

[Painel](#) / [Meus cursos](#) / [BCC36D.IC6A_CM](#) / [Sondagens \(Nota 1\)](#) / [Sondagem - Escaneamento com Nmap \(04/10/2022\)](#)

Iniciado em quarta, 5 out 2022, 19:31

Estado Finalizada

Concluída em quarta, 5 out 2022, 20:10

**Tempo
empregado** 39 minutos 13 segundos

Notas 11,83/20,00

Avaliar 5,92 de um máximo de 10,00(59,17%)

Questão 1

Incorreto

Atingiu 0,00 de 1,00

Os seguintes comandos retornarão os mesmos resultados, pois são equivalentes:

1. nmap 192.168.56.0/24
2. nmap 192.168.56.*
3. nmap 192.168.56.0-255

Escolha uma opção:

- ☐ Verdadeiro
- ☒ Falso ✖

A resposta correta é 'Verdadeiro'.

Questão 2

Incorreto

Atingiu 0,00 de 1,00

No Nmap, qual estado é retornado em uma porta TCP, quando essa porta está acessível, mas não há serviço?

- ☐ a. Filtered
- ☒ b. Unfiltered ✖
- ☐ c. closed
- ☐ d. Open

Sua resposta está incorreta.

A resposta correta é:

closed

Questão 3

Incorreto

Atingiu 0,00 de 1,00

Quando o Nmap é executado por um usuário normal (não root), este executa um scan utilizando apenas SYN, ou seja, sem completar o *three-way handshake*.

Escolha uma opção:

- ☒ Verdadeiro ✖
- ☐ Falso

É feito o *three-way handshake* completo

A resposta correta é 'Falso'.

Questão 4

Correto

Atingiu 1,00 de 1,00

Qual é a função da opção -Pn em um scan com Nmap?

- ☐ a. Descobrir o sistema operacional.
- ☐ b. Apresentar números de protocolos ao invés de nomes.
- ☐ c. Executar um dado script.
- ☒ d. Desabilitar o envio de ICMP echo request para o alvo. ✔

Sua resposta está correta.

A resposta correta é:

Desabilitar o envio de ICMP echo request para o alvo.

Questão 5

Correto

Atingiu 1,00 de 1,00

- ✓ (✓): este *scan* espera como resposta da vítima pacotes TCP com o bit ✓ ativo, caso seja retornado este tipo de pacote o Nmap analisa também o campo Window Size. A ideia é que portas TCP abertas, retornam um Window Size positivo e portas fechadas retornam um Window Size com valor zero (0).
- ✓ (✓): permite fazer *scan* do alvo sem enviar pacotes diretamente para ele. Isso é possível utilizando um *host zombie*. A técnica consiste basicamente em:
 - Enviar pacotes para o *host zombie* e verificar o número de identificação do *datagrama* ✓ (IPid) do *host zombie*;
 - Enviar um pacote do *host* realizando *scan*, para o alvo mas com endereço de origem como sendo do *host zombie* (*spoofing*);
 - Enviar pacotes para o *host zombie* novamente e ver o IPid. Se ele ✓ a porta está aberta, caso contrário está fechada.

Sua resposta está correta.

A resposta correta é:

- **[TCP Window]** (`[-sW]`): este *scan* espera como resposta da vítima pacotes TCP com o bit [RST] ativo, caso seja retornado este tipo de pacote o Nmap analisa também o campo Window Size. A ideia é que portas TCP abertas, retornam um Window Size positivo e portas fechadas retornam um Window Size com valor zero (0).
- **[TCP Idle]** (`[-sI]`): permite fazer *scan* do alvo sem enviar pacotes diretamente para ele. Isso é possível utilizando um *host zombie*. A técnica consiste basicamente em:
 - Enviar pacotes para o *host zombie* e verificar o número de identificação do *datagrama* [IP] (IPid) do *host zombie*;
 - Enviar um pacote do *host* realizando *scan*, para o alvo mas com endereço de origem como sendo do *host zombie* (*spoofing*);
 - Enviar pacotes para o *host zombie* novamente e ver o IPid. Se ele [cresceu] a porta está aberta, caso contrário está fechada.

Questão 6

Correto

Atingiu 1,00 de 1,00

Por padrão o Nmap realiza scan apenas com TCP, mas é possível realizar scan UDP utilizando a opção `-sU`. Todavia existe um grande problema com o *scan* UDP, pois o Kernel do Linux permite apenas uma mensagem ICMP de destino inalcançável por segundo. Ou seja, para escanear as 65.356 portas UDP demoraria mais ou menos 18 horas.

Escolha uma opção:

- ☒ Verdadeiro ✓
- ☐ Falso

A resposta correta é 'Verdadeiro'.

Questão 7

Incorreto

Atingiu 0,00 de 1,00

Qual opção indica o nível de velocidade mais lento possível no Nmap para scan de rede?

- ☒ a. sorrateiro ✖
- ☐ b. agressivo
- ☐ c. gentil
- ☐ d. insano
- ☐ e. paranoico

Sua resposta está incorreta.

A resposta correta é:
paranoico

Questão 8

Correto

Atingiu 1,00 de 1,00

Um scan TCP Maimon envia pacotes TCP com os bits FIN e ACK ativos. Se isso for enviado para sistemas BSD, esses vão: (i) descartar os pacotes, caso a porta estiver aberta; ou (ii) enviar um RST, caso a porta esteja fechada. É possível realizar esse tipo de scan no nmap utilizando a opção -sM.

Escolha uma opção:

- ☒ Verdadeiro ✔
- ☐ Falso

A resposta correta é 'Verdadeiro'.

Questão 9

Incorreto

Atingiu 0,00 de 1,00

No Nmap é possível alterar a velocidade do scan, isso pode ajudar a passar despercebido por sistemas de segurança, para aumentar ou diminuir essa velocidade basta utilizar a opção -v seguida de um número, sendo que esse número vai do 0 ao 5, sendo 0 o mais lento e 5 o mais rápido. Então seria um exemplo de comando nmap com a velocidade lenta: nmap -v2 192.168.56.101.

Escolha uma opção:

- ☒ Verdadeiro ✖
- ☐ Falso

-T2 seria a opção para velocidade no Nmap, não -v

A resposta correta é 'Falso'.

Questão 10

Correto

Atingiu 1,00 de 1,00

Relacione os tipos de scan com a sua opção do Nmap:

1. Com *three-way handshake* completo - ✓
2. Apenas com envio de SYN, sem completar o *three-way handshake* - ✓
3. Sem nenhum bit de controle ativo - ✓
4. Apenas com o bit FIN ativo - ✓
5. Apenas com os bits FIN e ACK ativos - ✓
6. Apenas com o bit ACK ativo - ✓

Sua resposta está correta.

A resposta correta é: Relacione os tipos de scan com a sua opção do Nmap:

1. Com *three-way handshake* completo - [-sT]
2. Apenas com envio de SYN, sem completar o *three-way handshake* - [-sS]
3. Sem nenhum bit de controle ativo - [-sN]
4. Apenas com o bit FIN ativo - [-sF]
5. Apenas com os bits FIN e ACK ativos - [-sM]
6. Apenas com o bit ACK ativo - [-sA]

Questão 11

Incorreto

Atingiu 0,00 de 1,00

Qual opção determina que o Nmap deve verificar se o host está ativo, mas sem identificar portas abertas?

- ☐ a. -sA
- ☐ b. -sN
- ☐ c. -sP
- ☒ d. -sS ✗
- ☐ e. -sT

Sua resposta está incorreta.

A resposta correta é:

-sP

Questão 12

Correto

Atingiu 1,00 de 1,00

É correto afirmar que o scan padrão de portas, realizado pelo Nmap, não reflete exatamente a serviço que está em execução em uma dada porta. Ou seja, o Nmap retorna que o serviço em execução na porta TCP/23 é o telnet, pois essa é a porta padrão do serviço, mas ele não tem certeza disso. Assim, para ter uma informação mais precisa, é necessário utilizar a opção -sV no Nmap, que então apresentará o software em execução na porta, bem como a versão.

Escolha uma opção:

- ☒ Verdadeiro ✓
- ☐ Falso

A resposta correta é 'Verdadeiro'.

Questão 13

Incorreto

Atingiu 0,00 de 1,00

É correto afirma que as duas opções Nmap, a seguir, produzem o mesmo tipo scan:

nmap -sM 192.168.56.1

e

nmap --scanflags 17 192.168.56.1

Escolha uma opção:

- ☐ Verdadeiro
- ☒ Falso ✗

A resposta correta é 'Verdadeiro'.

Questão 14

Correto

Atingiu 1,00 de 1,00

Qual ou quais desses são categorias de scripts do Nmap?

- ☒ a. vuln ✓
- ☒ b. dos ✓
- ☒ c. save ✓
- ☒ d. exploit ✓
- ☒ e. auth ✓

Sua resposta está correta.

As respostas corretas são:

auth,

dos,

exploit,

vuln,

save

Questão 15

Parcialmente correto

Atingiu 0,33 de 1,00

Qual ou quais opções estão escaneando todas as portas TCP disponíveis?

- ☐ a. -p 0-65535
- ☒ b. -p- ✓
- ☐ c. -p *
- ☐ d. -p 0,1,2,3-65535
- ☐ e. -p all

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.

As respostas corretas são:

-p-,

-p 0-65535,

-p 0,1,2,3-65535

Questão 16

Correto

Atingiu 1,00 de 1,00

Dada a saída do Nmap a seguir, responda corretamente qual ou quais opções geram tal saída:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-04 22:44 -03
Nmap scan report for 192.168.56.108
Host is up (0.00021s latency).
```

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:D8:C7:E8 (Oracle VirtualBox virtual NIC)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.22 seconds
```

- ☐ a. -Pn
- ☒ b. -sV ✓
- ☐ c. -sS
- ☐ d. -sT
- ☐ e. -O

Sua resposta está correta.

A resposta correta é:

-sV

Questão 17

Correto

Atingiu 1,00 de 1,00

O Nmap permite que você crie o seu próprio *scan* TCP, isso é possível passando uma dada opção seguida dos bits de controle TCP que devem estar ativados. Sendo assim qual é essa opção a ser passada para o Nmap?
(obs. vc deve colocar apenas o nome da opção, sem nenhum parâmetro, exemplo: --nomeOpção, ou apenas nomeOpção, e não --opção SYN, etc...)

Resposta:



A resposta correta é: --scanflags

Questão 18

Correto

Atingiu 1,00 de 1,00

O NSE permite realizar scans concatenando categorias de scripts, nomes de scripts e diretórios.

Escolha uma opção:

- ☒ Verdadeiro ✓
- ☐ Falso

A resposta correta é 'Verdadeiro'.

Questão 19

Correto

Atingiu 1,00 de 1,00

A opção -p no Nmap indica qual protocolo será escaneado. Esses protocolos são: TCP, UDP e ICMP.

Escolha uma opção:

- ☐ Verdadeiro
- ☒ Falso ✓

A resposta correta é 'Falso'.

Questão 20

Parcialmente correto

Atingiu 0,50 de 1,00

Qual ou quais opções do Nmap consultam o Sistema Operacional do sistema alvo?

- ☐ a. -A
- ☐ b. -SO
- ☐ c. -o
- ☒ d. -O ✓

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.

As respostas corretas são:

-O,

-A

◀ Sondagem - PenTeste (04/10/2022)

Seguir para...

Sondagem - Ganhando Acesso com Metasploit (04/10/2022) ►