

Forum:[Hack Forums](#)

Thread: [MetaSploit mysql_hashdump auxiliary](#)

7_R3X - June 9, 2017, 12:25 am

First off, I'm new to metasploit. That being said lets get to the problem.

There's an auxiliary scanner in metasploit for mysql. Upon Code show info it does not specifies any particular version for which it'd work, so I assume that it works for all the mysql versions(Assumption 1). A simple nmap port scan shows that there is definitely a mysql running on it's default port 3306.

Code Nmap scan report for ba.1f.be.static.xlhost.com (209.***.**.*)

Host is up (0.28s latency).

Not shown: 9992 filtered ports

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1433/tcp open ms-sql-s

[b]3306/tcp open mysql[b]

3389/tcp open ms-wbt-server

8080/tcp open http-proxy

Since Nmap can scan it, I assume that there's no firewall blocking it.(Assumption 2)

I set the target RHOST and tried to exploit it. I got an "Access Denied" message:

Code msf auxiliary(mysql_hashdump) > exploit

[-] 209.190.31.186:3306 - Access denied

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Please tell me what could be the reason for this "Access Denied" message. Also tell me if any of my assumptions are wrong. Metasploit seems interesting and I want to learn more about it.

hempuk - June 9, 2017, 5:39 am

hi 7_R3X

i just wanna say if you have taken the time to hash out the ip address you need to also hash out the dns name aswell.

As to why your getting Access denied this means that you dont have access to the database to run that module.

maybe try something like hydra and try bruteforcing the password or even try bruteforcing the RDP port as i bet the password is the same for both.

also try running your nmap scan with a -A as it gave me some reall jucy info...

7_R3X - June 9, 2017, 7:00 am

(Jun 9, 2017 05:39 AM)hempuk Wrote: [\[CITE\]](#) hi 7_R3X

i just wanna say if you have taken the time to hash out the ip address you need to also hash out the dns name aswell.

As to why your getting Access denied this means that you dont have access to the database to run that module.

maybe try something like hydra and try bruteforcing the password or even try bruteforcing the RDP port as i bet the password is the same for both.

also try running your nmap scan with a -A as it gave me some reall jucy info...
As for DNS name, it was resolved by nmap and is not the real DNS name so I didn't hash it out.
And thanks for the answer. I didn't know about -A parameter in nmap.

Privitespoof - June 9, 2017, 7:17 am
posting to check back later...

Nomad.Null - June 9, 2017, 9:22 am
slams head on desk
And they have port 445 exposed externally... what the fuck...

The-hunter22 - June 9, 2017, 10:29 am
(Jun 9, 2017 09:22 AM)True Demon Wrote: [CITE](#) *slams head on desk*
And they have port 445 exposed externally... what the fuck...
I have seen alot of this. Why is this bad?

7_R3X - June 9, 2017, 11:14 pm
Can anyone check if any of my assumption in the original post is wrong? I'd also like to know more about how to determine which exploit to use? For example, the port 80 here has http running. There are hundreds of exploits to chose from in metasploit on windows alone. Is it completely hit and trial? Or do I need to enumerate the target more to cut my list short? And if so, how do I go about doing that? Nmap, upon service scan (-sV), couldn't find if it's Apache or some other http service. So how do I get more information out of the system? Do we have more tools I need to learn about? And not just about http service, these questions goes for all the services running on this system and the systems I'll scan in the future!!!! How do you deal with all this? More importantly, how did you learn to deal with all this? What resources did you learn from?