

Cybersecurity 100 MCQ Practice Quiz

Topics: Bandit Lab Commands (20), OSI Model (20), Subnetting (20), Ports (10), OSINT (15), SSH & Networking Security (15).

Bandit Lab Commands (20)

1. Which command displays file contents?

- A) ls
- B) cat
- C) cd
- D) chmod

2. List hidden files?

- A) ls -a
- B) ls -h
- C) ls -l
- D) ls -r

3. Show current directory?

- A) pwd
- B) dir
- C) ls
- D) cd

4. Copy a file?

- A) mv
- B) cp
- C) scp
- D) copy

5. Move or rename file?

- A) mv
- B) rm
- C) rename
- D) del

6. Delete file?

- A) remove
- B) rm
- C) del
- D) erase

7. Show permissions?

- A) ls -l
- B) chmod
- C) whoami
- D) cat

8. Change file permission?

- A) chmod
- B) chown
- C) sudo
- D) perm

9. Change file owner?

- A) chmod
- B) chown
- C) own
- D) su

10. Show manual?

- A) help
- B) man

- C) doc
- D) guide

11. Search text inside files?

- A) grep
- B) find
- C) locate
- D) cat

12. Find files by name?

- A) locate
- B) search
- C) grep
- D) whereis

13. Show first 10 lines?

- A) head
- B) top
- C) less
- D) more

14. Show last 10 lines?

- A) bottom
- B) tail
- C) last
- D) more

15. Read file one page at a time?

- A) more
- B) less
- C) cat
- D) grep

16. Count words in file?

- A) count
- B) wc
- C) grep
- D) echo

17. Connect remote host?

- A) ssh user@host
- B) ftp
- C) connect
- D) telnet

18. Display processes?

- A) ps
- B) proc
- C) show
- D) top

19. Kill a process?

- A) stop
- B) kill PID
- C) end
- D) rm

20. Compress a file?

- A) gzip
- B) tar
- C) zip
- D) All of the above

OSI Model (20)

21. How many OSI layers?
 - A) 5
 - B) 6
 - C) 7
 - D) 8
22. Layer responsible for routing?
 - A) Network
 - B) Data Link
 - C) Transport
 - D) Session
23. Physical layer deals with?
 - A) Bits
 - B) Packets
 - C) Frames
 - D) Segments
24. Transport layer protocol?
 - A) TCP/UDP
 - B) IP
 - C) ARP
 - D) ICMP
25. Network layer uses?
 - A) IP
 - B) MAC
 - C) Port
 - D) DNS
26. Data link layer function?
 - A) Framing
 - B) Routing
 - C) Encryption
 - D) Segmentation
27. Session layer function?
 - A) Connection control
 - B) Routing
 - C) Framing
 - D) Error check
28. Application layer example?
 - A) HTTP
 - B) TCP
 - C) IP
 - D) Ethernet
29. Which layer ensures reliable delivery?
 - A) Transport
 - B) Network
 - C) Data Link
 - D) Session
30. MAC address works in which layer?
 - A) Data Link
 - B) Network
 - C) Physical
 - D) Transport
31. Encapsulation starts from?
 - A) Application
 - B) Physical
 - C) Network

D) Transport

32. Decapsulation starts from?

- A) Physical
- B) Application
- C) Network
- D) Transport

33. DNS works at which layer?

- A) Application
- B) Network
- C) Data Link
- D) Session

34. ARP works at which layer?

- A) Data Link
- B) Network
- C) Physical
- D) Transport

35. Which layer handles logical addressing?

- A) Network
- B) Data Link
- C) Transport
- D) Physical

36. Which layer segments data?

- A) Transport
- B) Network
- C) Session
- D) Physical

37. SMTP operates at?

- A) Application
- B) Session
- C) Network
- D) Transport

38. Frame check sequence belongs to?

- A) Data Link
- B) Physical
- C) Network
- D) Application

39. ICMP operates at?

- A) Network
- B) Data Link
- C) Transport
- D) Session

40. Flow control is at?

- A) Transport
- B) Network
- C) Application
- D) Session

Subnetting (20)

41. How many hosts in /24?
- A) 254
 - B) 255
 - C) 256
 - D) 512
42. Subnet mask of /26?
- A) 255.255.255.192
 - B) 255.255.255.128
 - C) 255.255.255.224
 - D) 255.255.255.0
43. /30 gives how many usable IPs?
- A) 2
 - B) 4
 - C) 6
 - D) 8
44. /28 usable hosts?
- A) 14
 - B) 16
 - C) 12
 - D) 10
45. Class C default mask?
- A) 255.255.255.0
 - B) 255.255.0.0
 - C) 255.0.0.0
 - D) 255.255.255.128
46. /25 means how many subnets?
- A) 2
 - B) 4
 - C) 8
 - D) 16
47. 192.168.10.64/26 usable range?
- A) 192.168.10.65–192.168.10.126
 - B) 192.168.10.64–192.168.10.127
 - C) 192.168.10.62–192.168.10.124
 - D) 192.168.10.63–192.168.10.125
48. Broadcast address of 10.0.0.0/8?
- A) 10.255.255.255
 - B) 10.0.0.255
 - C) 10.255.255.0
 - D) 10.10.10.255
49. Private IP range?
- A) 192.168.0.0–192.168.255.255
 - B) 172.16.0.0–172.31.255.255
 - C) 10.0.0.0–10.255.255.255
 - D) All of the above
50. /16 hosts?
- A) 65534
 - B) 254
 - C) 512
 - D) 1024
51. CIDR means?
- A) Classless Inter-Domain Routing
 - B) Class In Domain Range
 - C) Connectionless Data Routing

D) Circuit Data Route

52. What is 255.255.255.240 in CIDR?

- A) /28
- B) /29
- C) /30
- D) /31

53. Network ID of 192.168.15.77/28?

- A) 192.168.15.64
- B) 192.168.15.72
- C) 192.168.15.80
- D) 192.168.15.0

54. Which subnet mask gives 8 hosts?

- A) /29
- B) /28
- C) /27
- D) /30

55. First usable in 172.16.10.0/24?

- A) 172.16.10.1
- B) 172.16.10.0
- C) 172.16.10.254
- D) 172.16.10.255

56. Broadcast in /29 (example .0/29)?

- A) .7
- B) .8
- C) .6
- D) .5

57. How many /24 networks fit into /22?

- A) 4
- B) 8
- C) 16
- D) 1

58. IPv6 address size?

- A) 128 bits
- B) 64 bits
- C) 32 bits
- D) 256 bits

59. Link-local IPv6 prefix?

- A) fe80::/10
- B) fd00::/8
- C) ff00::/8
- D) fc00::/7

60. Multicast IPv6 prefix?

- A) ff00::/8
- B) fe80::/10
- C) fc00::/7
- D) fd00::/8

61. Usable hosts in /31?

- A) 0
- B) 1
- C) 2
- D) None

Ports (10)

62. SSH port?

- A) 22
- B) 23
- C) 80
- D) 21

63. FTP port?

- A) 20/21
- B) 22
- C) 25
- D) 110

64. HTTP port?

- A) 80
- B) 443
- C) 8080
- D) 22

65. HTTPS port?

- A) 443
- B) 80
- C) 25
- D) 22

66. DNS port?

- A) 53
- B) 110
- C) 143
- D) 25

67. SMTP port?

- A) 25
- B) 110
- C) 143
- D) 53

68. POP3 port?

- A) 110
- B) 25
- C) 53
- D) 80

69. IMAP port?

- A) 143
- B) 25
- C) 53
- D) 110

70. RDP port?

- A) 3389
- B) 80
- C) 21
- D) 22

71. Telnet port?

- A) 23
- B) 22
- C) 21
- D) 80

OSINT (15)

72. What does OSINT stand for?
- A) Open Source Intelligence
 - B) Open Security Internet
 - C) Online Surveillance Intelligence
 - D) None of the above
73. Tool used for email reconnaissance?
- A) theHarvester
 - B) Hydra
 - C) Nmap
 - D) Wireshark
74. Tool for metadata extraction?
- A) ExifTool
 - B) Hashcat
 - C) Netcat
 - D) Aircrack-ng
75. Tool for social media analysis?
- A) Maltego
 - B) Wireshark
 - C) Hydra
 - D) Nikto
76. Google dork example?
- A) site:example.com
 - B) port:80
 - C) find:admin
 - D) url:search
77. Tool to find breached emails?
- A) HavelBeenPwned
 - B) Nmap
 - C) Sublist3r
 - D) Wireshark
78. Social media username hunter?
- A) Sherlock
 - B) Gobuster
 - C) Hashcat
 - D) Nikto
79. Subdomain enumeration tool?
- A) Sublist3r
 - B) Gobuster
 - C) Dirb
 - D) Hydra
80. Website scanning tool?
- A) Nikto
 - B) Wireshark
 - C) Aircrack-ng
 - D) John the Ripper
81. DNS information tool?
- A) nslookup
 - B) Nmap
 - C) Nikto
 - D) Gobuster
82. What is Shodan?
- A) Search engine for internet-connected devices
 - B) Malware
 - C) Proxy

D) Port scanner

83. OSINT focuses on?

- A) Publicly available data
- B) Hacking servers
- C) Brute force attacks
- D) Malware development

84. Recon-ng is used for?

- A) OSINT automation
- B) Packet capture
- C) Password cracking
- D) Malware analysis

85. Tool for IP geolocation?

- A) ipinfo.io
- B) Hydra
- C) Hashcat
- D) Wireshark

86. What is SpiderFoot?

- A) OSINT automation tool
- B) Password cracker
- C) Port scanner
- D) Proxy tool

SSH & Networking Security (15)

87. SSH full form?
- A) Secure Shell
 - B) Super Server Host
 - C) Safe Socket Handler
 - D) Secure Host Handler
88. Generate SSH key?
- A) ssh-keygen
 - B) ssh-add
 - C) ssh-copy-id
 - D) ssh-config
89. Default SSH directory for user keys?
- A) ~/.ssh
 - B) /etc/ssh
 - C) /root/ssh
 - D) /home/keys
90. Copy SSH key to remote host?
- A) ssh-copy-id user@host
 - B) scp id_rsa user@host:~
 - C) rsync id_rsa user@host:~
 - D) ftp id_rsa user@host
91. SSH protocol runs over which transport?
- A) TCP
 - B) UDP
 - C) ICMP
 - D) Both TCP and UDP
92. Local port forwarding flag?
- A) -L
 - B) -R
 - C) -D
 - D) -P
93. Dynamic port forwarding flag (SOCKS proxy)?
- A) -D
 - B) -L
 - C) -R
 - D) -T
94. SSH config for server settings?
- A) /etc/ssh/sshd_config
 - B) ~/.ssh/config
 - C) /etc/ssh/ssh_config
 - D) /etc/config
95. Which key type is recommended modern default?
- A) Ed25519
 - B) DSA
 - C) RSA (1024)
 - D) MD5
96. Command to add private key to ssh-agent?
- A) ssh-add ~/.ssh/id_ed25519
 - B) ssh-add -l
 - C) ssh-keygen -t ed25519
 - D) ssh-copy-id
97. Disable password authentication in SSH config?
- A) PasswordAuthentication no
 - B) PasswordAuth no
 - C) UsePassword no

D) NoPassword yes

98. Which file holds authorized public keys on remote?

- A) ~/.ssh/authorized_keys
- B) ~/.ssh/known_hosts
- C) /etc/ssh/ssh_known_hosts
- D) ~/.ssh/id_rsa.pub

99. Agent forwarding allows?

- A) Use local keys on remote host
- B) Copy keys to remote
- C) Disable authentication
- D) Change passwords remotely

100. How to run a remote command over SSH?

- A) ssh user@host 'command'
- B) ssh -cmd user@host
- C) ssh -r user@host command
- D) ssh user@host -c command

101. Which tool can test SSH on a server during pentest?

- A) Nmap with ssh-brute scripts or Hydra
- B) Nikto
- C) ExifTool
- D) SpiderFoot

Answer Key

1. B) cat
2. A) ls -a
3. A) pwd
4. B) cp
5. A) mv
6. B) rm
7. A) ls -l
8. A) chmod
9. B) chown
10. B) man
11. A) grep
12. A) locate
13. A) head
14. B) tail
15. B) less
16. B) wc
17. A) ssh user@host
18. A) ps
19. B) kill PID
20. D) All of the above
21. C) 7
22. A) Network
23. A) Bits
24. A) TCP/UDP
25. A) IP
26. A) Framing
27. A) Connection control
28. A) HTTP
29. A) Transport
30. A) Data Link
31. A) Application
32. A) Physical
33. A) Application
34. A) Data Link
35. A) Network
36. A) Transport
37. A) Application
38. A) Data Link
39. A) Network
40. A) Transport
41. A) 254
42. A) 255.255.255.192
43. A) 2
44. A) 14
45. A) 255.255.255.0
46. A) 2
47. A) 192.168.10.65–192.168.10.126
48. A) 10.255.255.255
49. D) All of the above
50. A) 65534
51. A) Classless Inter-Domain Routing
52. A) /28
53. A) 192.168.15.64
54. A) /29
55. A) 172.16.10.1
56. A) .7
57. A) 4
58. A) 128 bits
59. A) fe80::/10

60. A) ff00::/8
61. A) 0
62. A) 22
63. A) 20/21
64. A) 80
65. A) 443
66. A) 53
67. A) 25
68. A) 110
69. A) 143
70. A) 3389
71. A) 23
72. A) Open Source Intelligence
73. A) theHarvester
74. A) ExifTool
75. A) Maltego
76. A) site:example.com
77. A) HavelBeenPwned
78. A) Sherlock
79. A) Sublist3r
80. A) Nikto
81. A) nslookup
82. A) Search engine for internet-connected devices
83. A) Publicly available data
84. A) OSINT automation
85. A) ipinfo.io
86. A) OSINT automation tool
87. A) Secure Shell
88. A) ssh-keygen
89. A) ~/.ssh
90. A) ssh-copy-id user@host
91. A) TCP
92. A) -L
93. A) -D
94. A) /etc/ssh/sshd_config
95. A) Ed25519
96. A) ssh-add ~/.ssh/id_ed25519
97. A) PasswordAuthentication no
98. A) ~/.ssh/authorized_keys
99. A) Use local keys on remote host
100. A) ssh user@host 'command'
101. A) Nmap with ssh-brute scripts or Hydra