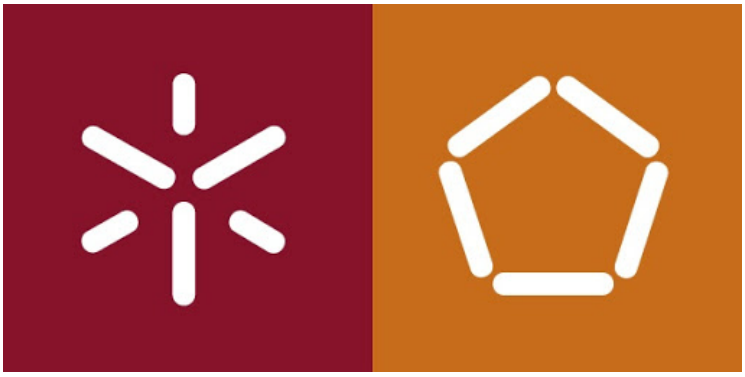
Tarefa Prática 2

Modelação e Caracterização de Tráfego

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



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

Sumário

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 1 - 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.

   INICIO RESPOSTA

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

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 aplicacionais;
   - 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

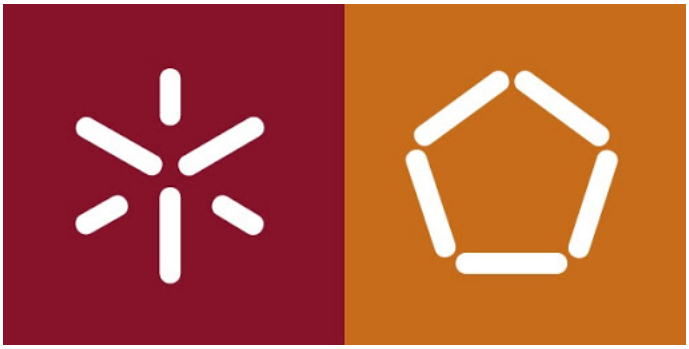


Figura 1. "X" em modelos de tamanhos diferentes

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

Tabela 2: Tabela com alguns exemplos

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).