TP2 – PL19

Tiago Matos Guedes

Eduardo Manuel Sousa Pereira - A70619

Questões e respostas

Nível aplicacional

1. **Aceda à página http://www.scom.uminho.pt e espere que o conteúdo seja carregado. Pare a captura. Para localizar mais facilmente o tráfego correspondente ao acesso web realizado, comece por filtrar pelo protocolo dns. Para tal, introduza dns na caixa do display filter e aplique o filtro. Localize a resolução do nome www.scom.uminho.pt. Identifique o endereço IP da estação que formulou a query e o tipo de query realizada.**

No.	Time	Source	Destination	Protocol	Length	Info
93	4.081750	192.168.1.87	192.168.1.254	DNS	78	Standard query 0x7215 A www.scom.uminho.pt
94	4.097304	192.168.1.254	192.168.1.87	DNS	94	Standard query response 0x7215 A www.scom.uminho.pt A 193.137.9.174
98	4.114060	192.168.1.87	192.168.1.254	DNS	89	Standard query 0x8d58 A nav.smartscreen.microsoft.com
103	4.130341	192.168.1.254	192.168.1.87	DNS	212	Standard query response 0x8d58 A nav.smartscreen.microsoft.com CNAME

O endereço IP da estação que formulou a query é 192.168.1.87 e é uma standard query.

2. **Identifique a trama com resposta à query formulada. Identifique também o servidor de nomes que deu a resposta, através do seu IP e nome.**

93	4.081750	192.168.1.87	192.168.1.254	DNS	78	Standard query 0x7215 A www.scom.uminho.pt
94	4.097304	192.168.1.254	192.168.1.87	DNS	94	Standard query response 0x7215 A www.scom.uminho.pt A 193.137.9.174
98	4.114060	192.168.1.87	192.168.1.254	DNS	89	Standard query 0x8d58 A nav.smartscreen.microsoft.com
103	4.130341	192.168.1.254	192.168.1.87	DNS	212	Standard query response 0x8d58 A nav.smartscreen.microsoft.com CNAME

O servidor de nomes que deu a resposta foi o dn3.uminho.pt e o seu ip é 193.137.16.65.

3. **Limpe o filtro anteriormente estabelecido e filtre agora pelos protocolos http || tcp.**

4. **Tente identificar as tramas correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP.**

5. **Com base na sequência de dados trocados entre cliente e servidor explique se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.**

Está a funcionar em modo persistente.

6. **Limpe o filtro anteriormente estabelecido e filtre agora pelo protocolo http.**

7. **Coloque o wireshark a capturar tráfego e faça hard refresh da página indicada anteriormente. Depois volte a aceder à mesma página mas sem fazer hard refresh. Pare a captura de tráfego. Identifique a principal diferença observada no tráfego HTTP entre carregar a referida página com e sem hard refresh. Quais os campos do cabeçalho HTTP envolvidos nesta ação? Qual a principal vantagem e desvantagem inerente ao hard refresh?**

A diferença é que o Hard Refresh tem de ir buscar todas as informações ao servidor, sendo que se houver alguma atualização realizada pelo servidor, um simples refresh não capta a informação toda.

8. **Aceda a https://alunos.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o wireshark. Porque razão o tráfego HTTP não é identificado como tal?**

Não está identificado como HTTP, porque o Wireshark não consegue decifrar, por isso lê como TLS.

Consultas ao serviço de resolução de nomes DNS

1. **Abra uma janela de comandos e execute nslookup. Para que serve a informação apresentada?**

```
C:\Users\eduar>nslookup
Default Server:  dns3.uminho.pt
Address:  193.137.16.65
```

A informação serve para informar o servidor que se vai trabalhar com este IP.

2. **Usando os registos do tipo A, identifique os endereços IPv4 dos servidores ww.uminho.pt e www.ebay.com.**

```
C:\Users\eduar>nslookup www.uminho.pt
Server:  dns3.uminho.pt
Address:  193.137.16.65

Name:    www.uminho.pt
Address:  193.137.9.114


C:\Users\eduar>nslookup www.ebay.com
Server:  dns3.uminho.pt
Address:  193.137.16.65

Non-authoritative answer:
Name:    e9428.a.akamaiedge.net
Address:  23.49.245.22
Aliases:  www.ebay.com
          slot9428.ebay.com.edgekey.net
```

3. **Usando os registos NS, identifique os servidores de nomes definidos para os domínios: “ebay.com”, “utad.pt” e “.”.**

```
> set q=NS
> ebay.com
Server:  dns3.uminho.pt
Address:  193.137.16.65

Non-authoritative answer:
ebay.com        nameserver = dns4.p06.nsone.net
ebay.com        nameserver = ns03.ebaydns.com
ebay.com        nameserver = ns04.ebaydns.com
ebay.com        nameserver = ns02.ebaydns.com
ebay.com        nameserver = dns3.p06.nsone.net
ebay.com        nameserver = ns01.ebaydns.com
ebay.com        nameserver = dns1.p06.nsone.net
ebay.com        nameserver = dns2.p06.nsone.net
```

```
> utad.pt
Server:  dns3.uminho.pt
Address:  193.137.16.65

Non-authoritative answer:
utad.pt nameserver = ns.utad.pt
utad.pt nameserver = marao.utad.pt
```

```
> .
Server:  dns3.uminho.pt
Address:  193.137.16.65

Non-authoritative answer:
(root)  nameserver = l.root-servers.net
(root)  nameserver = d.root-servers.net
(root)  nameserver = h.root-servers.net
(root)  nameserver = m.root-servers.net
(root)  nameserver = b.root-servers.net
(root)  nameserver = f.root-servers.net
(root)  nameserver = g.root-servers.net
(root)  nameserver = j.root-servers.net
(root)  nameserver = i.root-servers.net
(root)  nameserver = c.root-servers.net
(root)  nameserver = a.root-servers.net
(root)  nameserver = k.root-servers.net
(root)  nameserver = e.root-servers.net
```

4. **Usando o registo SOA, identifique o servidor DNS primário definido para o domínio uminho.pt. Em que difere o servidor primário de um servidor secundário? Qual o significado dos parâmetros temporais associados ao servidor primário?**

```
> uminho.pt
Server:  dns3.uminho.pt
Address:  193.137.16.65

uminho.pt
        primary name server = dns.uminho.pt
```

Tanto o DNS primário como o DNS secundário contêm informação, incluindo IP's, a identidade do administrador do domínio e informação de outros recursos.

A principal diferença entre eles, é que o DNS primário pode fazer alterações necessárias às informações contidas nos servidores DNS, enquanto que o DNS secundário, contém apenas cópias dos ficheiros, sendo que estas cópias são read-only. O DNS secundário só pode fazer pedidos ao DNS primário após este fazer as atualizações necessárias.

```
uminho.pt
        primary name server = dns.uminho.pt
        responsible mail addr = servicos.scom.uminho.pt
        serial  = 2021102711
        refresh = 14400 (4 hours)
        retry   = 7200 (2 hours)
        expire  = 1209600 (14 days)
        default TTL = 300 (5 mins)
```

Serial: Número que se dá cada vez que o DNS primário faz alguma atualização. Como o número tem de aumentar a cada atualização, normalmente este número corresponde à data da atualização.

Refresh: Tempo que o DNS primário demora a informar o DNS secundário se tem alguma atualização (14400 - 4 horas)

Retry: Tempo que demora até tentar dar Refresh novamente, caso o DNS primário não retorne nenhuma resposta em 4 horas. (7200 - 2 horas)

Expire: Tempo durante o qual o DNS secundário da Retry até determinar que não consegue comunicar com o DNS primário. Quando isto acontece o DNS secundário não dá resposta. (1209600 - 14 dias)

Default TTL: Tempo que o pacote pode permanecer na cache. Evita casos em que o pacote ficaria "perdido" na rede. (300 - 5 minutos)

5. **Usando os registos MX, diga quais os servidores de mail do domínio de mail alunos.uminho.pt. A que sistema são entregues preferencialmente as mensagens dirigidas a user@di.uminho.pt?**

```
> set q=MX
> alunos.uminho.pt
Server:  dns3.uminho.pt
Address:  193.137.16.65

alunos.uminho.pt        MX preference = 10, mail exchanger = alunos-uminho-pt.mail.protection.outlook.com
```

O servidor de mail do domínio de mail alunos.uminho.pt é alunos.uminho.pt.mail.protection@outlook.com.

```
Non-authoritative answer:
di.uminho.pt    MX preference = 0, mail exchanger = mx.uminho.pt
di.uminho.pt    MX preference = 10, mail exchanger = mx2.uminho.pt
> _
```

As mensagens dirigidas a user@di.uminho.pt são entregues preferencialmente a mx.uminho.pt.

6. **Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247? E sobre o endereço IPv4 193.136.9.254? A que sistemas correspondem? Experimente fazer uma query aos registos PTR para o nome 254.9.136.193.in-addr.arpa. E comente o resultado obtido.**

```
C:\Users\eduar>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> 2001:690:a00:1036:1113::247
Server:  dns.google
Address:  8.8.8.8

Name:    www.fccn.pt
Address:  2001:690:a00:1036:1113::247
```

Este IP corresponde ao www.fccn.pt.

```
> 193.136.9.254
Server:  dns.google
Address:  8.8.8.8

Name:    router-di.uminho.pt
Address:  193.136.9.254
```

Este IP corresponde ao router-di.uminho.pt.

```
> set q=PTR
> 254.9.136.193.in-addr.arpa
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
254.9.136.193.in-addr.arpa      name = router-di.uminho.pt
```

Se fizermos nslookup do IP 193.136.9.254 dá o mesmo resultado de fazer uma query aos registos PTR de 254.9.136.193.in-addr.arpa.

Ao fazermos nslookup de um IP, o sistema sabe que tem de aceder aos registos PTR para dar a resposta, daí a resposta, fazendo de uma forma ou de outra, ser a mesma.

7. Qual a diferença entre uma resposta adjetivada como *non-authorative answer* e uma *authorative answer* para uma determinada query?

Uma resposta “autoritativa” vem de um DNS considerado “autoritativo”, ou seja, um servidor de nomes que está no domínio em que se fez a pesquisa. Uma resposta “não-autoritativa” vem de um servidor que não está nesse domínio. Basicamente estes servidores estão a passar informação em 2ª mão.

Uso da camada de transportes por parte das aplicações

Capturando o tráfego nos momentos que considere adequados, observe atentamente como as várias aplicações utilizam o serviço de transporte, quando é efetuado:

a. Acesso via browser ao URL: http://marco.uminho.pt/CCG/

b. Acesso em ftp para ftp.di.uminho.pt (login: anonymous)

c. ping marco.uminho.pt

d. Acesso ssh para marco.uminho.pt

e. nslookup www.uminho.pt

f. traceroute cisco.di.uminho.pt

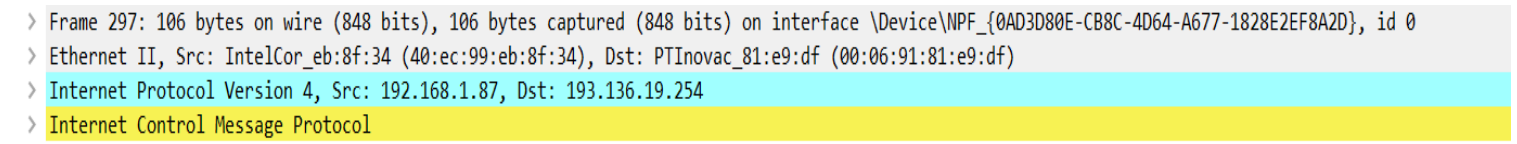
1. **Preencha a seguinte tabela com base nos resultados que obteve:**

Comando usado (aplicação)	Protocolo de transporte (se aplicável)	Porta de atendimento (se aplicável)
ping	Não aplicável.	Não aplicável.
traceroute	Não aplicável.	Não aplicável.
ftp	TCP	21
Browser http	TCP	80
nslookup / dig	UDP	443
ssh	TCP	22

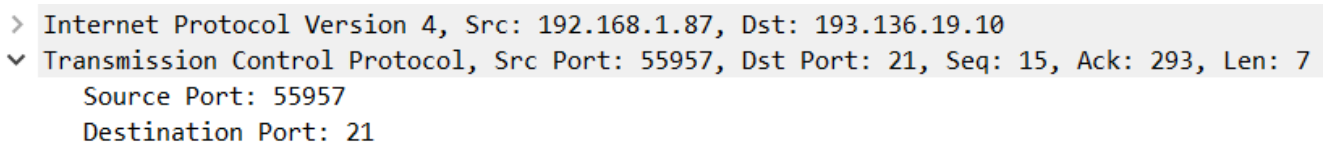
Ping: Como não aparece nada após o IP, significa que não chega ao nível de transporte, logo o protocolo de transporte não é aplicável, e não existe porta de atendimento.

```
Frame 32: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0AD3D80E-CB8C-4D64-A677-1828E2EF8A2D}, id 0
Ethernet II, Src: IntelCor_eb:8f:34 (40:ec:99:eb:8f:34), Dst: PTInovac_81:e9:df (00:06:91:81:e9:df)
Internet Protocol Version 4, Src: 192.168.1.87, Dst: 193.136.9.240
Internet Control Message Protocol
```

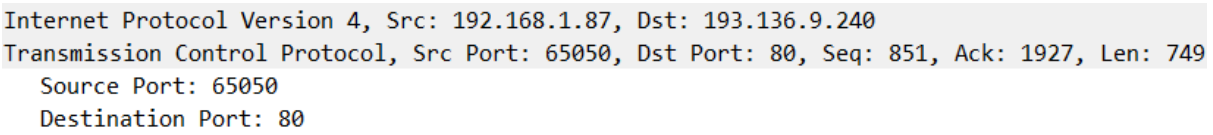
Tracerout: Como não aparece nada após o IP, significa que não chega ao nível de transporte, logo o protocolo de transporte não é aplicável, e não existe porta de atendimento.



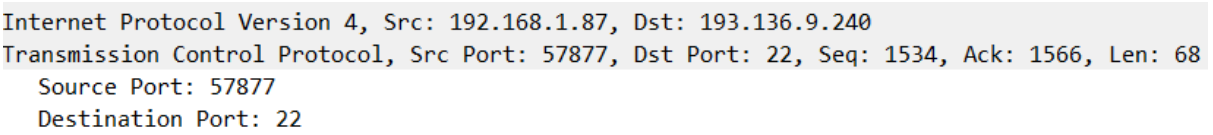
ftp:



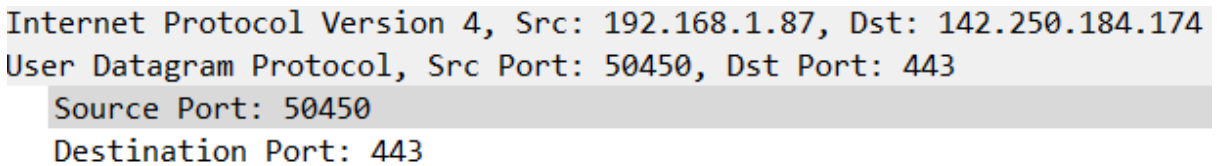
Browser:



ssh:



nslookup / dig:



Conclusões

Com este relatório aprendemos sobre os protocolos de transporte, TCP e UDP e as suas diferenças e aplicações.