Metasploitable 2 downloaded.

Installed

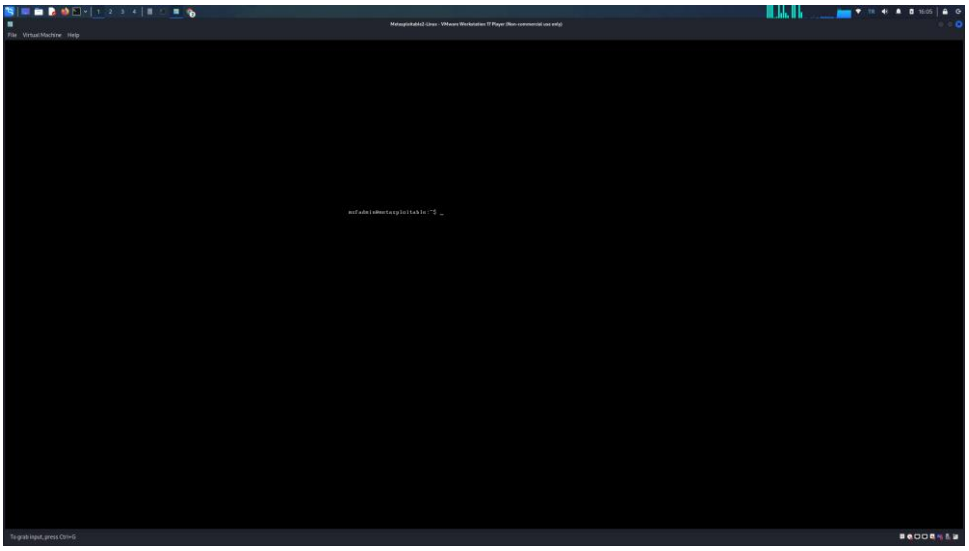
Metasploitable was downloaded directly from the following website. The vmware image was opened with a vmware virtual machine. Completed the installation from within.

To log in

username: msfadmin

password : msfadmin

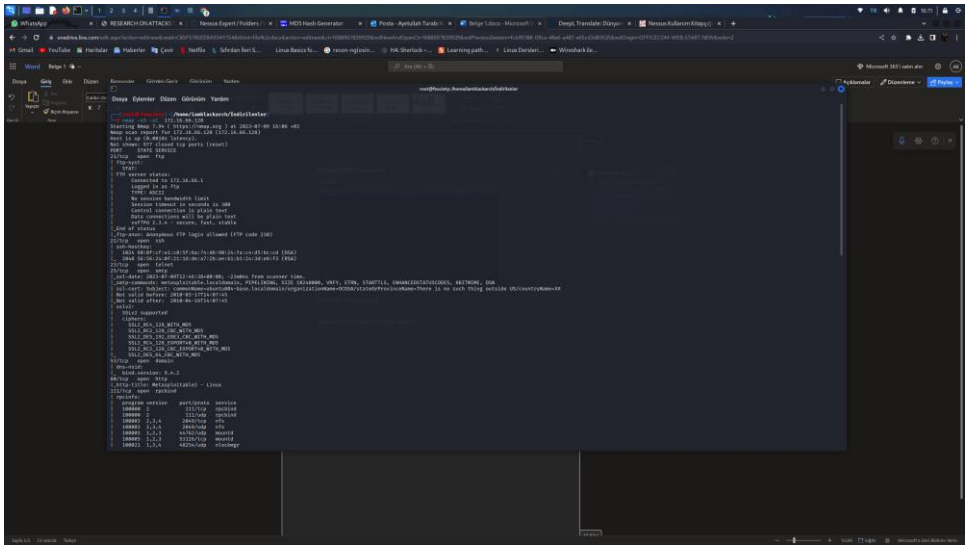
The terminal screen opened.

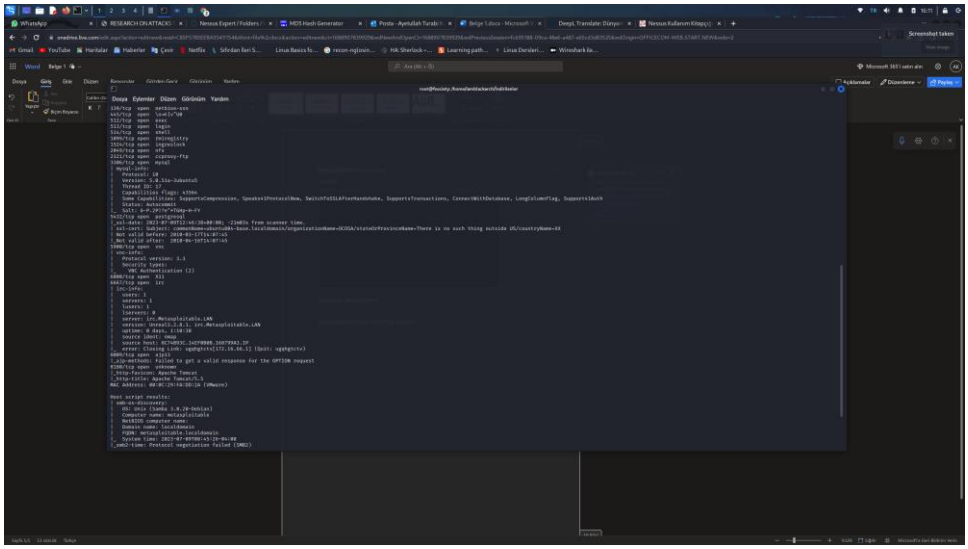


The ipv4 address was obtained with the ifconfig command and the nmap scan was started.

Nmap scan was performed.

A scan was performed with nmap using the -sS and -sC commands. open ports were detected. We started a scan that tells us which services are open on the open port.





nessus installation was performed. Opened.

Nessus Kurulum

https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{11596512905}-{118315026852}-{537515899088}_00026642_fy23&utm_promoter=tenable-hv-brand-00026642&utm_source=google&utm_term=nessus&utm_medium=cpc&utm_geo=emea&gclid=Cj0KCQjwtamlBhD3ARIsAARoaEwqI1S5a7JWtF59z-BkMs4uanGLVe9MqaV2YlWdQ08-rcrgwl4NhcsaAltvEALw_wcB

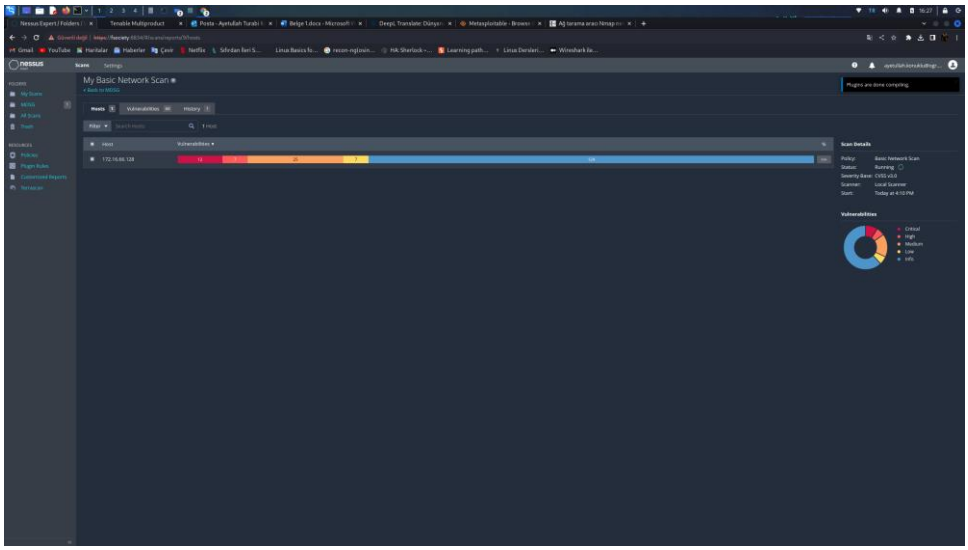
corporate identity is entered with the address. Then you register your student e-mail address. Nessus is downloaded with this mail address. You are authorized for the trial version.

The nessus server is started over the system. You can access the system with the name of your computer from the port assigned to you.

http://computerName:portnumber

The screen that opens will do the installations. And after the uploads are done, it will open a scan box for you. In the scan box, you can enter your IP address or your domain address and start the process.

We logged in with our IP address. And we are analyzing the detailed scan results.



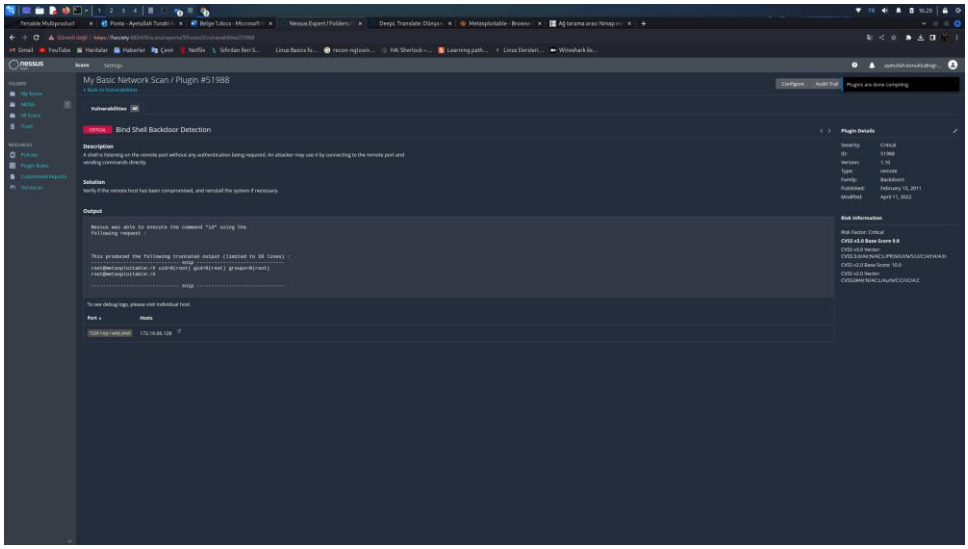
12 very high hazardous deficit

7 highly dangerous deficit

25 moderately dangerous open

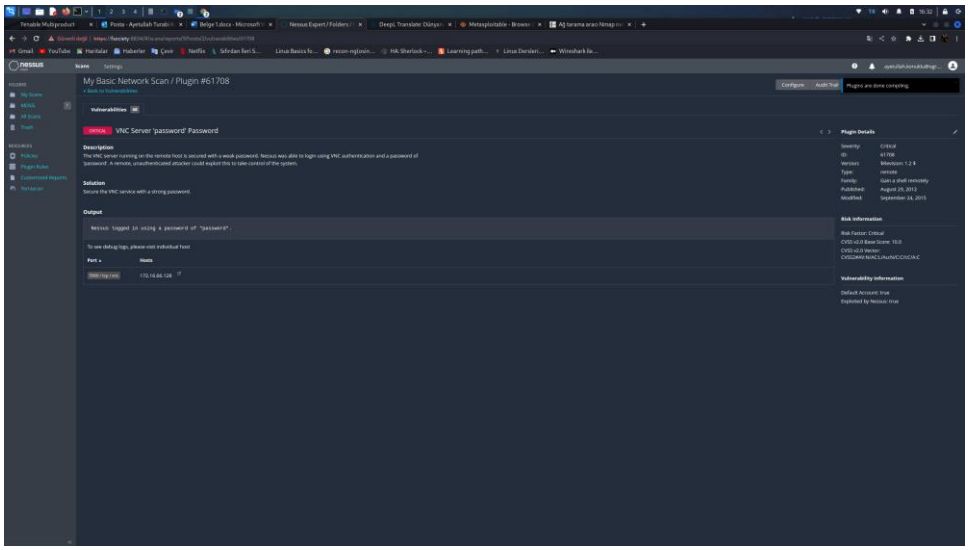
7 low hazardous deficit

Detected



This weakness is a back door.

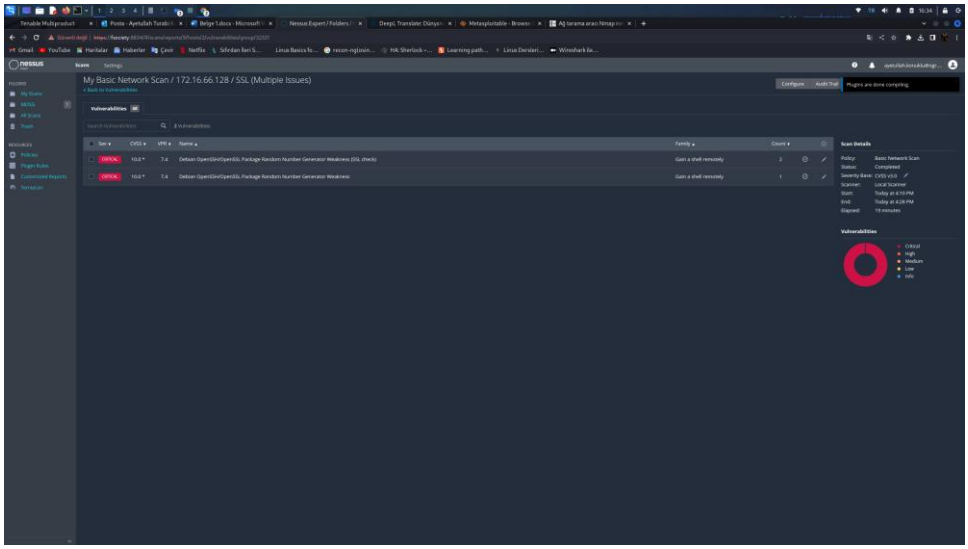
With it you can infiltrate the system, extract information from the system, inject information into the system and poison the system.



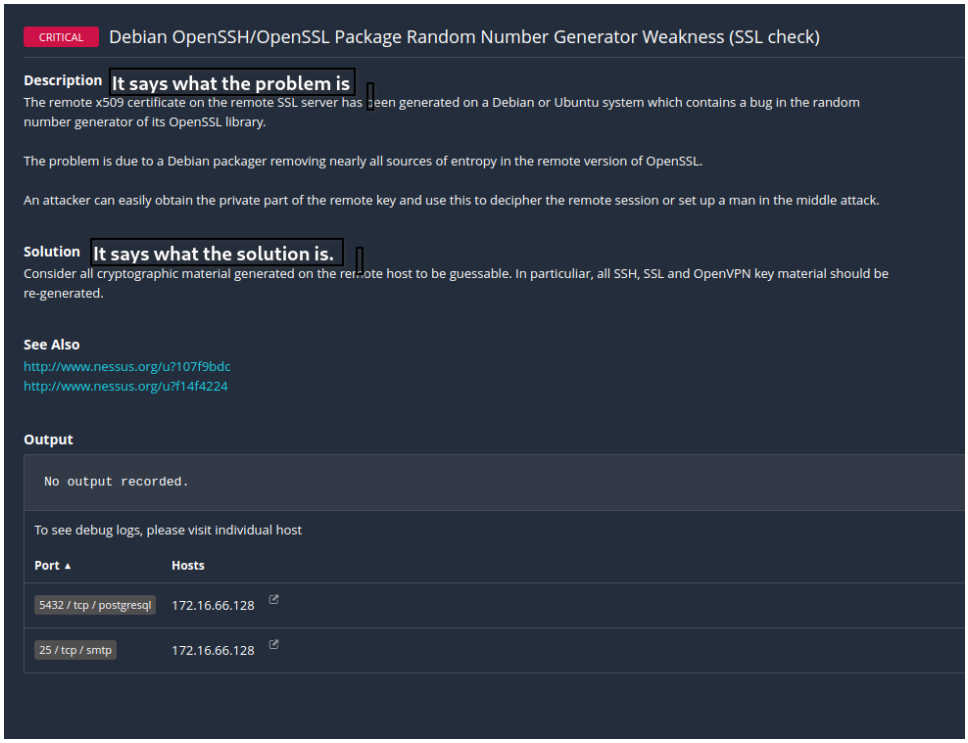
This vulnerability is an insecure password attempt.

Nessus says he logged into the system using the word PASSWORD. One more way to explain how insecure the system is. It's very simple to protect against this. You will need to create passwords that

are complex enough to be considered secure.



It mentions a basic ssl vulnerability. Since this ssl vulnerability is present in two different locations, there are two different types of vulnerabilities that are desired to be examined under the ssl heading.



When Nessus Vulnerabilities are examined one by one, it gives a detailed problem description and solution description. In this way, the user will see the weaknesses of their own website and will take action accordingly.

Overview :

By performing an nmap scan on the vulnerable machine, we have seen how many vulnerabilities are in the content of the machine. We have detailed these vulnerabilities in the same way through nessus and examined their data. With this data we had the chance to examine every stage necessary to infiltrate the system in the machine. We proposed to replace the "password" vulnerability, which is one of the critical vulnerabilities, with a strong password structure and we have carried out a study to make the system stronger in some way. In this way, we have closed a gap.

Source:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{11596512905}-{127200546844}-{537515852132}_00026642_fy23&utm_promoter=tenable-hv-brand-00026642&utm_source=google&utm_term=tenable&utm_medium=cpc&utm_geo=emea&gclid=Cj0KCQjwtamlBhD3ARIsAARoaExeY2F7JMvM64LEeOxlqoEc45Jt83M0OKb6kWddDnD90bLFqHCwMzoaAgZUEALw_wcB

https://siberbulten.com/teknik/ag-tarama-araci-nmap-nedir-nasil-kullanilir/