

Treinamento de Investigação Forense Digital – 427

Prova de pré-requisitos

Neste módulo, é recomendável que o aluno tenha familiaridade com Inglês Técnico, Administração Linux e Windows, TCP/IP, metodologias de detecção de invasores, metodologias de “exploits” usadas por hackers e metodologias de ataques em redes de computadores.

Este texto é feito em Inglês, pois o livro texto utilizado no curso é nessa língua e pelo fato de usarmos algumas referências em língua inglesa durante o curso.

1. In Linux, how do you get help about the command "cp"?

- a. whatis cp
- b. man cp
- c. cp ?

2. In Linux, how do you list all the files that are in the current directory?

- a. list all
- b. ls -full
- c. ls -a

3. In Linux, how do you rename file "new" in file "old"?

- a. mv new old
- b. cp new old
- c. rn new old

4. In Linux, how do you visualize the content of file "not_empty"?

- a. type not_empty
- b. cat not_empty
- c. more not_empty

5. In Linux, how do you install an RPM called junk.rpm on your system?

- a. install junk.rpm
- b. rpm -ivh junk.rpm
- c. query junk.rpm

6. In Linux, which command will tell you the directory you are currently in?

- a. pwd
- b. cd
- c. mkdir
- d. whatdir

7. In Linux, what server would you implement to provide windows/linux file sharing?

- a. Sendmail
- b. SSH
- c. SMB
- d. Xinetd

8. In Linux, how do you properly restart the secure shell server?

- a. restart sshd
- b. which sshd
- c. service sshd restart
- d. reboot

9. In Linux, how do you examine at the open TCP/IP ports on your machine?

- a. netstat -na
- b. ps -wauX
- c. ls ports
- d. grep /proc/sockets

10. In Linux, what is the command to interactively delete files?

- a. rm
- b. rm -d
- c. rm -i
- d. rm -a

11. In Linux, which command is used to edit a file?

- a. more
- b. vi
- c. sort
- d. cat

12. In Linux, what command is used for changing file permissions?

- a. chmod
- b. cdmod
- c. rdmod
- d. dmod

13. In Linux, how do you show all files (hidden and dot files) in a directory?

- a. ls -a
- b. ls -x
- c. ls
- d. ls -t

14. In Linux, the permission -rwxr--r-- represents in octal expression is:

- a. 777
- b. 666
- c. 744
- d. 711

15. In Linux, to bring up your eth0 interface with the IP address set to 192.168.2.1, you would execute the following command.

- a. ifconfig eth0 192.168.2.1
- b. set config eth0 192.168.2.1
- c. interface eth0 192.168.2.1
- d. network eth0 192.168.2.1

16. In Linux, which directory contains the configuration files for your linux system?

- a. usr
- b. etc
- c. bin
- d. proc

17. In Linux, which of the following commands is used to transfer the ownership of a file?

- a. trown
- b. chmod
- c. umask
- d. chown

18. In Linux, which of the following commands will abruptly terminate a process?

- a. kill -7
- b. kill -8
- c. kill -9
- d. kill -10

19. In Linux, when you look for a pattern in files which command will you use?

- a. hunt
- b. cat
- c. search
- d. grep

20. In Linux, three commands that hackers usually attempt to Trojan are:

- a. cat, xterm, grep
- b. netstat, ps, top
- c. vmware, sed, less

Respostas

1. b. man cp
2. c. ls -a
3. a. mv new old
4. b. cat not_empty
5. b. rpm -ivh junk.rpm
6. a. pwd
7. c. SMB
8. c. service sshd restart
9. a. netstat -na
10. c. rm -i
11. b. vi
12. a. chmod
13. a. ls -a
14. c. 744
15. a. ifconfig eth0 192.168.2.1
16. b. etc
17. d. chown
18. c. kill -9
19. d. grep
20. b. netstat, ps, top