Exam Questions 312-50v9

Certified Ethical Hacker Exam

https://www.2passeasy.com/dumps/312-50v9/

NEW QUESTION 1
A common cryptographically tool is the use of XOR. XOR the following binary value: 10110001
00111010

A. 10001011
B. 10011101
C. 11011000
D. 10111100

Answer: A

NEW QUESTION 2
What does a firewall check to prevent particularports and applications from getting packets into an organizations?

A. Transport layer port numbers and application layer headers
B. Network layer headers and the session layer port numbers
C. Application layer port numbers and the transport layer headers
D. Presentation layer headers and the session layer port numbers

Answer: A

NEW QUESTION 3
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?

A. Bounding
B. Mutating
C. Puzzing
D. Randomizing

Answer: C

NEW QUESTION 4
env x= ‘(){ :;};echo exploit ‘ bash –c ‘cat/etc/passwd
What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

A. Add new user to the passwd file
B. Display passwd contents to prompt
C. Change all password in passwd
D. Remove the passwd file.

Answer: B

NEW QUESTION 5
Which of the following describes the characteristics of a Boot Sector Virus?

A. Overwrites the original MBR and only executes the new virus code
B. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

Answer: C

NEW QUESTION 6
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known wardriving.
Which algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)
B. Temporal Key Integrity Protocol (TRIP)
C. Wi-Fi Protected Access (WPA)
D. Wi-Fi Protected Access 2(WPA2)

Answer: A

NEW QUESTION 7
An attacker changes the profile information of a particular user on a target website (the victim). The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker’s database.
<frame src=http://www/vulnweb.com/updataif.php Style=”display:none”></iframe> What is this type of attack (that can use either HTTP GET or HRRP POST) called?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. SQL Injection

D. Browser Hacking

Answer: A

NEW QUESTION 8
While using your bank's online servicing you notice the following stringin the URL bar: "http://www.MyPersonalBank/Account?Id=368940911028389&Damount=10980&Camount=21"
You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.
What type of vulnerability is present on this site?

A. SQL injection
B. XSS Reflection
C. Web Parameter Tampering
D. Cookie Tampering

Answer: C

NEW QUESTION 9
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up windows, webpage,or email warning from what looks like an officialauthority. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again.
Which term best matches this definition?

A. Spyware
B. Adware
C. Ransomware
D. Riskware

Answer: C

NEW QUESTION 10
Nation-state threat actors often discover vulnerabilitiesand hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability.
What is this style of attack called?

A. zero-hour
B. no-day
C. zero-day
D. zero-sum

Answer: C

NEW QUESTION 10
Perspective clients wantto see sample reports from previous penetration tests. What should you do next?

A. Share full reports, not redacted.
B. Share full reports, with redacted.
C. Decline but, provide references.
D. Share reports, after NDA is signed.

Answer: B

NEW QUESTION 11
What is the process of logging, recording, and resolving events that take place in an organization?

A. Metrics
B. Security Policy
C. Internal Procedure
D. Incident Management Process

Answer: D

NEW QUESTION 15
Risk = Threats x Vulnerabilities is referred to as the:

A. Threat assessment
B. Disaster recovery formula
C. BIA equation
D. Risk equation

Answer: D

NEW QUESTION 19
While performing online banking using a web browser, a user receives an email that contains alink to an interesting Web site. When the user clicks on the link, another web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank,

indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.
What web browser-based security vulnerability was exploited to compromise the user?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Web form input validation
D. Clickjacking

Answer: A

NEW QUESTION 22
Which of the following is component of a risk assessment?

A. Logical interface
B. DMZ
C. Administrative safeguards
D. Physical security

Answer: C

NEW QUESTION 24
Which of the following parameters describe LM Hash: I – The maximum password length is 14 characters.
II – There are no distinctions between uppercase and lowercase.
III – It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I
B. I and II
C. II
D. I, II and III

Answer: D

NEW QUESTION 29
When you are testing a web application, it is very useful to employ a prosy tool to save every request and response.Nyou can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?

A. Burpsuite
B. Dimitry
C. Proxychains
D. Maskgen

Answer: A

NEW QUESTION 30
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. Wificracker
B. WLAN-crack
C. Airguard
D. Aircrack-ng

Answer: D

NEW QUESTION 31
Which of the following is not a Bluetooth attack?

A. Bluejacking
B. Bluedriving
C. Bluesnarfing
D. Bluesmaking

Answer: B

NEW QUESTION 35
A hacker has successfully infected an internet-facing server, which he will then use to send junk mail, take part incoordinated attacks, or host junk email content.
Which sort of trojan infects this server?

A. Botnet Trojan
B. Banking Trojans
C. Ransomware Trojans
D. Turtle Trojans

Answer: A

NEW QUESTION 38
The phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the“landscape” looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. Network Mapping
B. Gaining access
C. Footprinting
D. Escalating privileges

Answer: C

NEW QUESTION 42
An incident investigator asks to receive a copy of the event from all firewalls, prosy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs the sequence of many of the logged events do not match up.
What is the most likely cause?

A. The network devices are not all synchronized
B. The securitybreach was a false positive.
C. The attack altered or erased events from the logs.
D. Proper chain of custody was not observed while collecting the logs.

Answer: C

NEW QUESTION 45
It is a regulation that has a set if guideline,which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.
Which of the following regulations best matches the description?

A. HIPAA
B. COBIT
C. ISO/IEC 27002
D. FISMA

Answer: A

NEW QUESTION 48
How does the Address Resolution Protocol (ARP) work?

A. It sends a reply packet for a specific IP, asking for the MAC address.
B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
C. It sends a request packet to all the network elements, asking for the domainname from a specific IP.
D. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.

Answer: D

NEW QUESTION 51
Which of these options is the most secure procedure for strong backup tapes?

A. In a climate controlled facility offsite
B. Inside the data center for faster retrieval in afireproof safe
C. In a cool dry environment
D. On a different floor in the same building

Answer: A

NEW QUESTION 52
A company’s security states that all web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
B. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
C. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
D. Attempts by attacks to access the user and password information stores in the company's SQL database.

Answer: C

NEW QUESTION 54
A Regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?

A. Move the financial data to another server on the same IP subnet
B. Place a front-end web server in a demilitarized zone that only handles external web traffic
C. Issue new certificates to the web servers from the root certificate authority
D. Require all employees to change their passwords immediately

Answer: A

NEW QUESTION 59
Which regulationdefines security and privacy controls for Federal information systems and organizations?

A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53

Answer: D

NEW QUESTION 63
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping but you didn't get any response back.
What is happening?

A. TCP/IP doesn't support ICMP.
B. ICMP could be disabled on the target server.
C. The ARP is disabled on the target server.
D. You need to run the ping command with root privileges.

Answer: A

NEW QUESTION 65
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet
B. Netstumbler
C. Abel
D. Nessus

Answer: A

NEW QUESTION 66
It isan entity or event with the potential to adversely impact a system through unauthorized access destruction disclosures denial of service or modification of data.
Which of the following terms best matches this definition?

A. Threat
B. Attack
C. Risk
D. Vulnerability

Answer: A

NEW QUESTION 71
As a Certified Ethical hacker, you were contracted by aprivate firm to conduct an external security assessment through penetration testing.
What document describes the specified of the testing, the associated violations, and essentially protects both the organization's interest and your li abilities as a tester?

A. Term of Engagement
B. Non-Disclosure Agreement
C. Project Scope
D. Service Level Agreement

Answer: B

NEW QUESTION 75
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

A. Nmap –T4 –F 10.10.0.0/24
B. Nmap –T4 –q 10.10.0.0/24
C. Nmap –T4 –O 10.10.0.0/24
D. Nmap –T4 –r 10.10.0.0/24

Answer: A

NEW QUESTION 76
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from the server will not be caught by a Network

Based Intrusion Detection System (NIDS).
Which is the best way to evade the NIDS?

A. Out of band signaling
B. Encryption
C. Alternate Data Streams
D. Protocol Isolation

Answer: B

NEW QUESTION 78
You are performing a penetration test. You achieved access via a bufferoverflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.
What should you do?

A. Do not transfer the money but steal the bitcoins.
B. Report immediately to the administrator.
C. Transfer money from the administrator's account to another account.
D. Do not report it and continue the penetration test.

Answer: B

NEW QUESTION 83
You have compromised a server on a network and successfully open a shell. You aimed to identify all operating systems running on the network. However, as you attemptto fingerprint all machines in the machines in the network using the nmap syntax below, it is not going through.
invictus@victim_server:~$nmap –T4 –O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxxx. QUITTING!
What seems to be wrong?

A. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
B. This is a common behavior for a corrupted nmap application.
C. OS Scan requires root privileged.
D. The nmap syntax is wrong.

Answer: D

NEW QUESTION 86
The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.
What tool can you use to view the network traffic being sent and received by the wireless router?

A. Netcat
B. Wireshark
C. Nessus
D. Netstat

Answer: B

NEW QUESTION 91
What is the most common method to exploit the "Bash Bug" or ShellShock" vulnerability?

A. SSH
B. SYN Flood
C. Manipulate format strings in text fields
D. Through Web servers utilizing CGI (CommonGateway Interface) to send a malformed environment variable to a vulnerable Web server

Answer: D

NEW QUESTION 94
You've just been hired to perform a pentest on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.
What is one of the first thing you should to when the job?

A. Start the wireshark application to start sniffing network traffic.
B. Establish attribution to suspected attackers.
C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
D. Interview all employees in the company to rule out possible insider threats.

Answer: C

NEW QUESTION 96
Which of the following is the successor of SSL?

A. RSA
B. GRE
C. TLS

D. IPSec

Answer: C

NEW QUESTION 98
Using Windows CMD, how would an attacker list all the shares to which the current user context hasaccess?

A. NET CONFIG
B. NET USE
C. NET FILE
D. NET VIEW

Answer: D

NEW QUESTION 99
An Intrusion Detection System(IDS) has alerted the network administrator to a possibly malicious sequence of packets went to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.
What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Intrusion Prevention System (IPS)
C. Vulnerability scanner
D. Network sniffer

Answer: B

NEW QUESTION 101
A new wireless client is configured to join a 802.11 network. Thisclient uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.
What is a possible source of this problem?

A. The client cannot see the SSID of the wireless network
B. The wireless client is not configured to use DHCP
C. The WAP does not recognize the client's MAC address
D. Client isconfigured for the wrong channel

Answer: C

NEW QUESTION 103
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do this fast and efficiently you must user regular expressions.
Which command-line utility are you most likely to use?

A. Notepad
B. MS Excel
C. Grep
D. Relational Database

Answer: C

NEW QUESTION 105
Ricardo wants to send secret messages to acompetitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message, the technique provides 'security through obscurity'. What technique is Ricardo using?

A. RSA algorithm
B. Steganography
C. Encryption
D. Public-key cryptography

Answer: B

NEW QUESTION 108
Which of the followingis the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns
B. Voice
C. Fingerprints
D. Height and Weight

Answer: D

NEW QUESTION 113
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark,and EtherPeek?

A. Nessus
B. Tcptraceroute
C. Tcptrace
D. OpenVAS

Answer: C

NEW QUESTION 114
It is a vulnerability in GNU's bash shell, discovered in September of 2004, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of service attacks to disrupt websites, and scan for other vulnerable devices (including routers).
Which of the following vulnerabilities is being described?

A. Shellshock
B. Rootshock
C. Shellbash
D. Rootshell

Answer: A

NEW QUESTION 117
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to www.MyPersonalBank.com, that the user is directed to a phishing site.
Which file does the attacker needto modify?

A. Hosts
B. Networks
C. Boot.ini
D. Sudoers

Answer: A

NEW QUESTION 118
Which of the following is considered the best way to prevent Personally Identifiable Information (PII) from web application vulnerabilities?

A. Use encrypted communications protocols to transmit PII
B. Use full disk encryption on all hard drives to protect PII
C. Use cryptographic storage to store all PII
D. Use a security token to log onto into all Web application that use PII

Answer: A

NEW QUESTION 119
Session splicing is an IDS evasiontechnique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.
Which tool can used to perform session splicing attacks?

A. Hydra
B. Burp
C. Whisker
D. Tcpsplice

Answer: C

NEW QUESTION 123
The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate theSLE, ARO, and ALE. Assume the EF = 1 (100%).
What is the closest approximate cost of this replacement and recovery operation per year?

A. $100
B. $146
C. 440
D. 1320

Answer: B

NEW QUESTION 128
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGI's?

A. Snort
B. Dsniff
C. Nikto
D. John the Ripper

Answer: C

NEW QUESTION 133
Which tool allows analysis and pen testers to examine links between data using graphs and link analysis?

A. Metasploit
B. Maltego
C. Wireshark
D. Cain &Abel

Answer: B

NEW QUESTION 135
The heartland bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2004-1060. Thisbug affects the OpenSSL implementation of the transport Layer security (TLS) protocols defined in RFC6520.
What types of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Root
B. Private
C. Shared
D. Public

Answer: A

NEW QUESTION 137
A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

A. Mitigate
B. Avoid
C. Accept
D. Delegate

Answer: D

NEW QUESTION 139
Which of the following tools can be used for passiveOS fingerprinting?

A. tcpdump
B. ping
C. nmap
D. Tracert

Answer: C

NEW QUESTION 143
After trying multiple exploits, you've gained root access to a Centos 6 answer. To ensure you maintain access. What would you do first?

A. Disable IPTables
B. Create User Account
C. Downloadand Install Netcat
D. Disable Key Services

Answer: C

NEW QUESTION 144
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal Network.
What is this type of DNS configuration commonly called?

A. DNS Scheme
B. DynDNS
C. Split DNS
D. DNSSEC

Answer: C

NEW QUESTION 145
Which of the following is an extremelycommon IDS evasion technique in the web world?

A. post knocking
B. subnetting
C. unicode characters
D. spyware

Answer: C

NEW QUESTION 146

When you are collecting information to perform a dataanalysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.
What command will help you to search files using Google as a search engine?

A. site:target.com file:xls username password email
B. domain: target.com archive:xls username password email
C. site: target.com filetype:xls username password email
D. inurl: target.com filename:xls username password email

Answer: C

NEW QUESTION 151
What is the best description of SQL Injection?

A. It is a Denial of Service Attack.
B. It is an attack used to modify code in an application.
C. It is and attack used to gain unauthorized access to a database.
D. It isa Man-in-the-Middle attack between your SQL Server and Web App Server.

Answer: D

NEW QUESTION 153
Under the “Post-attach Phase and Activities,” it is the responsibility of the tester to restore the system to a pre-test state.
Which of the following activities should not be included in this phase? I.Removing all files uploaded on the system
II.Cleaning all registry entries III.Mapping of network state
IV.Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included.

Answer: A

NEW QUESTION 154
You just set up a security system in your network. In what kind of system would you find thefollowing string of characters used as a rule within its configuration?
alert tcp any any ->192.168.100.0/24 21 (msg: "FTP on the network!";)

A. A firewall IPTable
B. A Router IPTable
C. An Intrusion Detection System
D. FTP Server rule

Answer: C

NEW QUESTION 155
You’ve gained physical access to a Windows 2008 R2 server which has as accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD.Which Linux tool has the ability to change any user’s password or to activate disabled Windows Accounts?

A. John the Ripper
B. CHNTPW
C. Cain & Abel
D. SET

Answer: A

NEW QUESTION 157
Which of the following is designed to indentify malicious attempts to penetrate systems?

A. Proxy
B. Router
C. Firewall
D. Intrusion Detection System

Answer: D

NEW QUESTION 162
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50v9 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50v9 Product From:

https://www.2passeasy.com/dumps/312-50v9/

Money Back Guarantee

312-50v9 Practice Exam Features:

* 312-50v9 Questions and Answers Updated Frequently

* 312-50v9 Practice Questions Verified by Expert Senior Certified Staff

* 312-50v9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-50v9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year