Vendor:GAQM

Exam Code:CEH-001

Exam Name: Certified Ethical Hacker (CEH)

Version: Demo

QUESTION 1

How can rainbow tables be defeated?

A. Password salting

B. Use of non-dictionary words

C. All uppercase character passwords

D. Lockout accounts under brute force password cracking attempts

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	%	%		Procent (zeichen)
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	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'

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 3

Which of the following statements would NOT be a proper definition for a Trojan Horse?

A. An authorized program that has been designed to capture keyboard keystroke while the user is unaware of such activity being performed

B. An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown (and probably unwanted) by the user

C. A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown (and probably unwanted) by the user

D. Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown (and definitely unwanted) by the user

Correct Answer: A

QUESTION 4

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

A. Host

B. Stateful

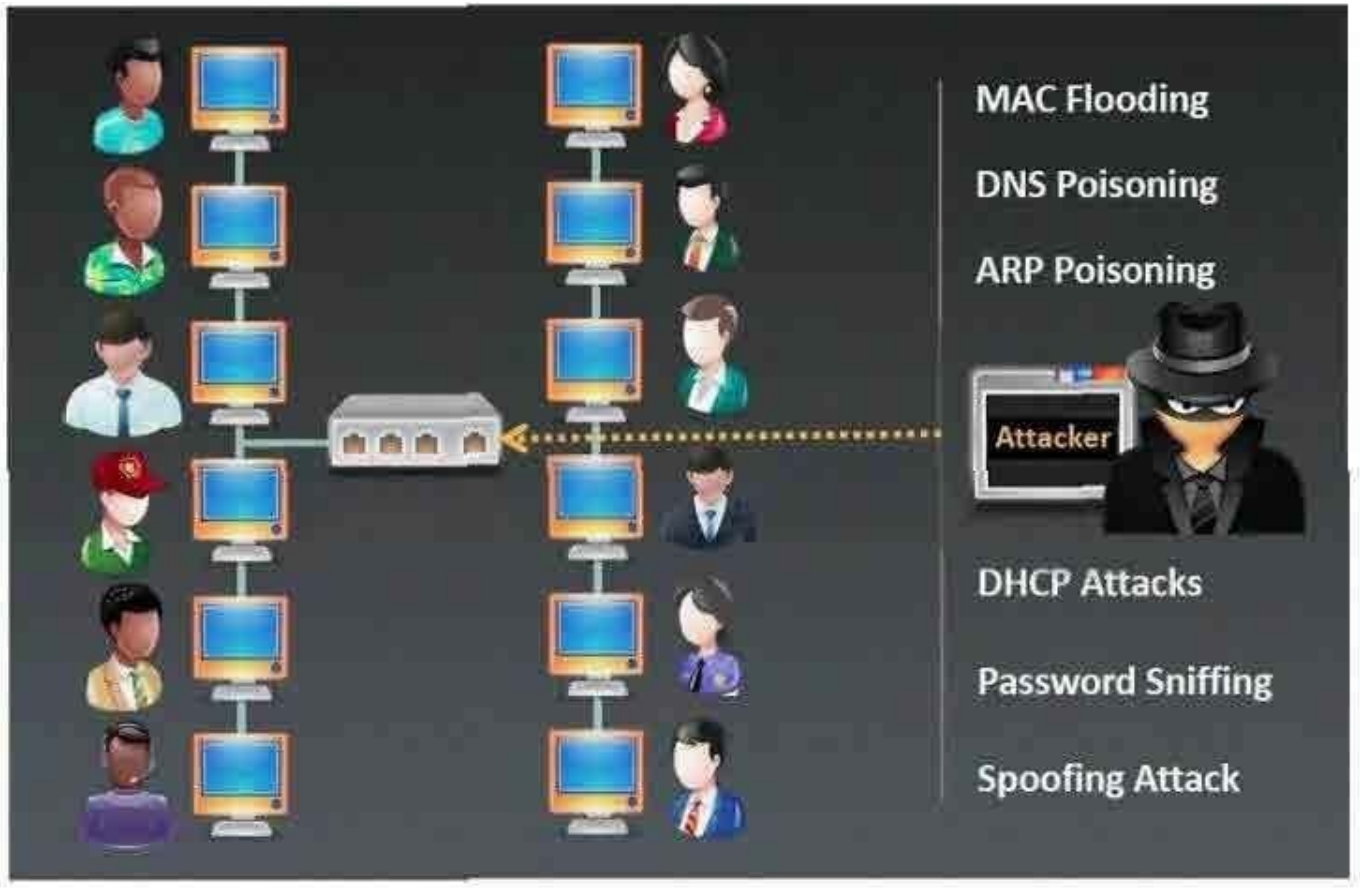
C. Stateless

D. Application

Correct Answer: C

QUESTION 5

Which type of sniffing technique is generally referred as MiTM attack?



A. Password Sniffing

B. ARP Poisoning

C. Mac Flooding

D. DHCP Sniffing

Correct Answer: B

QUESTION 6

A very useful resource for passively gathering information about a target company is:

A. Host scanning

B. Whois search

C. Traceroute

D. Ping sweep

Correct Answer: B

QUESTION 7

What is a primary advantage a hacker gains by using encryption or programs such as Loki?

A. It allows an easy way to gain administrator rights

B. It is effective against Windows computers

C. It slows down the effective response of an IDS

D. IDS systems are unable to decrypt it

E. Traffic will not be modified in transit

Correct Answer: D

QUESTION 8

What are the three types of authentication?

A. Something you: know, remember, prove

B. Something you: have, know, are

C. Something you: show, prove, are

D. Something you: show, have, prove

Correct Answer: B

QUESTION 9

A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.

B. The consultant may expose vulnerabilities of other companies.

C. The company accepting bids will want the same type of format of testing.

D. The company accepting bids will hire the consultant because of the great work performed.

Correct Answer: B

QUESTION 10

What is the essential difference between an `Ethical Hacker\\' and a `Cracker\\'?

A. The ethical hacker does not use the same techniques or skills as a cracker.

B. The ethical hacker does it strictly for financial motives unlike a cracker.

C. The ethical hacker has authorization from the owner of the target.

D. The ethical hacker is just a cracker who is getting paid.

Correct Answer: C

QUESTION 11

Which of the following is an example of IP spoofing?

A. SQL injections

B. Man-in-the-middle

C. Cross-site scripting

D. ARP poisoning

Correct Answer: B

QUESTION 12

Clive has been monitoring his IDS and sees that there are a huge number of ICMP Echo Reply packets that are being received on the external gateway interface. Further inspection reveals that they are not responses from the internal hosts\\' requests but simply responses coming from the Internet.

What could be the most likely cause?

A. Someone has spoofed Clive\\'s IP address while doing a smurf attack.

B. Someone has spoofed Clive\\'s IP address while doing a land attack.

C. Someone has spoofed Clive\\'s IP address while doing a fraggle attack.

D. Someone has spoofed Clive\\'s IP address while doing a DoS attack.

Correct Answer: A