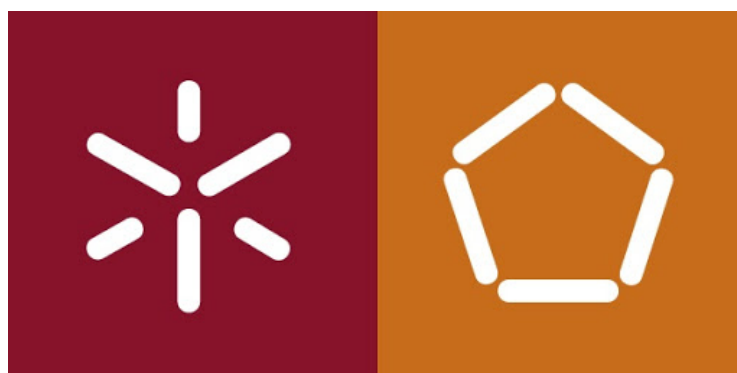


Tarefa Prática 2

Modelação e Caracterização de Tráfego

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



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

Sumário

Sumário	2
Objetivo	3
Parte I - Captura e análise de tráfego	3
Parte 2 - Filtragem de tráfego	4
Conclusão	5
Resultados	6
Anexo I.	7
Referências	8

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).

INICIO RESPOSTA

Protocolo de Transporte	Porta de Origem	Porta de Destino
HTTP	53355	80
FTP	20542	21
TFTP	60499	69
TELNET	545	23
SSH	55608	22
DNS	53068	53
ICMP	53	55616

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.

INICIO RESPOSTA

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

INICIO RESPOSTA

Conclusão

INICIO CONCLUSAO

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

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	Whiteboxes, Routers	Download speed result as a percentage of the user's best ever result
	Percentage Advertised	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 acceleratedUDP)	Download speed	Broadcom-based Routers	The download speed in Mbps when downloading (using UDP) random bytes from a test server

Tabela 3: Tabela com alguns exemplos

O experimento é pequeno para mostrar dados conclusivos, mas mostra indícios do comportamento dos parâmetros de maneira bastante consistente. Obviamente, alterações no algoritmo ou alterações na forma como o problema é representado devem alterar esse comportamento.

Futuros trabalhos podem ser feitos usando-se uma metodologia parecida, mas com modificações no algoritmo e no problema para validar os dados aqui obtidos.

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).