

[Painel](#) / [Meus cursos](#) / [BCC36D.IC6A_CM](#) / [Sondagens \(Nota 1\)](#) / [Sondagem - Práticas de Segurança \(18/10/2022\)](#)

Iniciado em segunda, 10 out 2022, 15:54

Estado Finalizada

Concluída em segunda, 10 out 2022, 16:08

**Tempo
empregado** 13 minutos 6 segundos

Notas 13,02/17,00

Avaliar 7,66 de um máximo de 10,00(76,57%)

Questão 1

Correto

Atingiu 1,00 de 1,00

É ou são considerados vantagens de reinstalar um sistema invadido em relação à recuperá-lo:

- ☐ a. Sistema fica menos tempo indisponível.
- ☐ b. Não apagar provas da invasão.
- ☒ c. Certeza de remover tudo o que o hacker fez. ✓
- ☐ d. Certeza de ter um sistema 100% seguro novamente.

Sua resposta está correta.

A resposta correta é:

Certeza de remover tudo o que o hacker fez.

Questão 2

Correto

Atingiu 1,00 de 1,00

Qual ou quais comandos apresentam os usuários logados no sistema atualmente?

- ☐ a. whois
- ☒ b. who ✓
- ☒ c. w ✓
- ☐ d. login

Sua resposta está correta.

As respostas corretas são:

w,

who

Questão 3

Parcialmente correto

Atingiu 0,67 de 1,00

Qual comando ou comandos Linux podem ser utilizados para filtrar informações nos arquivos de log?

- ☐ a. cut
- ☐ b. cat
- ☒ c. grep ✓
- ☒ d. tail ✓

Sua resposta está parcialmente correta.

Você selecionou corretamente 2.

As respostas corretas são:

grep,

cut,

tail

Questão 4

Correto

Atingiu 1,00 de 1,00

Fundamentado nos slides de práticas de segurança, apresente em ordem quais são os 8 passos para desativar serviços desnecessários:

1. Retirar a máquina de rede ✓ ;
2. Identificar os serviços que são realmente necessários ✓ ;
3. Determinar dependências dos serviços ✓ ;
4. Alterar a configuração do sistema de modo que apenas os serviços necessários estejam ativos ✓ ;
5. Reinicializar o sistema ✓ ;
6. Verificar se serviços desnecessários não estão sendo executados ✓ ;
7. Verificar se os serviços necessários estão sendo executados ✓ ;
8. Retornar a máquina à rede e verificar a conectividade da rede ✓ ;

Sua resposta está correta.

A resposta correta é:

Fundamentado nos slides de práticas de segurança, apresente em ordem quais são os 8 passos para desativar serviços desnecessários:

1. [Retirar a máquina de rede];
2. [Identificar os serviços que são realmente necessários];
3. [Determinar dependências dos serviços];
4. [Alterar a configuração do sistema de modo que apenas os serviços necessários estejam ativos];
5. [Reinicializar o sistema];
6. [Verificar se serviços desnecessários não estão sendo executados];
7. [Verificar se os serviços necessários estão sendo executados];
8. [Retornar a máquina à rede e verificar a conectividade da rede];

Questão 5

Correto

Atingiu 1,00 de 1,00

Qual comando Linux é mais indicado para identificar relacionamentos entre processos?

- ☒ a. pstree ✓
- ☐ b. ps a
- ☐ c. ps ax
- ☐ d. top

Sua resposta está correta.

A resposta correta é:

pstree

Questão 6

Parcialmente correto

Atingiu 0,75 de 1,00

Qual ou quais características normalmente são observadas para verificar a integridade dos sistemas de arquivos?

- ☒ a. alteração da permissão do arquivo ✓
- ☒ b. mudança do dono de arquivo ✓
- ☒ c. alteração no conteúdo do arquivo ✓
- ☐ d. alteração do inode

Sua resposta está parcialmente correta.

Você selecionou corretamente 3.

As respostas corretas são:

alteração da permissão do arquivo,

alteração do inode,

mudança do dono de arquivo,

alteração no conteúdo do arquivo

Questão 7

Correto

Atingiu 1,00 de 1,00

Dada a saída do comando ss a seguir, responda quantos servidores temos em execução neste host Linux?

```
ss -a --tcp
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN     0            128         0.0.0.0:db-lsp          0.0.0.0:*
LISTEN     0            128         0.0.0.0:ssh             0.0.0.0:*
TIME-WAIT  0            0          192.168.0.165:57488     172.217.28.238:https
ESTAB      0            0          192.168.0.165:33538     64.233.190.188:hpvroom
ESTAB      0            0          192.168.0.165:42014     162.125.19.131:https
ESTAB      0            0          192.168.0.165:52812     186.226.63.21:https
TIME-WAIT  0            0          192.168.0.165:56954     172.217.173.110:https
TIME-WAIT  0            0          192.168.0.165:43716     172.217.162.202:https
ESTAB      0            0          192.168.0.165:47310     149.154.175.209:https
TIME-WAIT  0            0          192.168.0.165:51872     172.217.29.142:https
ESTAB      0            0          192.168.0.165:49532     172.217.28.14:https
ESTAB      0            0          192.168.0.165:41886     162.125.19.131:https
ESTAB      0            0          192.168.0.165:47302     149.154.175.209:https
ESTAB      0            0          192.168.0.165:39074     162.125.19.130:https
ESTAB      0            0          192.168.0.165:40044     147.135.76.138:https
```

- ☐ a. 9
- ☐ b. 4
- ☐ c. 0
- ☒ d. 2 ✓
- ☐ e. 1

Sua resposta está correta.

A resposta correta é:






2

Questão 8

Parcialmente correto

Atingiu 0,60 de 1,00

O AIDE pode ajudar a monitorar danos potenciais no sistema de arquivos, isso normalmente é feito observando algumas características que no arquivo de configuração do AIDE são dadas por letras/caracteres. Assim, associe tais letras/caracteres com suas respectivas funções dentro do AIDE:

- ☐ u  verifica se o usuário do arquivo mudou;
- ☐ S  se o tamanho do arquivo foi alterado;
- ☐ p  se a permissão do arquivo foi alterada;
- ☐ md5  se a soma md5 do arquivo foi alterada;
- ☐ s  se o arquivo diminuiu de tamanho.

Sua resposta está parcialmente correta.

Você selecionou corretamente 3.

A resposta correta é:

O AIDE pode ajudar a monitorar danos potenciais no sistema de arquivos, isso normalmente é feito observando algumas características que no arquivo de configuração do AIDE são dadas por letras/caracteres. Assim, associe tais letras/caracteres com suas respectivas funções dentro do AIDE:



- [u] verifica se o usuário do arquivo mudou;
- [s] se o tamanho do arquivo foi alterado;
- [p] se a permissão do arquivo foi alterada;
- [md5] se a soma md5 do arquivo foi alterada;
- [S] se o arquivo diminuiu de tamanho.

Questão 9

Parcialmente correto

Atingiu 0,50 de 1,00

Como é possível identificar processos que utilizam conexões TCP em sistema Linux ?

- ☒ a. ps --tcp 
- ☒ b. netstat -ap --tcp 
- ☐ c. ip show tcp
- ☐ d. ss -ap --tcp

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.

As respostas corretas são:

netstat -ap --tcp,

ss -ap --tcp

Questão 10

Correto

Atingiu 1,00 de 1,00

O que o seguinte comando faz:

```
tail -f /var/log/messages
```

- ☐ a. Apresenta as primeiras linhas do arquivo de log
- ☐ b. Apresenta todo o arquivo de log
- ☒ c. Apresenta as últimas linhas do arquivo de log. ✓
- ☐ d. Apresenta a primeira coluna do arquivo de log

Sua resposta está correta.

A resposta correta é:

Apresenta as últimas linhas do arquivo de log.

Questão 11

Parcialmente correto

Atingiu 0,50 de 1,00

Qual ou quais ferramentas podemos utilizar no Linux para verificar danos potenciais no sistema de arquivos?

- ☒ a. AIDE ✓
- ☐ b. check
- ☒ c. Lsdisk ✗
- ☐ d. rpm

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.

As respostas corretas são:

AIDE,

rpm

Questão 12

Parcialmente correto

Atingiu 0,50 de 1,00

É ou são considerados vantagens de recuperar um sistema invadido em relação à reinstala-lo

- ☒ a. Não apagar provas da invasão. ✓
- ☐ b. Sistema fica menos tempo indisponível.
- ☐ c. Maior a chance de remover tudo o que o hacker fez.
- ☐ d. Certeza de ter um sistema 100% seguro novamente.

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.

As respostas corretas são:

Não apagar provas da invasão., Sistema fica menos tempo indisponível.

Questão 13

Correto

Atingiu 1,00 de 1,00

Qual ou quais comandos apresentam o status de processos em sistemas Linux?

- ☒ a. lsof ✓
- ☒ b. ps ✓
- ☒ c. top ✓
- ☒ d. htop ✓

Sua resposta está correta.

As respostas corretas são:

ps ,

lsof ,

top ,

htop

Questão 14

Correto

Atingiu 1,00 de 1,00

Dada a saída a seguir, constata-se que:

```
$ w
```

```
10:31:17 up 4 days, 16:18, 6 users, load average: 1,81, 2,15, 2,98
USUARIO TTY DE LOGIN@ OCIOSO JCPU PCPU O QUE
aluno tty1 :0 dom18 4dias 53:37 0.07s /usr/bin/startplasma-x11
aluno pts/0 :0 dom18 4dias 0.00s 45.48s /usr/bin/kded5
prof pts/1 :0 10:28 4.00s 0.10s 0.00s /bin/bash
root pts/3 10.0.0.254 10:29 4.00s 0.02s 0.01s w -f
prof tty2 - 10:30 1:16 0.00s 0.00s -bash
```

- ☐ a. Não há usuários conectados via rede.
- ☐ b. O usuário aluno está executando o bash em um terminal virtual, provavelmente no ambiente gráfico.
- ☐ c. O usuário prof não está logado no sistema.
- ☒ d. O usuário prof está logado localmente em um terminal da máquina ✓

Sua resposta está correta.

A resposta correta é:

O usuário prof está logado localmente em um terminal da máquina

Questão 15

Parcialmente correto

Atingiu 0,50 de 1,00

Qual comando(s) ou passos permitem bloquear usuários em sistemas Linux?

- ☐ a. `passwd -u`
- ☐ b. `passwd --lock`
- ☒ c. `passwd -l` ✓
- ☐ d. `password -l`

Sua resposta está parcialmente correta.

Você selecionou corretamente 1.

As respostas corretas são:

`passwd -l`,

`passwd --lock`

Questão 16

Incorreto

Atingiu 0,00 de 1,00

Qual opção do comando ps do Linux pode ser utilizado para relacionar usuários com processos?

- ☐ a. x
- ☐ b. g
- ☐ c. u
- ☒ d. a ✖

Sua resposta está incorreta.

A resposta correta é:

u

Questão 17

Correto

Atingiu 1,00 de 1,00

Qual é o caminho absoluto para o diretório de log de sistemas Linux?

Resposta: /var/log



A resposta correta é: /var/log

[◀ Sondagem - Ganhando Acesso com Metasploit \(04/10/2022\)](#)

Seguir para...

[01 - Segurança - Introdução ►](#)