



# ECCouncil

**Exam 412-79v8**

**EC-Council Certified Security Analyst (ECSA)**

Version: 10.3

**[ Total Questions: 196 ]**

**Question No : 1**

A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

- A. Shoulder surfing
- B. Phishing
- C. Insider Accomplice
- D. Vishing

**Answer: A**

**Question No : 2**

Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?



- A. Service-based Assessment Solutions
- B. Product-based Assessment Solutions
- C. Tree-based Assessment

D. Inference-based Assessment

**Answer: C**

Reference:[http://www.netsense.info/downloads/security\\_wp\\_mva.pdf](http://www.netsense.info/downloads/security_wp_mva.pdf)(page 12, tree-based assessment technology, second para)

**Question No : 3**

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a type and code field.



Which of the following ICMP messages will be generated if the destination port is not reachable?

- A. ICMP Type 11 code 1
- B. ICMP Type 5 code 3
- C. ICMP Type 3 code 2
- D. ICMP Type 3 code 3

**Answer: D**

**Question No : 4**

Which of the following attacks is an offline attack?

- A. Pre-Computed Hashes
- B. Hash Injection Attack

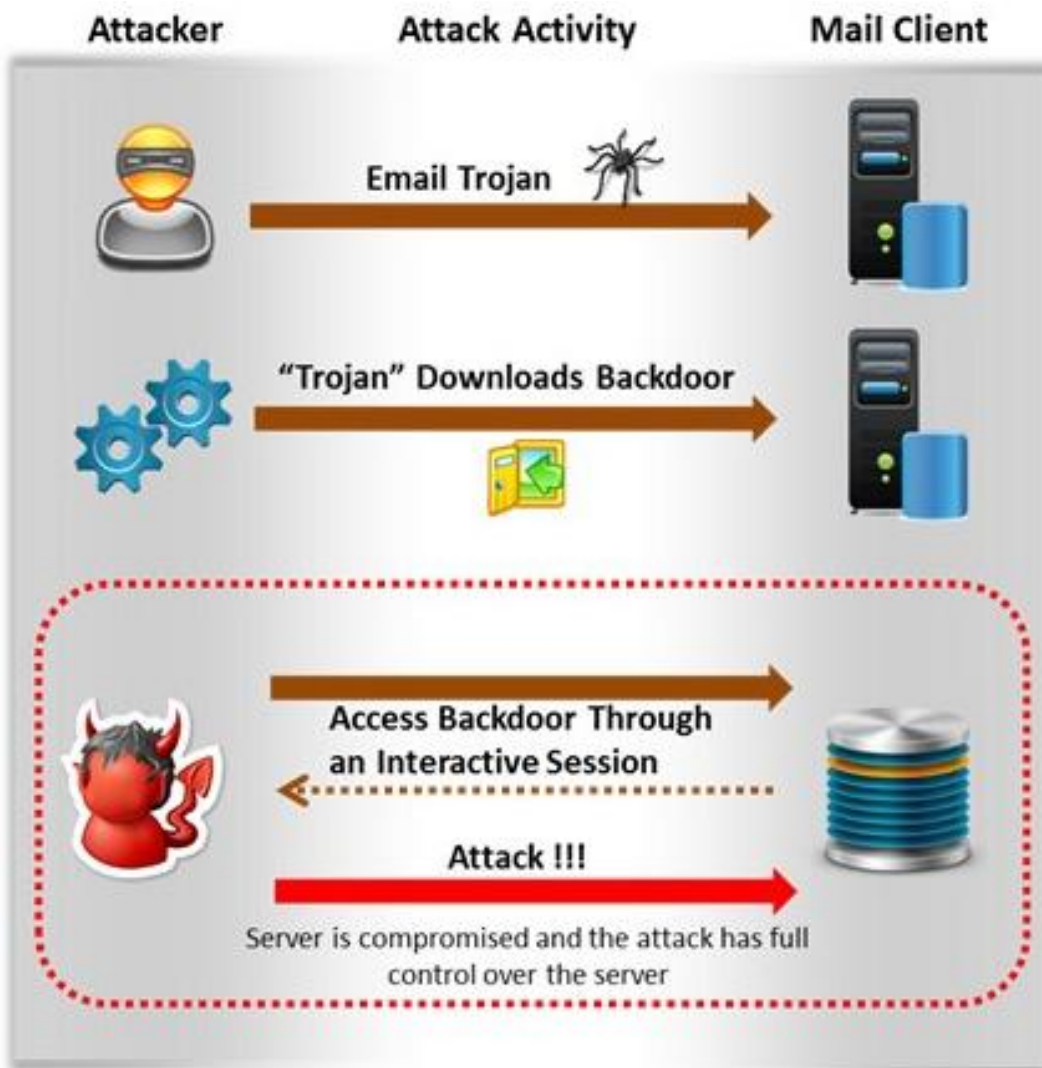
- C. Password Guessing
- D. Dumpster Diving

Answer: A

Reference: <http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html>

**Question No : 5**

Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.



Which of the following techniques do attackers use to create backdoors to covertly gather

critical information about a target machine?

- A. Internal network mapping to map the internal network of the target machine
- B. Port scanning to determine what ports are open or in use on the target machine
- C. Sniffing to monitor all the incoming and outgoing network traffic
- D. Social engineering and spear phishing attacks to install malicious programs on the target machine

**Answer: D**

**Question No : 6**

What is the maximum value of a “tinyint” field in most database systems?

- A. 222
- B. 224 or more
- C. 240 or less
- D. 225 or more

**Answer: D**

Reference:[http://books.google.com.pk/books?id=JUclAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--R5r&sig=1hMOYByxt7ebRJ4UEjbpXmijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI\\_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false](http://books.google.com.pk/books?id=JUclAAAAQBAJ&pg=SA3-PA3&lpg=SA3-PA3&dq=maximum+value+of+a+%E2%80%9Ctinyint%E2%80%9D+field+in+most+database+systems&source=bl&ots=NscGk--R5r&sig=1hMOYByxt7ebRJ4UEjbpXmijTQs&hl=en&sa=X&ei=pvgeVJnTCNDkaI_fgugO&ved=0CDYQ6AEwAw#v=onepage&q=maximum%20value%20of%20a%20%E2%80%9Ctinyint%E2%80%9D%20field%20in%20most%20database%20systems&f=false)

**Question No : 7**

Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?

- A. SYN Scan
- B. TCP Connect Scan
- C. XMAS Scan
- D. Null Scan

**Answer: A**

**Question No : 8**

TCP/IP provides a broad range of communication protocols for the various applications on the network. The TCP/IP model has four layers with major protocols included within each layer. Which one of the following protocols is used to collect information from all the network devices?

- A. Simple Network Management Protocol (SNMP)
- B. Network File system (NFS)
- C. Internet Control Message Protocol (ICMP)
- D. Transmission Control Protocol(TCP)

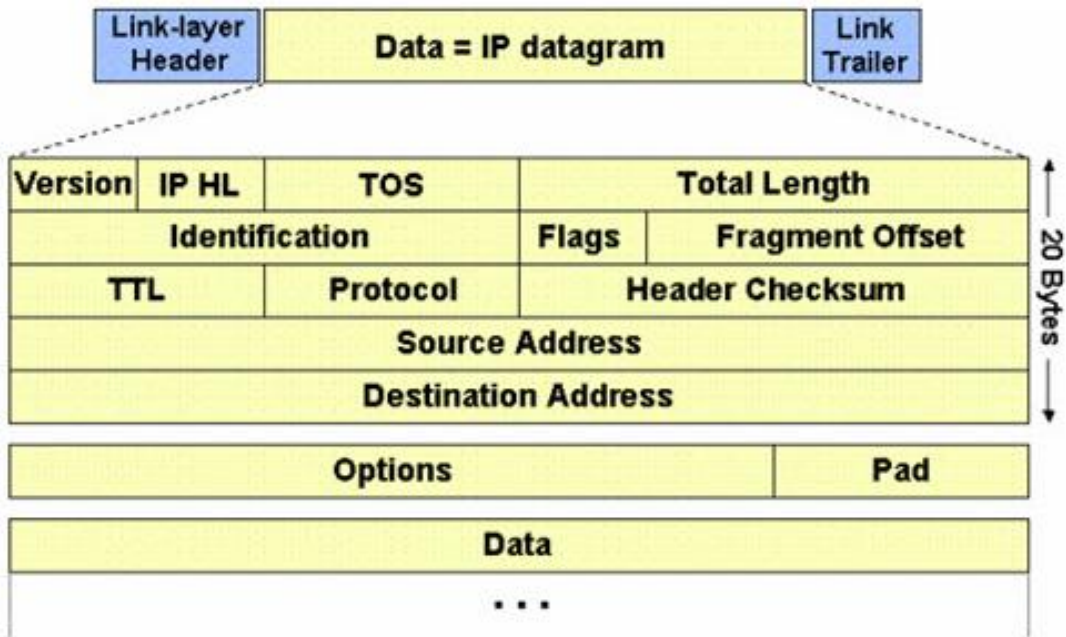
**Answer: A**

**Question No : 9**

The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 64K, most transmission links enforce a smaller maximum packet length limit, called a MTU.

The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences by allowing routers to fragment IP datagrams as necessary. The receiving station is responsible for reassembling the fragments back into the original full size IP datagram.

IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields in the IP header, are used for IP fragmentation and reassembly.



The fragment offset is 13 bits and indicates where a fragment belongs in the original IP datagram. This value is a:

- A. Multiple of four bytes
- B. Multiple of two bytes
- C. Multiple of eight bytes
- D. Multiple of six bytes

**Answer: C**

Reference: <http://www.freesoft.org/CIE/Course/Section3/7.htm>(fragment offset: 13 bits)

**Question No : 10**

Many security and compliance projects begin with a simple idea: assess the organization's risk, vulnerabilities, and breaches. Implementing an IT security risk assessment is critical to the overall security posture of any organization.

An effective security risk assessment can prevent breaches and reduce the impact of realized breaches.



What is the formula to calculate risk?

- A. Risk = Budget x Time
- B. Risk = Goodwill x Reputation
- C. Risk = Loss x Exposure factor
- D. Risk = Threats x Attacks

**Answer: C**

**Question No : 11**

What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

- A. Inference-based Assessment
- B. Service-based Assessment Solutions



- C. Product-based Assessment Solutions
- D. Tree-based Assessment

**Answer: A**

Reference:[http://www.businessweek.com/adsections/2005/pdf/wp\\_mva.pdf](http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf)(page 26, first para on the page)

**Question No : 12**

Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

- A. UDP and TCP
- B. TCP and SMTP
- C. SMTP
- D. UDP and SMTP

**Answer: A**

**Question No : 13**

Which one of the following components of standard Solaris Syslog is a UNIX command that is used to add single-line entries to the system log?

- A. "Logger"
- B. "/etc/syslog.conf"
- C. "Syslogd"
- D. "Syslogd.conf"

**Answer: A**

**Question No : 14**

Information gathering is performed to:

## Dumps with PDF and VCE ( +Free VCE Software )

- i) Collect basic information about the target company and its network
- ii) Determine the operating system used, platforms running, web server versions, etc.
- iii) Find vulnerabilities and exploits



Which of the following pen testing tests yields information about a company's technology infrastructure?

- A. Searching for web page posting patterns
- B. Analyzing the link popularity of the company's website
- C. Searching for trade association directories
- D. Searching for a company's job postings

**Answer: D**

### Question No : 15

The Web parameter tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

## Dumps with PDF and VCE ( +Free VCE Software )

This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.



What is the best way to protect web applications from parameter tampering attacks?

- A. Validating some parameters of the web application
- B. Minimizing the allowable length of parameters
- C. Using an easily guessable hashing algorithm
- D. Applying effective input field filtering parameters

**Answer: D**

### Question No : 16

Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

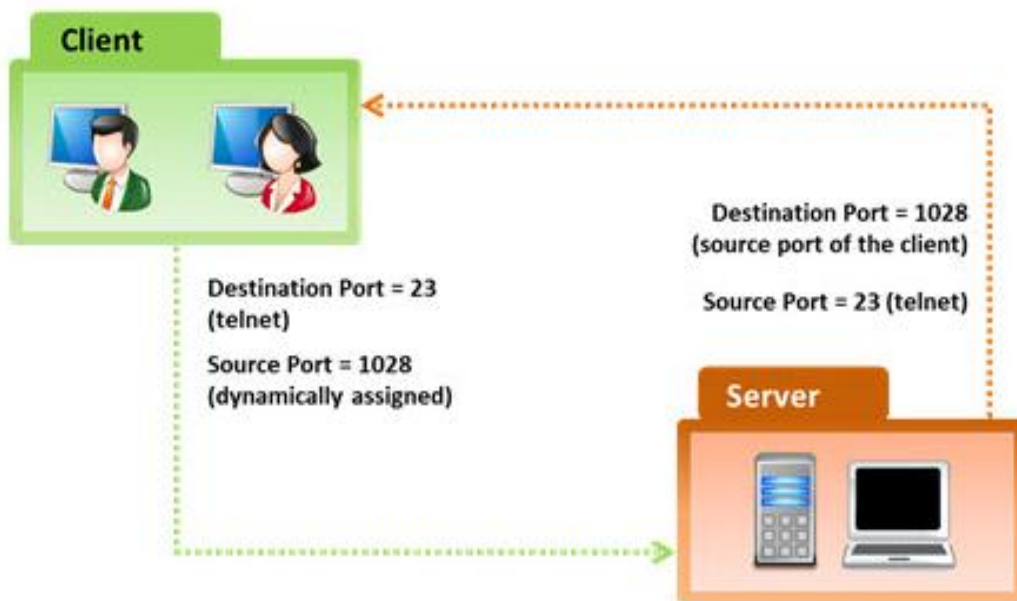
- A. Threat-Assessment Phase
- B. Pre-Assessment Phase
- C. Assessment Phase
- D. Post-Assessment Phase

**Answer: B**

### Question No : 17

In the TCP/IP model, the transport layer is responsible for reliability and flow control from source to the destination. TCP provides the mechanism for flow control by allowing the sending and receiving hosts to communicate. A flow control mechanism avoids the problem

with a transmitting host overflowing the buffers in the receiving host.



Which of the following flow control mechanism guarantees reliable delivery of data?

- A. Sliding Windows
- B. Windowing
- C. Positive Acknowledgment with Retransmission (PAR)
- D. Synchronization

**Answer: C**

Reference:<http://condor.depaul.edu/jkristof/technotes/tcp.html>(1.1.3 Reliability)

### Question No : 18

Which one of the following architectures has the drawback of internally considering the hosted services individually?

- A. Weak Screened Subnet Architecture
- B. "Inside Versus Outside" Architecture
- C. "Three-Homed Firewall" DMZ Architecture
- D. Strong Screened-Subnet Architecture

**Answer: C**

**Question No : 19**

Besides the policy implications of chat rooms, Internet Relay Chat (IRC) is frequented by attackers and used as a command and control mechanism. IRC normally uses which one of the following TCP ports?

- A. 6566 TCP port
- B. 6771 TCP port
- C. 6667 TCP port
- D. 6257 TCP port

**Answer: C**

**Question No : 20**

Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructions, encryption used, and web page behaviors?



- A. Check for Directory Consistency and Page Naming Syntax of the Web Pages
- B. Examine Server Side Includes (SSI)
- C. Examine Hidden Fields
- D. Examine E-commerce and Payment Gateways Handled by the Web Server

**Answer: C**

Reference:<http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction>(page 71)

### Question No : 21

Which of the following appendices gives detailed lists of all the technical terms used in the report?

- A. Required Work Efforts

- B. References
- C. Research
- D. Glossary

**Answer: D**

**Explanation:** Refere'<http://en.wikipedia.org/wiki/Glossary>

**Question No : 22**

Firewall and DMZ architectures are characterized according to its design. Which one of the following architectures is used when routers have better high-bandwidth data stream handling capacity?

- A. Weak Screened Subnet Architecture
- B. "Inside Versus Outside" Architecture
- C. "Three-Homed Firewall" DMZ Architecture
- D. Strong Screened-Subnet Architecture

**Answer: A**

**Question No : 23**

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.





Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

- A. Passive Assessment
- B. Host-based Assessment
- C. External Assessment
- D. Application Assessment

**Answer: D**

**Question No : 24**

The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a program specific signal and the handler for this calls the DropStats() function to output the current Snort statistics?

- A. SIGUSR1
- B. SIGTERM
- C. SIGINT
- D. SIGHUP



**Answer: A**

**Question No : 25**

HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using %xx notation, where 'xx' is the

- A. ASCII value of the character
- B. Binary value of the character
- C. Decimal value of the character
- D. Hex value of the character

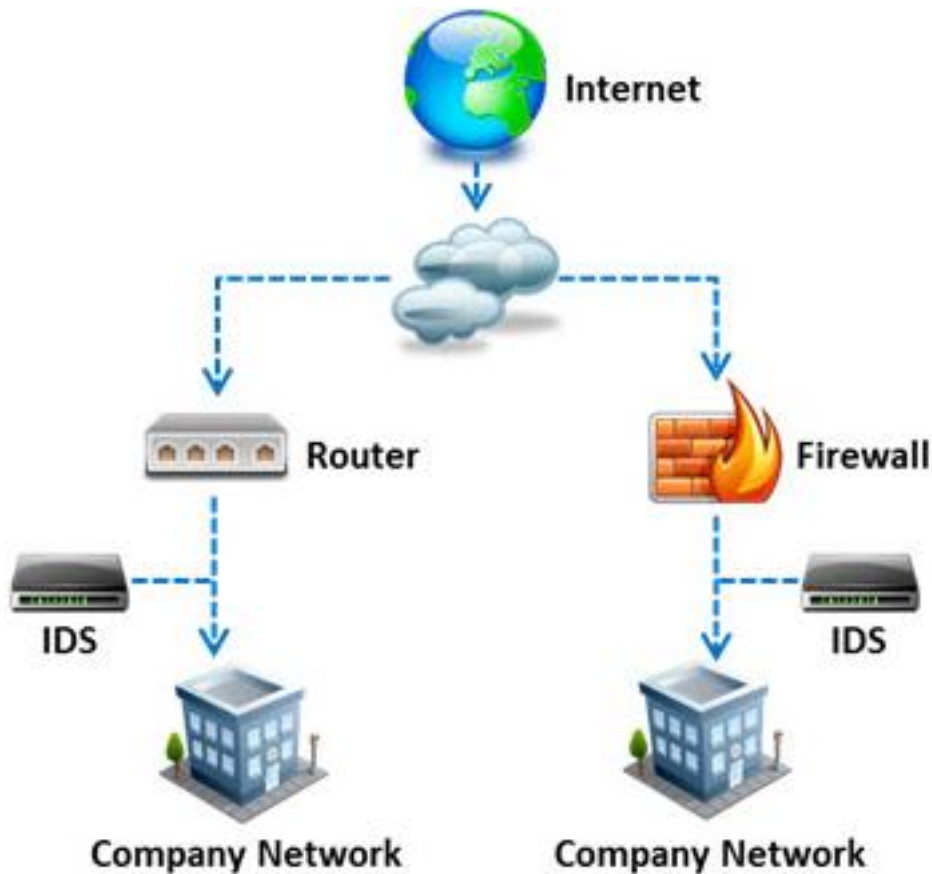
**Answer: D**

**Explanation:**

<https://books.google.nl/books?id=0RfANAwOUdIC&pg=PA720&lpg=PA720&dq=%22xx+notation%22+binary&source=bl&ots=pGMqass7ti&sig=rnlg1xZ78ScUvullTmDY3r7REuc&hl=nl&sa=X&ei=8C4dVYe1NorgasrzgoAL&ved=0CEQQ6AEwBQ#v=onepage&q=%22xx%20notation%22%20binary&f=false>

**Question No : 26**

What is a difference between host-based intrusion detection systems (HIDS) and network-based intrusion detection systems (NIDS)?



- A. NIDS are usually a more expensive solution to implement compared to HIDS.
- B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor and stop such intrusion events.
- C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.
- D. HIDS requires less administration and training compared to NIDS.

**Answer: C**

**Question No : 27**

A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product.” It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

- A. Orinoco chipsets
- B. Prism II chipsets
- C. Atheros Chipset

D. Cisco chipset

**Answer: B**

**Question No : 28**

The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. It is often used to raise the level of security awareness among employees.



The tester should demonstrate extreme care and professionalism during a social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.

Which of the following methods of attempting social engineering is associated with bribing, handing out gifts, and becoming involved in a personal relationship to befriend someone inside the company?

- A. Accomplice social engineering technique
- B. Identity theft
- C. Dumpster diving
- D. Phishing social engineering technique

**Answer: A**

**Question No : 29**

John, the penetration testing manager in a pen testing firm, needs to prepare a pen testing pricing report for a client.

Which of the following factors does he need to consider while preparing the pen testing pricing report?



- A. Number of employees in the client organization
- B. Complete structure of the organization
- C. Number of client computers to be tested and resources required to perform a pen test
- D. Number of servers available in the client organization

**Answer: C**

**Question No : 30**

Which of the following scan option is able to identify the SSL services?

- A. -sS
- B. -sV
- C. -sU
- D. -sT

**Answer: B**

Reference: [https://www.owasp.org/index.php/Testing\\_for\\_SSL-TLS\\_\(OWASP-CM-001\)](https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001))  
(blackboxtest and example, second para)

**Question No : 31**

Which of the following contents of a pen testing project plan addresses the strengths, weaknesses, opportunities, and threats involved in the project?

- A. Project Goal
- B. Success Factors
- C. Objectives
- D. Assumptions

Answer: D

**Question No : 32**

Identify the attack represented in the diagram below:



- A. Input Validation
- B. Session Hijacking
- C. SQL Injection
- D. Denial-of-Service

**Answer: B**

Reference:[http://en.wikipedia.org/wiki/Session\\_hijacking](http://en.wikipedia.org/wiki/Session_hijacking)

**Question No : 33**

If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

- A. Parameter tampering Attack
- B. Sql injection attack
- C. Session Hijacking
- D. Cross-site request attack

**Answer: D**

Reference:[https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

**Question No : 34**

DNS information records provide important data about:

- A. Phone and Fax Numbers
- B. Location and Type of Servers
- C. Agents Providing Service to Company Staff
- D. New Customer

**Answer: B**

**Question No : 35**

Which of the following has an offset field that specifies the length of the header and data?

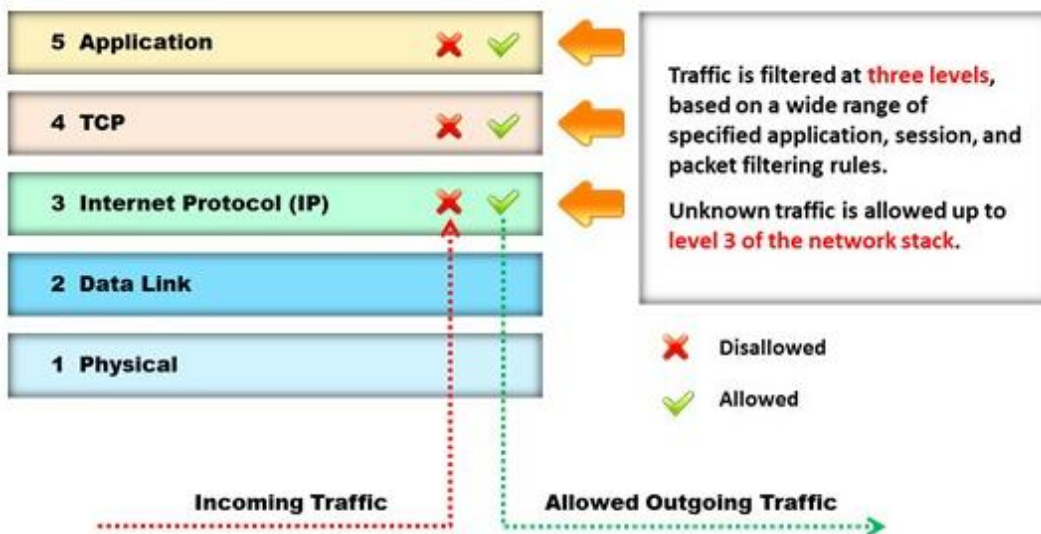
- A. IP Header
- B. UDP Header

- C. ICMP Header
- D. TCP Header

Answer: D

**Question No : 36**

Identify the type of firewall represented in the diagram below:



- A. Stateful multilayer inspection firewall
- B. Applicationlevel gateway
- C. Packet filter
- D. Circuit level gateway

Answer: A

Reference:<http://www.technicolorbroadbandpartner.com/getfile.php?id=4159>(page 13)

**Question No : 37**

The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.





Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

- A. Active Information Gathering
- B. Pseudonymous Information Gathering
- C. Anonymous InformationGathering
- D. Open Source or Passive Information Gathering

**Answer: A**

### Question No : 38

One of the steps in information gathering is to run searches on a company using complex keywords in Google.

terms appearing	anywhere in the page	Search for terms in the whole page, page title, or web address, links to the page you're looking for.
SafeSearch	Show most relevant results	Tell SafeSearch whether to filter sexually explicit content.
reading level	no reading level displayed	Find pages at one reading level or just view the level info.
file type	any format	Find pages in the format you prefer.
usage rights	not filtered by license	Find pages you are free to use yourself.

Advanced Search



Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?

- A. ROCHESTON fileformat:+ppt
- B. ROCHESTON ppt:filestring
- C. ROCHESTON filetype:ppt
- D. ROCHESTON +ppt:filesearch

**Answer: C**

Reference:<http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search-Google-Like-An-Expert.aspx>(specific document types)

**Question No : 39**

Wireless communication allows networks to extend to places that might otherwise go untouched by the wired networks. When most peoplesay 'Wireless' these days, they are referring to one of the 802.11 standards. There are three main 802.11 standards: B, A, and G. Which one of the following 802.11 types uses DSSS Modulation, splitting the 2.4ghz band into channels?

- A. 802.11b
- B. 802.11g
- C. 802.11-Legacy
- D. 802.11n

**Answer: A**

**Question No : 40**

What is the difference between penetration testingand vulnerability testing?



- A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of 'in-depth ethical hacking'
- B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities
- C. Vulnerability testing is more expensive than penetration testing
- D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

**Answer: A**

**Question No : 41**

This is a group of people hired to give details of the vulnerabilities present in the system found after a penetration test. They are elite and extremely competent penetration testers and intrusion analysts. This team prepares a report on the vulnerabilities in the system, attack methods, and how to defend against them.



What is this team called?

- A. Blue team
- B. Tiger team
- C. Gorilla team

D. Lion team

**Answer: B**

**Question No : 42**

Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

- A. Unannounced Testing
- B. Double Blind Testing
- C. Announced Testing
- D. Blind Testing

**Answer: B**

**Question No : 43**

Which of the following methods is used to perform server discovery?

- A. Banner Grabbing
- B. Whois Lookup
- C. SQL Injection
- D. SessionHijacking

**Answer: B**

Reference:<http://luizfirmino.blogspot.com/2011/09/server-discovery.html>

**Question No : 44**

Which among the following information is not furnished by the Rules of Engagement (ROE) document?

- A. Techniques for data collection from systems upon termination of the test
- B. Techniques for data exclusion from systems upon termination of the test

- C. Details on how data should be transmitted during and after the test
- D. Details on how organizational data is treated throughout and after the test

**Answer: A**

**Question No : 45**

Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

- A. Packet Sniffer Mode
- B. Packet Logger Mode
- C. Network Intrusion Detection System Mode
- D. Inline Mode

**Answer: A**

**Question No : 46**

During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

- A. TCP Sequence Number Prediction
- B. IPID State Number Prediction
- C. TCP State Number Prediction
- D. IPID Sequence Number Prediction

**Answer: A**

Reference:<http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction>(p.43)

**Question No : 47**

A firewall's decision to forward or reject traffic in network filtering is dependent upon which of the following?

- A. Destination address
- B. Port numbers
- C. Source address
- D. Protocol used

**Answer: D**

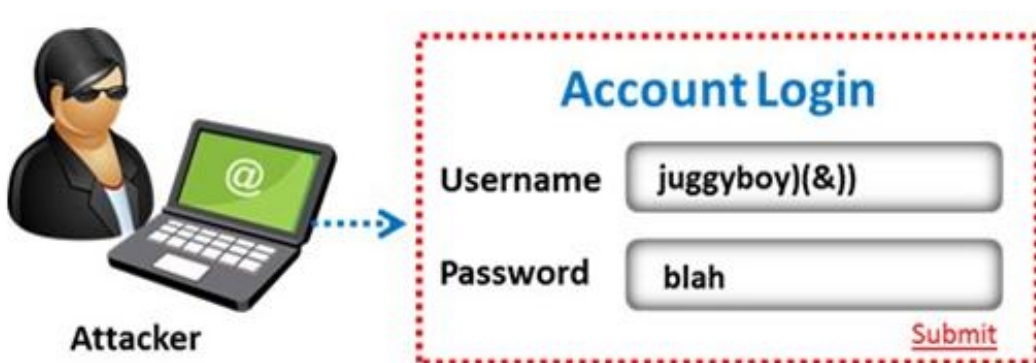
Reference:[http://www.vicomsoft.com/learning-center/firewalls/\(what does a firewall do\)](http://www.vicomsoft.com/learning-center/firewalls/(what%20does%20a%20firewall%20do))

**Question No : 48**

The amount of data stored in organizational databases has increased rapidly in recent years due to the rapid advancement of information technologies. A high percentage of these data is sensitive, private and critical to the organizations, their clients and partners.

Therefore, databases are usually installed behind internal firewalls, protected with intrusion detection mechanisms and accessed only by applications. To access a database, users have to connect to one of these applications and submit queries through them to the database. The threat to databases arises when these applications do not behave properly and construct these queries without sanitizing user inputs first.

Identify the injection attack represented in the diagram below:



- A. Frame Injection Attack
- B. LDAP Injection Attack
- C. XPath Injection Attack
- D. SOAP Injection Attack

**Answer: B**

Reference: <https://www.blackhat.com/presentations/bh-europe-08/Alonso-Parada/Whitepaper/bh-eu-08-alonso-parada-WP.pdf>( page 3 to 5)

**Question No : 49**

Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.



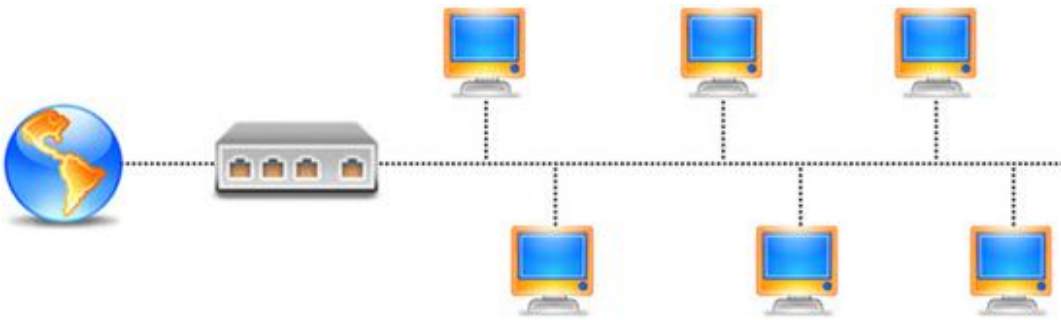
Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

- A. Web Penetration Testing
- B. Functionality Testing
- C. Authorization Testing
- D. Source Code Review

**Answer: D**

**Question No : 50**

Port numbers are used to keep track of different conversations crossing the network at the same time. Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers have the assigned ranges.



Port numbers above 1024 are considered which one of the following?

- A. Dynamically assigned port numbers
- B. Statically assigned port numbers
- C. Well-known port numbers
- D. Unregistered port numbers

**Answer: A**

Reference:[http://stackoverflow.com/questions/136709/what-port-number-should-i-use-when-testing-connections-in-my-local-intranet-in\(see post 4\)](http://stackoverflow.com/questions/136709/what-port-number-should-i-use-when-testing-connections-in-my-local-intranet-in(see post 4))

**Question No : 51**

The framework primarily designed to fulfill a methodical and organized way of addressing five threat classes to network and that can be used to access, plan, manage, and maintain secure computers and communication networks is:

- A. Nortells Unified Security Framework
- B. The IBM Security Framework
- C. Bell Labs Network Security Framework



D. Microsoft Internet Security Framework

**Answer: C**

**Question No : 52**

Identify the data security measure which defines a principle or state that ensures that an action or transaction cannot be denied.

- A. Availability
- B. Integrity
- C. Authorization
- D. Non-Repudiation

**Answer: D**

Reference:[http://en.wikipedia.org/wiki/Information\\_security\(non-repudiation\)](http://en.wikipedia.org/wiki/Information_security(non-repudiation))

**Question No : 53**

Before performing the penetration testing, there will be a pre-contract discussion with different pen-testers (the team of penetration testers) to gather a quotation to perform pen testing.





Which of the following factors is NOT considered while preparing a price quote to perform pen testing?

- A. Total number of employees in the client organization
- B. Type of testers involved
- C. The budget required
- D. Expected time required to finish the project

**Answer: A**

**Question No : 54**

What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?

- A. Connect Scanning Techniques
- B. SYN Scanning Techniques
- C. Stealth Scanning Techniques
- D. Port Scanning Techniques

**Answer: C**

Reference:[http://www.pc-freak.net/tutorials/hacking\\_info/arkin%20network%20scanning%20techniques.pdf](http://www.pc-freak.net/tutorials/hacking_info/arkin%20network%20scanning%20techniques.pdf)(page 7

**Question No : 55**

Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers. Which one of the following cannot handle routing protocols properly?

- A. "Internet-router-firewall-net architecture"
- B. "Internet-firewall-router-net architecture"
- C. "Internet-firewall/router(edge device)-net architecture"
- D. "Internet-firewall -net architecture"

**Answer: B**

**Question No : 56**

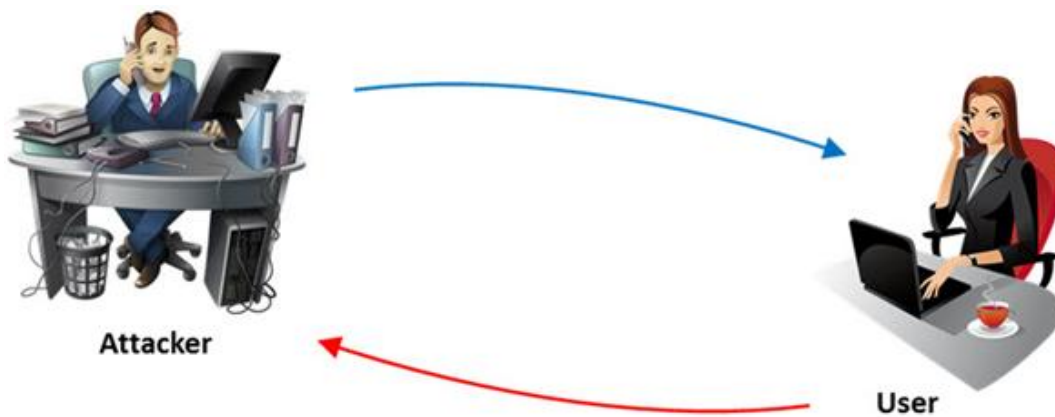
Which one of the following commands is used to search one or more files for a specific pattern and it helps in organizing the firewall log files?

- A. grpck
- B. grep
- C. gpgv
- D. gprn

**Answer: B**

**Question No : 57**

The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?

- A. Phishing
- B. Spoofing
- C. Tapping
- D. Vishing

**Answer: D**

**Question No : 58**

Which of the following acts related to information security in the US establish that the management of an organization is responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

- A. USA Patriot Act 2001
- B. Sarbanes-Oxley 2002
- C. Gramm-Leach-Bliley Act (GLBA)
- D. California SB 1386

**Answer: A**

Reference:<http://www.sec.gov/rules/final/33-8238.htm>(see background)

**Question No : 59**

## Dumps with PDF and VCE ( +Free VCE Software )

An attacker injects malicious query strings in user input fields to bypass web service authentication mechanisms and to access back-end databases. Which of the following attacks is this?

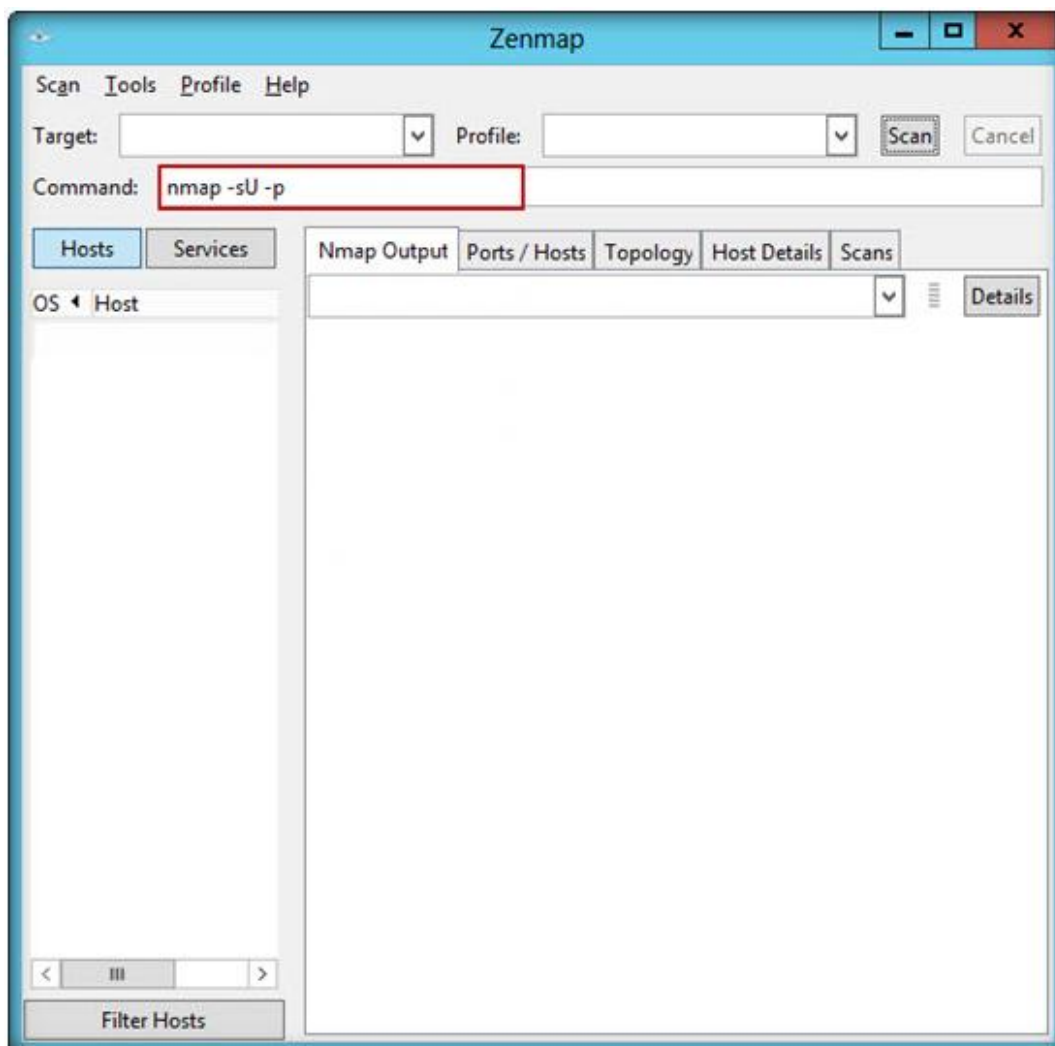
- A. Frame Injection Attack
- B. LDAP Injection Attack
- C. XPath Injection Attack
- D. SOAP Injection Attack

**Answer: D**

**Explanation:** [http://luizfirmino.blogspot.com/2011\\_09\\_01\\_archive.html](http://luizfirmino.blogspot.com/2011_09_01_archive.html)

### Question No : 60

John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.



Which one of the following Nmap commands will he use to findit?

- A. nmap -sU -p 389 10.0.0.7
- B. nmap -sU -p 123 10.0.0.7
- C. nmap -sU -p 161 10.0.0.7
- D. nmap -sU -p 135 10.0.0.7

**Answer: B**

**Question No : 61**

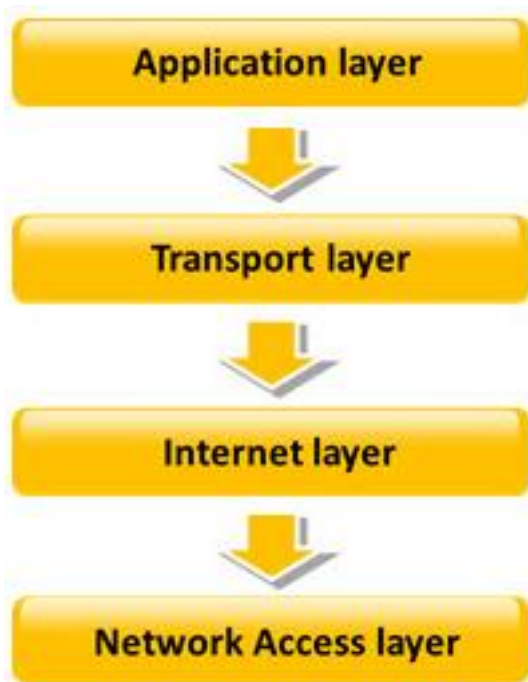
Which one of the following acts related to the information security in the US fix the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting?

- A. California SB 1386
- B. Sarbanes-Oxley 2002
- C. Gramm-Leach-Bliley Act (GLBA)
- D. USA Patriot Act 2001

**Answer: B**

**Question No : 62**

TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.



Which of the following TCP/IP layers selects the best path through the network for packets to travel?

- A. Transport layer
- B. Network Access layer
- C. Internet layer
- D. Application layer

**Answer: C**

**Question No : 63**

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.

### Microsoft Exams List

<a href="#">70-246 Dump PDF VCE</a>	<a href="#">70-485 Dump PDF VCE</a>	<a href="#">70-742 Dump PDF VCE</a>	<a href="#">98-366 Dump PDF VCE</a>
<a href="#">70-247 Dump PDF VCE</a>	<a href="#">70-486 Dump PDF VCE</a>	<a href="#">70-743 Dump PDF VCE</a>	<a href="#">98-367 Dump PDF VCE</a>
<a href="#">70-331 Dump PDF VCE</a>	<a href="#">70-487 Dump PDF VCE</a>	<a href="#">70-744 Dump PDF VCE</a>	<a href="#">98-368 Dump PDF VCE</a>
<a href="#">70-332 Dump PDF VCE</a>	<a href="#">70-488 Dump PDF VCE</a>	<a href="#">70-761 Dump PDF VCE</a>	<a href="#">98-369 Dump PDF VCE</a>
<a href="#">70-333 Dump PDF VCE</a>	<a href="#">70-489 Dump PDF VCE</a>	<a href="#">70-762 Dump PDF VCE</a>	<a href="#">98-372 Dump PDF VCE</a>
<a href="#">70-334 Dump PDF VCE</a>	<a href="#">70-490 Dump PDF VCE</a>	<a href="#">70-765 Dump PDF VCE</a>	<a href="#">98-373 Dump PDF VCE</a>
<a href="#">70-339 Dump PDF VCE</a>	<a href="#">70-491 Dump PDF VCE</a>	<a href="#">70-768 Dump PDF VCE</a>	<a href="#">98-374 Dump PDF VCE</a>
<a href="#">70-341 Dump PDF VCE</a>	<a href="#">70-492 Dump PDF VCE</a>	<a href="#">70-980 Dump PDF VCE</a>	<a href="#">98-375 Dump PDF VCE</a>
<a href="#">70-342 Dump PDF VCE</a>	<a href="#">70-494 Dump PDF VCE</a>	<a href="#">70-981 Dump PDF VCE</a>	<a href="#">98-379 Dump PDF VCE</a>
<a href="#">70-345 Dump PDF VCE</a>	<a href="#">70-496 Dump PDF VCE</a>	<a href="#">70-982 Dump PDF VCE</a>	<a href="#">MB2-700 Dump PDF VCE</a>
<a href="#">70-346 Dump PDF VCE</a>	<a href="#">70-497 Dump PDF VCE</a>	<a href="#">74-343 Dump PDF VCE</a>	<a href="#">MB2-701 Dump PDF VCE</a>
<a href="#">70-347 Dump PDF VCE</a>	<a href="#">70-498 Dump PDF VCE</a>	<a href="#">74-344 Dump PDF VCE</a>	<a href="#">MB2-702 Dump PDF VCE</a>
<a href="#">70-348 Dump PDF VCE</a>	<a href="#">70-499 Dump PDF VCE</a>	<a href="#">74-409 Dump PDF VCE</a>	<a href="#">MB2-703 Dump PDF VCE</a>
<a href="#">70-354 Dump PDF VCE</a>	<a href="#">70-517 Dump PDF VCE</a>	<a href="#">74-678 Dump PDF VCE</a>	<a href="#">MB2-704 Dump PDF VCE</a>
<a href="#">70-383 Dump PDF VCE</a>	<a href="#">70-532 Dump PDF VCE</a>	<a href="#">74-697 Dump PDF VCE</a>	<a href="#">MB2-707 Dump PDF VCE</a>
<a href="#">70-384 Dump PDF VCE</a>	<a href="#">70-533 Dump PDF VCE</a>	<a href="#">77-420 Dump PDF VCE</a>	<a href="#">MB2-710 Dump PDF VCE</a>
<a href="#">70-385 Dump PDF VCE</a>	<a href="#">70-534 Dump PDF VCE</a>	<a href="#">77-427 Dump PDF VCE</a>	<a href="#">MB2-711 Dump PDF VCE</a>
<a href="#">70-410 Dump PDF VCE</a>	<a href="#">70-640 Dump PDF VCE</a>	<a href="#">77-600 Dump PDF VCE</a>	<a href="#">MB2-712 Dump PDF VCE</a>
<a href="#">70-411 Dump PDF VCE</a>	<a href="#">70-642 Dump PDF VCE</a>	<a href="#">77-601 Dump PDF VCE</a>	<a href="#">MB2-713 Dump PDF VCE</a>
<a href="#">70-412 Dump PDF VCE</a>	<a href="#">70-646 Dump PDF VCE</a>	<a href="#">77-602 Dump PDF VCE</a>	<a href="#">MB2-714 Dump PDF VCE</a>
<a href="#">70-413 Dump PDF VCE</a>	<a href="#">70-673 Dump PDF VCE</a>	<a href="#">77-603 Dump PDF VCE</a>	<a href="#">MB2-715 Dump PDF VCE</a>
<a href="#">70-414 Dump PDF VCE</a>	<a href="#">70-680 Dump PDF VCE</a>	<a href="#">77-604 Dump PDF VCE</a>	<a href="#">MB2-716 Dump PDF VCE</a>
<a href="#">70-417 Dump PDF VCE</a>	<a href="#">70-681 Dump PDF VCE</a>	<a href="#">77-605 Dump PDF VCE</a>	<a href="#">MB2-717 Dump PDF VCE</a>
<a href="#">70-461 Dump PDF VCE</a>	<a href="#">70-682 Dump PDF VCE</a>	<a href="#">77-881 Dump PDF VCE</a>	<a href="#">MB2-718 Dump PDF VCE</a>
<a href="#">70-462 Dump PDF VCE</a>	<a href="#">70-684 Dump PDF VCE</a>	<a href="#">77-882 Dump PDF VCE</a>	<a href="#">MB5-705 Dump PDF VCE</a>
<a href="#">70-463 Dump PDF VCE</a>	<a href="#">70-685 Dump PDF VCE</a>	<a href="#">77-883 Dump PDF VCE</a>	<a href="#">MB6-700 Dump PDF VCE</a>
<a href="#">70-464 Dump PDF VCE</a>	<a href="#">70-686 Dump PDF VCE</a>	<a href="#">77-884 Dump PDF VCE</a>	<a href="#">MB6-701 Dump PDF VCE</a>
<a href="#">70-465 Dump PDF VCE</a>	<a href="#">70-687 Dump PDF VCE</a>	<a href="#">77-885 Dump PDF VCE</a>	<a href="#">MB6-702 Dump PDF VCE</a>
<a href="#">70-466 Dump PDF VCE</a>	<a href="#">70-688 Dump PDF VCE</a>	<a href="#">77-886 Dump PDF VCE</a>	<a href="#">MB6-703 Dump PDF VCE</a>
<a href="#">70-467 Dump PDF VCE</a>	<a href="#">70-689 Dump PDF VCE</a>	<a href="#">77-887 Dump PDF VCE</a>	<a href="#">MB6-704 Dump PDF VCE</a>
<a href="#">70-469 Dump PDF VCE</a>	<a href="#">70-692 Dump PDF VCE</a>	<a href="#">77-888 Dump PDF VCE</a>	<a href="#">MB6-705 Dump PDF VCE</a>
<a href="#">70-470 Dump PDF VCE</a>	<a href="#">70-695 Dump PDF VCE</a>	<a href="#">77-891 Dump PDF VCE</a>	<a href="#">MB6-884 Dump PDF VCE</a>
<a href="#">70-473 Dump PDF VCE</a>	<a href="#">70-696 Dump PDF VCE</a>	<a href="#">98-349 Dump PDF VCE</a>	<a href="#">MB6-885 Dump PDF VCE</a>
<a href="#">70-480 Dump PDF VCE</a>	<a href="#">70-697 Dump PDF VCE</a>	<a href="#">98-361 Dump PDF VCE</a>	<a href="#">MB6-886 Dump PDF VCE</a>
<a href="#">70-481 Dump PDF VCE</a>	<a href="#">70-698 Dump PDF VCE</a>	<a href="#">98-362 Dump PDF VCE</a>	<a href="#">MB6-889 Dump PDF VCE</a>
<a href="#">70-482 Dump PDF VCE</a>	<a href="#">70-734 Dump PDF VCE</a>	<a href="#">98-363 Dump PDF VCE</a>	<a href="#">MB6-890 Dump PDF VCE</a>
<a href="#">70-483 Dump PDF VCE</a>	<a href="#">70-740 Dump PDF VCE</a>	<a href="#">98-364 Dump PDF VCE</a>	<a href="#">MB6-892 Dump PDF VCE</a>
<a href="#">70-484 Dump PDF VCE</a>	<a href="#">70-741 Dump PDF VCE</a>	<a href="#">98-365 Dump PDF VCE</a>	<a href="#">MB6-893 Dump PDF VCE</a>

### Cisco Exams List

<a href="#">010-151 Dump PDF VCE</a>	<a href="#">350-018 Dump PDF VCE</a>	<a href="#">642-737 Dump PDF VCE</a>	<a href="#">650-667 Dump PDF VCE</a>
<a href="#">100-105 Dump PDF VCE</a>	<a href="#">352-001 Dump PDF VCE</a>	<a href="#">642-742 Dump PDF VCE</a>	<a href="#">650-669 Dump PDF VCE</a>
<a href="#">200-001 Dump PDF VCE</a>	<a href="#">400-051 Dump PDF VCE</a>	<a href="#">642-883 Dump PDF VCE</a>	<a href="#">650-752 Dump PDF VCE</a>
<a href="#">200-105 Dump PDF VCE</a>	<a href="#">400-101 Dump PDF VCE</a>	<a href="#">642-885 Dump PDF VCE</a>	<a href="#">650-756 Dump PDF VCE</a>
<a href="#">200-120 Dump PDF VCE</a>	<a href="#">400-151 Dump PDF VCE</a>	<a href="#">642-887 Dump PDF VCE</a>	<a href="#">650-968 Dump PDF VCE</a>
<a href="#">200-125 Dump PDF VCE</a>	<a href="#">400-201 Dump PDF VCE</a>	<a href="#">642-889 Dump PDF VCE</a>	<a href="#">700-001 Dump PDF VCE</a>
<a href="#">200-150 Dump PDF VCE</a>	<a href="#">400-251 Dump PDF VCE</a>	<a href="#">642-980 Dump PDF VCE</a>	<a href="#">700-037 Dump PDF VCE</a>
<a href="#">200-155 Dump PDF VCE</a>	<a href="#">400-351 Dump PDF VCE</a>	<a href="#">642-996 Dump PDF VCE</a>	<a href="#">700-038 Dump PDF VCE</a>
<a href="#">200-310 Dump PDF VCE</a>	<a href="#">500-006 Dump PDF VCE</a>	<a href="#">642-997 Dump PDF VCE</a>	<a href="#">700-039 Dump PDF VCE</a>
<a href="#">200-355 Dump PDF VCE</a>	<a href="#">500-007 Dump PDF VCE</a>	<a href="#">642-998 Dump PDF VCE</a>	<a href="#">700-101 Dump PDF VCE</a>
<a href="#">200-401 Dump PDF VCE</a>	<a href="#">500-051 Dump PDF VCE</a>	<a href="#">642-999 Dump PDF VCE</a>	<a href="#">700-104 Dump PDF VCE</a>
<a href="#">200-601 Dump PDF VCE</a>	<a href="#">500-052 Dump PDF VCE</a>	<a href="#">644-066 Dump PDF VCE</a>	<a href="#">700-201 Dump PDF VCE</a>
<a href="#">210-060 Dump PDF VCE</a>	<a href="#">500-170 Dump PDF VCE</a>	<a href="#">644-068 Dump PDF VCE</a>	<a href="#">700-205 Dump PDF VCE</a>
<a href="#">210-065 Dump PDF VCE</a>	<a href="#">500-201 Dump PDF VCE</a>	<a href="#">644-906 Dump PDF VCE</a>	<a href="#">700-260 Dump PDF VCE</a>
<a href="#">210-250 Dump PDF VCE</a>	<a href="#">500-202 Dump PDF VCE</a>	<a href="#">646-048 Dump PDF VCE</a>	<a href="#">700-270 Dump PDF VCE</a>
<a href="#">210-255 Dump PDF VCE</a>	<a href="#">500-254 Dump PDF VCE</a>	<a href="#">646-365 Dump PDF VCE</a>	<a href="#">700-280 Dump PDF VCE</a>
<a href="#">210-260 Dump PDF VCE</a>	<a href="#">500-258 Dump PDF VCE</a>	<a href="#">646-580 Dump PDF VCE</a>	<a href="#">700-281 Dump PDF VCE</a>
<a href="#">210-451 Dump PDF VCE</a>	<a href="#">500-260 Dump PDF VCE</a>	<a href="#">646-671 Dump PDF VCE</a>	<a href="#">700-295 Dump PDF VCE</a>
<a href="#">210-455 Dump PDF VCE</a>	<a href="#">500-265 Dump PDF VCE</a>	<a href="#">646-985 Dump PDF VCE</a>	<a href="#">700-501 Dump PDF VCE</a>
<a href="#">300-070 Dump PDF VCE</a>	<a href="#">500-275 Dump PDF VCE</a>	<a href="#">648-232 Dump PDF VCE</a>	<a href="#">700-505 Dump PDF VCE</a>
<a href="#">300-075 Dump PDF VCE</a>	<a href="#">500-280 Dump PDF VCE</a>	<a href="#">648-238 Dump PDF VCE</a>	<a href="#">700-601 Dump PDF VCE</a>
<a href="#">300-080 Dump PDF VCE</a>	<a href="#">500-285 Dump PDF VCE</a>	<a href="#">648-244 Dump PDF VCE</a>	<a href="#">700-602 Dump PDF VCE</a>
<a href="#">300-085 Dump PDF VCE</a>	<a href="#">500-290 Dump PDF VCE</a>	<a href="#">648-247 Dump PDF VCE</a>	<a href="#">700-603 Dump PDF VCE</a>
<a href="#">300-101 Dump PDF VCE</a>	<a href="#">500-801 Dump PDF VCE</a>	<a href="#">648-375 Dump PDF VCE</a>	<a href="#">700-701 Dump PDF VCE</a>
<a href="#">300-115 Dump PDF VCE</a>	<a href="#">600-199 Dump PDF VCE</a>	<a href="#">648-385 Dump PDF VCE</a>	<a href="#">700-702 Dump PDF VCE</a>
<a href="#">300-135 Dump PDF VCE</a>	<a href="#">600-210 Dump PDF VCE</a>	<a href="#">650-032 Dump PDF VCE</a>	<a href="#">700-703 Dump PDF VCE</a>
<a href="#">300-160 Dump PDF VCE</a>	<a href="#">600-211 Dump PDF VCE</a>	<a href="#">650-042 Dump PDF VCE</a>	<a href="#">700-801 Dump PDF VCE</a>
<a href="#">300-165 Dump PDF VCE</a>	<a href="#">600-212 Dump PDF VCE</a>	<a href="#">650-059 Dump PDF VCE</a>	<a href="#">700-802 Dump PDF VCE</a>
<a href="#">300-180 Dump PDF VCE</a>	<a href="#">600-455 Dump PDF VCE</a>	<a href="#">650-082 Dump PDF VCE</a>	<a href="#">700-803 Dump PDF VCE</a>
<a href="#">300-206 Dump PDF VCE</a>	<a href="#">600-460 Dump PDF VCE</a>	<a href="#">650-127 Dump PDF VCE</a>	<a href="#">810-403 Dump PDF VCE</a>
<a href="#">300-207 Dump PDF VCE</a>	<a href="#">600-501 Dump PDF VCE</a>	<a href="#">650-128 Dump PDF VCE</a>	<a href="#">820-424 Dump PDF VCE</a>
<a href="#">300-208 Dump PDF VCE</a>	<a href="#">600-502 Dump PDF VCE</a>	<a href="#">650-148 Dump PDF VCE</a>	<a href="#">840-425 Dump PDF VCE</a>
<a href="#">300-209 Dump PDF VCE</a>	<a href="#">600-503 Dump PDF VCE</a>	<a href="#">650-159 Dump PDF VCE</a>	
<a href="#">300-210 Dump PDF VCE</a>	<a href="#">600-504 Dump PDF VCE</a>	<a href="#">650-281 Dump PDF VCE</a>	
<a href="#">300-320 Dump PDF VCE</a>	<a href="#">640-692 Dump PDF VCE</a>	<a href="#">650-393 Dump PDF VCE</a>	
<a href="#">300-360 Dump PDF VCE</a>	<a href="#">640-875 Dump PDF VCE</a>	<a href="#">650-472 Dump PDF VCE</a>	
<a href="#">300-365 Dump PDF VCE</a>	<a href="#">640-878 Dump PDF VCE</a>	<a href="#">650-474 Dump PDF VCE</a>	
<a href="#">300-370 Dump PDF VCE</a>	<a href="#">640-911 Dump PDF VCE</a>	<a href="#">650-575 Dump PDF VCE</a>	
<a href="#">300-375 Dump PDF VCE</a>	<a href="#">640-916 Dump PDF VCE</a>	<a href="#">650-621 Dump PDF VCE</a>	
<a href="#">300-465 Dump PDF VCE</a>	<a href="#">642-035 Dump PDF VCE</a>	<a href="#">650-663 Dump PDF VCE</a>	
<a href="#">300-470 Dump PDF VCE</a>	<a href="#">642-732 Dump PDF VCE</a>	<a href="#">650-665 Dump PDF VCE</a>	
<a href="#">300-475 Dump PDF VCE</a>	<a href="#">642-747 Dump PDF VCE</a>	<a href="#">650-754 Dump PDF VCE</a>	



## HOT EXAMS

### Cisco

[100-105 Dumps VCE PDF](#)  
[200-105 Dumps VCE PDF](#)  
[300-101 Dumps VCE PDF](#)  
[300-115 Dumps VCE PDF](#)  
[300-135 Dumps VCE PDF](#)  
[300-320 Dumps VCE PDF](#)  
[400-101 Dumps VCE PDF](#)  
[640-911 Dumps VCE PDF](#)  
[640-916 Dumps VCE PDF](#)

### Microsoft

[70-410 Dumps VCE PDF](#)  
[70-411 Dumps VCE PDF](#)  
[70-412 Dumps VCE PDF](#)  
[70-413 Dumps VCE PDF](#)  
[70-414 Dumps VCE PDF](#)  
[70-417 Dumps VCE PDF](#)  
[70-461 Dumps VCE PDF](#)  
[70-462 Dumps VCE PDF](#)  
[70-463 Dumps VCE PDF](#)  
[70-464 Dumps VCE PDF](#)  
[70-465 Dumps VCE PDF](#)  
[70-480 Dumps VCE PDF](#)  
[70-483 Dumps VCE PDF](#)  
[70-486 Dumps VCE PDF](#)  
[70-487 Dumps VCE PDF](#)

### CompTIA

[220-901 Dumps VCE PDF](#)  
[220-902 Dumps VCE PDF](#)  
[N10-006 Dumps VCE PDF](#)  
[SY0-401 Dumps VCE PDF](#)