



10,0

Segunda Avaliação

Nome: PABLO BUSATTO

1. Marque V para as alternativas Verdadeiras e F para as Falsas. (1,2p)

- (V) O serviço DNSSEC possui carga computacional maior do que o serviço DNS convencional.
(V) O serviço DNSSEC gera um tráfego de mensagens superior ao serviço DNS convencional.
(V) Existem domínios em que a adoção do DNSSEC é obrigatória.
(F) DNS e DNSSEC compartilham o mesmo conjunto de RRs.
(F) Os servidores raiz que atendem ao serviço DNSSEC são exclusivos para este serviço.
(V) Poluição de cache é uma vulnerabilidade que afeta o serviço DNS.

2. Associe a primeira coluna com a segunda. Coloque zero onde não há associação. (1,8p)

1. SYN (2) Utilizada para confirmar segmentos TCP previamente enviados.
2. ACK (1) Utilizada em varreduras do tipo *stealth* no *nmap*.
3. RST (4) Encerra uma conexão TCP.
4. FIN (3) Reinicializa uma conexão TCP.
5. URG (5) Indica que *buffers* não devem ser utilizados.
6. PSH (6) Segmentos com essa *flag* devem ser processados imediatamente. (SEIS)

3. Utilizando-se do comando `dig gmail.com -t NS` para realizar consultas DNS foi obtida a resposta mostrada na Figura 1. Sobre as informações mostradas, responda o que se pede:

- i. Quantos servidores de nomes estão disponíveis em `google.com`? Justifique. (0,5p)
4 SERVIDORES DE NOMES: NS1.GOOGLE.COM, NS2.GOOGLE.COM, NS3.GOOGLE.COM E NS4.GOOGLE.COM

- ii. Pode-se afirmar que cada servidor possui endereços IPv6 e Ipv4? Justifique. (0,5p)
SIM, POIS TODOS ELES APRESENTAM RRs DO TIPO A (IPv4) E DO TIPO AAAA (IPv6).

4. Considerando uma rede de datagramas que utiliza endereços de 8 bits. Suponha que um roteador use a correspondência do prefixo mais longo como estratégia de roteamento e tenha a tabela de repasse mostrada na Tabela 4. Dados os datagramas com endereços de destino mostrados abaixo, qual seria a interface que cada datagrama deve ser encaminhado? Justifique. (1,5p)

- a. 10110000
INTERFACE 0 (0), POIS INICIA COM 10, SENDO O MAIS ESPECÍFICO PARA ESSE CASO.
b. 00001111
INTERFACE 3 (TRÊS), POR NÃO CORRESPONDER A NENHUM PREFIXO DAS OUTRAS INTERFACES.
c. 11000101
INTERFACE 0 (ZERO), POIS INICIA COM 1 E NÃO HÁ INTERFACE MAIS ESPECÍFICA.

Prefixo	Interface
1	0
10	1
111	2
senão	3

Tabela 1: Tabela de repasse com endereços de 8 bits.

MacBookPro-JRB-3:~ roberto1\$ dig google.com -t NS

```
;; <<>> DiG 9.10.6 <<>> google.com -t NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26568
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com. IN NS

;; ANSWER SECTION:
google.com. 160232 IN NS ns3.google.com.
google.com. 160232 IN NS ns2.google.com.
google.com. 160232 IN NS ns1.google.com.
google.com. 160232 IN NS ns4.google.com.

;; ADDITIONAL SECTION:
ns3.google.com. 160232 IN A 216.239.36.10
ns1.google.com. 344907 IN A 216.239.32.10
ns4.google.com. 160232 IN A 216.239.38.10
ns2.google.com. 160232 IN A 216.239.34.10
ns3.google.com. 160232 IN AAAA 2001:4860:4802:36::a
ns1.google.com. 160232 IN AAAA 2001:4860:4802:32::a
ns4.google.com. 160232 IN AAAA 2001:4860:4802:38::a
ns2.google.com. 160232 IN AAAA 2001:4860:4802:34::a

;; Query time: 4 msec
;; SERVER: 187.18.187.4#53(187.18.187.4)
;; WHEN: Mon Oct 30 13:35:55 -03 2023
;; MSG SIZE rcvd: 287
```

Figura 1: Saída do comando dig.

5. Abaixo é mostrada a saída do comando `nmap -O scanme.nmap.org`. Sobre as informações mostradas responda ao que se pede: (1 ponto)

MacBookPro-JRB-3:~ roberto1\$ sudo nmap -O scanme.nmap.org

Password:

Starting Nmap 7.93 (<https://nmap.org>) at 2023-10-30 12:59 -03

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.12s latency).

Not shown: 996 closed tcp ports (reset)

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

9929/tcp	open	nping-echo
----------	------	------------

31337/tcp	open	Elite
-----------	------	-------

Device type: general purpose

Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (91%)

OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2

Aggressive OS guesses: Linux 5.0 - 5.4 (91%), Linux 5.4 (90%), Linux 3.10 - 4.11 (89%), Linux 4.15 - 5.6 (89%), Linux 2.6.32 (89%), Linux 2.6.32 or 3.10 (89%), Linux 4.4 (89%), Linux 5.0 - 5.3 (88%), Linux 5.6 (89%), Linux 2.6.32 (89%), Linux 2.6.32 or 3.10 (89%), Linux 4.4 (89%), Linux 5.0 - 5.3 (88%), Linux 5.6 (89%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 19 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>

Nmap done: 1 IP address (1 host up) scanned in 9.23 seconds

- a. É possível afirmar com certeza que o sistema operacional rodando na máquina `scanme.nmap.org` é Linux? Justifique, (0,5p)

NÃO, PORÉM É MOSTRADA UMA PROBABILIDADE MUITO ALTA DE SER UM SISTEMA OPERACIONAL LINUX 5.X|3.X|4.X|2.6.X, DE 91%.

- b. Quais os possíveis estados que as portas mostradas podem assumir numa varredura com `nmap`? (0,5p)

OPEN, CLOSED E FILTERED (ABERTA, FECHADA E FILTRADA)

- c. Cite um dos tipos de varredura disponíveis com o `nmap`. (0,5p)

TCP SYN STEALTH

6. A Figura 2 mostra uma captura de pacotes realizada com Wireshark entre uma máquina de origem (191.235.123.80) e uma máquina de destino (192.168.1.11). Sobre as informações mostradas pergunte-se:

- a. Quais os segmentos que estão relacionados ao estabelecimento de conexão entre origem e destino? Justifique. (0,5p)

Nos 56, 57 e 58, pois correspondem aos segmentos do 3-way HANDSHAKE, com envio do SYN, SYN-ACK e ACK.

- b. Quais os segmentos relacionados a finalização da conexão entre origem e destino? (0,5p)

NENHUM, POIS NÃO HÁ NA IMAGEM SEGMENTOS COM A FLAG FIN.

