Fitur:

- Fake filesystem dengan kemampuan untuk menambahkan/menghapus file. Full fake filesystem termasuk menyerupai instalasi Debian 5.0.
- Membuat fake file content seolah-olah penyerang berhasil masuk.
- Menyimpan log serangan.
- Sama seperti Kojoney, Kippo menyimpan file unduhan dengan wget untuk pemeriksaan nanti.

Instalasi Kippo:

"apt-get install authbind" // install authbind

```
root@sam-VirtualBox:/home/sam# apt-get install authbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  authbind
0 upgraded, 1 newly installed, 0 to remove and 449 not upgraded.
Need to get 19,6 kB of archives.
After this operation, 101 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu/ trusty/main authbind i386 2.1.1 [19,6
 kB]
Fetched 19,6 kB in 1s (12,0 kB/s)
Selecting previously unselected package authbind.
(Reading database ... 168187 files and directories currently installed.)
Preparing to unpack .../authbind_2.1.1_i386.deb ...
Unpacking authbind (2.1.1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up authbind (2.1.1) ...
```

"useradd -d /home/kippo -g sudo -s /bin/bash -m kippo" // menambahkan penguna baru kippo non-root untuk menjalankan kippo sebagai grup sudo.

```
root@sam-VirtualBox:/home/sam# useradd -d /home/kippo -g sudo -s /bin/bash -m kippo
```

"touch /etc/authbind/byport/22" // membuat file baru.

```
root@sam-VirtualBox:/home/sam# touch /etc/authbind/byport/22
```

"chown kippo /etc/authbind/byport/22" // mengubah izin hanya kippo yang dibolehkan.

```
root@sam-VirtualBox:/home/sam# chown kippo /etc/authbind/byport/22
```

"sudo apt-get install openssh-server" // menginstall openssh-server.

```
root@sam-VirtualBox:/etc/ssh# sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libck-connector0 ncurses-term openssh-client openssh-sftp-server
  ssh-import-id
Suggested packages:
  libpam-ssh keychain monkeysphere rssh molly-guard
The following NEW packages will be installed:
  libck-connector0 ncurses-term openssh-server openssh-sftp-server
  ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 5 newly installed, 0 to remove and 441 not upgraded.
Need to get 1.199 kB of archives.
After this operation, 3.488 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

"service ssh start" // mengaktifkan service ssh.

```
root@sam-VirtualBox:/etc/ssh# sudo service ssh start
start: Job is already running: ssh
```

“nano /etc/ssh/sshd_config” // mengubah port 22 menjadi 2222 pada file konfigurasi ssh_config.

```
root@sam-VirtualBox:/etc/ssh# ls
moduli       ssh_host_dsa_key      ssh_host_ecdsa_key.pub    ssh_host_rsa_key
ssh_config   ssh_host_dsa_key.pub  ssh_host_ed25519_key      ssh_host_rsa_key.pub
sshd_config  ssh_host_ecdsa_key    ssh_host_ed25519_key.pub  ssh_import_id
root@sam-VirtualBox:/etc/ssh# nano ssh_config
Use "fg" to return to nano.

[2]+  Stopped                 nano ssh_config
```

```
  GNU nano 2.2.6                        File: ssh_config

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 22
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
#   EscapeChar ~

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

```
  GNU nano 2.2.6                        File: ssh_config                                  Modified

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.
```

```
Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 2222
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
#   EscapeChar ~

^G Get Help       ^O WriteOut       ^R Read File      ^Y Prev Page      ^K Cut Text       ^C Cur Pos
^X Exit           ^J Justify        ^W Where Is       ^V Next Page      ^U UnCut Text     ^T To Spell
```

“service ssh restart” // merestart service ssh.

```
root@sam-VirtualBox:/etc/ssh# service ssh restart
ssh stop/waiting
ssh start/running, process 8991
```

“apt-get install python-dev openssl python-openssl python-pyasn1 python-twisted” // menginstall kippo dependensi karena kippo ssh membutuhkan beberapa library python.

```
root@sam-VirtualBox:/home/sam# apt-get install python-dev openssl python-openssl python-pyasn1 python-twisted
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-openssl is already the newest version.
python-openssl set to manually installed.
The following extra packages will be installed:
  libexpat1 libexpat1-dev libpython-dev libpython2.7 libpython2.7-dev
  libpython2.7-minimal libpython2.7-stdlib python-twisted-conch
  python-twisted-lore python-twisted-mail python-twisted-names
  python-twisted-news python-twisted-runner python-twisted-words python2.7
  python2.7-dev python2.7-minimal
Suggested packages:
  python-twisted-runner-dbg python2.7-doc binfmt-support
The following NEW packages will be installed:
  libexpat1-dev libpython-dev libpython2.7-dev python-dev python-pyasn1
  python-twisted python-twisted-conch python-twisted-lore python-twisted-mail
  python-twisted-names python-twisted-news python-twisted-runner
  python-twisted-words python2.7-dev
The following packages will be upgraded:
  libexpat1 libpython2.7 libpython2.7-minimal libpython2.7-stdlib openssl
  python2.7 python2.7-minimal
7 upgraded, 14 newly installed, 0 to remove and 442 not upgraded.
Need to get 28,0 MB of archives.
After this operation, 36,9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main libexpat1 i386 2.1.0-4ubuntu1.3 [71,3 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main python2.7 i386 2.7.6-8ubuntu0.3 [197 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main libpython2.7 i386 2.7.6-8ubuntu0.3 [978 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main libpython2.7-stdlib i386 2.7.6-8ubuntu0.3 [1.848 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main python2.7-minimal i386 2.7.6-8ubuntu0.3 [1.116 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main libpython2.7-minimal i386 2.7.6-8ubuntu0.3 [307 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main libexpat1-dev i386 2.1.0-4ubuntu1.3 [113 kB]
Get:8 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main libpython2.7-dev i386 2.7.6-8ubuntu0.3 [21,8 MB]
Get:9 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main openssl i386 1.0.1f-1ubuntu2.22 [480 kB]
Get:10 http://id.archive.ubuntu.com/ubuntu/ trusty/main libpython-dev i386 2.7.5-5ubuntu3 [7.090 B]
Get:11 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main python2.7-dev i386 2.7.6-8ubuntu0.3 [269 kB]
Get:12 http://id.archive.ubuntu.com/ubuntu/ trusty/main python-dev i386 2.7.5-5ubuntu3 [1.176 B]
Get:13 http://id.archive.ubuntu.com/ubuntu/ trusty/main python-pyasn1 all 0.1.7-1ubuntu2 [44,2 kB]
Get:14 http://id.archive.ubuntu.com/ubuntu/ trusty/main python-twisted-lore all 13.2.0-1ubuntu1 [65,8 kB]
Get:15 http://id.archive.ubuntu.com/ubuntu/ trusty/main python-twisted-mail all 13.2.0-1ubuntu1 [168 kB]
Get:16 http://id.archive.ubuntu.com/ubuntu/ trusty/main python-twisted-names all 13.2.0-1ubuntu1 [78,4 kB]
```

“apt-get install subversion” // menginstall kippo menggunakan subversion.

```
root@sam-VirtualBox:/home/sam# apt-get install subversion
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  subversion-tools db5.3-util
The following NEW packages will be installed:
  subversion
0 upgraded, 1 newly installed, 0 to remove and 442 not upgraded.
Need to get 276 kB of archives.
After this operation, 1.352 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main subversion i386 1.8.8-1ubuntu3.2 [276 kB]
Fetched 276 kB in 5s (49,4 kB/s)
Selecting previously unselected package subversion.
(Reading database ... 168876 files and directories currently installed.)
Preparing to unpack .../subversion_1.8.8-1ubuntu3.2_i386.deb ...
Unpacking subversion (1.8.8-1ubuntu3.2) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up subversion (1.8.8-1ubuntu3.2) ...
```

“su kippo” // mengganti user menjadi kippo.

```
root@sam-VirtualBox:/home/sam# su kippo
```

“apt-get install git” // menginstall git

```
root@sam-VirtualBox:/home/sam# apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-arch git-bzr git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 442 not upgraded.
Need to get 3.021 kB of archives.
After this operation, 22,0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://id.archive.ubuntu.com/ubuntu/ trusty/main liberror-perl all 0.17-1.
1 [21,1 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main git-man all 1:1.9
.1-1ubuntu0.4 [699 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu/ trusty-updates/main git i386 1:1.9.1-
1ubuntu0.4 [2.301 kB]
```

“git clone https://github.com/desaster/kippo.git” // download latest kippo version dari GitHub.

```
root@sam-VirtualBox:/home/sam# git clone https://github.com/desaster/kippo.git
Cloning into 'kippo'...
remote: Counting objects: 1544, done.
remote: Total 1544 (delta 0), reused 0 (delta 0), pack-reused 1544
Receiving objects: 100% (1544/1544), 2.64 MiB | 102.00 KiB/s, done.
Resolving deltas: 100% (929/929), done.
Checking connectivity... done.
```

“cp kippo.cfg.dist kippo.cfg; nano kippo.cfg” // mengubah nama file konfigurasi dan mengubah port 2222 menjadi 22 pada konfigurasi kippo.

```
root@sam-VirtualBox:/home/sam/kippo# ls
data  doc        honeyfs  kippo.cfg.dist  log        start.sh  txtcmds
dl    fs.pickle  kippo    kippo.tac       README.md  stop.sh   utils
root@sam-VirtualBox:/home/sam/kippo# cp kippo.cfg.dist kippo.cfg
root@sam-VirtualBox:/home/sam/kippo# nano kippo.cfg
```

```
  GNU nano 2.2.6                File: kippo.cfg

#
# Kippo configuration file (kippo.cfg)
#

[honeypot]

# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
#ssh_addr = 0.0.0.0

# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 2222

# Hostname for the honeypot. Displayed by the shell prompt of the virtual
# environment.
#
                              [ Read 201 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

```
  GNU nano 2.2.6                File: kippo.cfg                Modified

#
# Kippo configuration file (kippo.cfg)
#

[honeypot]

# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
#ssh_addr = 0.0.0.0

# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 22

# Hostname for the honeypot. Displayed by the shell prompt of the virtual
# environment.
#

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

“nano start.sh” // mengubah konfigurasi start.sh pada kippo ssh “twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid” menjadi “authbind twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid”

```
root@sam-VirtualBox:/home/sam/kippo# nano start.sh
```

```
  GNU nano 2.2.6                File: kippo.cfg                Modified

#
# Kippo configuration file (kippo.cfg)
#

[honeypot]

# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
#ssh_addr = 0.0.0.0

# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 22

# Hostname for the honeypot. Displayed by the shell prompt of the virtual
# environment.
#

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

```
  GNU nano 2.2.6                          File: start.sh

#!/bin/sh

set -e

cd $(dirname $0)

if [ "$1" != "" ]
then
    VENV="$1"

    if [ ! -d "$VENV" ]
    then
        echo "The specified virtualenv \"$VENV\" was not found!"
        exit 1
    fi

    if [ ! -f "$VENV/bin/activate" ]
    then
        echo "The specified virtualenv \"$VENV\" was not found!"
        exit 2
    fi

    echo "Activating virtualenv \"$VENV\""
    . $VENV/bin/activate
fi

twistd --version

echo "Starting kippo in the background..."
twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid
```

```
  GNU nano 2.2.6                          File: start.sh                                  Modified

#!/bin/sh

set -e

cd $(dirname $0)

if [ "$1" != "" ]
then
    VENV="$1"

    if [ ! -d "$VENV" ]
    then
        echo "The specified virtualenv \"$VENV\" was not found!"
        exit 1
    fi

    if [ ! -f "$VENV/bin/activate" ]
    then
        echo "The specified virtualenv \"$VENV\" was not found!"
        exit 2
    fi

    echo "Activating virtualenv \"$VENV\""
    . $VENV/bin/activate
fi

twistd --version

echo "Starting kippo in the background..."
authbind --deep twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid
```

“./start.sh” // menjalankan kippo ssh.

```
kippo@sam-VirtualBox:/home/sam/kippo$ ./start.sh
```

IV. Daftar Pustaka

- Anonim, 2016, Kippo, [online], (https://en.wikipedia.org/wiki/Kippo, diakses tanggal 25 April 2017)
- Anonim, 2016, Kippo, [online], (https://github.com/desaster/kippo, diakses tanggal 25 April 2017)
- Anonim, 2014, Pengertian dan Klasifikasi Honeypot, [online], (http://www.kajianpustaka.com/2014/07/pengertian-dan-klasifikasi-honeypot.html, diakses tanggal 25 April 2017)
- Anonim, 2013, How To Install Kippo, an SSH Honeypot, on an Ubuntu Cloud Server, [online], (https://www.digitalocean.com/community/tutorials/how-to-install-kippo-an-ssh-honeypot-on-an-ubuntu-cloud-server, diakses tanggal 25 April 2017)