

312-50V8^{Q&As}

Certified Ethical Hacker v8

Pass NetApp 312-50V8 Exam with 100% Guarantee

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

<https://www.leads4pass.com/312-50v8.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



QUESTION 1

To scan a host downstream from a security gateway, Firewalking:

- A. Sends a UDP-based packet that it knows will be blocked by the firewall to determine how specifically the firewall responds to such packets
- B. Uses the TTL function to send packets with a TTL value set to expire one hop past the identified security gateway
- C. Sends an ICMP '\administratively prohibited\' packet to determine if the gateway will drop the packet without comment.
- D. Assesses the security rules that relate to the target system before it sends packets to any hops on the route to the gateway

Correct Answer: B

QUESTION 2

An NMAP scan of a server shows port 69 is open. What risk could this pose?

- A. Unauthenticated access
- B. Weak SSL version
- C. Cleartext login
- D. Web portal data leak

Correct Answer: A

QUESTION 3

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected.

What testing method did you use?

- A. Piggybacking
- B. Tailgating
- C. Evesdropping
- D. Social engineering

Correct Answer: D

QUESTION 4

A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

- A. Mitigate
- B. Avoid
- C. Accept
- D. Delegate

Correct Answer: D

QUESTION 5

The "Gray box testing" methodology enforces what kind of restriction?

- A. Only the external operation of a system is accessible to the tester.
- B. Only the internal operation of a system is known to the tester.
- C. The internal operation of a system is completely known to the tester.
- D. The internal operation of a system is only partly accessible to the tester.

Correct Answer: D

QUESTION 6

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet.

How will you achieve this without raising suspicion?

- A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
- C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Correct Answer: C

QUESTION 7

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

- A. Forensic attack
- B. ARP spoofing attack
- C. Social engineering attack
- D. Scanning attack

Correct Answer: C

QUESTION 8

What does a type 3 code 13 represent?(Choose two.)

- A. Echo request
- B. Destination unreachable
- C. Network unreachable
- D. Administratively prohibited
- E. Port unreachable
- F. Time exceeded

Correct Answer: BD

QUESTION 9

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

- A. Configure the Web Server to deny requests involving "hex encoded" characters
- B. Create rules in IDS to alert on strange Unicode requests
- C. Use SSL authentication on Web Servers
- D. Enable Active Scripts Detection at the firewall and routers

Correct Answer: B

QUESTION 10

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.

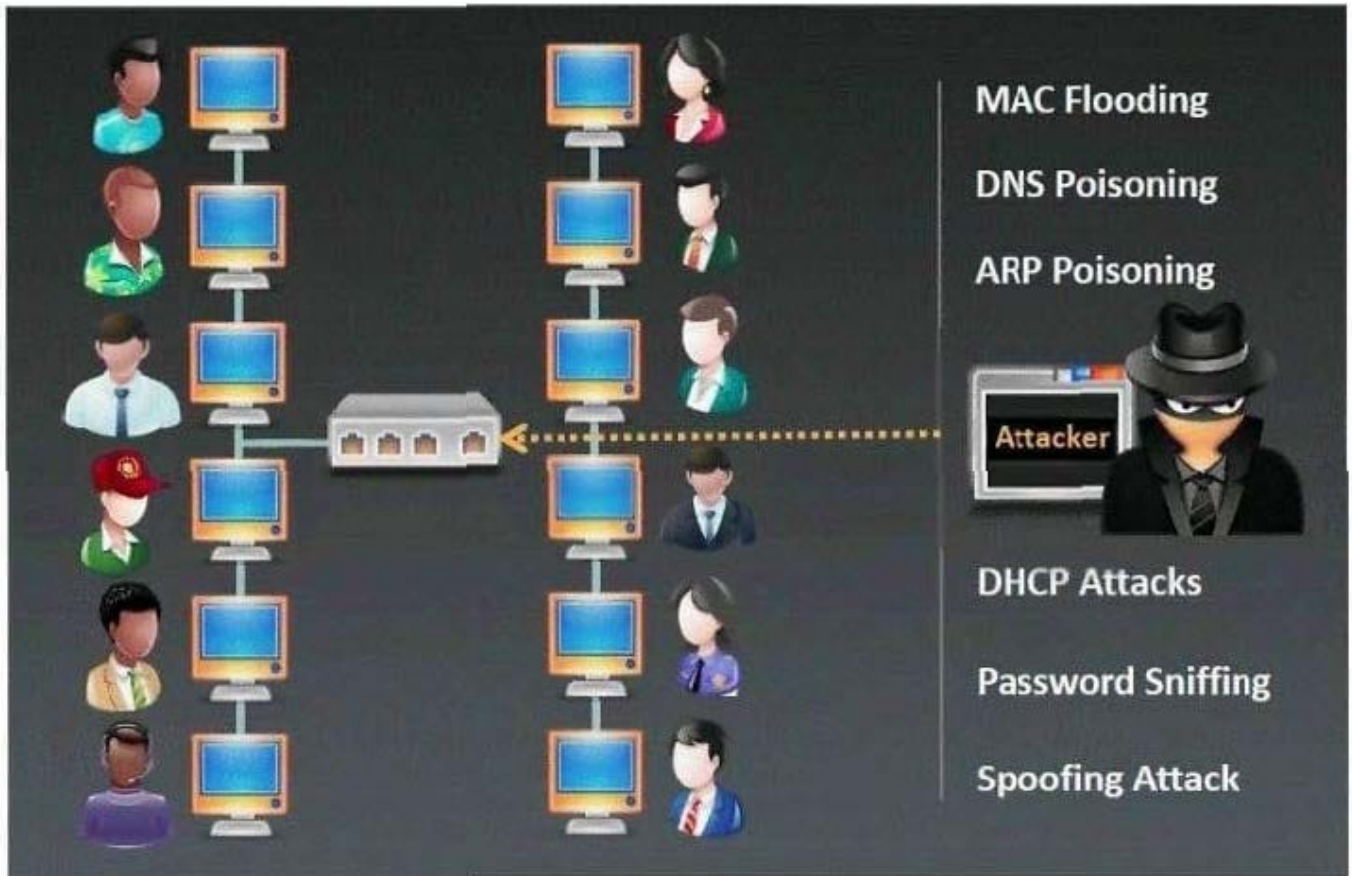
What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

Correct Answer: B

QUESTION 11

Which type of sniffing technique is generally referred as MiTM attack?



- A. Password Sniffing
- B. ARP Poisoning
- C. Mac Flooding
- D. DHCP Sniffing

Correct Answer: B

QUESTION 12

A bank stores and processes sensitive privacy information related to home loans.

However, auditing has never been enabled on the system.

What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Correct Answer: B

QUESTION 13

Which of the following is NOT a reason 802.11 WEP encryption is vulnerable?

- A. There is no mutual authentication between wireless clients and access points
- B. Automated tools like AirSnort are available to discover WEP keys
- C. The standard does not provide for centralized key management
- D. The 24 bit Initialization Vector (IV) field is too small

Correct Answer: C

QUESTION 14

What are the three phases involved in security testing?

- A. Reconnaissance, Conduct, Report
- B. Reconnaissance, Scanning, Conclusion
- C. Preparation, Conduct, Conclusion
- D. Preparation, Conduct, Billing

Correct Answer: C

QUESTION 15

When Jason moves a file via NFS over the company\\'s network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

- A. macof
- B. webspay
- C. filesnarf
- D. nfscopy

Correct Answer: C

[312-50V8 PDF Dumps](#)

[312-50V8 Practice Test](#)

[312-50V8 Braindumps](#)