indicate?

A. A buffer overflow attack has been attempted.
B. A buffer overflow attack has already occurred.
C. A firewall has been breached and this is logged.
D. An intrusion detection system has been triggered.
E. The system has crashed.

Correct Answer: A

QUESTION 165

This is an example of whois record.

```
Registrant:
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA

Registrar: Jason Springfield (http://www. jspringfield.com)
Domain Name: jspringfield.com
Created on: 29-DEC-10
Expires on: 29-DEC-14
Last Updated on: 23-FEB-11

Administrative Contact:
Contact, Admin Jack_Smith@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.6744
360.253.3556

Technical Contact:
Contact, Technical Sheela_Ravin@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.3456
360.253.2675

Billing Contact:
Contact, Technical David_Bruce@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.6654
360.253.1256

Domain servers (DNS) in listed order:
NS1.jspringfield.com
NS2.jspringfield.com
```

Sometimes a company shares a little too much information on their organization through public domain records. Based on the above whois record, what can an attacker do? (Select 2 answers)

A. Search engines like Google, Bing will expose information listed on the WHOIS record.
B. An attacker can attempt phishing and social engineering on targeted individuals using the information from WHOIS record.
C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record.
D. IRS Agents will use this information to track individuals using the WHOIS record information.

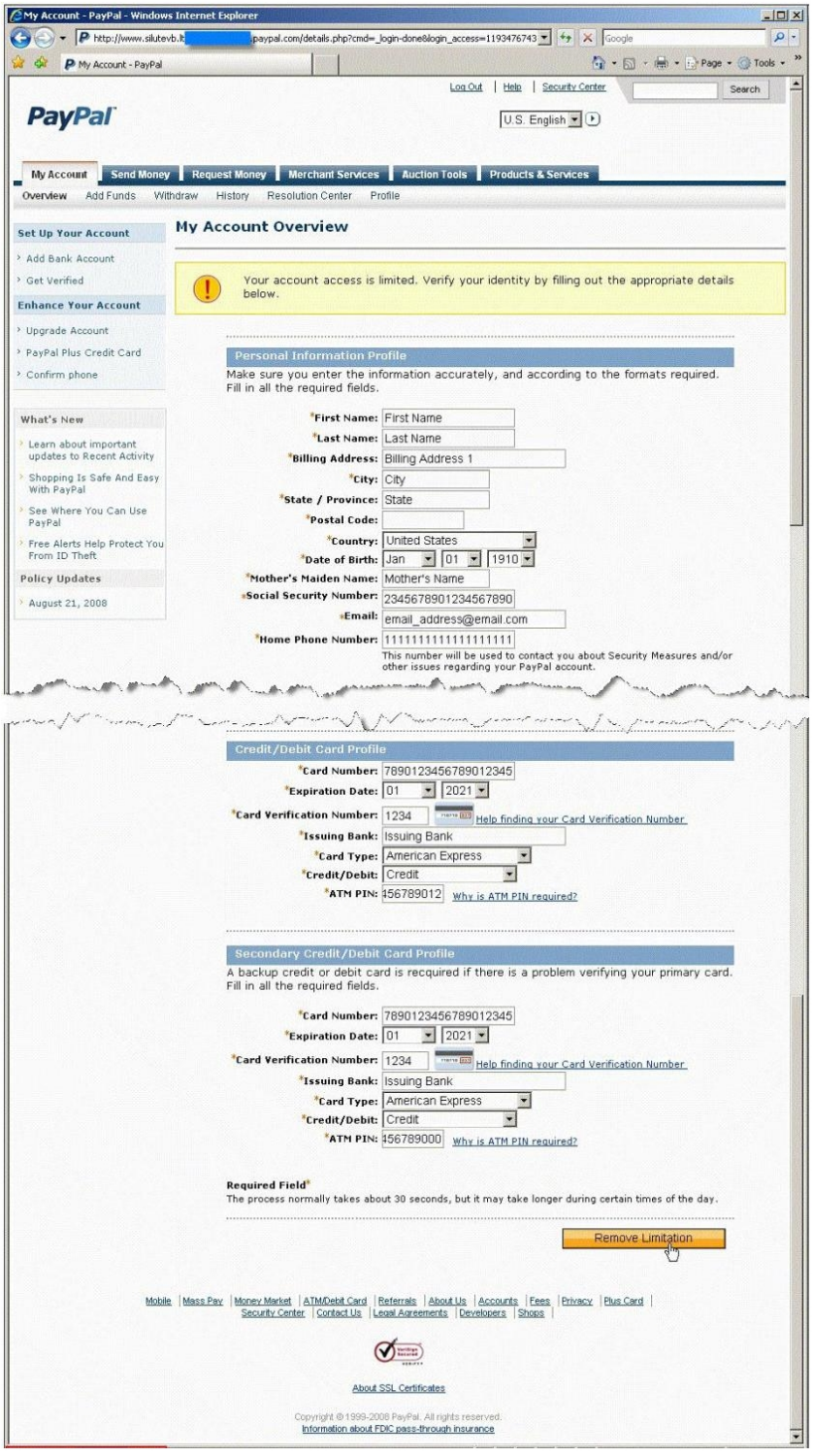
Correct Answer: BC

QUESTION 166
Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to-date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall.
B. They are using HTTP tunneling software that allows them to communicate with protocols in a way it was not intended.
C. They have been able to compromise the firewall, modify the rules, and give themselves proper access.
D. They are using an older version of Internet Explorer that allow them to bypass the proxy server.

Correct Answer: B

QUESTION 167
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details.



Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information.
B. Do not trust telephone numbers in e-mails or popup ads.
C. Review credit card and bank account statements regularly.

D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks.
E. Do not send credit card numbers, and personal or financial information via e-mail.

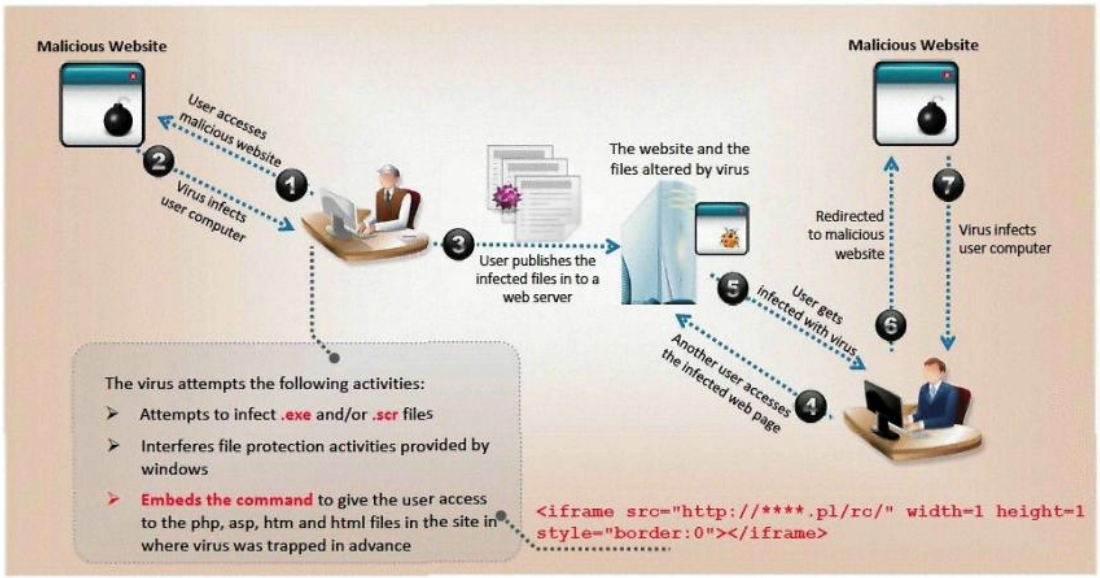
Correct Answer: D

QUESTION 168
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

A. Take over the session
B. Reverse sequence prediction
C. Guess the sequence numbers
D. Take one of the parties offline

Correct Answer: C

QUESTION 169
ViruXine.W32 virus hides their presence by changing the underlying executable code. This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

```
1.  lots of encrypted code
2.  ...
3.  Decryption_Code:
4.  C = C + 1
5.  A = Encrypted
6.  Loop:
7.  B = *A
8.  C = 3214 * A
9.  B = B XOR CryptoKey
10. *A = B
11. C = 1
12. C = A + B
13. A = A + 1
14. GOTO Loop IF NOT A = Decryption_Code
15. C = C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

What is this technique called?

A. Polymorphic Virus
B. Metamorphic Virus
C. Dravidic Virus
D. Stealth Virus

Correct Answer: A

QUESTION 170

"Testing the network using the same methodologies and tools employed by attackers" Identify the correct terminology that defines the above statement.

A. Vulnerability Scanning
B. Penetration Testing
C. Security Policy Implementation
D. Designing Network Security

Correct Answer: B

QUESTION 171

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches. If these switches' ARP cache is successfully flooded, what will be the result?

A. The switches will drop into hub mode if the ARP cache is successfully flooded.
B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.