312-50Q&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.passapply.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

Leonard is a systems administrator who has been tasked by his supervisor to slow down or lessen the amount of SPAM their company receives on a regular basis. SPAM being sent to company email addresses has become a large problem within the last year for them. Leonard starts by adding SPAM prevention software at the perimeter of the network. He then builds a black list, white list, turns on MX callbacks, and uses heuristics to stop the incoming SPAM. While these techniques help some, they do not prevent much of the SPAM from coming in. Leonard decides to use a technique where his mail server responds very slowly to outside connected mail servers by using multi-line SMTP responses. By responding slowly to SMTP connections, he hopes that SPAMMERS will see this and move on to easier and faster targets.

What technique is Leonard trying to employ here to stop SPAM?

A. To stop SPAM, Leonard is using the technique called Bayesian Content Filtering

B. Leonard is trying to use the Transparent SMTP Proxy technique to stop incoming SPAM

C. This technique that Leonard is trying is referred to as using a Sender Policy Framework to aid in SPAM prevention

D. He is using the technique called teergrubing to delay SMTP responses and hopefully stop SPAM

Correct Answer: D

Teergrubing FAQ

What does a UBE sender really need? What does he sell?

A certain amount of sent E-Mails per minute. This product is called Unsolicited Bulk E-Mail.

How can anyone hit an UBE sender?

By destroying his working tools.

What?

E-Mail is sent using SMTP. For this purpose a TCP/IP connection to the MX host of the recipient is established. Usually a computer is able to hold about 65500 TCP/IP connections from/to a certain port. But in most cases it\\'s a lot less due to

limited resources.

If it is possible to hold a mail connection open (i.e. several hours), the productivity of the UBE sending equipment is dramatically reduced. SMTP offers continuation lines to hold a connection open without running into timeouts.

A teergrube is a modified MTA (mail transport agent) able to do this to specified senders.

Incorrect answer:

Sender Policy Framework (SPF) deals with allowing an organization to publish "Authorized" SMTP servers for their organization through DNS records.

QUESTION 2

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company\\'s network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place. Your peer, Peter Smith who works at the same department disagrees with you. He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain. What is Peter Smith talking about?

A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain

B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks

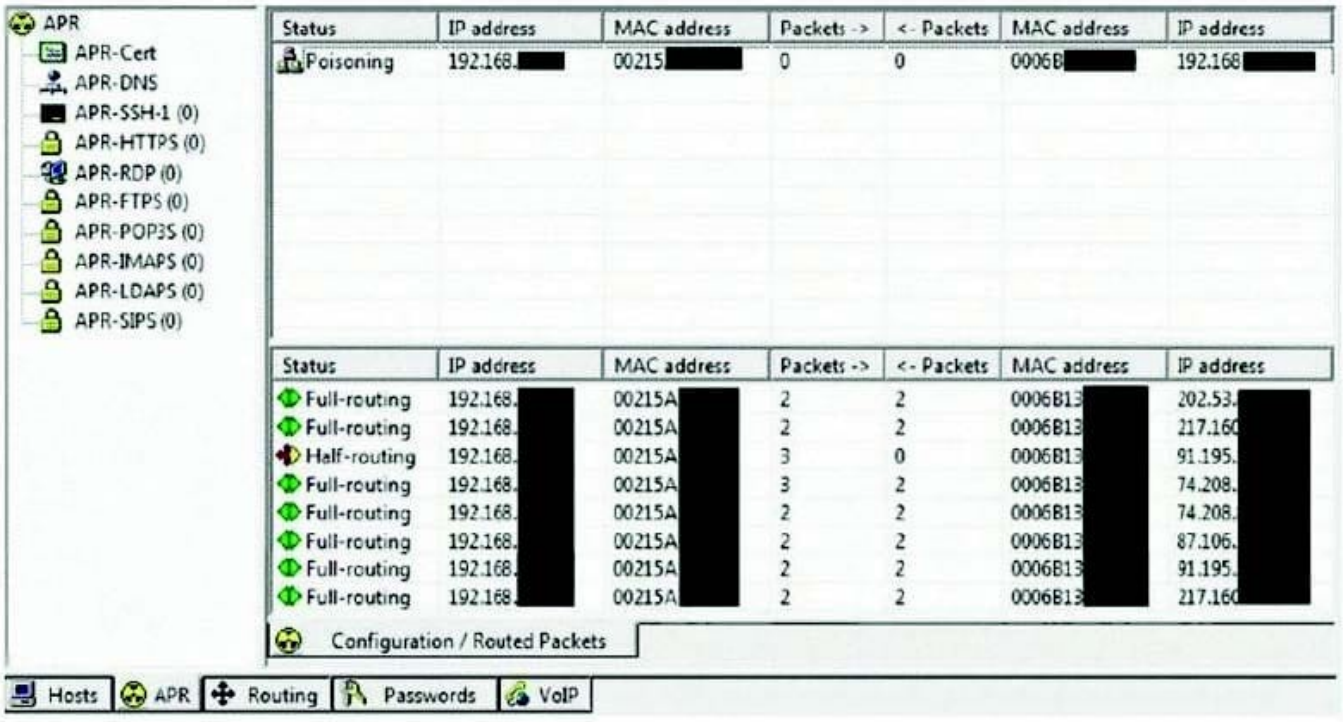
C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks

D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

Correct Answer: A

QUESTION 3

This tool is widely used for ARP Poisoning attack. Name the tool.



A. Cain and Able

B. Beat Infector

C. Poison Ivy

D. Webarp Infector

Correct Answer: A

QUESTION 4

When working with Windows systems, what is the RID of the true administrator account?

A. 500

B. 501

C. 1000

D. 1001

E. 1024

F. 512

Correct Answer: A

Because of the way in which Windows functions, the true administrator account always has a RID of 500.

QUESTION 5

What does FIN in TCP flag define?

A. Used to close a TCP connection

B. Used to abort a TCP connection abruptly

C. Used to indicate the beginning of a TCP connection

D. Used to acknowledge receipt of a previous packet or transmission

Correct Answer: A

The FIN flag stands for the word FINished. This flag is used to tear down the virtual connections created using the previous flag (SYN), so because of this reason, the FIN flag always appears when the last packets are exchanged between a connection.