

Forum:[Hack Forums](#)

Thread: [Eternal blue not working \(same network\)](#)

Blackshield_real - June 14, 2017, 2:43 am

I'm getting positive results from auxiliary scanner that victim is vulnerable and NMAP says port 445 is open. I cannot ping the victim though idk for what reason now. I'm using this elevenPaths version "<https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit>"

Can anyone help? got an updated version??

Golden_Receiver - June 14, 2017, 9:43 am

Pretty sure they patched Eternal Blue like a week after the UK Hospital scandal and the WannaCry breakout.

Qismon - September 4, 2017, 6:28 pm

Yeah its patched but there are still plenty more out there that are vulnerable. Anyone interested let me know, I have a special exploit kit for this. ?

Hyrax - September 4, 2017, 9:19 pm

One of the NMAP scripts is a SMB exploit checker (not sure the actual name), but it will check to see if the host is actually vulnerable (Metasploit has a module to do this as well). Also, afaik most public version of the exploit have limited platforms for which they work (Windows 7 and Windows Server 2008 last I used it), so you might want to check that as well.

THC - September 4, 2017, 11:13 pm

Unless you know for sure that the OS that your target is using is vulnerable, it is very safe to assume that they are running a version of windows that has been patched.

Qismon - September 22, 2017, 4:28 pm

(Sep 4, 2017 11:13 PM)M.D. Wrote: [\[CITE\]](#) Unless you know for sure that the OS that your target is using is vulnerable, it is very safe to assume that they are running a version of windows that has been patched.

Still plenty more out there and the Metasploit Scan module is good but limited.

After you find a vulnerable machine you still need to verify the SMB pipe names.

hi_man - September 22, 2017, 10:05 pm

I guess it is Patched for most of the Systems.

But yes, Many are vulnerable yet.

Try with official Metasploit Eternal blue. May that works.

It is working for me and may it also works for you too.