

Forum: [Hack Forums](#)

Thread: [Metasploit exploit error](#)

Adam2017 - August 13, 2018, 2:03 pm

Hi guys I downloaded a ruby script from exploit-db.com and copied into the exploits folder of metasploit, hoping the exploit would work but I get this error message "Exploit aborted due to failure : unknown: 501 5.1.7 Bad sender address syntax "

I set the RHOST to my target metasploitable machine on my virtual network and set the MAILTO field to my email

but as above when I run the exploit I get that error,

any idea what I could be doing wrong?

thanks

lurking - August 13, 2018, 2:07 pm

I'm pretty sure that's an SMTP issue? What is the goal of the script you are trying to execute & what does it abuse/use to gain you whatever (access, information, etc).

CyberStrike - August 13, 2018, 2:22 pm

Generally 500 errors in SMTP are email filter issues or a bad sender address. For example you send an executable to an email address most corporate IDS will catch that type of attachment.

fire_w1re - August 13, 2018, 5:29 pm

What module are you running exactly??

Adam2017 - August 14, 2018, 5:31 am

thanks guys for the replies,

and yes I should have mentioned it is an smtp exploit

Exim < 4.90.1 - 'base64d' Remote Code Execution by straight blast

here is a description of the attack

According to its banner, the version of Exim running on the remote host is prior to 4.90.1. It is, therefore, potentially affected by a buffer overflow vulnerability. A flaw exists base64d() function due to improper validation of parsed messages. A remote attacker could potentially cause a buffer overflow condition and execute arbitrary code.

I did a port scan on my metasploitable machine to find out that prt 25 SMTP was open on it