Wargames server 1.0 Jackula's way

By Jackula

June 17, 2003

I was never so experienced in hacking, and never hid my IP or erased logs coz I figured if the sys admin knows what they were doing they would catch me breaking in anyway, coz nothing is that 100% secure. Nowadays technology is so advanced and yet so insecure that you won't know if the sky is gonna fall on you when you are reading a newspaper in the bathroom.

I thought I was never gonna penetrate Wargames, until that day when they installed Samba on their servers, coz samba had a vulnerability, a buffer overflow in their code and one can use this vulnerability to gain root privileges. L337 huh? Did I ever told u that I want to marry my computer when I come out of puberty? I reckon that'd be pretty soon coz I met this hottest chick the other day, and she says my computer is just as big as my ego.

Pointing my browser to http://www.astalavista.net/data/sambal.c I downloaded the sourcecode of that exploit, why code one myself when there is already one on Altavista? I didn't pay them money for nothing. However, to my dismay, when I compiled sambal.c it didn't recognize Wargames as a Samba vulnerable server. But all I had to do is remove all the sections in the code:

```
if (force == 0) {

                        if (is_samba(argv[optind], 2) != 0) {
                                fprintf(stderr, "+ Host is not running
samba!\n\n");
                                return -1;
                        }

                        fprintf(stderr, "+ Host is running samba.\n");
                }
```

So that sambal.c will continue to do what it does best even if it doesn't recognize it as a Samba vulnerable server.

Then bingo! I got r00t access, but like Auzy said in his whitepaper, u can't see anything! I had to type pwd once in awhile to figure out where I was. When to /home first, hoping the index file was there, but it wasn't. But eventually I found the srv folder than contained all the files where I could add my name to.

Damn that britany_one_more_time.mid sucked, and when I tried to wget a new midi, I'd get that annoying 'Auzy@wants.to.bone.britany' segmentation fault, but mwahahaha, I found a way to get around that and put up J.S.Bach's Toccata and Fugue in D-, God I love classical music, but I later changed it back coz I guess Auzy should still have more authority coz he hacked it sooner than I did.

I added some javascript to the index file, not annoying ones, but they keep getting deleted by *SOMEONE*, I won't name names, but you know who you are!

One thing I like to conclude in my whitepaper, I'm serious about this one.

"I Love Linda LHY", and for all people who's reading this, I just want to share the love I have for her:

Thy skin is that earthly guard,
Shielding us beings from sin, disregard.
Flying crystals from thy eye,
Bathing us while you fly,
Gold and gentle, those wings by,
Thousands they drop, under moonlight.

Thy bequeath sweetened winds,
Rush ‘n hush the smell of spring,
For you have made roses red,
My heart bleeds until you kiss it dry.
Thy eyes shut, world no more,
The moon, the sun, the sky, the stars.
All living things, and I,
Will cease to dine.

Her birthday is coming up, if you can think of any gifts I can give her, please U2U me.