

Forum:[Hack Forums](#)

Thread: [How to exploit ANY \(unpatched\) windows machine older then version 10! Nr1 exploit](#)

pinkhat - February 4, 2018, 6:03 pm

I have studied the art of pentesting and since i did that i know exactly what hacking is (for me)
It was in the past only about finding cracking tools in youtube (ful of malicious files) an hoping for 1 to work ? Then i found out about backtrack, kali linux and i learned how to use metasploit and i learned how every android device is basicly an linux machine :D .

I wil update this tutorial tommorow, where i wil teach u how to :

setup a pentesting lab
instal kali on a vm
and then use this exploit to show you the damage this exploit can do if used wrong (like the wannne cry virus)

Also i wil teach u what meterpreter is and how cool it is.. See ya

?Apocalypse - February 4, 2018, 6:07 pm

Not allow here, take it somewhere else.

pinkhat - February 4, 2018, 6:08 pm

u want me to delete it or remove to another section ?

CyberStrike - February 5, 2018, 3:22 am

I voted zero first the teaser really doesn't work, then you are using ms17-10, third your lab needs to have AD, smbv1 enabled and another machine, then you need to not be patched (KB4013389). Microsoft released a "special" patch for Windows 7, an eol product just because it is still used in corporate, home users accounted for about 3.61% of all the infections of wannacry. So that means that these poor people ran either the exe or the original PDF that was sent out, there was no spreading since they had no AD/samba and that was the end of the infection on their network.

Then assuming we have no clue what meterpreter is, I am sure that some bastard doesn't know what meterpreter is, but come on. Also instead of having your own simple resource script in metasploit so after exploitation maybe it uses bitslocker to encrypt the target VM's HD instead you are going to use wannacry? Dude I am not saying that you may or may not know your stuff, you probably do but just don't assume that everyone here is so skid that they have no concept and we all are buffons. Take a minute and look around before

Edit: OP how about instead of using wannacry have the same general setup two machines use AD and after compromising the first machine attack the second machine in the same way, or whatever you wish and I do apologize if I came across as rude or anything like that, I just ask that you not assume that everyone here has the brains of tomatoes.

Blackshield_real - February 6, 2018, 6:29 am

(Feb 5, 2018 04:22 AM)sirru5h Wrote: [CITE](#) I voted zero first the teaser really doesn't work, then you are using ms17-10, third your lab needs to have AD, smbv1 enabled and another machine, then you need to not be patched (KB4013389). Microsoft released a "special" patch for Windows 7, an eol product just because it is still used in corporate, home users accounted for about 3.61% of all

the infections of wannacry. So that means that these poor people ran either the exe or the original PDF that was sent out, there was no spreading since they had no AD/samba and that was the end of the infection on their network.

Then assuming we have no clue what meterpreter is, I am sure that some bastard doesn't know what meterpreter is, but come on. Also instead of having your own simple resource script in metasploit so after exploitation maybe it uses bitslocker to encrypt the target VM's HD instead you are going to use wannacry? Dude I am not saying that you may or may not know your stuff, you probably do but just don't assume that everyone here is so skid that they have no concept and we all are buffons. Take a minute and look around before

Edit: OP how about instead of using wannacry have the same general setup two machines use AD and after compromising the first machine attack the second machine in the same way, or whatever you wish and I do apologize if I came across as rude or anything like that, I just ask that you not assume that everyone here has the brains of tomatoes.

Ouch!

monika1246 - February 6, 2018, 8:36 am

good stuff keep the good work ;)

MrDickFeynman - February 7, 2018, 12:28 pm

(Feb 6, 2018 07:29 AM)Blackshield_real Wrote: [\[CITE\]](#) Ouch!

he did say it on the most gentle way ever possible