312-50$^{\text{Q\&As}}$

Ethical Hacker Certified

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

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

https://www.leads4pass.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

You are concerned that someone running PortSentry could block your scans, and you decide to slow your scans so that no one detects them. Which of the following commands will help you achieve this?

A. nmap -sS -PT -PI -O -T1

B. nmap -sO -PT -O -C5

C. nmap -sF -PT -PI -O

D. nmap -sF -P0 -O

Correct Answer: A

-T[0-5]: Set timing template (higher is faster)

QUESTION 2

The GET method should never be used when sensitive data such as credit is being sent to a CGI program. This is because any GET command will appear in the URL and will be logged by any servers. For example, let\\'s say that you\\'ve

entered your credit card information into a form that uses the GET method. The URL may appear like this:

https://www.xsecurity-bank.com/creditcard.asp?cardnumber=454543433532234 The GET method appends the credit card number to the URL. This means that anyone with access to a server log will be able to obtain this information.

How would you protect from this type of attack?

A. Replace the GET with POST method when sending data

B. Never include sensitive information in a script

C. Use HTTOS SSLV3 to send the data instead of plain HTTPS

D. Encrypt the data before you send using GET method

Correct Answer: A

If the method is "get", the user agent takes the value of action, appends a ? to it, then appends the form data set, encoded using the application/x-www-form- urlencoded content type. The user agent then traverses the link to this URI. If the method is "post" --, the user agent conducts an HTTP post transaction using the value of the action attribute and a message created according to the content type specified by the enctype attribute.

QUESTION 3

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall

B. They are using an older version of Internet Explorer that allow them to bypass the proxy server

C. They have been able to compromise the firewall, modify the rules, and give themselves proper access

D. They are using tunneling software that allows them to communicate with protocols in a way it was not intended

Correct Answer: D

This can be accomplished by, for example, tunneling the http traffic over SSH if you have a SSH server answering to your connection, you enable dynamic forwarding in the ssh client and configure Internet Explorer to use a SOCKS Proxy for network traffic.

QUESTION 4

An nmap command that includes the host specification of 202.176.56-57.* will scan _______ number of hosts.

A. 2

B. 256

C. 512

D. Over 10,000

Correct Answer: C

The hosts with IP address 202.176.56.0-255 and 202.176.56.0-255 will be scanned (256+256=512)

QUESTION 5

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts.

Which of the following features makes this possible? (Choose two)

A. It used TCP as the underlying protocol.

B. It uses community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. It is used by all network devices on the market.

Correct Answer: BC

Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly \\'READ\\' and \\'WRITE\\' (or PUBLIC and PRIVATE). If an attacker is able to guess a PUBLIC community string, they would be able to read SNMP data (depending on which MIBs are installed) from the remote device. This information might include system time, IP addresses, interfaces, processes running, etc. Version 1 of SNMP has been criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext.