

SEC504^{Q&As}

Hacker Tools, Techniques, Exploits and Incident Handling

Pass SANS SEC504 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/sec504.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by SANS
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Which of the following methods can be used to detect session hijacking attack?

- A. nmap
- B. Brutus
- C. ntop
- D. sniffer

Correct Answer: D

QUESTION 2

Fill in the blank with the appropriate word.

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.

- A. canary

Correct Answer: A

QUESTION 3

Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.

```
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176- 1.nv.nv.cox.net
(68.98.176.1)
12.169 ms 14.958 ms 13.416 ms 3 ip68-98-176-1.nv.nv.cox.net
(68.98.176.1)
13.948 ms ip68-100-0-1.nv.nv. cox.net (68.100.0.1) 16.743 ms 16.207 ms 4 ip68-100-0137.nv.nv.cox.net
(68.100.0.137) 17.324 ms 13.933 ms 20.938 ms 5 68.1.1.4
(68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7
unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms "PassGuide" - 8
so-0-10.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9 so- 7-0-0.gar1.
NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms 10 so- 4-00.edge1.NewYork1.Level3.
net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms 11 uunet-level3- oc48.NewYork1.Level3.net
```

(209.244.160.12) 21.411 ms 19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78)
21.203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms
23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms
33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms
49.466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.
NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6- 0.GW5.MIA1.ALTER.NET
(152.63.82.73) 51.897 ms 50.280 ms 53.647 ms 18 PassGuidegw1. customer.alter.net (65.195.239.14)
51.921 ms 51.571 ms 56.855 ms 19 www.PassGuide.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20
www.PassGuide.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms

Which of the following is the most like cause of this issue?

- A. An application firewall
- B. Intrusion Detection System
- C. Network Intrusion system
- D. A stateful inspection firewall

Correct Answer: D

QUESTION 4

Which of the following statements about smurf is true?

- A. It is a UDP attack that involves spoofing and flooding.
- B. It is an ICMP attack that involves spoofing and flooding.
- C. It is an attack with IP fragments that cannot be reassembled.
- D. It is a denial of service (DoS) attack that leaves TCP ports open.

Correct Answer: B

QUESTION 5

What is the purpose of configuring a password protected screen saver on a computer?

- A. For preventing unauthorized access to a system.
- B. For preventing a system from a Denial of Service (DoS) attack.
- C. For preventing a system from a social engineering attack.

D. For preventing a system from a back door attack.

Correct Answer: A

[SEC504 PDF Dumps](#)

[SEC504 Practice Test](#)

[SEC504 Study Guide](#)