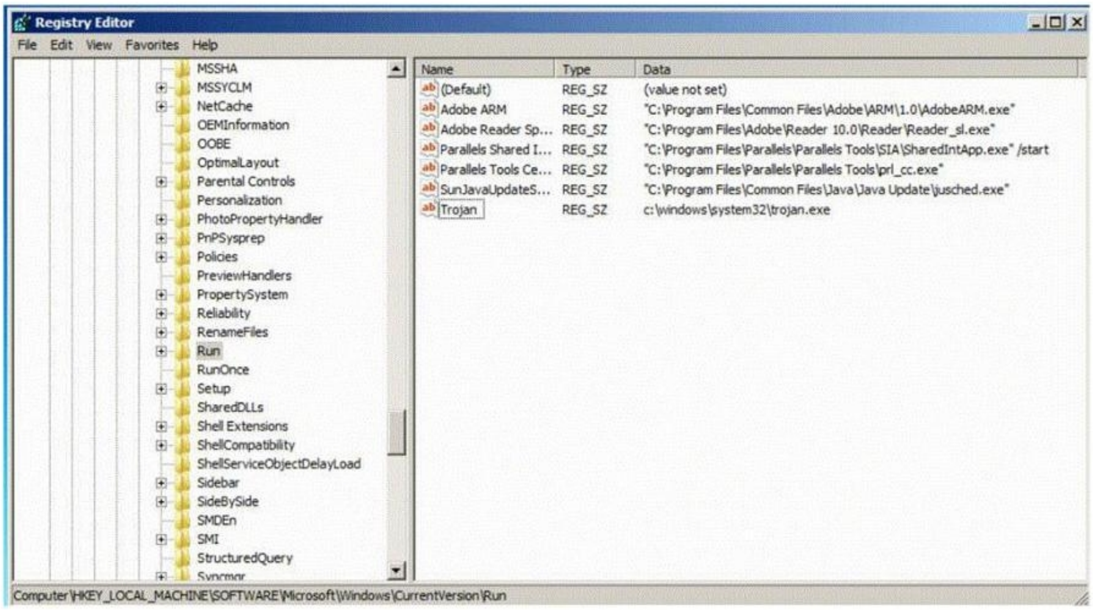
A. Jacob is seeing a Smurf attack.
B. Jacob is seeing a SYN flood.
C. He is seeing a SYN/ACK attack.
D. He has found evidence of an ACK flood.

Correct Answer: B

QUESTION 220

Which of the following Registry location does a Trojan add entries to make it persistent on Windows 7? (Select 2 answers)



Name	Type	Data
(Default)	REG_SZ	(value not set)
Adobe ARM	REG_SZ	"C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
Adobe Reader Sp...	REG_SZ	"C:\Program Files\Adobe\Reader 10.0\Reader\Reader_sl.exe"
Parallels Shared I...	REG_SZ	"C:\Program Files\Parallels\Parallels Tools\SIA\SharedIntApp.exe" /start
Parallels Tools Ce...	REG_SZ	"C:\Program Files\Parallels\Parallels Tools\prl_cc.exe"
SunJavaUpdateS...	REG_SZ	"C:\Program Files\Common Files\Java\Java Update\jusched.exe"
Trojan	REG_SZ	c:\windows\system32\trojan.exe

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\System32\CurrentVersion\ Run
C. HKEY_CURRENT_USER\Software\Microsoft\Windows\System32\CurrentVersion\Run
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Correct Answer: AD

QUESTION 221

Perimeter testing means determining exactly what your firewall blocks and what it allows. To conduct a good test, you can spoof source IP addresses and source ports. Which of the following command results in packets that will appear to originate from the system at 10.8.8.8? Such a packet is useful for determining whether the firewall is allowing random packets in or out of your network.

A. hping3 -T 10.8.8.8 -S netbios -c 2 -p 80
B. hping3 -Y 10.8.8.8 -S windows -c 2 -p 80
C. hping3 -O 10.8.8.8 -S server -c 2 -p 80
D. hping3 -a 10.8.8.8 -S springfield -c 2 -p 80

Correct Answer: D

QUESTION 222

The GET method should never be used when sensitive data such as credit card is being sent to a CGI program. This is because any GET command will appear in the URL, and will be logged by any servers. For example, let's say that you've entered your credit card information into a form that uses the GET method. The URL may appear like this:

https://www.xsecurity-bank.com/creditcard.asp?cardnumber=453453433532234

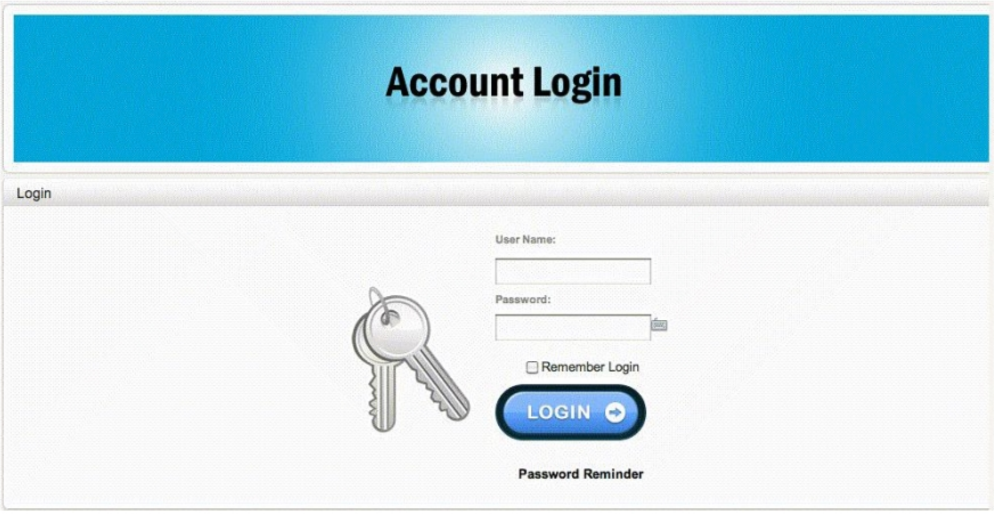
The GET method appends the credit card number to the URL. This means that anyone with access to a server log will be able to obtain this information. How would you protect from this type of attack?

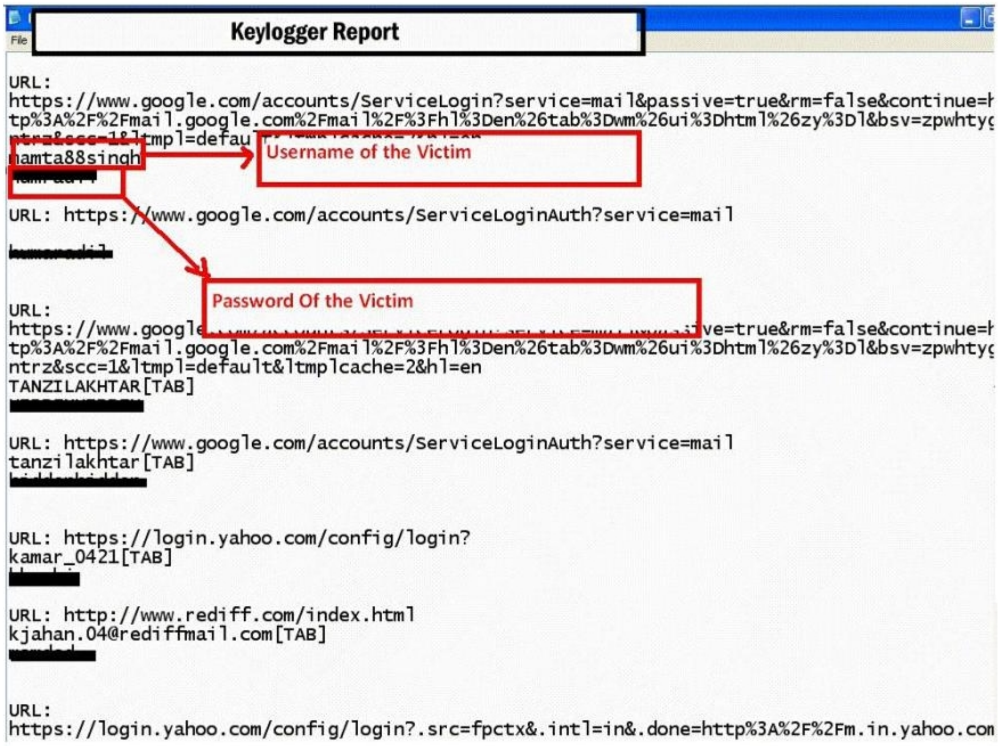
A. Never include sensitive information in a script.
B. Use HTTPS SSLv3 to send the data instead of plain HTTPS.
C. Replace the GET with POST method when sending data.
D. Encrypt the data before you send using GET method.

Correct Answer: C

QUESTION 223

Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.





Keylogger Report

```
URL:
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=h
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtyg
ntrz&scc=1&ltmpl=defau
namta88singh
[redacted]

URL: https://www.google.com/accounts/ServiceLoginAuth?service=mail

[redacted]


URL:
https://www.googl                                        ve=true&rm=false&continue=h
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtyg
ntrz&scc=1&ltmpl=default&ltmplcache=2&hl=en
TANZILAKHTAR[TAB]
[redacted]

URL: https://www.google.com/accounts/ServiceLoginAuth?service=mail
tanzilakhtar[TAB]
[redacted]


URL: https://login.yahoo.com/config/login?
kamar_0421[TAB]
[redacted]

URL: http://www.rediff.com/index.html
kjahan.04@rediffmail.com[TAB]
[redacted]


URL:
https://login.yahoo.com/config/login?.src=fpctx&.intl=in&.done=http%3A%2F%2Fm.in.yahoo.com
```

How will you defend against hardware keyloggers when using public computers and Internet Kiosks? (Select 4 answers)

A. Alternate between typing the login credentials and typing characters somewhere else in the focus window.

B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording.

C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.

D. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfsd". Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsd".

E. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfsd". Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsd".

Correct Answer: ACDE

QUESTION 224

Lauren is performing a network audit for her entire company. The entire network is comprised of around 500 computers. Lauren starts an ICMP ping sweep by sending one IP packet to the broadcast address of the network, but only receives responses from around five hosts. Why did this ping sweep only produce a few responses?

A. Only Windows systems will reply to this scan.
B. A switched network will not respond to packets sent to the broadcast address.
C. Only Linux and Unix-like (Non-Windows) systems will reply to this scan.
D. Only servers will reply to this scan.

Correct Answer: C

QUESTION 225

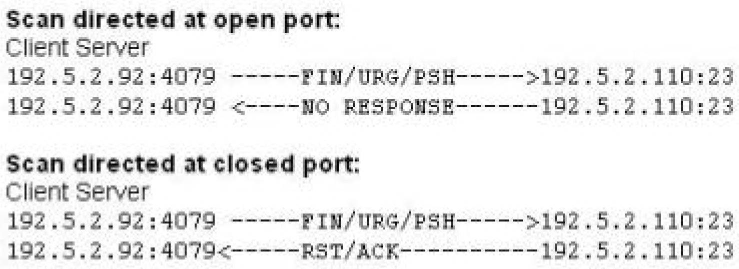
Wayne is the senior security analyst for his company. Wayne is examining some traffic logs on a server and came across some inconsistencies. Wayne finds some IP packets from a computer purporting to be on the internal network. The packets originate from 192.168.12.35 with a TTL of 15. The server replied to this computer and received a response from 192.168.12.35 with a TTL of 21. What can Wayne infer from this traffic log?

A. The initial traffic from 192.168.12.35 was being spoofed.
B. The traffic from 192.168.12.25 is from a Linux computer.
C. The TTL of 21 means that the client computer is on wireless.
D. The client computer at 192.168.12.35 is a zombie computer.

Correct Answer: A

QUESTION 226

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

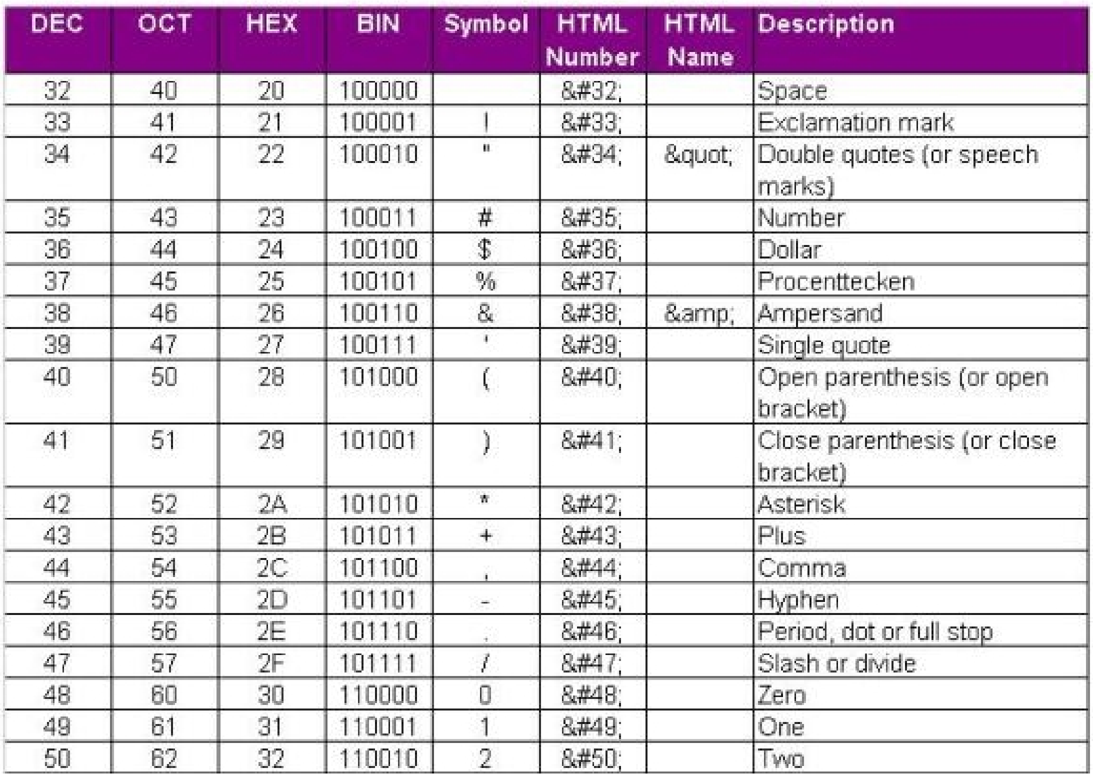
C. XMAS Scan

D. SYN Stealth Scan

Correct Answer: C

QUESTION 227

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;		Procenttecken
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