**wowHoneypot**

設定ファイル：~/wowhoneypot/config.txt

# Install

<https://github.com/morihisa/WOWHoneypot>

$sudo apt update/upgrade

$ufw設定(22, 80, 8080)

$sudo vi /etc/ufw/before.rules（↓参照3）

* + 「\*filter」より前に下記の４行を追記する。

----------------------------------------------------------------------

\*nat

:PREROUTING ACCEPT [0:0]

-A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080

COMMIT

----------------------------------------------------------------------

$sudo ufw reload

$cd ~/

$git clone https://github.com/morihisa/WOWHoneypot.git wowhoneypot

$cd wowhoneypot

$python3 ./wowhoneypot.py

#Script

<https://qiita.com/hogehuga/items/cad931485f58ae487d53#%E8%87%AA%E5%8B%95%E8%B5%B7%E5%8B%95%E8%A8%AD%E5%AE%9A%E3%81%A8%E7%A2%BA%E8%AA%8D>

$vi /home/webadmin/wowhoneypot.sh

----------------------------------------------------------------------

#!/bin/bash

cd /home/webadmin/wowhoneypot

/usr/bin/python3 /home/webadmin/wowhoneypot/wowhoneypot.py ----------------------------------------------------------------------

$chmod 775 wowhoneypot.sh

$vi /etc/systemd/system/wowhoneypot.service

----------------------------------------------------------------------

[Unit]

Description=WoWHoneypot daemon

Documentation=https://github.com/morihisa/WOWHoneypot

[Service]

ExecStart = /home/webadmin/wowhoneypot.sh

ExecRestart = /bin/kill -WINCH ${MAINPID} ; /home/webadmin/wowhoneypot.sh

ExecStop = /bin/kill -WINCH ${MAINPID}

Restart = no

Type = simple

User = webadmin

Group = webadmin

[Install]

WantedBy = multi-user.target

----------------------------------------------------------------------

$chmod 755 /etc/systemd/system/wowhoneypot.service

$systemctl enable wowhoneypot.service

$systemctl start wowhoneypot.service

$ps -ef | grep wowhoneypot

$chown -R webadmin:root /home/webadmin/wowhoneypot/

＃SSL対応化

<https://graneed.hatenablog.com/entry/2018/06/14/231740#1-WOWHoneypot%E3%81%AESSL%E5%AF%BE%E5%BF%9C>

1. ufw設定（443, 44333）
2. $sudo vi /etc/ufw/before.rules（↓参照3）
   * 「\*filter」より前に下記の４行を追記する。

----------------------------------------------------------------------

\*nat

:PREROUTING ACCEPT [0:0]

-A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 44333

COMMIT

----------------------------------------------------------------------

1. $sudo ufw reload
2. $mkdir wowhoneypotssl
3. $cd wowhoneypotssl
4. $cp　（必要なものをwowhoneypot/からコピー）
5. 資料を参考にwowhoneypot.pyとconfig.txtをいじる
6. $openssl req -new -x509 -keyout ./server.pem -out ./server.pem -days 365 -nodes
7. python3 ./wowhoneypot.py

-memo-

Country Name (2 letter code) [AU]:JP  
State or Province Name (full name) [Some-State]:Saitama  
Locality Name (eg, city) [Default City]:Hatoyama-machi  
Organization Name (eg, company) [Default Company Ltd]:TDU  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:info.rd.dendai.ac.jp  
Email Address []:

＃エラー

（#Script）wowhoneypotsslの実行ファイルが起動できなかったので、おかしいと思い、実行ファイルの実行者をrootにしたところできた。なのでwebadminでもできるように、以下のコマンドでwowhoneypotsslディレクトリの配下全ての所有グループと所有ユーザーをwebadminに変えた。

$chown -R webadmin:webadmin /home/webadmin/wowhoneypotssl/

#cron設定

<https://plaza.rakuten.co.jp/nwnote/diary/201901020000/>

#systemctlのサービス削除手順

$systemctl stop [servicename]

$systemctl disable [servicename]

$rm /etc/systemd/system/[servicename]

$rm /etc/systemd/system/[servicename] symlinks that might be related

$systemctl daemon-reload

$systemctl reset-failed

＃擬似Dionaea作成

1. config.txt
   1. Apache --> nginx
2. /art/default配下
   1. post.htmlとsample.htmlは削除
   2. hello.htmlを書き換え

<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>

<title>404 - Not Found</title>

</head>

<body>

<h1>404 - Not Found</h1>

</body>

</html>

1. /art配下
   1. res200.html作成

<html>

<head>

<title>Test</title>

</head>

<body>

<h1>test</h1>

</body>

</html>

* 1. res501.html作成

<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>

<title>501 - Not Implemented</title>

</head>

<body>

<h1>501 - Not Implemented</h1>

</body>

</html>

1. mrrules.xml書き換え（dio-mrrules.txtを参照）
2. $systemctl restart wowhoneypot.service
3. ssl側も同様
4. $systemctl restart wowhoneypotssl.service

#正規C Aによる署名付き証明書の作成（DNS-01チャレンジ）

<https://qiita.com/gbgb-ojisan/items/be8a35270a84b6b7ca2e>

$git clone https://github.com/letsencrypt/letsencrypt

$cd letsencrypt

$letsencrypt-auto --help

$./certbot-auto certonly --manual --server https://acme-v02.api.letsencrypt.org/directory --preferred-challenges dns -d info.rd.dendai.ac.jp -m 17rd225@ms.dendai.ac.jp --agree-tos --manual-public-ip-logging-ok

// 出てきた文字列をDNSサーバ管理者に渡して、自分はEnterも押さずに待機

// DNSサーバ側ができたらEnter

// 結果はwow/let’s\_encrypt.txt

// 作成された証明書等は/etc/letsencrypt/live/$domein/

// 9.15 〜 12.15

#ドメインやIPアドレスで情報取得

$nslookup example.co.jp

$dig \*\*\*（ドメイン）

$whois \*\*\*

$host \*\*\*(ドメイン)

#ポートスキャン

$nmap -sT -sU -T3 -A -v http://xx.xx.xx.xx

#証明書確認コマンド

$openssl s\_client -connect 133.14.14.248:443 -showcerts

#ログ収集自動化計画

$chmod 754 hoge.sh

$chmod 754 analysis.py

$service cron start

$cp /etc/crontab /etc/cron.d/cron\_test

$vi /etc/cron.d/cron\_test

#毎日正子にシェルスクリプトを実行する

0 0 \* \* \* root /bin/sh /home/hoge/automate.sh

#リスタート

00 0,6,12,18 \* \* \* root /bin/sh /home/restart.sh

$service cron restart