

Forum:[Hack Forums](#)

Thread: [Metasploit : Windows pc on same network error](#)

Kevin_1998 - October 4, 2017, 12:49 pm

Whenever I try to use Metasploit to exploit Windows pc on LAN. I get this error.
Even though the IP address of victim is correct it shows following error .
I used rport value as 445 .is it correct or should it be another ?
Please anybody help me to fix this problem.
Anyone who is expert please resolve this error :

Exploit aborted due to failure: no-target: No matching target
Exploit completed, but no session was created.

Thank you !

SIM-1456221 - October 4, 2017, 12:56 pm

What is your RHOST showing m8

Kevin_1998 - October 6, 2017, 1:24 am

I read that this technique is outdated , windows 10 got patch for that though .. is there any other any technique to hack any other windows pc on same network (LAN) without actually deploying payload in to victims pc.
Anyone who knows please share and help in learning ...

Thank You !

@ ? ?Pa?a?DoX ?
Thanks buddy ..

SIM-1456221 - October 6, 2017, 5:31 am

(Oct 6, 2017 01:24 AM)Kevin_1998 Wrote: [CITE](#) I read that this technique is outdated , windows 10 got patch for that though .. is there any other any technique to hack any other windows pc on same network (LAN) without actually deploying payload in to victims pc.
Anyone who knows please share and help in learning ...

Thank You !

@ ? ?Pa?a?DoX ?

Thanks buddy ..It's possible that it still works,
PHP Code

<?php

Exploit aborted due to failure: no-target: No matching target
means that the RHOST is wrong, what is the RHOST showing?

Death - October 6, 2017, 5:54 am

What exploit are you using my friend?

Kevin_1998 - October 6, 2017, 10:36 am

(Oct 6, 2017 05:54 AM)linuxdaddy Wrote: [\[CITE\]](#) What exploit are you using my friend?
exploit(ms08_067_netapi)

(Oct 6, 2017 05:31 AM)? ?Pa?a?DoX ? Wrote: [\[CITE\]](#) It's possible that it still works,
PHP Code
<?php

Exploit aborted due to failure: no-target: No matching target
means that the RHOST is wrong, what is the RHOST showing?RHOST is accepting the given IP
address. But after that it shows nothing but the error I mentioned above in post#1.
But as you said it is still possible..
Can you please tell me how to do it ?

Thank you !

SIM-1456221 - October 6, 2017, 11:01 am

(Oct 6, 2017 10:36 AM)Kevin_1998 Wrote: [\[CITE\]](#) exploit(ms08_067_netapi)

RHOST is accepting the given IP address. But after that it shows nothing but the error I mentioned
above in post#1.
But as you said it is still possible..
Can you please tell me how to do it ?

Thank you !
For Windows 10 use blue..whatever

Kevin_1998 - October 6, 2017, 12:49 pm

(Oct 6, 2017 11:01 AM)? ?Pa?a?DoX ? Wrote: [\[CITE\]](#) For Windows 10 use blue..whatever
You mean .. eternalblue ?

Nomad.Null - October 6, 2017, 12:49 pm

No matching target corresponds to the TARGET setting which refers to the OS, architecture and
version. If an exploit is not built for the OS you are targeting, you will receive this error. MS08-067
was patched after Windows XP SP3 and has rarely been seen since, which is why you are getting
this error.

You need to understand the concept of fingerprinting which is the process of scanning targets to
identify their OS version and architecture. Tools like Nmap are commonly used for this. The nmap
-O <target_ip> is the switch specifically used for identifying the OS.

When and if Nmap is able to determine the host operating system, you can begin searching for
exploits in that version. But you are not likely to have much luck on a fully patched version of
Windows 10. Try practicing on a Windows XP or 7 virtual machine to get the hang of it, or try a
Capture the Flag site like hackthebox.eu.

If you don't know shit about using metasploit, you should be reading books on the subject. I suggest
Mastering Metasploit.

Fenixz - October 6, 2017, 12:51 pm

Bro i think it's might to help you..

Edit : I can't post links go to google > "ms08_067_netapi" and first one site "rapid7".
check the "Targets".

Nomad.Null - October 6, 2017, 12:51 pm

(Oct 6, 2017 12:49 PM)Kevin_1998 Wrote: [\[CITE\]](#) You mean .. eternalblue ?

Yes, but it won't work on a fully patched version of Windows 10. If it does, you'd better update that bitch before you contract internet AIDS.

Kevin_1998 - October 6, 2017, 12:56 pm

(Oct 6, 2017 12:49 PM)True Demon Wrote: [\[CITE\]](#) No matching target corresponds to the TARGET setting which refers to the OS, architecture and version. If an exploit is not built for the OS you are targeting, you will receive this error. MS08-067 was patched after Windows XP SP3 and has rarely been seen since, which is why you are getting this error.

You need to understand the concept of fingerprinting which is the process of scanning targets to identify their OS version and architecture. Tools like Nmap are commonly used for this. The nmap -O <target_ip> is the switch specifically used for identifying the OS.

When and if Nmap is able to determine the host operating system, you can begin searching for exploits in that version. But you are not likely to have much luck on a fully patched version of Windows 10. Try practicing on a Windows XP or 7 virtual machine to get the hang of it, or try a Capture the Flag site like hackthebox.eu.

If you don't know shit about using metasploit, you should be reading books on the subject. I suggest Mastering Metasploit.

Hey there ! I'm reading your book these days ...

But I have simple doubt , is there any necessity to become MASTER(and yes I mean it !) in programming language to learn hacking .. I mean having a sufficient knowledge about programming language is sufficient or not for learning networking and hacking ?

Nomad.Null - October 6, 2017, 10:13 pm

(Oct 6, 2017 12:56 PM)Kevin_1998 Wrote: [\[CITE\]](#) Hey there ! I'm reading your book these days ...

But I have simple doubt , is there any necessity to become MASTER(and yes I mean it !) in programming language to learn hacking .. I mean having a sufficient knowledge about programming language is sufficient or not for learning networking and hacking ?

Let me clarify... "Mastering Metasploit" is the title of a book.

<https://www.amazon.com/Mastering-Metasploit-Nipun-Jaswal/dp/1782162224?SubscriptionId=AKIAJLSHYTFIVPWUY6Q&tag=duckduckgo-d-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1782162224>

And no, it is not necessary to "master" a programming language. In fact, I'm not very good at it myself. I make quick and dirty scripts, and my exploit code looks like total shit. I do not follow coding best-practices, and I have never made a fully functional, stand-alone application on my own. I'm by no means a masterful or even a decent/functional programmer, but I can make my code work, and I know how to google better than the average bear. I can hack things together and make it work or break it if I want to.

Pick a language or two, get decent with it/them, and use them when you need them. Truth be told, there's no such thing as becoming a "master" of a language. Remember, programming is basically problem-solving. You can always come up with clever and creative ways to solve problems with code. Certain languages are better suited to solving certain problems. Being creative and persistent are often more valuable in this case than being a good programmer. ?

Kevin_1998 - October 6, 2017, 11:22 pm

@ True Demon

I am telling about your book "The hacker's ethos " the experience till now is awesome ...

How do we get reputed here ?

Which are the best site to learn hacking stuff according to you ?

Nomad.Null - October 7, 2017, 11:56 am

Reputed? Generally, if you want respect in the community you have to contribute. You can do it in different ways like writing tutorials and guides or building tools and scripts, but it all comes from putting effort into your research and sharing your findings with the public. It's not exactly a science.

There is no "best site" to learn hacking. You have to draw knowledge from different sources and perform research on your own. There are plenty of sites, books and blogs that focus on certain topics like programming, web app security, buffer overflow and memory exploitation, application security, and tons of other things. If you want, I can give you a list of sites I recommend for these sorts of things.

hackthebox.eu - CTF site for practice attacking web and network services

vulnhub.com - Site containing vulnerable Virtual Machines for personal security labs

youtube.com - Just in general, youtube has a lot of video tutorials for all kinds of things. If you have a question, someone probably has an answer on video.

corelan.be - Corelan is dedicated to the study and development of Windows and application exploitation, and also developed Mona for Immunity Debugger.

www.cybrary.it - FREE online courses for IT, networking, and security skills, including hacking and programming courses

pluralsight - PAID online tutorial site for learning IT skills.

lynda.com - PAID online tutorial site maintained by LinkedIn.com & Microsoft. Course completion is reflected in your LinkedIn profile, which is good for job seekers.

gentilkiwi.com - Blog by the developer of the Mimikatz tool. Lots of cool tutorials and information about Windows privilege escalation and post exploitation here.

fuzzysecurity.com - Active blog containing hacking tutorials, scripting guides, tips, tricks, and tutorials for exploitation.

warroom.securestate.com - Blog by the SecureState security company with tutorials and information constantly being added by their penetration tester staff.

blog.rapid7.com - Blog by Rapid7 security company with info constantly being added. They also actively maintain the Metasploit Framework.

FireEye.com/blog - Blog by FireEye which usually contains information about latest breaches and zero-day exploits discovered in the wild. Mostly good for hacking news.

#.com - Yeah, Krebs might be kind of a jerk, but he puts out good info, so I'm including him here.

^ Lol, I love the censorship here

Kevin_1998 - October 7, 2017, 12:42 pm

@True Demon

Thank you so much buddy ..

Did the blueborne exploit release if yes how can I get it .. I wan't to do it practically

SIM-1456221 - October 7, 2017, 3:13 pm

(Oct 6, 2017 12:49 PM)Kevin_1998 Wrote: [\[CITE\]](#) You mean .. eternalblue ?
ye lmao that one. try that one.