# 312-50V8$^{Q\&As}$

Certified Ethical Hacker v8

## Pass EC-COUNCIL 312-50V8 Exam with 100% Guarantee

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

**https://www.geekcert.com/312-50v8.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

**QUESTION 1**

Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen.

What are you most likely to infer from this?

A. The services are protected by TCP wrappers

B. There is a honeypot running on the scanned machine

C. An attacker has replaced the services with trojaned ones

D. This indicates that the telnet and SMTP server have crashed

Correct Answer: A

**QUESTION 2**

Here is the ASCII Sheet.

| DEC | OCT | HEX | BIN | Symbol | HTML Number | HTML Name | Description |
|---|---|---|---|---|---|---|---|
| 32 | 40 | 20 | 100000 | |   | | Space |
| 33 | 41 | 21 | 100001 | ! | ! | | Exclamation mark |
| 34 | 42 | 22 | 100010 | " | " | " | Double quotes (or speech marks) |
| 35 | 43 | 23 | 100011 | # | # | | Number |
| 36 | 44 | 24 | 100100 | $ | $ | | Dollar |
| 37 | 45 | 25 | 100101 | % | % | | Procenttecken |
| 38 | 46 | 26 | 100110 | & | & | & | Ampersand |
| 39 | 47 | 27 | 100111 | ' | ' | | Single quote |
| 40 | 50 | 28 | 101000 | ( | ( | | Open parenthesis (or open bracket) |
| 41 | 51 | 29 | 101001 | ) | ) | | Close parenthesis (or close bracket) |
| 42 | 52 | 2A | 101010 | * | * | | Asterisk |
| 43 | 53 | 2B | 101011 | + | + | | Plus |
| 44 | 54 | 2C | 101100 | , | , | | Comma |
| 45 | 55 | 2D | 101101 | - | - | | Hyphen |
| 46 | 56 | 2E | 101110 | . | . | | Period, dot or full stop |
| 47 | 57 | 2F | 101111 | / | / | | Slash or divide |
| 48 | 60 | 30 | 110000 | 0 | 0 | | Zero |
| 49 | 61 | 31 | 110001 | 1 | 1 | | One |
| 50 | 62 | 32 | 110010 | 2 | 2 | | Two |
| 51 | 63 | 33 | 110011 | 3 | 3 | | Three |
| 52 | 64 | 34 | 110100 | 4 | 4 | | Four |
| 53 | 65 | 35 | 110101 | 5 | 5 | | Five |
| 54 | 66 | 36 | 110110 | 6 | 6 | | Six |
| 55 | 67 | 37 | 110111 | 7 | 7 | | Seven |
| 56 | 70 | 38 | 111000 | 8 | 8 | | Eight |
| 57 | 71 | 39 | 111001 | 9 | 9 | | Nine |
| 58 | 72 | 3A | 111010 | : | : | | Colon |
| 59 | 73 | 3B | 111011 | ; | ; | | Semicolon |
| 60 | 74 | 3C | 111100 | < | < | < | Less than (or open angled bracket) |
| 61 | 75 | 3D | 111101 | = | = | | Equals |
| 62 | 76 | 3E | 111110 | > | > | > | Greater than (or close angled bracket) |
| 63 | 77 | 3F | 111111 | ? | ? | | Question mark |
| 64 | 100 | 40 | 1000000 | @ | @ | | At symbol |
| 65 | 101 | 41 | 1000001 | A | A | | Uppercase A |
| 66 | 102 | 42 | 1000010 | B | B | | Uppercase B |
| 67 | 103 | 43 | 1000011 | C | C | | Uppercase C |
| 68 | 104 | 44 | 1000100 | D | D | | Uppercase D |
| 69 | 105 | 45 | 1000101 | E | E | | Uppercase E |
| 70 | 106 | 46 | 1000110 | F | F | | Uppercase F |
| 71 | 107 | 47 | 1000111 | G | G | | Uppercase G |
| 72 | 110 | 48 | 1001000 | H | H | | Uppercase H |
| 73 | 111 | 49 | 1001001 | I | I | | Uppercase I |
| 74 | 112 | 4A | 1001010 | J | J | | Uppercase J |
| 75 | 113 | 4B | 1001011 | K | K | | Uppercase K |
| 76 | 114 | 4C | 1001100 | L | L | | Uppercase L |
| 77 | 115 | 4D | 1001101 | M | M | | Uppercase M |
| 78 | 116 | 4E | 1001110 | N | N | | Uppercase N |
| 79 | 117 | 4F | 1001111 | O | O | | Uppercase O |
| 80 | 120 | 50 | 1010000 | P | P | | Uppercase P |
| 81 | 121 | 51 | 1010001 | Q | Q | | Uppercase Q |
| 82 | 122 | 52 | 1010010 | R | R | | Uppercase R |
| 83 | 123 | 53 | 1010011 | S | S | | Uppercase S |
| 84 | 124 | 54 | 1010100 | T | T | | Uppercase T |
| 85 | 125 | 55 | 1010101 | U | U | | Uppercase U |
| 86 | 126 | 56 | 1010110 | V | V | | Uppercase V |
| 87 | 127 | 57 | 1010111 | W | W | | Uppercase W |
| 88 | 130 | 58 | 1011000 | X | X | | Uppercase X |
| 89 | 131 | 59 | 1011001 | Y | Y | | Uppercase Y |
| 90 | 132 | 5A | 1011010 | Z | Z | | Uppercase Z |
| 91 | 133 | 5B | 1011011 | [ | [ | | Opening bracket |
| 92 | 134 | 5C | 1011100 | \ | \ | | Backslash |
| 93 | 135 | 5D | 1011101 | ] | ] | | Closing bracket |
| 94 | 136 | 5E | 1011110 | ^ | ^ | | Caret - circumflex |
| 95 | 137 | 5F | 1011111 | _ | _ | | Underscore |
| 96 | 140 | 60 | 1100000 | ` | ` | | Grave accent |
| 97 | 141 | 61 | 1100001 | a | a | | Lowercase a |
| 98 | 142 | 62 | 1100010 | b | b | | Lowercase b |
| 99 | 143 | 63 | 1100011 | c | c | | Lowercase c |
| 100 | 144 | 64 | 1100100 | d | d | | Lowercase d |
| 101 | 145 | 65 | 1100101 | e | e | | Lowercase e |
| 102 | 146 | 66 | 1100110 | f | f | | Lowercase f |
| 103 | 147 | 67 | 1100111 | g | g | | Lowercase g |
| 104 | 150 | 68 | 1101000 | h | h | | Lowercase h |
| 105 | 151 | 69 | 1101001 | i | i | | Lowercase i |
| 106 | 152 | 6A | 1101010 | j | j | | Lowercase j |
| 107 | 153 | 6B | 1101011 | k | k | | Lowercase k |
| 108 | 154 | 6C | 1101100 | l | l | | Lowercase l |
| 109 | 155 | 6D | 1101101 | m | m | | Lowercase m |
| 110 | 156 | 6E | 1101110 | n | n | | Lowercase n |
| 111 | 157 | 0F | 1101111 | o | o | | Lowercase o |
| 112 | 160 | 70 | 1110000 | p | p | | Lowercase p |
| 113 | 161 | 71 | 1110001 | q | q | | Lowercase q |
| 114 | 162 | 72 | 1110010 | r | r | | Lowercase r |

You want to guess the DBO username juggyboy (8 characters) using Blind SQL Injection technique. What is the correct syntax?

A. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 106) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 117) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=103) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=98) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=121) WAITFOR DELAY '00:00:10'--

B. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 134,156,111,136,186,145,144,188) WAITFOR DELAY '00:00:10'

C. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 144) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= 123) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=156) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=187) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=199) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=133) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=111) WAITFOR DELAY '00:00:10'

http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))=122) WAITFOR DELAY '00:00:10'--

D. http://www.jspringfield.com/page.aspx?id=1; IF (ASCII(lower(substring((USER),1,1)))= j,u,g,g,y,b,o,y) WAITFOR DELAY '00:00:10'

A. Option A

B. Option B

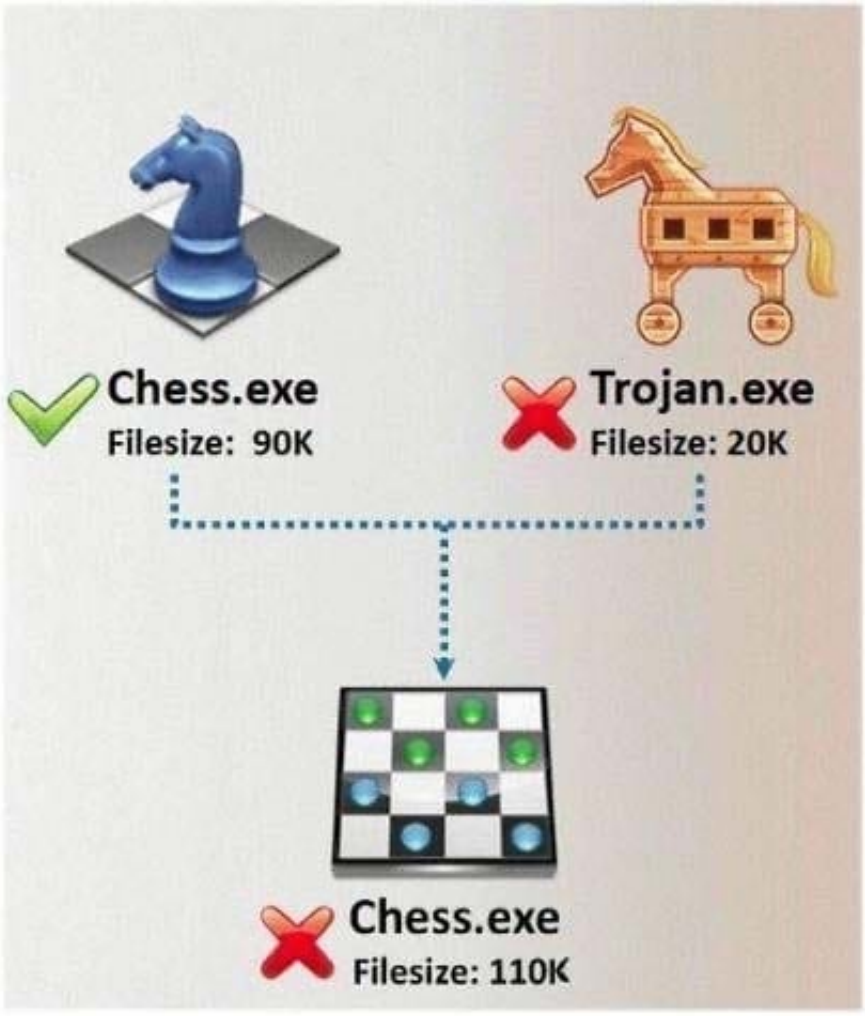
C. Option C

D. Option D

Correct Answer: A

**QUESTION 3**

In Trojan terminology, what is required to create the executable file chess.exe as shown below?




A. Mixer

B. Converter

C. Wrapper

D. Zipper

Correct Answer: C

**QUESTION 4**

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

Correct Answer: A

**QUESTION 5**

Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA

B. When a secondary SOA is higher that a primary SOA

C. When a primary name server has had its service restarted

D. When a secondary name server has had its service restarted

E. When the TTL falls to zero

Correct Answer: A