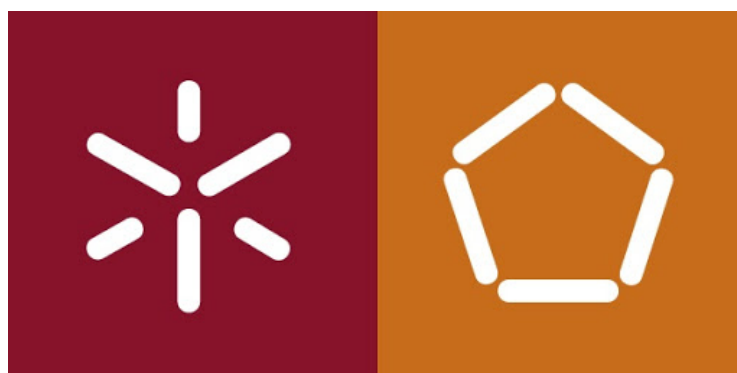


Tarefa Prática 2

Modelação e Caracterização de Tráfego

PG39254 - Igor Araújo
PG39255 - Matheus Gonçalves
PG41017 - I-Ping



Departamento de Informática
Universidade do Minho
Braga - Portugal
11 de março de 2020

Sumário

Sumário	2
Objetivo	3
Parte I - Captura e análise de tráfego	3
Parte 2 - Filtragem de tráfego	4
Conclusão	7
Resultados	8
Anexo I.	9
Referências	10

Objetivo

O objetivo desse trabalho é realizar a captura, visualização, análise e filtragem de tráfego de rede, onde no final desse relatório o grupo vai estar mais familiarizado com as ferramentas e os conceitos de captura e análise de tráfego.

Parte I - Captura e análise de tráfego

- a) Inicie a captura de tráfego na interface de rede disponível. Faça uma primeira análise comparativa dos cabeçalhos e formatos dos PDUs do protocolos TCP, UDP e IP. Identifique para cada um deles os campos geralmente utilizados na classificação de tráfego:

O protocolo TCP possui header que contém diversos campos, mas os campos que são utilizados geralmente para identificação e classificação de um tráfego são as portas de origem e destino, e da mesma maneira para o UDP. Além destas, para a melhor classificação do tráfego é utilizado também os campos da PDU da camada de redes IP, que utilizam os endereços de origem e destino IP o número de protocolo, assim é formada a 5 tupla. Em posse desses parâmetros é possível em muitos casos classificar o tráfego. Porém a cada dia novas aplicações com diversos tipos de tráfegos são enviadas através de tráfegos encriptados o que torna ainda mais difícil sua identificação e classificação. Pode-se observar tais campos mencionados na figura 1.

```

  Internet Protocol Version 4, Src: 172.26.63.165, Dst: 193.137.16.65
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 87
      Identification: 0xe71e (59166)
    > Flags: 0x0000
      Fragment offset: 0
      Time to live: 128
      Protocol: UDP (17)
      Header checksum: 0x95ed [validation disabled]
      [Header checksum status: Unverified]
      Source: 172.26.63.165
      Destination: 193.137.16.65
  User Datagram Protocol, Src Port: 49941, Dst Port: 53
    Source Port: 49941
    Destination Port: 53
    Length: 67
    Checksum: 0x28e1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
    > [Timestamps]
  > Domain Name System (query)
```

Figura 1. Exemplificação de PDU.

b) Utilizando o sniffer em modo de captura, proceda à invocação de várias aplicações conhecidas, nomeadamente:

- Acesso via browser ao URL: `http://marco.uminho.pt`
- Acesso ftp (anonymous): `ftp.di.uminho.pt`
- Acesso em tftp para router-ext (193.136.9.33)
- Acesso via telnet para router-ext (193.136.9.33) ou para router-lab (192.168.90.254)
- Acesso ssh para qualquer host da sala de aula
- Resolução de nomes usando `nslookup www.uminho.pt`
- `traceroute cisco.uminho.pt`

e construa uma tabela onde, para cada aplicação, conste o protocolo de transporte e a porta de atendimento do servidor (quando aplicável).

Protocolo de Transporte	Porta de Origem	Porta de Destino
HTTP	6	87837
FTP	7	78
TFTP		69
TELNET	545	23
SSH	88	22
DNS	88	53
ICMP	88	53

Tabela 1. Tabela de aplicações

Parte 2 - Filtragem de tráfego

a) Explore e descreva:

- i A utilidade dos filtros de captura e visualização;
- ii A sintaxe e semântica dos filtros.

Dê alguns exemplos simples de utilização dos mesmos.

INICIO RESPOSTA

b) Baseando-se nas tramas capturadas acima (1.b), e em outros exemplos que achar conveniente, explore a utilidade e utilização dos filtros de captura e visualização, nomeadamente na captura/visualização de:

- protocolos aplicativos;

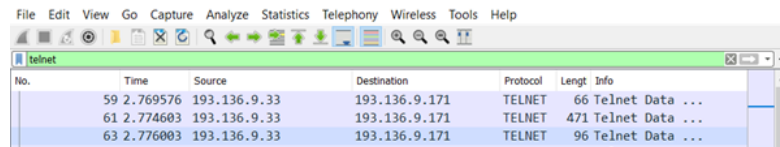
- protocolos de transporte;
- endereços IP;
- pacotes com valores específicos nos campos principais dos cabeçalhos de transporte e rede (ver opção "+Expression");
- pacotes com flags de iniciação e termino de conexões TCP;

Exemplifique a exploração que realizou, indicando a sintaxe utilizada nos filtros e, muito sucintamente os resultados obtidos.

INICIO RESPOSTA

- c) Para uma das aplicações que usam o protocolo TCP (e.g. Telnet router-ext), explore a opção "Analyse - Follow TCP Stream". Indique os filtros automaticamente aplicados por essa opção. Discuta eventuais fragilidades de segurança e confidencialidade dos dados.

Com a opção de filtragem via menu Analyse > Follow > TCP Stream, é possível selecionar um pacote entra vários capturados e reunir todos os pacotes que pertencem ao mesmo stream de dados. Neste caso foi feito inicialmente uma filtragem pelo protocolo Telnet, conforme visto na figura 2 abaixo:



No.	Time	Source	Destination	Protocol	Length	Info
59	2.769576	193.136.9.33	193.136.9.171	TELNET	66	Telnet Data ...
61	2.774603	193.136.9.33	193.136.9.171	TELNET	471	Telnet Data ...
63	2.776003	193.136.9.33	193.136.9.171	TELNET	96	Telnet Data ...

Figura 2. Exemplo lista de stream.

Em seguida foi utilizado o menu Analyse > Follow > TCP Stream, mencionado anteriormente e com isso foi possível agrupar todos os pacotes pertencentes ao stream de pacotes pertencentes ao stream do pacote selecionado, inclusive aqueles que não são exclusivamente de protocolo Telnet, conforme visto a seguir na figura 3.

Como pode também ser visto na figura 3 o filtro que é gerado pelo menu executado basicamente é filtrar na captura pelo stream TCP de número 6 que sintaticamente possui a expressão (tcp.stream eq 6), o trecho tcp.stream indica intuitivamente que quer se filtrar por streams TCP e a parte (eq 6) indica que o stream específico que se deseja é o de número igual (eq) a 6. E o mais interessante do resultado da ação executado pelo menu selecionado é a reconstrução e apresentação das trocas de mensagens trocadas entre origem e destino, de tal forma que seja possível capturar e entender uma troca de mensagens por completo, se forem enviados em texto claro, que é o caso do protocolo Telnet. Tal resultado é visualizado na figura 4

No.	Time	Source	Destination	Protocol	Length	Info
56	2.763150	193.136.9.171	193.136.9.33	TCP	66	55707 → 23 [SYN] Seq=
57	2.765317	193.136.9.33	193.136.9.171	TCP	60	23 → 55707 [SYN, ACK]
58	2.765510	193.136.9.171	193.136.9.33	TCP	54	55707 → 23 [ACK] Seq=
59	2.769576	193.136.9.33	193.136.9.171	TELNET	66	Telnet Data ...
61	2.774603	193.136.9.33	193.136.9.171	TELNET	471	Telnet Data ...
62	2.774758	193.136.9.171	193.136.9.33	TCP	54	55707 → 23 [ACK] Seq=
63	2.776003	193.136.9.33	193.136.9.171	TELNET	96	Telnet Data ...
64	2.778872	193.136.9.171	193.136.9.33	TELNET	57	Telnet Data ...

Figura 3. Exemplo lista de stream.

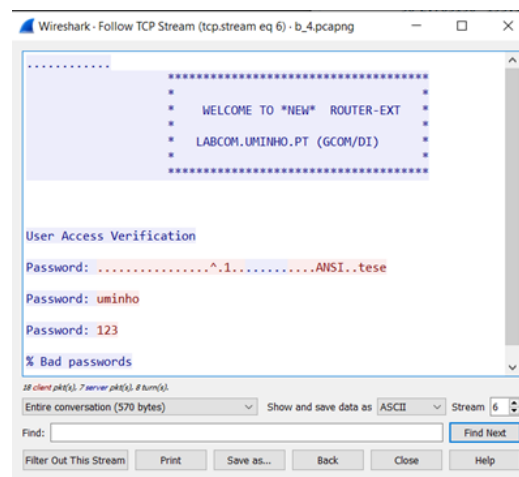


Figura 4. Montando o stream.

Os trechos apresentados marcados em azul foram recebidos pelo destinatário e em vermelho pela a origem, que está a tentar aceder ao equipamento via protocolo Telnet. Assim vemos de forma clara o password que foi digitado pelo utilizador. Desta forma mostra a fragilidade do protocolo Telnet, bem como outros protocolos que transmitem suas mensagens via texto claro, caso sejam transmitidos conteúdos sensíveis como senhas, informações bancárias e outros, tais dados estarão expostos e a comprometer a confidencialidade das informações caso haja um utilizador malicioso a sniffar os pacotes que são transmitidos pela rede.

d) Analise e identifique dados estatísticos da sua captura de pacotes.

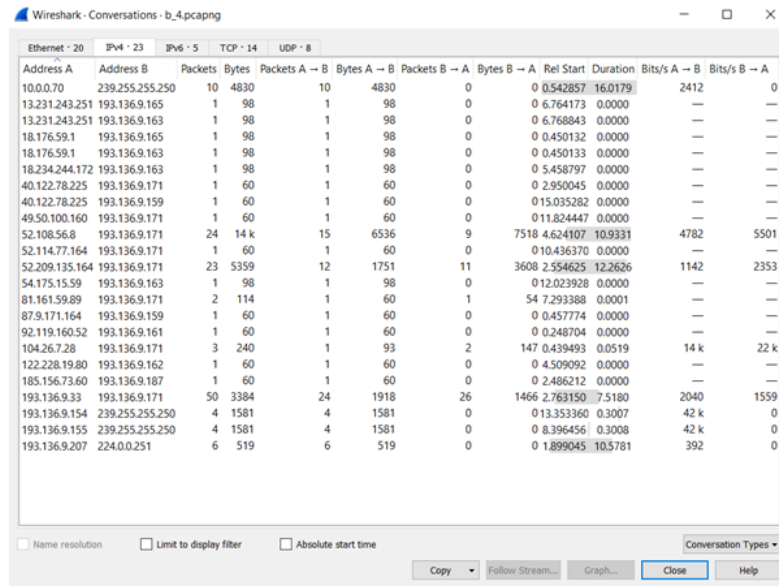
Dentre as capturas realizadas selecionou-se a referente ainda ao Telnet. Na tela principal já é possível verificar a quantidade de pacotes capturados no total e quantos estão sendo exibidos, quando há um filtro aplicado.

CRIAR TABELA AQUI:

Quantidade de pacotes capturados: 352

Total de pacotes exibidos: 50(14.2%)

Outra opção para se obter mais estatísticas é utilizar o menu Statistics, nele há uma lista de opções. Uma delas que é interessante é o Conversation, nesta são compiladas todas as conversas entre origem X e destino Y para os protocolos Ethernet, Ipv4, Ipv6, TCP e UDP, sendo essas opções distribuídas em abas, conforme visto abaixo na figura 5.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.0.0.70	239.255.255.250	10	4830	10	4830	0	0	0.542857	16.0179	2412	0
13.231.243.251	193.136.9.165	1	98	1	98	0	0	6.764173	0.0000	—	—
13.231.243.251	193.136.9.163	1	98	1	98	0	0	6.768843	0.0000	—	—
18.176.59.1	193.136.9.165	1	98	1	98	0	0	0.450132	0.0000	—	—
18.176.59.1	193.136.9.163	1	98	1	98	0	0	0.450133	0.0000	—	—
18.234.244.172	193.136.9.163	1	98	1	98	0	0	0.5458797	0.0000	—	—
40.122.78.225	193.136.9.171	1	60	1	60	0	0	2.950045	0.0000	—	—
40.122.78.225	193.136.9.159	1	60	1	60	0	0	0.15035282	0.0000	—	—
49.50.100.160	193.136.9.171	1	60	1	60	0	0	0.11824447	0.0000	—	—
52.108.56.8	193.136.9.171	24	14 k	15	6536	9	7518	4.624107	10.9331	4782	5501
52.114.77.164	193.136.9.171	1	60	1	60	0	0	0.10436370	0.0000	—	—
52.209.135.164	193.136.9.171	23	5359	12	1751	11	3608	2.554625	12.2626	1142	2353
54.175.15.59	193.136.9.163	1	98	1	98	0	0	0.12023928	0.0000	—	—
81.161.59.89	193.136.9.171	2	114	1	60	1	54	7.293388	0.0001	—	—
87.9.171.164	193.136.9.159	1	60	1	60	0	0	0.457774	0.0000	—	—
92.119.160.52	193.136.9.161	1	60	1	60	0	0	0.248704	0.0000	—	—
104.26.7.28	193.136.9.171	3	240	1	93	2	147	0.439493	0.0519	14 k	22 k
122.228.19.80	193.136.9.162	1	60	1	60	0	0	0.4509092	0.0000	—	—
185.156.73.60	193.136.9.187	1	60	1	60	0	0	0.2486212	0.0000	—	—
193.136.9.33	193.136.9.171	50	3384	24	1918	26	1466	2.763150	7.5180	2040	1559
193.136.9.154	239.255.255.250	4	1581	4	1581	0	0	0.13353360	0.3007	42 k	0
193.136.9.155	239.255.255.250	4	1581	4	1581	0	0	0.8396456	0.3008	42 k	0
193.136.9.207	224.0.0.251	6	519	6	519	0	0	1.899045	10.5781	392	0

Figura 5. Tabela conversation.

Outra estatística interessante é listagem hierárquica dos protocolos, nela pode-se ver a representatividade de cada protocolo e subprotocolo no total da captura. Essa estatística pode ser visualizada na figura 6.

E outra forma de visualizar estatísticas é na opção File Properties do menu Statistics, que pode ser visualizado na figura 7

Quantidade de pacotes capturados: 352

Total de pacotes exibidos: 50(14.2%)

Conclusão

INICIO CONCLUSAO

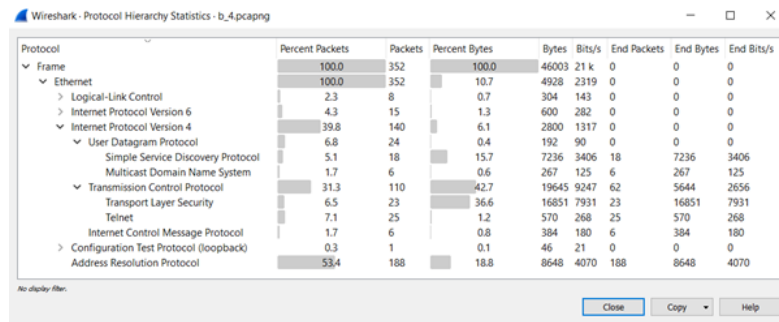


Figura 6. Tabela de estatística hierárquica.

Resultados

Os resultados dos experimentos se encontram na tabela 1.

Parâmetros			Geração até chegar à solução					Desempenho	
Grade	Mutação	População	95% de confiança	1º Quartil	Mediana	3º Quartil	Indivíduos	IC	
3x3	0,1	10	2	1000	16	167	435	1670	96,17%
3x3	0,01	10	1	1000	12	132	383	1320	92,42%
3x3	0,001	10	2	1000	40	197	430	1970	97,87%
3x3	0	10	2	1000	32	135	404	1350	92,85%
3x3	0,1	100	1	6	2	3	4	300	44,37%
3x3	0,01	100	1	7	2	3	4	300	44,37%
3x3	0,001	100	1	7	2	3	4	300	44,37%
3x3	0	100	1	8	2	3	4	300	44,37%
3x3	0,1	1000	1	2	1	1	1	1000	85,84%
3x3	0,01	1000	1	2	1	1	1	1000	85,84%
3x3	0,001	1000	1	2	1	1	1	1000	85,84%
3x3	0	1000	1	3	1	1	1	1000	85,84%
4x4	0,1	10	406	1000	1000	1000	1000	10000	
4x4	0,01	10	535	1000	1000	1000	1000	10000	
4x4	0,001	10	241	1000	1000	1000	1000	10000	
4x4	0	10	185	1000	1000	1000	1000	10000	
4x4	0,1	100	5	27	11	14	17	1400	2,11%

Tabela 2. Resultados brutos



Figura 7. File Properties.

Anexo I

Test	Metric	Plataform	Description
Download (TCP)	Download speed	Whiteboxes, Routers, Android, iOS	The download speed in Mbps when downloading (using TCP) random bytes from a test server
	TCP Retransmissions	Whiteboxes, Routers	The number of retransmitted TCP segments/packets
	Burst download speed	Whiteboxes, Routers	The download speed during the first 5 seconds of a test
	Sustained download speed	Whiteboxes, Routers	The download speed of the test during the last 5 seconds
	Percentage Best	of Whiteboxes, Routers	Download speed result as a percentage of the user's best ever result
	Percentage Advertised	of Whiteboxes, Routers	Download speed result as a percentage of their package's advertised downstream speed
Download (HTML5)	Download speed	Web	The download speed in Mbps when downloading (using TCP) random bytes from a test server using HTML5 APIs(WebSockets and Fetch)
Download (Lightweight UDP)	Download speed	Whiteboxes, Routers	The download speed in Mbps when downloading (using UDP) from a test server, using less data than the TCP test
Download (Hardware accelerate)	Download speed	Broadcom-based Routers	The download speed in Mbps when downloading (using UDP) random

Referências

- [1] de Castro, L.N.: Fundamentals of Natural Computing: Basic Concepts, Algorithms, and Applications. CRC Press (2006).
- [2] Felleisen, M., Findler, R.B., Flatt, M.: The Racket Manifesto. LIPIcs-Leibniz. (2015).
- [3] Deb, K., Agrawal, S.: Understanding interactions among genetic algorithm parameters. Foundations of Genetic Algorithms. (1999).