the third packet of the handshake, not the first.

B. RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.

C. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall.

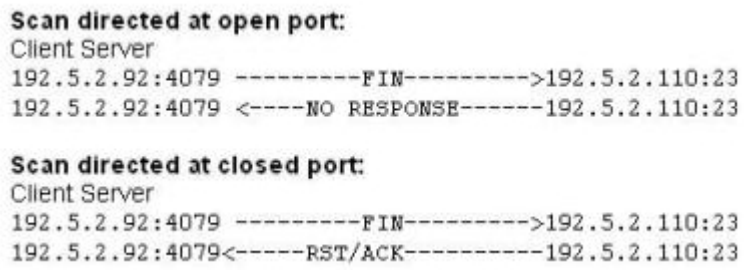
D. Stack Tweaking. TCP stacks can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection.

E. Micro Blocks. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object.

Correct Answer: ABDE

QUESTION 32

What type of port scan is shown below?



A. Idle Scan

B. FIN Scan

C. XMAS Scan

D. Windows Scan

Correct Answer: B

QUESTION 33

Stephanie works as a records clerk in a large office building in downtown Chicago. On Monday, she went to a mandatory security awareness class (Security5) put on by her company's IT department. During the class, the IT department informed all employees that everyone's Internet activity was thenceforth going to be monitored. Stephanie is worried that her Internet activity might give her supervisor reason to write her up, or worse get her fired. Stephanie's daily work duties only consume about four hours of her time, so she usually spends the rest of the day surfing the web. Stephanie really enjoys surfing the Internet but definitely does not want to get fired for it. What should Stephanie use so that she does not get in trouble for surfing the Internet?

A. Stealth IE
B. Stealth Anonymizer
C. Stealth Firefox
D. Cookie Disabler

Correct Answer: B

QUESTION 34
Neil is a network administrator working in Istanbul. Neil wants to setup a protocol analyzer on his network that will receive a copy of every packet that passes through the main office switch. What type of port will Neil need to setup in order to accomplish this?

A. Neil will have to configure a Bridged port that will copy all packets to the protocol analyzer.
B. Neil will need to setup SPAN port that will copy all network traffic to the protocol analyzer.
C. He will have to setup an Ether channel port to get a copy of all network traffic to the analyzer.
D. He should setup a MODS port which will copy all network traffic.

Correct Answer: B

QUESTION 35
In TCP communications there are 8 flags; FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. These flags have decimal numbers assigned to them:

- FIN = 1
- SYN = 2
- RST = 4
- PSH = 8
- ACK = 16
- URG = 32
- ECE = 64
- CWR = 128

Jason is the security administrator of ASPEN Communications. He analyzes some traffic using Wireshark and has enabled the following filters.

```
((tcp.flags == 0x02) || (tcp.flags == 0x12) ) || ((tcp.flags == 0x10) && (tcp.ack==1) && (tcp.len==0))
```

What is Jason trying to accomplish here?

A. SYN, FIN, URG and PSH
B. SYN, SYN/ACK, ACK
C. RST, PSH/URG, FIN
D. ACK, ACK, SYN, URG

Correct Answer: B

QUESTION 36
Jayden is a network administrator for her company. Jayden wants to prevent MAC spoofing on all the Cisco switches in the network. How can she accomplish this?

A. Jayden can use the command. ip binding set.
B. Jayden can use the command. no ip spoofing.
C. She should use the command. no dhcp spoofing.
D. She can use the command. ip dhcp snooping binding.

Correct Answer: D

QUESTION 37
Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". Here is the output of the SIDs:

```
S-1-5-21-1125394485-807628933-549785860-100 John
S-1-5-21-1125394485-807628933-549785860-652 Rebecca
S-1-5-21-1125394485-807628933-549785860-412 Sheela
S-1-5-21-1125394485-807628933-549785860-999 Shawn
S-1-5-21-1125394485-807628933-549785860-777 Somia
S-1-5-21-1125394485-807628933-549785860-500 Chang
S-1-5-21-1125394485-807628933-549785860-555 Micah
```

From the above list identify the user account with System Administrator privileges?

A. John
B. Rebecca
C. Sheela
D. Shawn
E. Somia
F. Chang
G. Micah

Correct Answer: F

QUESTION 38

What is the problem with this ASP script (login.asp)?

```
strsql = "SELECT * FROM Users where where Username='" + Login1.UserName
+ "' and Pass='" + password + "'
try
{
OleDbConnection con = new OleDbConnection(connectionstring);
con.Open();
OleDbCommand cmd = new OleDbCommand(strsql, con);
OleDbDataReader dr = cmd.ExecuteReader();
if (dr.HasRows)
{
If (dr.Read())
{
Session["username"] = Login1.UserName;
Response.Redirect("Mainpage.aspx", false);
else
{
Response.Redirect("Login.aspx", false);
}
}
}
dr.Dispose();
con.Close();
}
catch (Exception ex)
{
ClientScript.RegisterStartupScript(this.GetType(), "msg",
"<script>alert('" + ex.Message + "')</script>");
```

A. The ASP script is vulnerable to Cross Site Scripting attack.
B. The ASP script is vulnerable to Session Splice attack.
C. The ASP script is vulnerable to XSS attack.
D. The ASP script is vulnerable to SQL Injection attack.

Correct Answer: D

QUESTION 39

Google uses a unique cookie for each browser used by an individual user on a computer. This cookie contains information that allows Google to identify records about that user on its database. This cookie is submitted every time a user launches a Google search, visits a site using AdSense etc. The information stored in Google's database, identified by the cookie, includes:

- Everything you search for using Google
- Every web page you visit that has Google AdSense ads

How would you prevent Google from storing your search keywords?

A. Block Google Cookie by applying Privacy and Security settings in your web browser.
B. Disable the Google cookie using Google Advanced Search settings on Google Search page.
C. Do not use Google but use another search engine Bing which will not collect and store your search keywords.
D. Use MAC OS X instead of Windows 7. Mac OS has higher level of privacy controls by default.

Correct Answer: A

QUESTION 40
How many bits encryption does SHA-1 use?

A. 64 bits
B. 128 bits
C. 256 bits
D. 160 bits

Correct Answer: D

QUESTION 41
In Trojan terminology, what is required to create the executable file chess.exe as shown below?