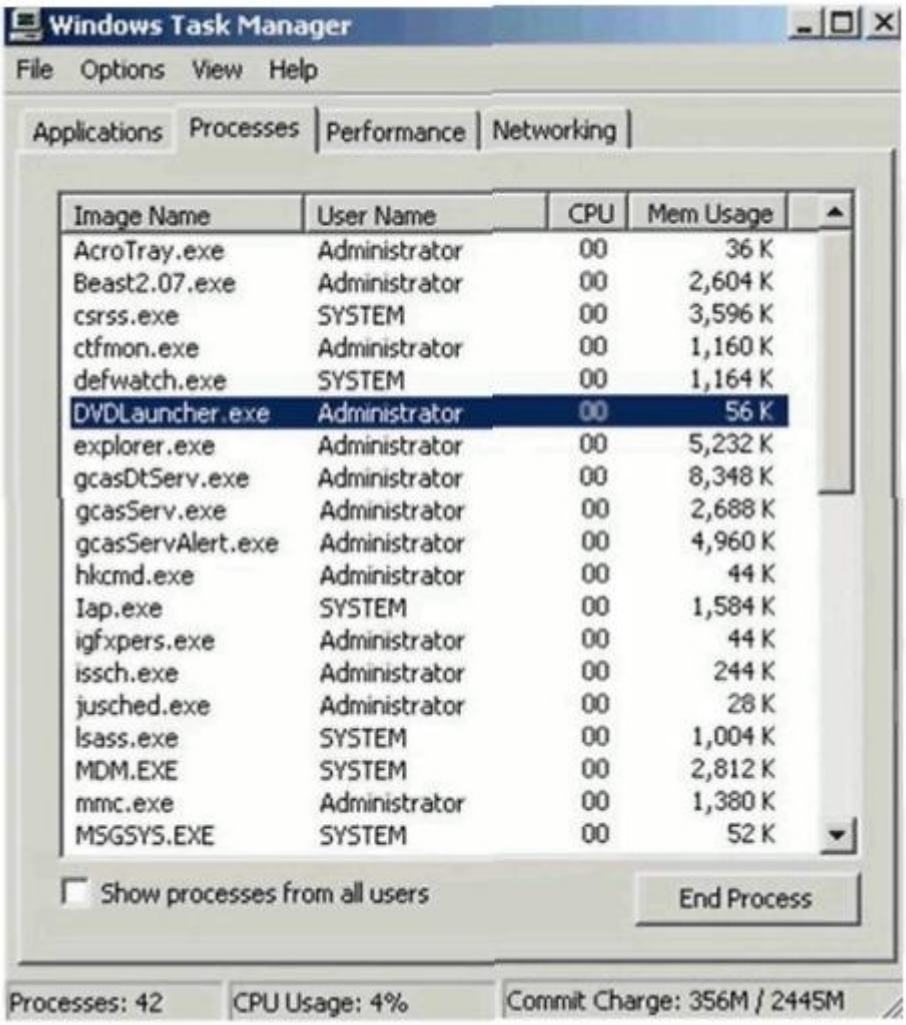


What has William just installed?

A. Zombie Zapper (ZoZ)
B. Remote Access Trojan (RAT)
C. Bot IRC Tunnel (BIT)
D. Root Digger (RD)

Correct Answer: B

QUESTION 110

John the hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct MITM attack. What is the destination MAC address of a broadcast frame?

A. 0xFFFFFFFFFFFF
B. 0xDDDDDDDDDDDD
C. 0xAAAAAAAAAAAA

D. 0xBBBBBBBBBBBB

Correct Answer: A

QUESTION 111

You are gathering competitive intelligence on an organization. You notice that they have jobs listed on a few Internet job-hunting sites. There are two jobs for network and system administrators. How can this help you in foot printing the organization?

A. To learn about the IP range used by the target network.
B. To identify the number of employees working for the company.
C. To test the limits of the corporate security policy enforced in the company.
D. To learn about the operating systems, services and applications used on the network.

Correct Answer: D

QUESTION 112

TCP packets transmitted in either direction after the initial three-way handshake will have which of the following bit set?

A. SYN flag
B. ACK flag
C. FIN flag
D. XMAS flag

Correct Answer: B

QUESTION 113

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server in your organization. They notice that there is excessive number of functions in the source code that might lead to buffer overflow. These C++ functions do not check bounds. Identify the line in the source code that might lead to buffer overflow?

```
1. #include <stdio.h>
2. void stripnl(char *str) {
3. while(strlen(str) && ( (str[strlen(str) - 1] == 13) ||
4. ( str[strlen(str) - 1] == 10 ))) {

5. str[strlen(str) - 1] = 0;
6. }
7. }
8.
9. int main() {
10. FILE *infile;
11. char fname[40];
12. char line[100];
13. int lcount;
14.
15. /* Read in the filename */
16. printf("Enter the name of a ascii file: ");
17. fgets(fname, sizeof(fname), stdin);
18.
19. /* We need to get rid of the newline char. */
20. stripnl(fname);
21.
22. /* Open the file. If NULL is returned there was an error */
23. if((infile = fopen(fname, "r")) == NULL) {
24. printf("Error Opening File.\n");
25. exit(1);
26. }
27.
28. while( fgets(line, sizeof(line), infile) != NULL ) {
29. /* Get each line from the infile */
30. lcount++;
31. /* print the line number and data */
32. printf("Line %d: %s", lcount, line);
33. }
34.
35. fclose(infile); /* Close the file */
```

A. 9A.9

B. 17B.17

C. 20C.20

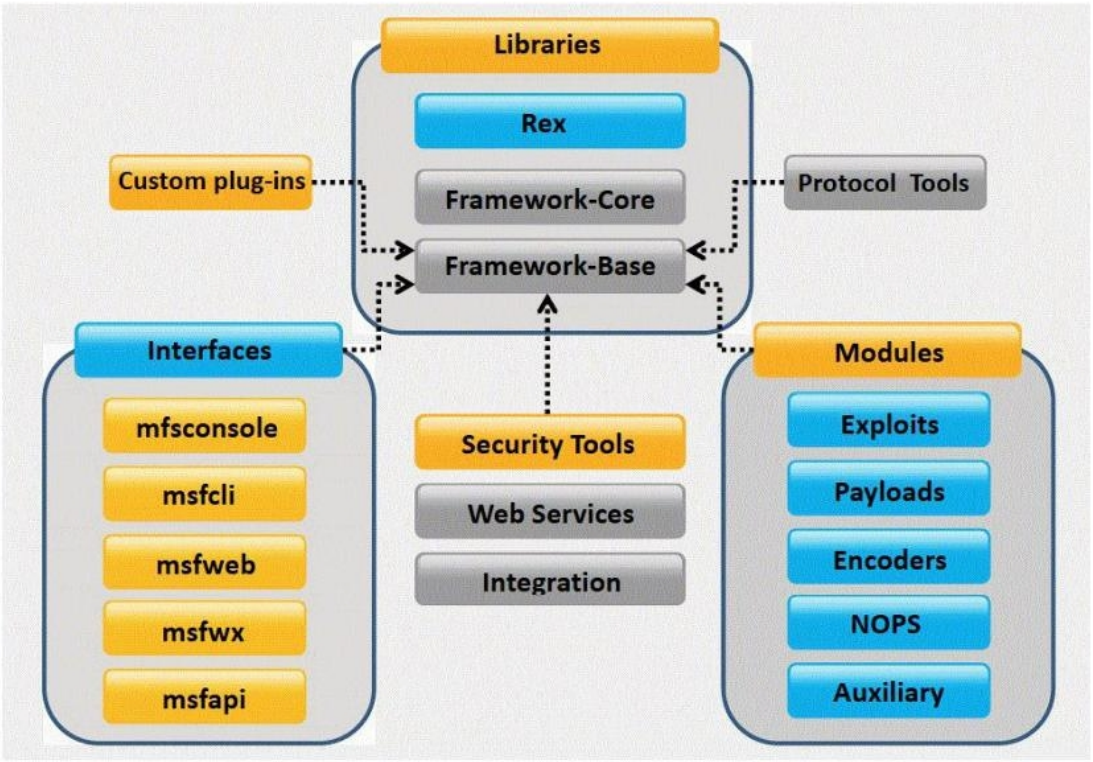
D. 32D.32

E. 35E.35

Correct Answer: B

QUESTION 114

What framework architecture is shown in this exhibit?



A. Core Impact
B. Metasploit
C. Immunity Canvas
D. Nessus

Correct Answer: B

QUESTION 115

Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

A. Image Hide
B. Snow
C. Gif-It-Up
D. NiceText

Correct Answer: B

QUESTION 116
You have chosen a 22 character word from the dictionary as your password. How long will it take to crack the password by an attacker?

A. 16 million years
B. 5 minutes
C. 23 days
D. 200 years

Correct Answer: B

QUESTION 117
While testing web applications, you attempt to insert the following test script into the search area on the company's web site:

<script>alert('Testing Testing Testing')</script>

Later, when you press the search button, a pop up box appears on your screen with the text "Testing Testing Testing". What vulnerability is detected in the web application here?

A. Cross Site Scripting
B. Password attacks
C. A Buffer Overflow
D. A hybrid attack

Correct Answer: A

QUESTION 118
What techniques would you use to evade IDS during a Port Scan? (Select 4 answers)

A. Use fragmented IP packets.
B. Spoof your IP address when launching attacks and sniff responses from the server.
C. Overload the IDS with Junk traffic to mask your scan.
D. Use source routing (if possible).
E. Connect to proxy servers or compromised Trojaned machines to launch attacks.

Correct Answer: ABDE