312-50 Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.pass4itsure.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. True

B. False

Correct Answer: B

Digital signatures enable the recipient of information to verify the authenticity of the information\\'s origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. Instead of encrypting information using someone else\\'s public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.

QUESTION 2

Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Covert keylogger

B. Stealth keylogger

C. Software keylogger

D. Hardware keylogger

Correct Answer: D

As the hardware keylogger never interacts with the Operating System it is undetectable by anti-virus or anti-spyware products.

QUESTION 3

After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

1.

mkdir -p /etc/X11/applnk/Internet/.etc

2.

mkdir -p /etc/X11/applnk/Internet/.etcpasswd

3.

touch -acmr /etc/passwd /etc/X11/applnk/Internet/.etcpasswd

4.

touch -acmr /etc /etc/X11/applnk/Internet/.etc

5.

passwd nobody -d

6.

/usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash

7.

passwd dns -d

8.

touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd

9.

touch -acmr /etc/X11/applnk/Internet/.etc /etc

A. IUSR_

B. acmr, dns

C. nobody, dns

D. nobody, IUSR_

Correct Answer: C

Passwd is the command used to modify a user password and it has been used together with the usernames nobody and dns.

QUESTION 4

Jim\\'s Organization just completed a major Linux roll out and now all of the organization\\'s systems are running Linux 2.5 Kernel. The roll out expenses has posed constraints on purchasing other essential security equipment and software. The organization requires an option to control network traffic and also perform stateful inspection of traffic going into and out of the DMZ, which built-in functionality of Linux can achieve this?

A. IP ICMP

B. IP Sniffer

C. IP tables

D. IP Chains

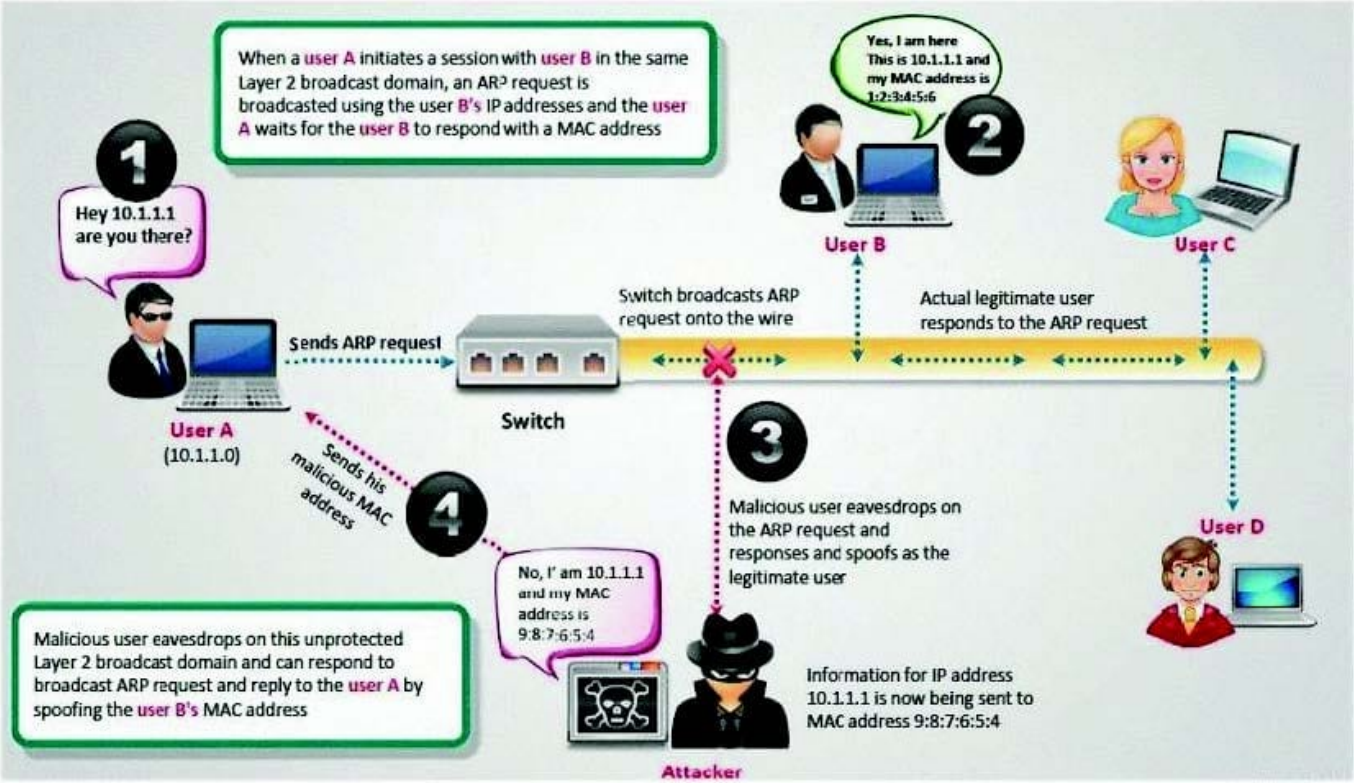
Correct Answer: C

iptables is the name of the user space tool by which administrators create rules for the packet filtering and NAT modules. While technically iptables is merely the tool which controls the packet filtering and NAT components within the kernel, the name iptables is often used to refer to the entire infrastructure, including netfilter, connection tracking and

NAT, as well as the tool itself. iptables is a standard part of all modern Linux distributions.

QUESTION 5

How do you defend against ARP Poisoning attack? (Select 2 answers)



A. Enable DHCP Snooping Binding Table

B. Restrict ARP Duplicates

C. Enable Dynamic ARP Inspection

D. Enable MAC snooping Table

Correct Answer: AC

QUESTION 6

What is the correct order of steps in CEH System Hacking Cycle?

A. Step 1. Gaining Access
Step 2. Escalating Privileges
Step 3. Executing Applications
Step 4. Hiding Files
Step 5. Covering Tracks

B. Step 1. Covering Tracks
Step 2. Hiding Files
Step 3. Escalating Privileges
Step 4. Executing Applications
Step 5. Gaining Access

C. Step 1. Executing Applications
Step 2. Gaining Access
Step 3. Covering Tracks
Step 4. Escalating Privileges
Step 5. Hiding Files

D. Step 1. Escalating Privileges
Step 2. Gaining Access
Step 3. Executing Applications
Step 4. Covering Tracks
Step 5. Hiding Files

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 7

Which programming language is NOT vulnerable to buffer overflow attacks?

A. Java

B. ActiveX

C. C++

D. Assembly Language

Correct Answer: A

Perl and Java has boundary checking, hence buffer overflows don\\'t occur. On the other hand, Perl and Java don\\'t offer access to the system that is as deep as some programs need.

QUESTION 8

While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:

Starting nmap V. 3.10ALPHA9 (www.insecure.org/nmap/) Interesting ports on 172.121.12.222: (The 1592 ports scanned but not shown below are in state: filtered) Port State Service 21/tcp open ftp 25/tcp open smtp 53/tcp closed domain 80/tcp open http 443/tcp open https Remote operating system guess: Too many signatures match to reliably guess the OS. Nmap run completed -- 1 IP address (1 host up) scanned in 277.483 seconds

What should be your next step to identify the OS?

A. Perform a firewalk with that system as the target IP

B. Perform a tcp traceroute to the system using port 53

C. Run an nmap scan with the -v-v option to give a better output

D. Connect to the active services and review the banner information

Correct Answer: D

Most people don\\'t care about changing the banners presented by applications listening to open ports and therefore you should get fairly accurate information when grabbing banners from open ports with, for example, a telnet application.

QUESTION 9

You are scanning the target network for the first time. You are able to detect few convention open ports. While attempting to perform conventional service identification by connecting to the open ports, the scan yields either bad or no result. As you are unsure of the protocols in use, you want to discover as many different protocols as possible. Which of the following scan options can help you achieve this?

A. Nessus sacn with TCP based pings

B. Netcat scan with the switches

C. Nmap scan with the P (ping scan) switch

D. Nmap with the O (Raw IP Packets switch

Correct Answer: D

-sO IP protocol scans: This method is used to determine which IP protocols are supported on a host. The technique is to send raw IP packets without any further protocol header to each specified protocol on the target machine. If we receive an ICMP protocol unreachable message, then the protocol is not in use. Otherwise we assume it is open. Note that some hosts (AIX, HP-UX, Digital UNIX) and firewalls may not send protocol unreachable messages.

QUESTION 10

A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service.

Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks

the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.

Fake E-mail

From: FEDEX Packet Service
Subject: FEDEX Packet N0338795951

Dear Sir/Madam,

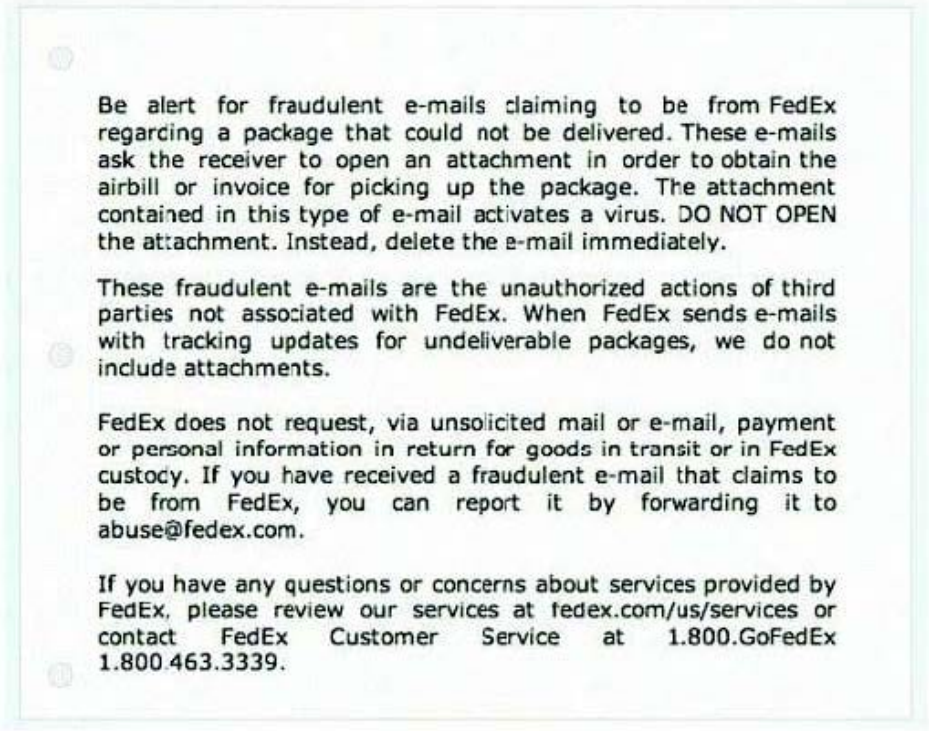
Unfortunately we were not able to deliver postal package you sent on July the 1st in time because the recipient's address is not correct.

Please print out the invoice copy attached and collect the package at our office.

Your Sincerely FEDEX

[File Attached: Fedex-Tracking-number.zip]

Legit E-mail



Be alert for fraudulent e-mails claiming to be from FedEx regarding a package that could not be delivered. These e-mails ask the receiver to open an attachment in order to obtain the airbill or invoice for picking up the package. The attachment contained in this type of e-mail activates a virus. DO NOT OPEN the attachment. Instead, delete the e-mail immediately.

These fraudulent e-mails are the unauthorized actions of third parties not associated with FedEx. When FedEx sends e-mails with tracking updates for undeliverable packages, we do not include attachments.

FedEx does not request, via unsolicited mail or e-mail, payment or personal information in return for goods in transit or in FedEx custody. If you have received a fraudulent e-mail that claims to be from FedEx, you can report it by forwarding it to abuse@fedex.com.

If you have any questions or concerns about services provided by FedEx, please review our services at fedex.com/us/services or contact FedEx Customer Service at 1.800.GoFedEx 1.800.463.3339.

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments. Fraudulent e-mail and legit e-mail that arrives in your inbox contain the fedex.com as the sender of the mail.

How do you ensure if the e-mail is authentic and sent from fedex.com?

A. Verify the digital signature attached with the mail, the fake mail will not have Digital ID at all

B. Check the Sender ID against the National Spam Database (NSD)

C. Fake mail will have spelling/grammatical errors

D. Fake mail uses extensive images, animation and flash content

Correct Answer: A

QUESTION 11

Angela is trying to access an education website that requires a username and password to login. When Angela clicks on the link to access the login page, she gets an error message stating that the page can\\'t be reached. She contacts the website\\'s support team and they report that no one else is having any issues with the site. After handing the issue over to her company\\'s IT department, it is found that the education website requires any computer accessing the site must be able to respond to a ping from the education\\'s server. Since Angela\\'s computer is behind a corporate firewall, her computer can\\'t ping the education website back.

What ca Angela\\'s IT department do to get access to the education website?

A. Change the IP on Angela\\'s Computer to an address outside the firewall

B. Change the settings on the firewall to allow all incoming traffic on port 80

C. Change the settings on the firewall all outbound traffic on port 80

D. Use a Internet browser other than the one that Angela is currently using

Correct Answer: A

Allowing traffic to and from port 80 will not help as this will be UDP or TCP traffic and ping uses ICMP. The browser used by the user will not make any difference. The only alternative here that would solve the problem is to move the computer to outside the firewall.

QUESTION 12

Steven is the senior network administrator for Onkton Incorporated, an oil well drilling company in Oklahoma City. Steven and his team of IT technicians are in charge of keeping inventory for the entire company; including computers, software, and oil well equipment. To keep track of everything, Steven has decided to use RFID tags on their entire inventory so they can be scanned with either a wireless scanner or a handheld scanner. These RFID tags hold as much information as possible about the equipment they are attached to. When Steven purchased these tags, he made sure they were as state of the art as possible. One feature he really liked was the ability to disable RFID tags if necessary. This comes in very handy when the company actually sells oil drilling equipment to other companies. All Steven has to do is disable the RFID tag on the sold equipment and it cannot give up any information that was previously stored on it. What technology allows Steven to disable the RFID tags once they are no longer needed?

A. Newer RFID tags can be disabled by using Terminator Switches built into the chips

B. RFID Kill Switches built into the chips enable Steven to disable them

C. The company\\'s RFID tags can be disabled by Steven using Replaceable ROM technology

D. The technology used to disable an RFIP chip after it is no longer needed, or possibly stolen, is called RSA Blocking

Correct Answer: D

http://www.rsa.com/rsalabs/node.asp?id=2060

QUESTION 13

Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?

A. Rebecca should make a recommendation to disable the () system call

B. Rebecca should make a recommendation to upgrade the Linux kernel promptly

C. Rebecca should make a recommendation to set all child-process to sleep within the execve()

D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can\\'t elevate privilege

Correct Answer: B

QUESTION 14

When Nmap performs a ping sweep, which of the following sets of requests does it send to the target device?

A. ICMP ECHO_REQUEST and TCP SYN

B. ICMP ECHO_REQUEST and TCP ACK

C. ICMP ECHO_REPLY and TFP RST

D. ICMP ECHO_REPLY and TCP FIN

Correct Answer: B

The default behavior of NMAP is to do both an ICMP ping sweep (the usual kind of ping) and a TCP port 80 ACK ping sweep. If an admin is logging these this will be fairly characteristic of NMAP.

QUESTION 15

Jeffery works at a large financial firm in Dallas, Texas as a securities analyst. Last week, the IT department of his company installed a wireless network throughout the building. The problem is, is that they are only going to make it available to upper management and the IT department.

Most employees don\\'t have a problem with this since they have no need for wireless networking, but Jeffery would really like to use wireless since he has a personal laptop that he works from as much as he can. Jeffery asks the IT manager if he could be allowed to use the wireless network but he is turned down. Jeffery is not satisfied, so he brings his laptop in to work late one night and tries to get access to the network. Jeffery uses the wireless utility on his laptop, but cannot see any wireless networks available. After about an hour of trying to figure it out, Jeffery cannot get on the company\\'s wireless network. Discouraged, Jeffery leaves the office and goes home.

The next day, Jeffery calls his friend who works with computers. His friend suggests that his IT department might have turned off SSID broadcasting, and that is why he could not see any wireless networks. How would Jeffrey access the wireless network?

A. Run WEPCrack tool and brute force the SSID hashes

B. Jam the wireless signal by launching denial of service attack

C. Sniff the wireless network and capture the SSID that is transmitted over the wire in plaintext

D. Attempt to connect using wireless device default SSIDs

Correct Answer: C