UC/Curso: Segurança em Redes de Computadores/MIETI

Grupo 4:

* José Pedro Afonso Rocha a70020
* Luís Pedro Lobo de Araújo a73232

**Trabalho Prático 4; ExemploTrafego1.pcap**

1. **Home net = 193.137.8.0/24**

|  |
| --- |
| **Endereços** |
| 193.137.8.106 |
| 193.137.8.215 |
| 193.137.8.142 |
| 193.137.8.95 |
| 193.137.8.157 |
| 193.137.8.138 |
| 193.137.8.114 |
| 193.137.8.125 |

**2. Estratégia de análise**

Uma vez analisados todos os endereços IP’s envolvidos em trocas de pacotes, para identificar a Home net e respetivos endereços utilizados, iremos analisar as diferentes sessões TCP e UDP e identificar os protocolos utilizados em cada uma. Desta forma é possível identificar o intuito de cada sessão e possíveis tentativas de acesso indevido a recursos ou informações, verificando também a utilização de protocolos mais vulneráveis.

Para tal iremos utilizar ferramentas do Wireshark tal como, TCP e UDP Streams, estatísticas de protocolos e de IP. Foi ainda utilizada a seguinte fonte para uma melhor utilização do Wireshark: <https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>

**3. Síntese da análise**

Tabela - TCP streams.

|  |  |  |  |
| --- | --- | --- | --- |
| Nº ordem ou *streams* | Tempo (s) | Src/Dest | Comentário |
| 0-15 | 1.4573  a  3.9039 | 193.137.8.106 porta 1137 a 1152  193.137.8.215 porta 80 | Conexão ao servidor do moodle para obter página web e respetivos ficheiros associados;  Foram usadas 16 streams no total, e ainda ocorreram erros e retransmissões em alguns pacotes. |
| 16 | 17.0402  a  82.4942 | 193.137.8.106 porta 1153  66.249.91.17 porta 80 | Sessão HTTP com servidor de mail da Google;  A sessão envolveu a transferência de 9 pacotes e 2,3 KBytes. |
| 17 | 23.8193  a  35.1868 | 193.137.8.106 porta 1154  193.137.8.95 porta 21 | Tentativa de ligação FTP via piano.dsi.uminho.pt como utilizador anónimo;  A sessão envolveu a transferência de 14 pacotes e 136 Bytes |
| 18 | 54.2574  a  82.8460 | 193.137.8.106 porta 1156  193.137.8.95 porta 23 | Ligação telnet a piano.dsi.uminho.pt, tentativa de login com utilizador guest;  A sessão envolveu a transferência de 53 pacotes e 288 Bytes, ocorrendo erros e retransmissão em alguns pacotes. |
| 19 | 97.0018  a  106.0008 | 87.28.58.222 porta 11132  193.137.8.157 porta 30797 | Tentativa de conexão. A sessão envolveu o envio de 3 pacotes SYN. |
| 20 | 98.6079  a  107.6016 | 87.28.58.222 porta 11139  193.137.8.157 porta 443 | Tentativa de conexão (HTTPS). A sessão envolveu o envio de 3 pacotes SYN. |
| 21 | 100.2218  a  109.2037 | 87.28.58.222 porta 11141  193.137.8.157 porta 80 | Tentativa de conexão (HTTP). A sessão envolveu o envio de 3 pacotes SYN. |
| 22 | 137.5350  a  137.9978 | 193.137.8.106 porta 1157  66.249.91.17 porta 80 | Nova sessão HTTP com servidor de mail da Google;  A sessão envolveu a transferência de 8 pacotes e 2,3 KBytes. |
| 23 | 143.6646  a  152.8189 | 193.137.8.106 porta 1158  193.137.8.142 porta 445 | Sessão SMB para transferência de ficheiros;  Ocorreram erros e retransmissões em alguns pacotes.  A sessão envolveu a transferência de 98 pacotes e 10 KBytes. |
| 24 | 143.6769  a  143.7210 | 193.137.8.106 porta 1158  193.137.8.142 porta 139 | Tentativa de sessão SMB via porta 139 (NetBIOS para sistemas mais antigos). |

Tabela - UDP streams.

|  |  |  |  |
| --- | --- | --- | --- |
| Nº ordem ou *streams* | Tempo (s) | Src/Dest | Comentário |
| 0 | 23.7797  a  23.7921 | 193.137.8.106 porta 1030  193.137.8.142 porta 53 | Pedido ao servidor de DNS para obter ip de piano.dsi.uminho.pt;  É enviado o pedido e recebida a resposta, usando apenas 2 pacotes. |
| 1 | 25.5357  a  31.5515 | 41.244.211.188 porta 35953  193.137.8.157 porta 30797 | Dados recebidos via UDP.  A sessão envolveu a transferência de 3 pacotes e 324 Bytes. |
| 2 | 31.2717  a  37.3150 | 84.41.174.73 porta 38337  193.137.8.157 porta 30797 | Dados recebidos via UDP.  A sessão envolveu a transferência de 3 pacotes e 282 Bytes. |
| 3 | 31.2798  a  33.3168 | 217.70.68.212 porta 59342  193.137.8.114 porta 23897 | Dados recebidos via UDP.  A sessão envolveu a transferência de 2 pacotes e 168 Bytes. |
| 4 | 93.7230  a  95.7453 | 193.137.8.138 porta 39284  193.137.8.157 porta 30797 | Dados recebidos via UDP.  A sessão envolveu a transferência de 2 pacotes e 164 Bytes. |
| 5 | 106.4534  a  108.5093 | 84.91.17.250 porta 54035  193.137.8.157 porta 30797 | Dados recebidos via UDP.  A sessão envolveu a transferência de 2 pacotes e 144 Bytes. |
| 6 | 118.3012  a  124.3279 | 81.64.154.175 porta 43622  193.137.8.157 porta 30797 | Dados recebidos via UDP.  A sessão envolveu a transferência de 3 pacotes e 279 Bytes. |
| 7 | 143.6721 | 193.137.8.142 porta 137  193.137.8.106 porta 137 | Sessão NetBIOS Name Service (NBNS) com resposta ao pedido SMB;  A sessão envolveu um pacote de 62 Bytes. |

## Atividades suspeitas e vulnerabilidades encontradas

Após a análise de todo o tráfego, foram encontradas algumas atividades menos usais que podem ser consideradas como suspeitas, tais como:

* Na stream TCP 17 existe uma tentativa de ligação FTP como utilizador anónimo;
* Na stream TCP 18 existe uma tentativa de login via telnet com o utilizador guest;
* Nas stream TCP 19, 20 e 21 existe uma tentativa de conexão, poderá ser um scan das portas e serviços ativos;
* Na stream TCP 23 foi criada uma sessão SMB, este protocolo apresenta algumas vulnerabilidades conhecidas, e o seu uso pode ser perigoso, caso os sistemas não estejam atualizados com as suas correções (patch).

## Análise estatística

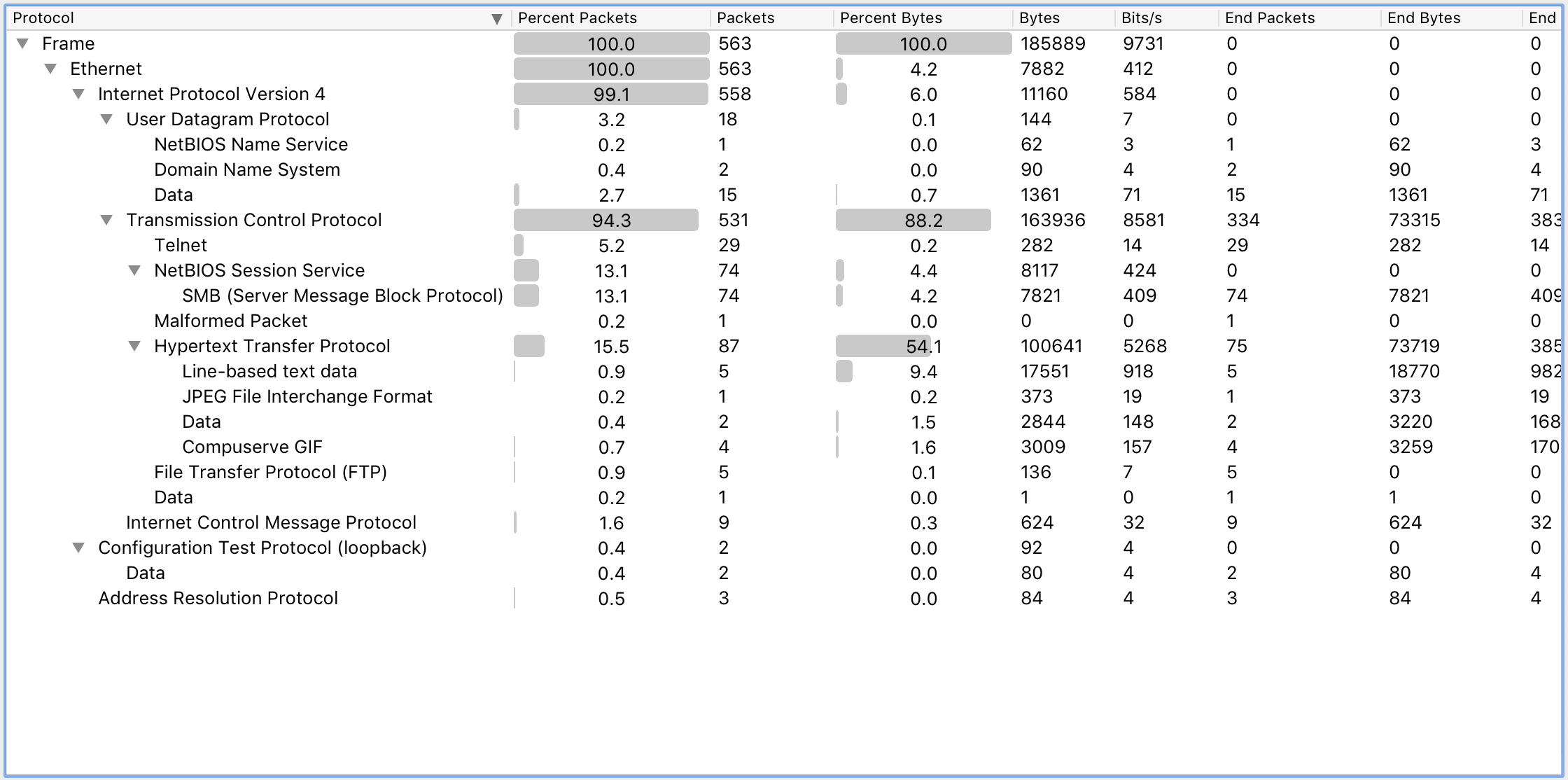


Figura – Hierarquia e estatísticas de protocolos usados.

Observando a Figura 1, podemos encontrar os seguintes protocolos utilizados:

* UDP – Protocolo usado sobre IP sem garantia de fiabilidade na entrega dos pacotes;
* TCP – Protocolo usado sobre IP com estabelecimento de uma sessão entre os intervenientes e com garantia de fiabilidade;
* DNS – Sistema hierárquico de gestão de nomes de domínios, traduz nomes para endereços IP;
* NBNS – Função idêntica ao DNS mas no âmbito das redes locais (NetBIOS/Windows);
* Telnet – Permite uma comunicação baseada em texto, bidirecional e interativa, através de uma conexão virtual ao terminal;
* SMB – Disponibiliza o acesso partilhado em rede a ficheiros e impressoras;
* HTTP – Protocolo da camada de aplicação para a transmissão de informação de *Hypertext*, a base da comunicação com servidores Web e os navegadores;
* FTP – Protocolo para transferência de ficheiros em rede;
* ARP – Permite o mapeamento de endereços de rede (IP) para endereços físicos (MAC);
* ICMP – Protocolo de controlo integrante do IP, permite fornecer relatórios de erros à fonte remetente;
* Loop – Usado para o mesmo efeito do ping, mas na camada de ligação de dados.

No entanto os protocolos com um maior número de pacotes são TCP com 94.3% vs 3.2% do UDP, contando principalmente com a utilização de pacotes HTTP (15.5%) e SMB (13.1%).

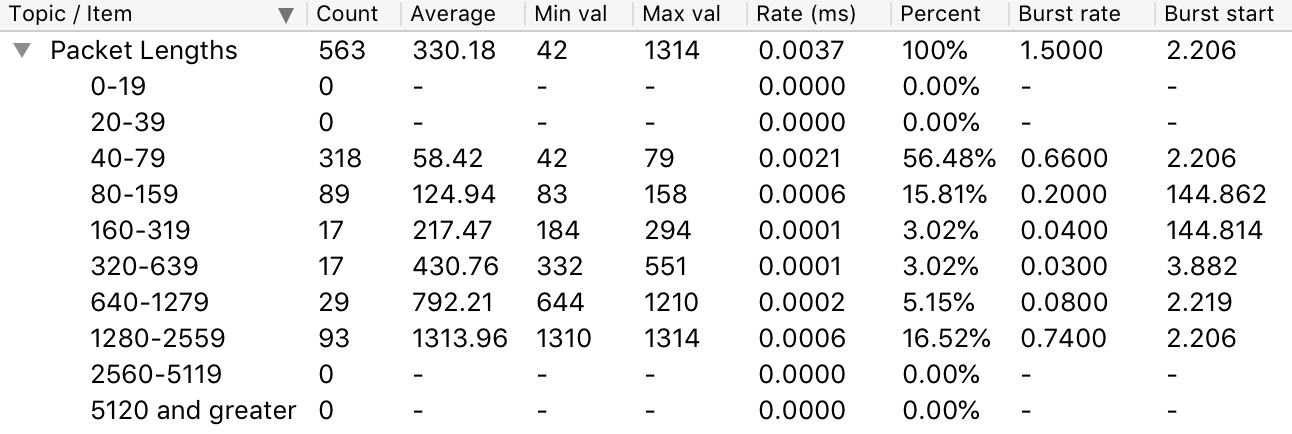


Figura - Tamanhos dos pacotes analisados.

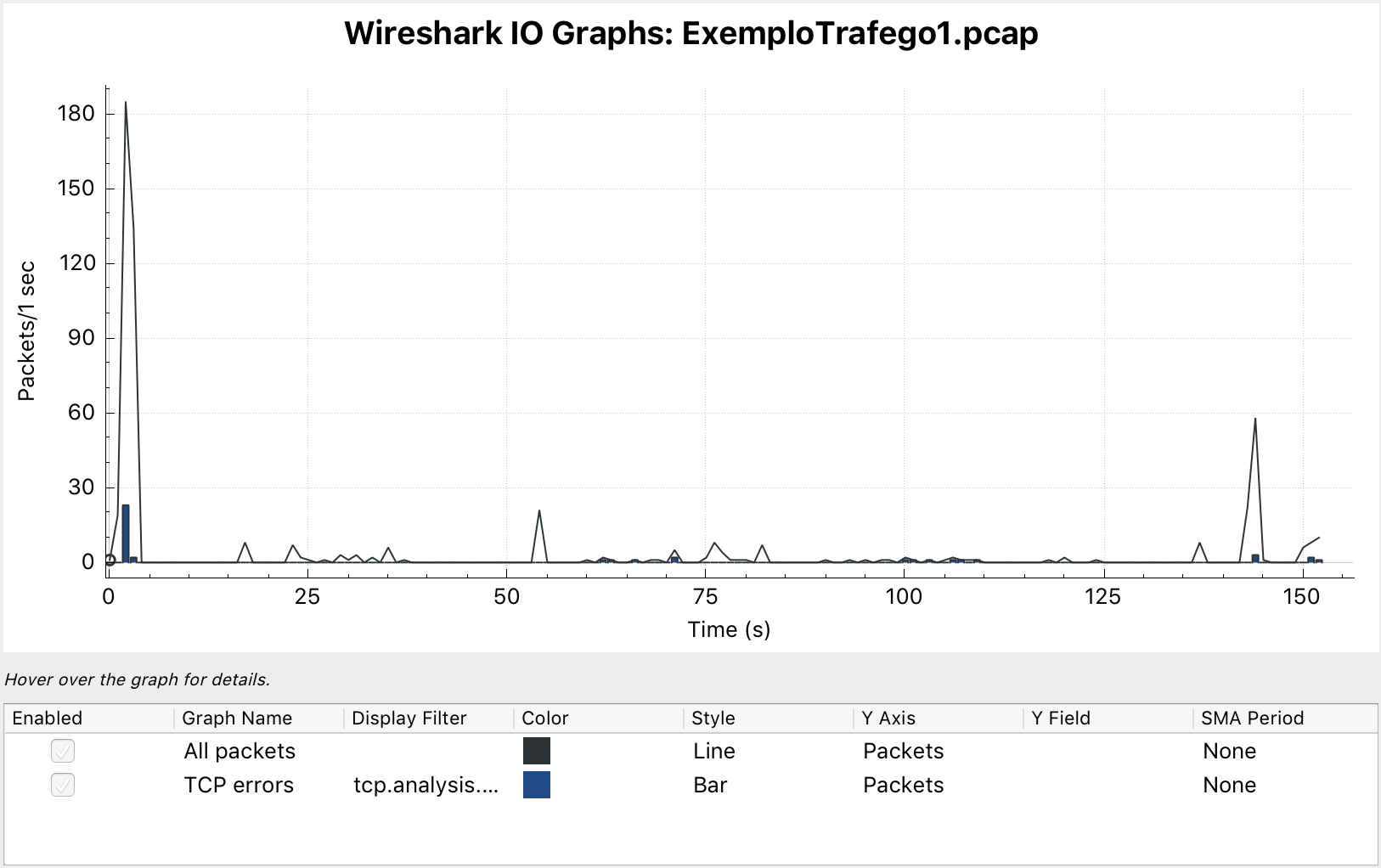


Figura - Timeline do tráfego gerado.

Na Figura 2 e na Figura 3 podemos encontrar mais algumas estatísticas relativas ao tamanho dos pacotes analisados e ainda à distribuição temporal da transferência de pacotes.