QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

ECSAv10 Dumps
ECSAv10 Braindumps
ECSAv10 Real Questions
ECSAv10 Practice Test
ECSAv10 dumps free

ECCouncil

ECSAv10

EC-Council Certified Security Analyst

Question: 134

An organization has deployed a web application that uses encoding technique before transmitting the data over the Internet. This encoding technique helps the organization to hide the confidential data such as user credentials, email attachments, etc. when in transit. This encoding technique takes 3 bytes of binary data and divides it into four chunks of 6 bits. Each chunk is further encoded into respective printable character. Identify the encoding technique employed by the organization?

A. Unicode encoding
B. Base64 encoding
C. URL encoding
D. HTMS encoding

Answer: B

Question: 135

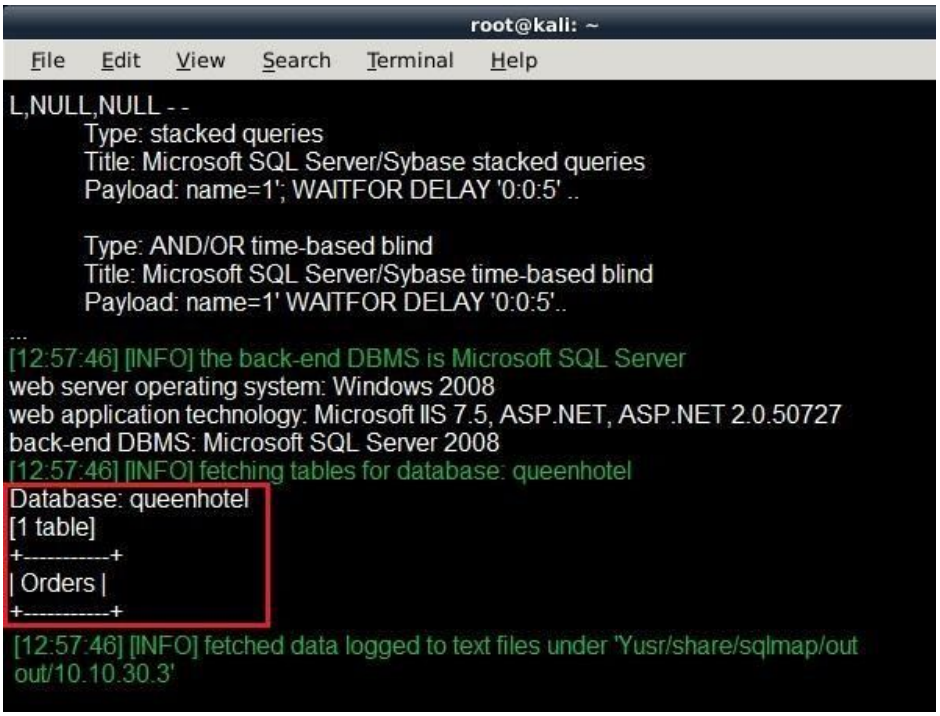
During an internal network audit, you are asked to see if there is any RPC server running on the network and if found, enumerate the associate RPC services. Which port would you scan to determine the RPC server and which command will you use to enumerate the RPC services?

A. Port 111, rpcinfo
B. Port 111, rpcenum
C. Port 145, rpcinfo
D. Port 145, rpcenum

Answer: A

Question: 136

Richard is working on a web app pen testing assignment for one of his clients. After preliminary information, gathering and vulnerability scanning Richard runs the SQLMAP tool to extract the database information. Which of the following commands will give Richard an output as shown in the screenshot?

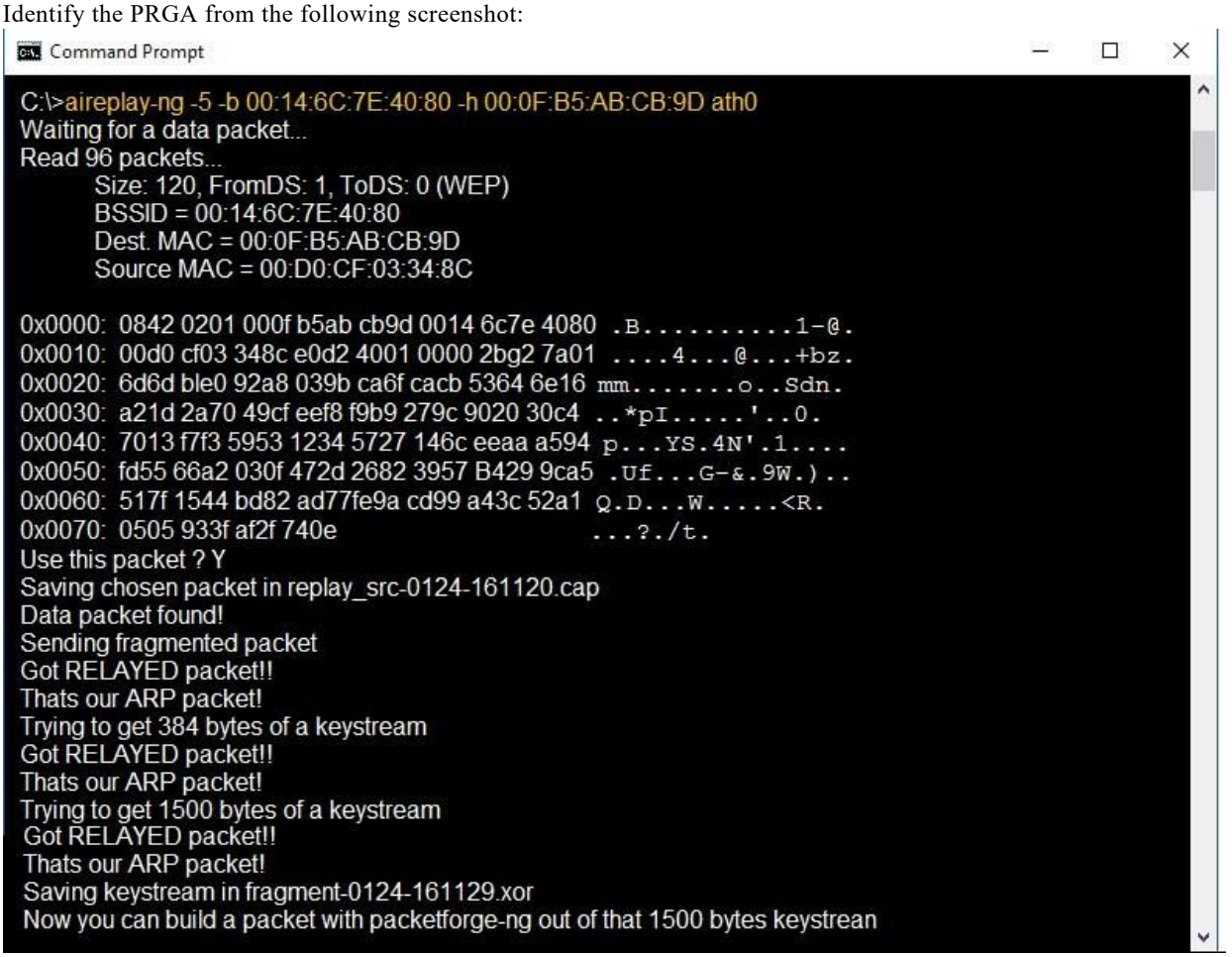


A. sqlmap -url http://quennhotel.com/about.aspx?name=1 -D queenhotel –tables
B. sqlmap -url http://quennhotel.com/about.aspx?name=1 -dbs
C. sqlmap -url http://quennhotel.com/about.aspx?name=1 -D queenhotel -T –columns
D. sqlmap -url http://quennhotel.com/about.aspx?name=1 -database queenhotel -tables

Answer: A

Question: 137

Identify the PRGA from the following screenshot:



A. replay_src-0124-161120.cap
B. fragment-0124-161129.xor
C. 0505 933f af2f 740e
D. 0842 0201 000f b5ab cd9d 0014 6c7e 4080

Answer: A

Question: 138

Sandra, a wireless network auditor, discovered her client is using WEP. To prove the point that the WEP encryption is very weak, she wants to decrypt some WEP packets. She successfully captured the WEP data packets, but could not reach the content as the data is encrypted.
Which of the following will help Sandra decrypt the data packets without knowing the key?
A. Fragmentation Attack
B. Chopchop Attack
C. ARP Poisoning Attack
D. Packet injection Attack

Answer: B

Question: 139

Peter, a disgruntled ex-employee of Zapmaky Solutions Ltd., is trying to jeopardize the company's website http://zapmaky.com. He conducted the port scan of the website by using the Nmap tool to extract the information about open ports and their corresponding services. While performing the scan, he recognized that some of his requests are being blocked by the firewall deployed by the IT personnel of Zapmaky and he wants to bypass the same. For evading the firewall, he wanted to employ the stealth scanning technique which is an incomplete TCP three-way handshake method that can effectively bypass the firewall rules and logging mechanisms. Which if the following Nmap commands should Peter execute to perform stealth scanning?
A. nmap -sT -v zapmaky.com
B. nmap -T4 -A -v zapmaky.com
C. nmap -sX -T4 -A -v zapmaky.com
D. nmap -sN -A zapmaky.com

Answer: A

Question: 140

Richard, a penetration tester was asked to assess a web application. During the assessment, he discovered a file upload field where users can upload their profile pictures. While scanning the page for vulnerabilities, Richard found a file upload exploit on the website. Richard wants to test the web application by uploading a malicious PHP shell, but the web page denied the file upload. Trying to get around the security, Richard added the 'jpg' extension to the end of the file.
The new file name ended with '.php.jpg'. He then used the Burp suite tool and removed the 'jpg" extension from the request while uploading the file. This enabled him to successfully upload the PHP shell. Which of the following techniques has Richard implemented to upload the PHP shell?

A. Session stealing
B. Cookie tampering
C. Cross site scripting
D. Parameter tampering

Answer: D

Question: 141

Joseph, a penetration tester, was hired by Xsecurity Services. Joseph was asked to perform a pen test on a client's network. He was not provided with any information about the client organization except the company name. Identify the type of testing Joseph is going to perform for the client organization?

A. White-box Penetration Testing
B. Black-box Penetration Testing
C. Announced Testing
D. Grey-box Penetration Testing

Answer: B

Question: 142

An organization deployed Microsoft Azure cloud services for running their business activities. They appointed Jamie, a security analyst for performing cloud penetration testing. Microsoft prohibits certain tests to be carried out on their platform.
Which of the following penetration testing activities Jamie cannot perform on the Microsoft Azure cloud service?

A. Post scanning
B. Denial-of-Service
C. Log monitoring
D. Load testing

Answer: B

Question: 143

Sam was asked to conduct penetration tests on one of the client's internal networks. As part of the testing process, Sam performed enumeration to gain information about computers belonging to a domain, list of shares on the individual hosts in the network, policies and passwords. Identify the enumeration technique.

A. NTP Enumeration
B. NetBIOS Enumeration
C. DNS Enumeration
D. SMTP Enumeration

Answer: B

Question: 144

Jason is working on a pen testing assignment. He is sending customized ICMP packets to a host in the target network. However, the ping requests to the target failed with "ICMP Time Exceeded Type = 11" error messages. What can Jason do to overcome this error?

A. Set a Fragment Offset
B. Increase the Window size in the packets
C. Increase the TTL value in the packets
D. Increase the ICMP header length

Answer: C

Question: 145

A hacker initiates so many invalid requests to a cloud network host that the host uses all its resources responding to invalid requests and ignores the legitimate requests. Identify the type of attack

A. Denial of Service (DoS) attacks
B. Side Channel attacks
C. Man-in-the-middle cryptographic attacks
D. Authentication attacks

Answer: A

Question: 146

Thomas is an attacker and he skimmed through the HTML source code of an online shopping website for the presence of any vulnerabilities that he can exploit. He already knows that when a user makes any selection of items in the online shopping webpage, the selection is typically stored as form field values and sent to the application as an HTTP request (GET or POST) after clicking the Submit button. He also knows that some fields related to the selected items are modifiable by the user (like quantity, color, etc.) and some are not (like price). While skimming through the HTML code, he identified that the price field values of the items are present in the HTML code. He modified the price field values of certain items from $200 to $2 in the HTML code and submitted the request successfully to the application. Identify the type of attack performed by Thomas on the online shopping website?

A. Session poisoning attack
B. Hidden field manipulation attack
C. HTML embedding attack
D. XML external entity attack

Answer: C

Question: 147

Steven is performing a wireless network audit. As part of the engagement, he is trying to crack a WPA-PSK key. Steven has captured enough packets to run aircrack-ng and discover the key, but aircrack-ng did not yield any result, as there were no authentication packets in the capture.

Which of the following commands should Steven use to generate authentication packets?

A. aireplay-ng –deauth 11 -a AA:BB:CC:DD:EE:FF
B. airmon-ng start eth0
C. airodump-ng –write capture eth0
D. aircrack-ng.exe -a 2 -w capture.cap

Answer: A

Question: 148

Irin is a newly joined penetration tester for XYZ Ltd. While joining, as a part of her training, she was instructed about various legal policies and information securities acts by her trainer. During the training, she was informed about a specific information security act related to the conducts and activities like it is illegal to perform DoS attacks on any websites or applications, it is illegal to supply and own hacking tools, it is illegal to access unauthorized computer material, etc. To which type of information security act does the above conducts and activities best suit?

A. Police and Justice Act 2006
B. Data Protection Act 1998
C. USA Patriot Act 2001
D. Human Rights Act 1998

Answer: B

Question: 149

Adam is an IT administrator for Syncan Ltd. He is designated to perform various IT tasks like setting up new user accounts, managing backup/ restores, security authentications and passwords, etc. Whilst performing his tasks, he was asked to employ the latest and most secure authentication protocol to encrypt the passwords of users that are stored in the Microsoft Windows OS-based systems. Which of the following authentication protocols should Adam employ in order to achieve the objective?

A. LANMAN
B. Kerberos

C. NTLM
D. NTLMv2

Answer: C

Question: 150

Michael, a Licensed Penetration Tester, wants to create an exact replica of an original website, so he can browse and spend more time analyzing it. Which of the following tools will Michael use to perform this task?
A. VisualRoute
B. NetInspector
C. BlackWidow
D. Zaproxy

Answer: C