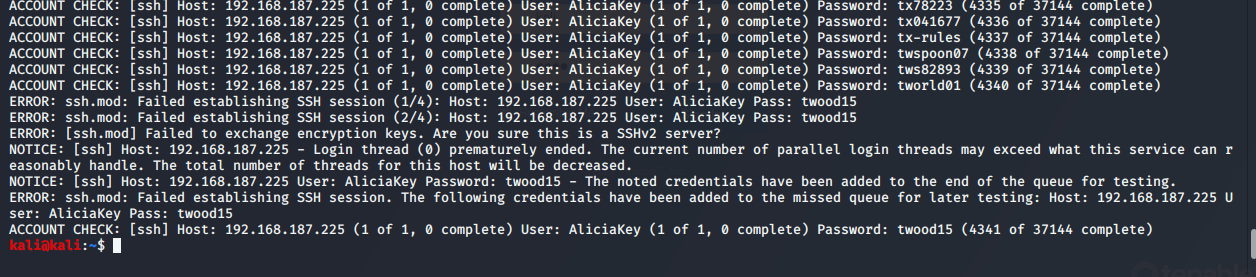
Task 1:

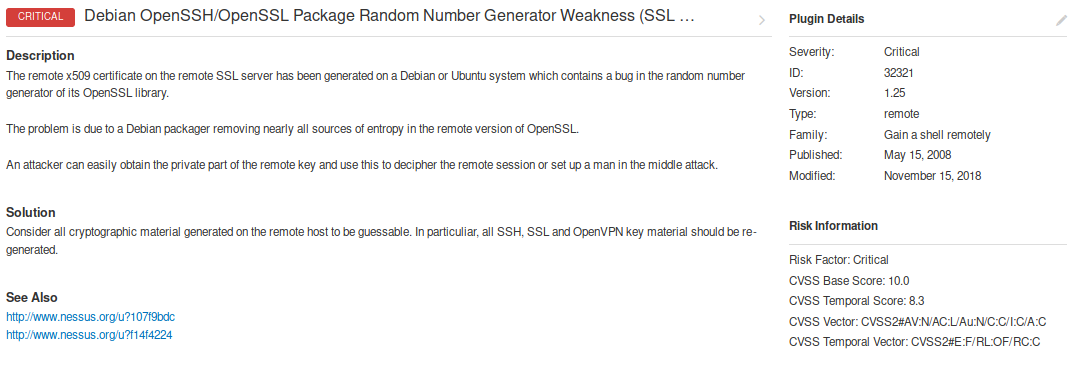
Looking at the IP 192.168.187.225, we can see that some of the potential targets that we can try to attack with a dictionary attack using medusa, hydra or ncrack are port 22/tcp/ssh, 5432/tcp/postgresql and 25/tcp/smtp.I have decided to go for the ssh service on port 22.

During my attack, I first used medusa to try and get the password for the username “AliciaKey.” The result was far from satisfactory as I would continuously get false positives, for example my first run got me “password1” taking mere seconds of my time, but the second run took 2.5 hours getting “twood15” with the following errors(below). With similar results on the user “pjcrowley”

I then proceeded to use ncrack which took 4 hours to get through the dictionary but came up with the password “RHcp123!!!”

The duration of this type of attack is very long but as long as you have a great dictionary it is a decent method.

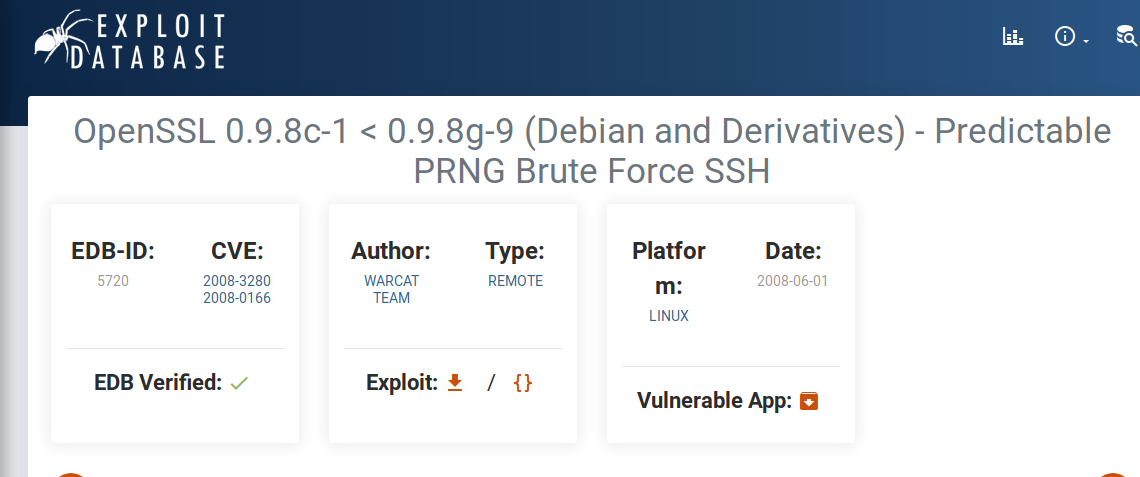
Task 2:

Chosen vulnerability: 

CVE#: CVE-2008-0166

Impact: This vulnerability allows for the attacker to get the key certification of the network due to a bug in the OpenSSL library. Getting the key would allow the attacker to use the man in the middle attack by acting as the server that a user is trying to connect to. With the key in hand, the server will not know any better if it is connected to the right server. It will believe that it is indeed connected to the right one.

Exploit on exploit-db: <https://www.exploit-db.com/exploits/5720>



Exploit on metasploit:



Since I can not find the exploit on metasploit I will focus on the one on exploit-db.

The exploit is done by searching through the files and looking for the key. As soon as it finds the key, it will tell the user and will execute and say something similar to: ssh -lroot -p22 -i /file\_path/file IP\_Address. And from there you can use it to attack the user and gain more information if necessary.