Iniciado em	sexta, 14 abr 2023, 15:01
Estado	Finalizada
Concluída em	sexta, 14 abr 2023, 15:08
Tempo empregado	7 minutos 56 segundos
Notas	10,63/20,00
Avaliar	**5,32** de um máximo de 10,00(**53,17**%)

Questão **1**

Parcialmente correto

Atingiu 0,50 de 1,00

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

a. -o

b. -A

c. -SO

d. -O ✔

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.
As respostas corretas são:
-O,

-A

Questão **2**

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 **3**

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 **4**

Parcialmente correto

Atingiu 0,33 de 1,00

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

- a. -p-
- b. -p 0,1,2,3-65335
- c. -p 0-65535 ✔
- d. -p all ✖
- e. -p *

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.
As respostas corretas são:
-p-,

-p 0-65535,

-p 0,1,2,3-65335

Questão **5**

Parcialmente correto

Atingiu 0,80 de 1,00

Qual ou quais desses são categorias de scripts do Nmap?

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

Sua resposta está parcialmente correta.

Você selecionou corretamente 4.

As respostas corretas são:
auth,

dos,

exploit,

vuln,

save

Questão **6**

Correto

Atingiu 1,00 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 ✔

A resposta correta é 'Falso'.

Questão **7**

Correto

Atingiu 1,00 de 1,00

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

a. -sA

b. -sT

c. -sS

d. -sN

e. -sP ✔

Sua resposta está correta.

A resposta correta é:
-sP

Questão **8**

Correto

Atingiu 1,00 de 1,00

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

a. Desabilitar o envio de ICMP echo request para o alvo. ✔

b. Executar um dado script.

c. Apesentar números de protocolos ao invés de nomes.

d. Descobrir o sistema operacional.

Sua resposta está correta.

A resposta correta é:
Desabilitar o envio de ICMP echo request para o alvo.

Questão **9**

Incorreto

Atingiu 0,00 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 **10**

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 **11**

Correto

Atingiu 1,00 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 **12**

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. Open ✖
b. closed
c. Unfiltrered
d. Filtrered

Sua resposta está incorreta.

A resposta correta é:
closed

Questão **13**

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 **14**

Incorreto

Atingiu 0,00 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: -p ✖

A resposta correta é: --scanflags

Questão **15**

Correto

Atingiu 1,00 de 1,00

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 ✔

-sV -sW -sI

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 **16**

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 **17**

Incorreto

Atingiu 0,00 de 1,00

- -sW ✖ (-sI ✖): este *scan* espera como resposta da vítima pacotes TCP com o bit TCP ✖ 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 Window ✖ (TCP NULL ✖): 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* TCP Maimon ✖ (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 RST ✖ a porta está aberta, caso contrário está fechada.

Sua resposta está incorreta.

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 **18**

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. -sT
- [x] c. -sV ✔
- [x] d. -sS ✖
- [ ] e. -O

Sua resposta está correta.

A resposta correta é:
-sV

Questão **19**

Incorreto

Atingiu 0,00 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

-p é a porta

A resposta correta é 'Falso'.

Questão **20**

Incorreto

Atingiu 0,00 de 1,00

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

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

Sua resposta está incorreta.

A resposta correta é:
paranoico

◄ Sondagem - PenTeste (14/04/2023)

Seguir para...

Sondagem - Ganhando Acesso com Metasploit (14/04/2023) ►