UC/Curso: MIETI

Grupo 2:

- Hélder Duarte A75121

-Manuel Coutinho A76569

-Hugo Pereira A48319

Trabalho Prático 4; ExemploTrafego1.pcap

1. Home net:

   192.137.8.0/24 → scom3.uminho.pt

2. **Estratégia de análise**

   A abordagem de análise à captura de tráfego em questão, passou pelas seguintes etapas:

   - Identificação dos IP's envolvidos (através da ferramenta de "*endpoints*" do WireShark):
   - Tráfego TCP (através da ferramenta de "*conversations*" do WireShark):
     - Ordenar as conversações por ordem temporal;
     - Analisar o conteúdo de cada *stream*;
     - Se o conteúdo for suspeito analisar os seus pacotes e:
       - Confirmar se não houve alteração dos pacotes standard (ACK, SYN, etc);
       - Confirmar portas usadas;
       - Verificar protocolos usados e de que forma.

   - Trafego UDP (através da ferramenta de "*conversations*" do WireShark):
     - Ordenar as conversações por ordem temporal;
     - Verificar se existe relação com as *streams* TCP e se sim verificar a sua relação.
     - Análise do seu conteúdo.
   - Análise dos restantes protocolos.

3. Síntese da análise

IPs:

41.244.211.188 → Camarões → VIETTEL-CM-AS

81.64.154.175 → França → SFR SA

84.41.174.73 → Holanda → Esprit Telecom B.V.

84.91.17.250 →Portugal → Nowo Communications, S.A.

66.249.91.17 → Estados Unidos → Google

87.28.58.222 → Itália → Telecom Italia

Trafego TCP:

Nº ordem ou *streams*	Tempo (s)	Src/Dest	Observações
TCP 0	1.4420	193.137.8.106 portas 1137 193.137.8.215 porta 80	Sessão HTTP entre o cliente com o servidor (moodle.dsi.uminho.pt) que tem como objetivo pedir o *índex.html* da página. Não ocorreram situações de erro nesta *stream.* A sessão envolveu a transferência de 35 pacotes e 19,477 kBytes de informação.
TCP 1-15	2.443260	193.137.8.106 portas 1138 – 1152 193.137.8.215 porta 80	Cada *stream* corresponde ao pedido de cada um dos itens que a pagina web em questão necessita para apresentar o seu conteúdo. De salientar que em algumas das *streams* pode-se encontrar uns pacotes "TCP DUP" que são gerados por *timeouts* ocorridos do lado do servidor. É nas *streams* 1 e 3 que se podem encontrar exemplos destes pacotes. A sessão envolveu a transferência de 302 pacotes e 135,222 Kbytes de informação.
TCP 16	65.4540	193.137.8.106 porta 1153 66.249.91.17 porta 80	É estabelecida uma nova sessão HTTP com o servidor "mail.google.com" sem ocorrência de erros. Nesta stream são visíveis excertos de emails, os quais não são encriptados sendo possível ver na integra qual a informação trocada. Identificamos que o email do login foi eu.nuno@gmail.com. Nos emails identificamos as várias entradas da caixa de email assim como o inicio da mensagem trocadas. Foram enviados 9 pacotes de dados, do 340 ao 347 e o pacote

			425 no total de 2842 Bytes. O 425 é referente a um pacote [RST, ACK] por parte do cliente terminando a sessão. Suspeitamos que este RST, ACK esteja relacionado com um *timeout*.
TCP 17	11.3674	193.137.8.106 porta 1154 193.137.8.95 porta 21	Foi estabelecida uma sessão FTP com o endereço piano.dsi.uminho.pt. Foi feita uma tentativa de *login* com o utilizador *anonymous*, sendo que o servidor rejeitou esta conexão com o código 530 que representa utilizador desconhecido. De seguida o utilizador fechou a ligação o que pode ser comprovado com o código 221. Foram trocados 14 pacotes, do 352 ao 373 com um total de 918 Bytes transferidos.
TCP 18	28.5886	193.137.8.106 porta 1156 193.137.8.95 porta 23	Foi estabelecida uma sessão com o servidor TELNET (porta 23) na qual é feita a tentativa de login na página piano.dsi.uminho.pt com Login: "guest" e *Password: "*guest" sem sucesso. É possível observar os dados devido à inexistência de encriptação deste protocolo. Foram transferidos 53 pacotes, do 375 ao 431 com um total de 3239 Bytes transferidos.
TCP 19	8.9989	193.137.8.106 porta 30797 193.137.8.215 porta 11132	Tentativa de estabelecer uma ligação que não obteve resposta Foram enviados 3 pacotes, sendo o 1º a ligação inicial e os seguintes pacotes de retransmissão por *timeout*. Total de 372 bytes transferidos.
TCP 20	8.9937	87.28.58.222 porta 11139 193.137.8.157 porta 443	Tentativa de estabelecer uma ligação que não obteve resposta Foram enviados 3 pacotes, sendo o 1º a ligação inicial e os seguintes pacotes de retransmissão por *timeout*. Total de 372 bytes transferidos.
TCP 21	8.9819	87.28.58.222 porta 11141 193.137.8.157 porta 80	Tentativa de estabelecer uma ligação que não obteve resposta Foram enviados 3 pacotes, sendo o 1º a ligação inicial e os seguintes pacotes de retransmissão por *timeout*. Total de 372 bytes transferidos.
TCP 22	0.4628	193.137.8.106 porta 1157 66.249.91.17 porta 80	Visto que na Stream 16 existiu um [RST ACK] que terminou a ligação com o servidor, nesta stream é estabelecida uma nova sessão HTTP com o servidor "mail.google.com" sem ocorrência de erros. Tal como na stream 16 é possível ver excertos de emails, visto que os emails, continuam a não estar encriptados. Foram trocados 8 pacotes de dados, do 451 ao 458 no total de 2788 Bytes. O 425 é referente a um pacote [RST, ACK] por parte do cliente terminando a sessão. Suspeitamos que este RST, ACK esteja relacionado com um *timeout*.

TCP 23 TCP 24	9.1543 0.0441	193.137.8.106 porta 1158 193.137.8.142 porta 445 193.137.8.106 porta 1159 193.137.8.142 porta 139	É estabelecida uma sessão SMB de partilha de ficheiros, que pela quantidade de tráfego trocada da a entender que apenas houve navegação entre a arvore de ficheiros disponibilizada na partilha, ou seja não houve transferência de ficheiros. Vê-se claramente três sessões diferentes por parte de 2 utilizadores, "BOCASJNR\hsantos" que foi estabelecida e o que parece ser duas tentativas de entrada com acesso *root*, que foram recusadas. Podemos ainda observar alguns "NT Cancel Request" que são pedidos de navegação que foram posteriormente cancelados. Foram trocados 98 pacotes de dados, num total de 17,168K Bytes.

Tráfego UDP:

Nº ordem ou *streams*	Tempo (s)	Src / Dest	Observações
0	0.0124s	192.137.8.106 porta 1030 192.137.8.142 porta 53	É um pedido de DNS referente à tradução do endereço *piano.dsi.uminho.pt* para o seu IP. Teve como resposta do servidor de DNS da universidade do Minho (IP) o IP 192.137.8.95. Este pedido surgiu quando na *stream* TCP 17 é efetuada uma ligação FTP. Foram trocados 4 pacotes com um total de 348 Bytes.
1	6.0158	41.244.211.188 porta 35953 193.137.8.157 porta 30797	Enviado de tráfego que não informação suficiente para tirar qualquer tipo de conclusão. Foram enviados 15 pacotes com um total de 1991 Bytes.
2	6.0433	84.41.174.73 porta 38337 193.137.8.157 porta 30797	
3	2.0370	217.70.68.212 porta 59342 193.137.8.114 porta 23897	
4	2.0223	193.137.8.138 porta 39284 193.137.8.157 porta 30797	
5	2.0559	84.91.17.250 porta 54035 193.137.8.157 porta 30797	
6	6.0266	81.64.154.175 porta 43622 193.137.8.157 porta 30797	
7	0.0000	193.137.8.106 porta 137 193.137.8.142 porta 137	Este pacote é referente à *stream* TCP 24, ou seja, ao serviço SMB e tem como propósito fazer o mesmo trabalho que um serviço de DNS, isto é traduzir de nome para IP mas do protocolo NBNS que pertence ao serviço NetBIOS.

Protocolos previamente não referenciados:

Com a quantidade encontrada de tráfego dos protocolos ARP e ICMP, 0.5% e 1.6% respetivamente, consideramos que estes não levantam qualquer suspeita quanto ao seu uso.

Dados estatísticos:

- Número total de pacotes capturados: 563
- Tempo decorrido para a captura: 152.819s
- Número médio de pacotes capturados por segundo: 3,7
- Tamanho médio dos pacotes capturados: 330,5 Bytes
- Total de bytes capturados: 185889
- Média de bytes capturados por segundo: 1216
- Média de bits capturados por segundo: 9731