



# 312-50V8<sup>Q&As</sup>

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target.

Which of the following could be the most likely cause behind this lack of response? Select 4.

- A. UDP is filtered by a gateway
- B. The packet TTL value is too low and cannot reach the target
- C. The host might be down
- D. The destination network might be down
- E. The TCP windows size does not match
- F. ICMP is filtered by a gateway

Correct Answer: ABCF

### QUESTION 2

What type of port scan is shown below?

```
Scan directed at open port:
```

```
Client Server
192.5.2.92:4079 ----FIN/URG/PSH---->192.5.2.110:23
192.5.2.92:4079 <---NO RESPONSE-----192.5.2.110:23
```

```
Scan directed at closed port:
```

```
Client Server
192.5.2.92:4079 ----FIN/URG/PSH---->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK-----192.5.2.110:23
```

- A. Idle Scan
- B. Windows Scan
- C. XMAS Scan
- D. SYN Stealth Scan

Correct Answer: C



### QUESTION 3

Here is the ASCII Sheet.



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



A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.

Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy
- C. Remote-access policy
- D. Permissive policy

Correct Answer: C

---

#### QUESTION 5

To see how some of the hosts on your network react, Winston sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established he sends RST packets to those hosts to stop the session. Winston has done this to see how his intrusion detection system will log the traffic.

What type of scan is Winston attempting here?

- A. Winston is attempting to find live hosts on your company's network by using an XMAS scan.
- B. He is utilizing a SYN scan to find live hosts that are listening on your network.
- C. This type of scan he is using is called a NULL scan.
- D. He is using a half-open scan to find live hosts on your network.

Correct Answer: D

[312-50V8 VCE Dumps](#)

[312-50V8 Study Guide](#)

[312-50V8 Brindumps](#)