Correct Answer: C

QUESTION 73

Jake works as a system administrator at Acme Corp. Jason, an accountant of the firm befriends him at the canteen and tags along with him on the pretext of appraising him about potential tax benefits. Jason waits for Jake to swipe his access card and follows him through the open door into the secure systems area. How would you describe Jason's behavior within a security context?

A. Smooth Talking
B. Swipe Gating
C. Tailgating
D. Trailing

Correct Answer: C

QUESTION 74

While performing a ping sweep of a local subnet you receive an ICMP reply of Code 3/Type 13 for all the pings you have sent out. What is the most likely cause of this?

A. The firewall is dropping the packets.
B. An in-line IDS is dropping the packets.
C. A router is blocking ICMP.
D. The host does not respond to ICMP packets.

Correct Answer: C

QUESTION 75

Consider the following code:

URL:http://www.certified.com/search.pl?
text=<script>alert(document.cookie)</script>

If an attacker can trick a victim user to click a link like this, and the Web application does not validate input, then the victim's browser will pop up an alert showing the users current set of cookies. An attacker can do much more damage, including stealing passwords, resetting your home page, or redirecting the user to another Web site. What is the countermeasure against XSS scripting?

A. Create an IP access list and restrict connections based on port number.
B. Replace "<" and ">" characters with "& l t;" and "& g t;" using server scripts.

C. Disable JavaScript in IE and Firefox browsers.
D. Connect to the server using HTTPS protocol instead of HTTP.

Correct Answer: B

QUESTION 76

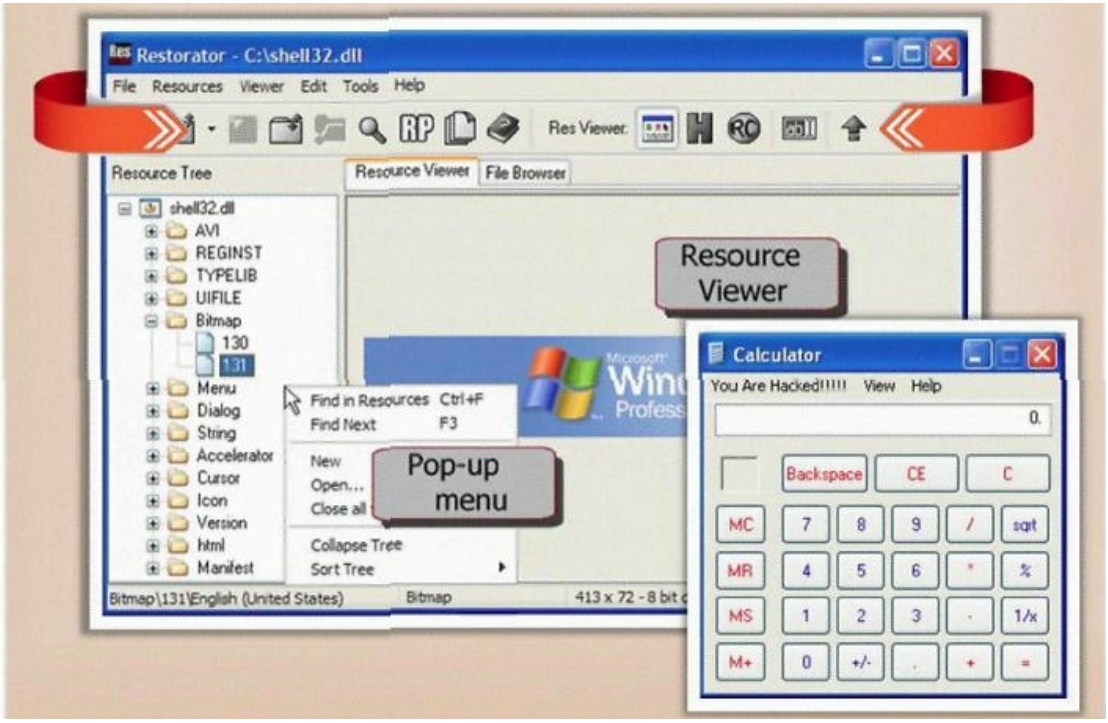
Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet. But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule. Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder's attempts. Samuel wants to completely block hackers brute force attempts on his network. What are the alternatives to defending against possible brute-force password attacks on his site?

A. Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users.
B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at the Firewall manually.
C. Enforce complex password policy on your network so that passwords are more difficult to brute force.
D. You cannot completely block the intruders attempt if they constantly switch proxies.

Correct Answer: D

QUESTION 77

What type of Trojan is this?



A. RAT Trojan
B. E-Mail Trojan
C. Defacement Trojan
D. Destructing Trojan
E. Denial of Service Trojan

Correct Answer: C

QUESTION 78

Maintaining a secure Web server requires constant effort, resources, and vigilance from an organization. Securely administering a Web server on a daily basis is an essential aspect of Web server security. Maintaining the security of a Web server will usually involve the following steps:

1. Configuring, protecting, and analyzing log files
2. Backing up critical information frequently
3. Maintaining a protected authoritative copy of the organization's Web content
4. Establishing and following procedures for recovering from compromise
5. Testing and applying patches in a timely manner
6. Testing security periodically.

In which step would you engage a forensic investigator?

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6

Correct Answer: D

QUESTION 79

In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

A. EEP
B. ESP
C. EAP
D. EIP

Correct Answer: D

QUESTION 80

Web servers often contain directories that do not need to be indexed. You create a text file with search engine indexing restrictions and place it on the root directory of the Web Server.

User-agent: *
Disallow: /images/
Disallow: /banners/
Disallow: /Forms/
Disallow: /Dictionary/
Disallow: /_borders/
Disallow: /_fpclass/
Disallow: /_overlay/
Disallow: /_private/
Disallow: /_themes/

What is the name of this file?

A. robots.txt
B. search.txt
C. blocklist.txt
D. spf.txt

Correct Answer: A

QUESTION 81

An attacker has successfully compromised a remote computer. Which of the following comes as one of the last steps that should be taken to ensure that the compromise cannot be traced back to the source of the problem?

A. Install patches
B. Setup a backdoor
C. Install a zombie for DDOS
D. Cover your tracks

Correct Answer: D

QUESTION 82

Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server. Which of the following commands extracts the HINFO record?

A.

```
c:> nslookup
> Set type=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

B.

```
c:> nslookup
> Set dns=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

C.