

Lab 5a: UDP e DNS

Aluno: Guilherme Rodriguez Vicentin

E-mail: vicentingr@gmail.com

1 - Análise dos protocolos TCP/UDP/DNS

Neste primeiro exercício, iremos monitorar os pacotes enviados do cliente 1 para o servidor web. Para isso, utilizaremos o nome de domínio `web.inf634.br` ao invés do endereço de IP diretamente. Desta forma, conseguiremos observar o processo de resolução de nomes de domínio também.

```
$ docker exec -it cliente1 bash
```

```
root@cliente1:/# tcpdump -i eth0 -n -s 0 -w /home/lab5a-tarefa1.pcap &
root@cliente1:/# links http://web.inf534.br
root@cliente1:/# killall tcpdump
```

Agora, vamos analisar o arquivo `lab5a-tarefa1.pcap` no Wireshark.

1.1 - Análise do pacote DNS

User Datagram Protocol, Src Port: 59328, Dst Port: 53

Source Port: 59328

Destination Port: 53

Length: 39

Checksum: 0x827e [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

[Timestamps]

UDP payload (31 bytes)

User Datagram Protocol, Src Port: 53, Dst Port: 59328

Source Port: 53

Destination Port: 59328

Length: 55

Checksum: 0x828e [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

[Timestamps]

UDP payload (47 bytes)

Podemos observar que o cliente enviou uma requisição DNS para o servidor DNS (porta 53) utilizando o protocolo UDP na camada de transporte e recebeu uma resposta.

lab5a-tarefa1.pcap

Apply a display filter ... <=>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::42:aff:fe0a::...	ff02::9	RIPng	126	Command Response, Version 1
2	3.173499	10.10.10.100	224.0.0.9	RIPv2	86	Response
3	5.767882	10.10.10.10	10.10.100.40	DNS	73	Standard query 0xb4f2 A web.inf534.br
4	5.767888	10.10.10.10	10.10.100.40	DNS	73	Standard query 0x01ef AAAA web.inf534.br
5	5.768058	10.10.100.40	10.10.10.10	DNS	89	Standard query response 0xb4f2 A web.inf534
6	5.768201	10.10.100.40	10.10.10.10	DNS	101	Standard query response 0x01ef AAAA web.inf
7	5.768435	2001:db8:2021:10::...	2001:db8:2021:100::...	TCP	94	35662 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=
8	5.768703	2001:db8:2021:100::...	2001:db8:2021:10::...	TCP	94	80 → 35662 [SYN, ACK] Seq=0 Ack=1 Win=64260
9	5.768722	2001:db8:2021:10::...	2001:db8:2021:100::...	TCP	86	35662 → 80 [ACK] Seq=1 Ack=1 Win=64896 Len=
10	5.768970	2001:db8:2021:10::...	2001:db8:2021:100::...	HTTP	694	GET / HTTP/1.1
11	5.769032	2001:db8:2021:100::...	2001:db8:2021:10::...	TCP	86	80 → 35662 [ACK] Seq=1 Ack=609 Win=64128 Le
12	5.769336	2001:db8:2021:100::...	2001:db8:2021:10::...	HTTP	489	HTTP/1.1 200 OK (text/html)
13	5.769344	2001:db8:2021:10::...	2001:db8:2021:100::...	TCP	86	35662 → 80 [ACK] Seq=609 Ack=404 Win=64512
14	8.004197	fe80::42:aff:fe0a::...	ff02::9	RIPng	126	Command Response, Version 1
15	10.874232	02:42:0a:0a:0a:0a	02:42:0a:0a:0a:64	ARP	42	Who has 10.10.10.100? Tell 10.10.10.10
16	10.874265	fe80::42:aff:fe0a::...	2001:db8:2021:10::...	ICMPv6	86	Neighbor Solicitation for 2001:db8:2021:10:
17	10.874295	02:42:0a:0a:0a:64	02:42:0a:0a:0a:0a	ARP	42	10.10.10.100 is at 02:42:0a:0a:0a:64
18	10.874312	fe80::42:aff:fe0a::...	2001:db8:2021:10::...	ICMPv6	86	Neighbor Solicitation for 2001:db8:2021:10:
19	10.874351	2001:db8:2021:10::...	fe80::42:aff:fe0a::...	ICMPv6	78	Neighbor Advertisement 2001:db8:2021:10::10
20	10.874325	02:42:0a:0a:0a:64	02:42:0a:0a:0a:0a	ARP	42	Who has 10.10.10.10? Tell 10.10.10.100
21	10.874384	02:42:0a:0a:0a:0a	02:42:0a:0a:0a:64	ARP	42	10.10.10.10 is at 02:42:0a:0a:0a:0a
22	10.874406	2001:db8:2021:10::...	fe80::42:aff:fe0a::...	ICMPv6	78	Neighbor Advertisement 2001:db8:2021:10::10
23	11.653236	2001:db8:2021:10::...	2001:db8:2021:100::...	TCP	86	35662 → 80 [FIN, ACK] Seq=609 Ack=404 Win=6
24	11.653408	2001:db8:2021:100::...	2001:db8:2021:10::...	TCP	86	80 → 35662 [FIN, ACK] Seq=404 Ack=610 Win=6
25	11.653423	2001:db8:2021:10::...	2001:db8:2021:100::...	TCP	86	35662 → 80 [ACK] Seq=610 Ack=405 Win=64512
26	12.173857	10.10.10.100	224.0.0.9	RIPv2	86	Response
27	15.005550	fe80::42:aff:fe0a::...	ff02::9	RIPng	126	Command Response, Version 1

> Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured
 > Ethernet II, Src: 02:42:0a:0a:0a:64 (02:42:0a:0a:0a:64), D:
 > Internet Protocol Version 6, Src: fe80::42:aff:fe0a:a64, D:
 > User Datagram Protocol, Src Port: 521, Dst Port: 521
 > RIPng

0000 33 33 00 00 00 09 02 42 0a 0a 0a 64 86 dd 6c 07 33
 0010 9f f0 00 48 11 ff fe 80 00 00 00 00 00 00 00 42 ...
 0020 0a ff fe 0a 0a 64 ff 02 00 00 00 00 00 00 00 ...
 0030 00 00 00 00 00 09 02 09 02 09 00 48 11 96 02 01 ...
 0040 00 00 20 01 0d b8 20 21 00 10 00 00 00 00 00 ...
 0050 00 00 00 00 40 01 20 01 0d b8 20 21 00 50 00 ...
 0060 00 00 00 00 00 00 00 00 40 01 20 01 0d b8 20 21 ...
 0070 01 00 00 00 00 00 00 00 00 00 00 00 40 02 ...

Figure 1: Tarefa 1

1.2 - Análise do pacote TCP

Abaixo podemos acompanhar o handshake TCP entre o cliente e o servidor web. Podemos ver o envio do SYN por parte do cliente e a resposta SYN/ACK do servidor. Por fim, o cliente envia o ACK para finalizar o handshake. A comunicação é realizada entre as portas 35662 (cliente) e 80 (servidor).

Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 0, Len: 0

```
Source Port: 35662
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 2959018940
[Next Sequence Number: 1      (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
Window: 64800
[Calculated window size: 64800]
Checksum: 0x9d12 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOO)
[Timestamps]
```

Transmission Control Protocol, Src Port: 80, Dst Port: 35662, Seq: 0, Ack: 1, Len: 0

```
Source Port: 80
Destination Port: 35662
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 2072583494
[Next Sequence Number: 1      (relative sequence number)]
Acknowledgment Number: 1      (relative ack number)
Acknowledgment number (raw): 2959018941
1010 .... = Header Length: 40 bytes (10)
Flags: 0x012 (SYN, ACK)
Window: 64260
[Calculated window size: 64260]
Checksum: 0x9d12 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
```

Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP)
[Timestamps]
[SEQ/ACK analysis]

Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 35662
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2959018941
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2072583495
1000 = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window: 507
[Calculated window size: 64896]
[Window size scaling factor: 128]
Checksum: 0x9d0a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]

1.3 - Análise do pacote DNS

Observando os mesmos pacotes do item 1.1, porém agora na camada de aplicação ao invés de transporte, podemos ver o conteúdo da requisição DNS.

Domain Name System (query)
Transaction ID: 0xb4f2
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries

```
web.inf534.br: type A, class IN
[Response In: 5]
```

```
Domain Name System (query)
Transaction ID: 0x01ef
Flags: 0x0100 Standard query
  0... .. = Response: Message is a query
  .000 0... .. = Opcode: Standard query (0)
  .... ..0. .... = Truncated: Message is not truncated
  .... ...1 .... = Recursion desired: Do query recursively
  .... .... .0.. .... = Z: reserved (0)
  .... .... ...0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  web.inf534.br: type AAAA, class IN
[Response In: 6]
```

Estamos solicitando o endereço IP do domínio `web.inf534.br` utilizando tanto o tipo A (IPv4) quanto AAAA (IPv6).

Obtivemos de resposta os seguintes pacotes:

```
Domain Name System (response)
Transaction ID: 0xb4f2
Flags: 0x8580 Standard query response, No error
  1... .. = Response: Message is a response
  .000 0... .. = Opcode: Standard query (0)
  .... .1.. .... = Authoritative: Server is an authority for domain
  .... ..0. .... = Truncated: Message is not truncated
  .... ...1 .... = Recursion desired: Do query recursively
  .... .... 1... .. = Recursion available: Server can do recursive queries
  .... .... .0.. .... = Z: reserved (0)
  .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authentic
  .... .... ...0 .... = Non-authenticated data: Unacceptable
  .... .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  web.inf534.br: type A, class IN
    Name: web.inf534.br
    [Name Length: 13]
    [Label Count: 3]
```

```

        Type: A (1) (Host Address)
        Class: IN (0x0001)
Answers
    web.inf534.br: type A, class IN, addr 10.10.100.10
[Request In: 3]
[Time: 0.000256000 seconds]

Domain Name System (response)
Transaction ID: 0x01ef
Flags: 0x8580 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .1... .. = Authoritative: Server is an authority for domain
    .... ..0... .. = Truncated: Message is not truncated
    .... ...1... .. = Recursion desired: Do query recursively
    .... .... 1... .. = Recursion available: Server can do recursive queries
    .... .... .0... .. = Z: reserved (0)
    .... .... ..0... .. = Answer authenticated: Answer/authority portion was not authentic
    .... .... ...0... .. = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
    web.inf534.br: type AAAA, class IN
        Name: web.inf534.br
        [Name Length: 13]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
Answers
    web.inf534.br: type AAAA, class IN, addr 2001:db8:2021:100::10
[Request In: 4]
[Time: 0.000313000 seconds]

```

Recebemos os IPs 10.10.100.10 e 2001:db8:2021:100::10 como resposta para os tipos A e AAAA, respectivamente.

1.4 - Análise do protocolo HTTP

Por fim, podemos observar a requisição HTTP feita pelo cliente ao servidor web. Requisitamos a página principal do domínio `web.inf534.br`.

```

Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: web.inf534.br\r\n

```


2 - Registros DNS

Neste exercício, iremos rodar o seguinte comando a partir do cliente 1 e analisar o resultado.

```
$ docker exec -it cliente1 bash
```

```
root@cliente1:/# tcpdump -i eth0 -n -s 0 -w /home/lab5a-tarefa2.pcap &
root@cliente1:/# ping -n -4 R1.inf543.br
```

Recebemos a resposta do servidor de DNS, dizendo que não existe um registro para o domínio R1.inf543.br.

```
9  3.370487  10.10.100.40  10.10.10.10 DNS 151 Standard query response 0xb1a4 No such n
10 3.370538  10.10.100.40  10.10.10.10 DNS 151 Standard query response 0x94a1 No such n
```

Para resolver o problema, podemos adicionar um registro DNS para o domínio R1.inf543.br no servidor DNS.

Buscando nos arquivos de configuração do servidor DNS, encontramos o arquivo /etc/bind/master/inf534.zone com os seguintes registros:

```
dns:/# cat /etc/bind/master/inf534.zone
$TTL 86400
```

```
@ IN SOA inf534.br root.inf534.br (
    2023040901
    3600
    900
    604800
    86400
)
```

```
@      IN NS dns
; servidor de dns com apelido para bind
dns      IN A   10.10.10.40
bind      IN CNAME dns
; clientes, tanto IPv4 como IPv6
cliente1  IN A   10.10.10.10
          IN AAAA 2001:db8:2021:10::10
cliente2  IN A   10.10.10.20
          IN AAAA 2001:db8:2021:10::20
cliente3  IN A   10.10.10.30
          IN AAAA 2001:db8:2021:10::30
; servidor web (IPv4 e IPv6) e com apelido para www
web       IN A   10.10.100.10
          IN AAAA 2001:db8:2021:100::10
www       IN CNAME web
; servidores ftp e ssh
```



```
ftp          IN A   10.10.100.20
             IN AAAA 2001:db8:2021:100::20
ssh          IN A   10.10.100.30
             IN AAAA 2001:db8:2021:100::30
```

Adicionamos o registro para o domínio `R1.inf543.br` no arquivo de configuração do servidor DNS.

```
; Roteador 1, valores encontrados em docker-compose.yml
R1          IN A   10.10.10.100
            IN AAAA 2001:db8:2021:10::100
```