Information Assurance & Auditing
4th Year – 1st Semester

Assignment

Student Registration Number	Student Name with Initials
IT 17 0635 24	Wickramaarachchi P.M

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

8th May 2020

Declaration

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Table of Contents Page

List of Figures

List of Tables

1 Introduction

What is Windows Auditing?

Security can be considered as an increasing concern for every industry specially for information technology field. The security plan for computers should contain policies and procedures to verify the given access rights for users and there should be mechanisms to verify that given access rights have been deployed in an efficient and effective way [1]. Therefore, Windows auditing can be described as a way of gaining the information on the effectiveness of security practices and a way to track the events. Windows network forensics are helped by the information of particular events. Then the security issues can be detected easily [1].

Used Tools for Auditing Windows 7 Box

In order to do the vulnerability assessment for Windows 7 box, two types of tools have been used. They are,

- Nmap
- Nessus

Nmap

Nmap is a tool which is free and open source, can be used for vulnerability assessments and it is a network scanner. Hosts and computer network services can be discovered by using Nmap. There, the packets are sent, and the responses are analyzed. Host discovering, services discovering and detecting operating systems are some features of Nmap.

Four types of output formats are provided by Nmap and all interactive outputs are saved into a file.

- XML
- Normal
- Grepable
- Interactive

Nmap can be used in black hat hacking also. Unauthorized servers, unauthorized computers can be searched by system administrators by using Nmap tool.

Nessus

Nessus is developed by Tenable, as a proprietary vulnerability scanner. It can be described as a tool that used in vulnerability assessments and penetration testing. Non-enterprise users can get the Nessus tool for free and there are few options for enterprise usage [3].

- Tenable.io
- Nessus Agents
- Nessus Professional
- Nessus Manager

Benefits of using Nessus

- User friendly and policy creation can be done in a simple way
- Entire network can be scanned in a easy manner.
- More technologies can be scanned, and more vulnerabilities can be uncovered compared to other solutions.
- Unlimited assessment is provided for low price.
- Scanning is accurate.
- Latest threats can be prevented by plugins.
- Can be scaled safely.
- Can be migrated to tenable.io if vulnerabilities are getting increase.

2 Audit Scope

Audit check list for Windows 7 box

- Audit for Windows 7 has been conducted according to the following check list.
- Driver Improper Interaction with Windows Kernel Vulnerability
- Windows Fax Services Cover Page Editor Vulnerability
- Win32k Improper Message Handling Vulnerability
- Win32k.sys Elevation of Privilege Vulnerability
- Win32k Window Class Vulnerability
- Windows MFC Document Title Updating Buffer Overflow Vulnerability
- GDI Access Violation Vulnerability
- Windows OLE Remote Code Execution Vulnerability
- Insecure Library Loading Vulnerability
- Directory Traversal Elevation of Privilege Vulnerability

3 Auditing Windows 7 Box Using Nmap and Nessus

Create two virtual machines using OracleVM VirtualBox software.

- Windows 7 virtual machine
- Kali Linux virtual machine

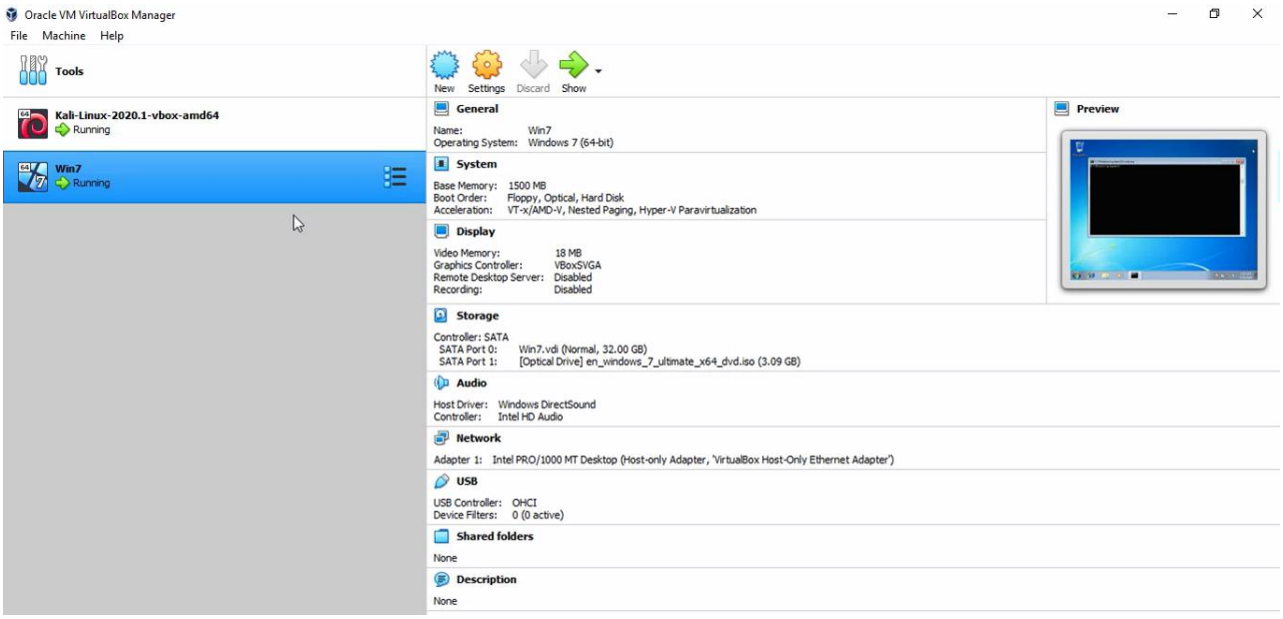

Figure 3.1:Create two virtual machines using OracleVM VirtualBox

Connect two virtual machines for a same network.

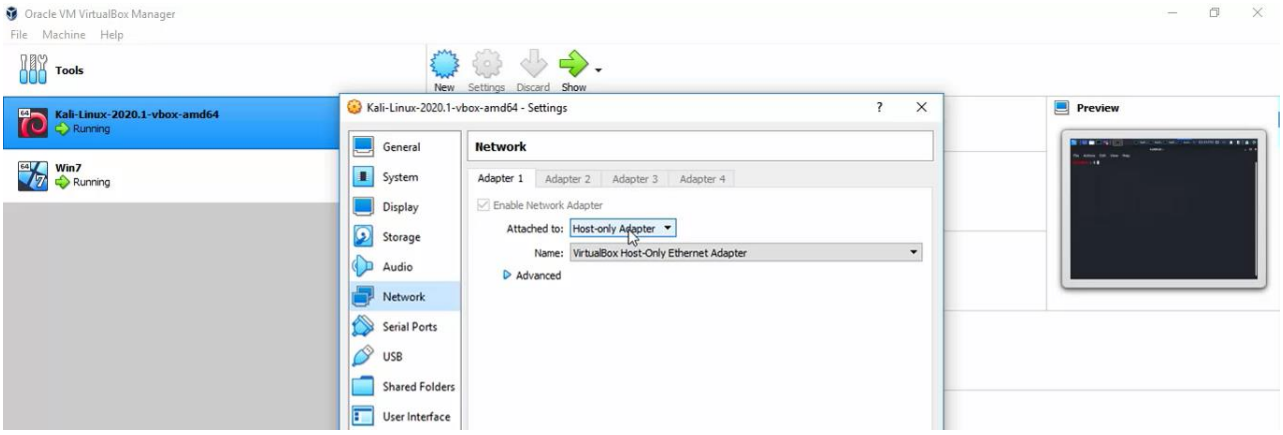

Figure 3.2:Connecting Kali Linux VM to Host-only Adapter

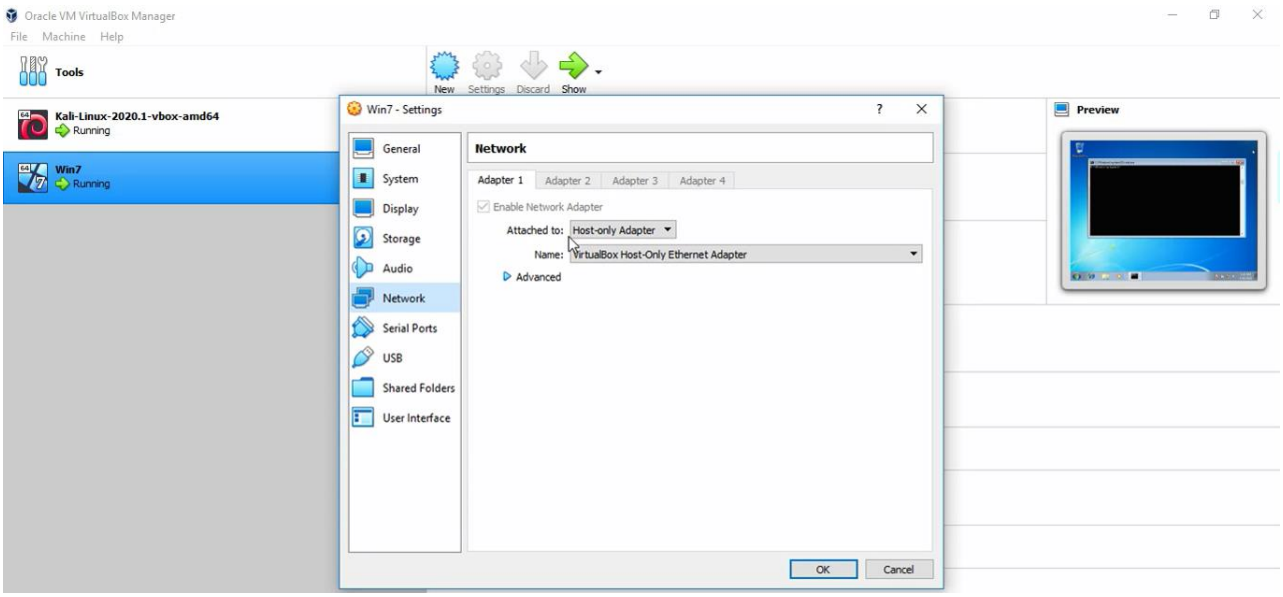

Figure 3.3:Connecting Windows 7 VM to Host-only Adapter

Then find the IP address of Windows 7 virtual machine using “ipconfig” command.

IP address of Windows 7 VM is 192.168.56.101, as shown in following figure and this is the target of our vulnerability assessment.

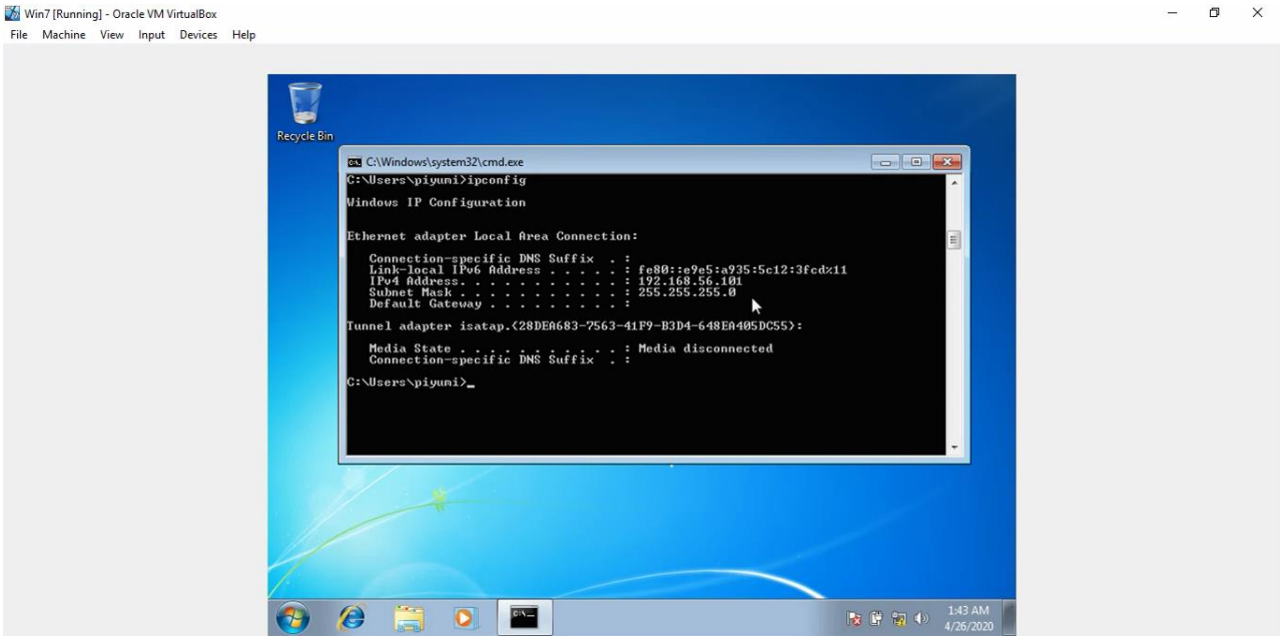

Figure 3.4:Finding the IP address of target

Check the connectivity between two virtual machines. For that we have to ping from Kali Linux virtual machine to Windows 7 virtual machine using below command.

ping 192.168.56.101

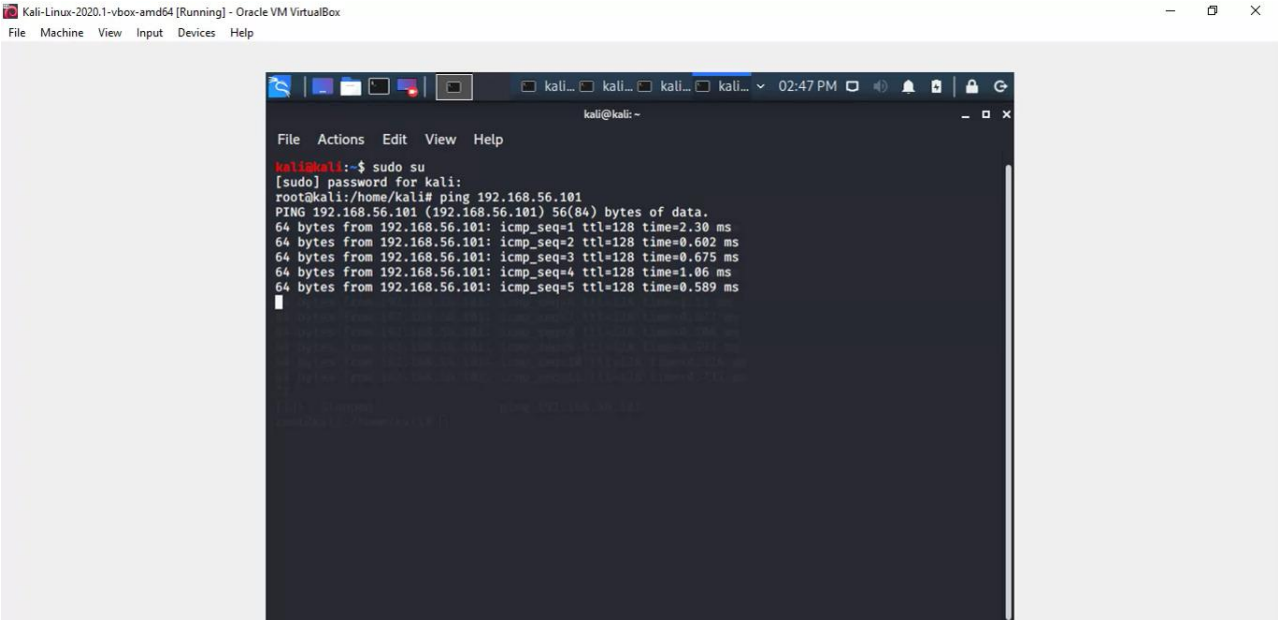

Figure 3.5:Ping from Kali Linux VM to target

Then issue the command “nmap”. Then it all the commands will be listed down that can be used under nmap.

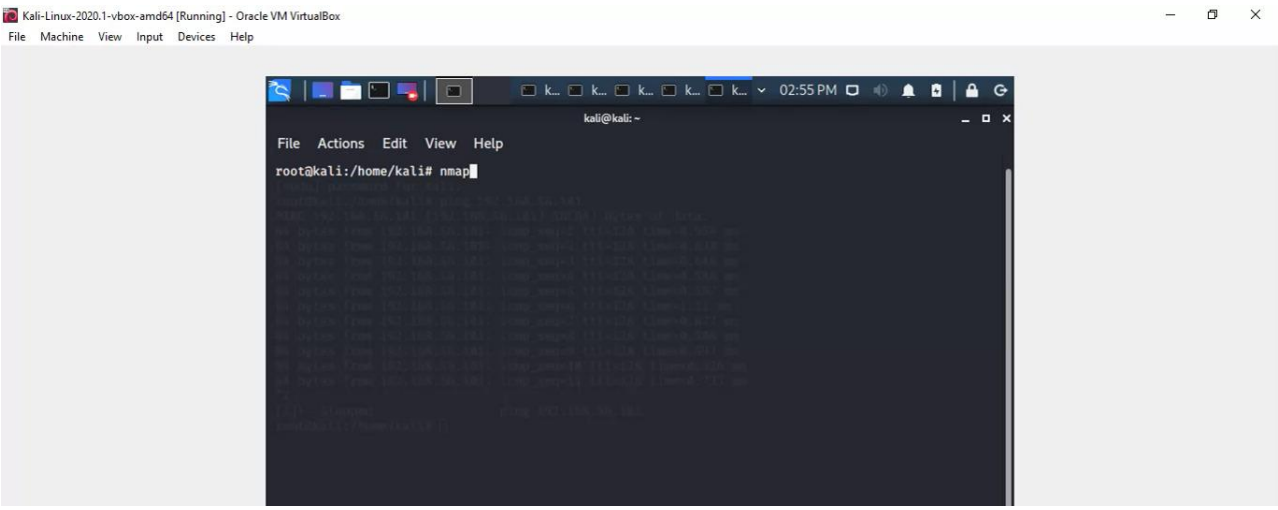

Figure 3.6:Issuing “nmap” comand

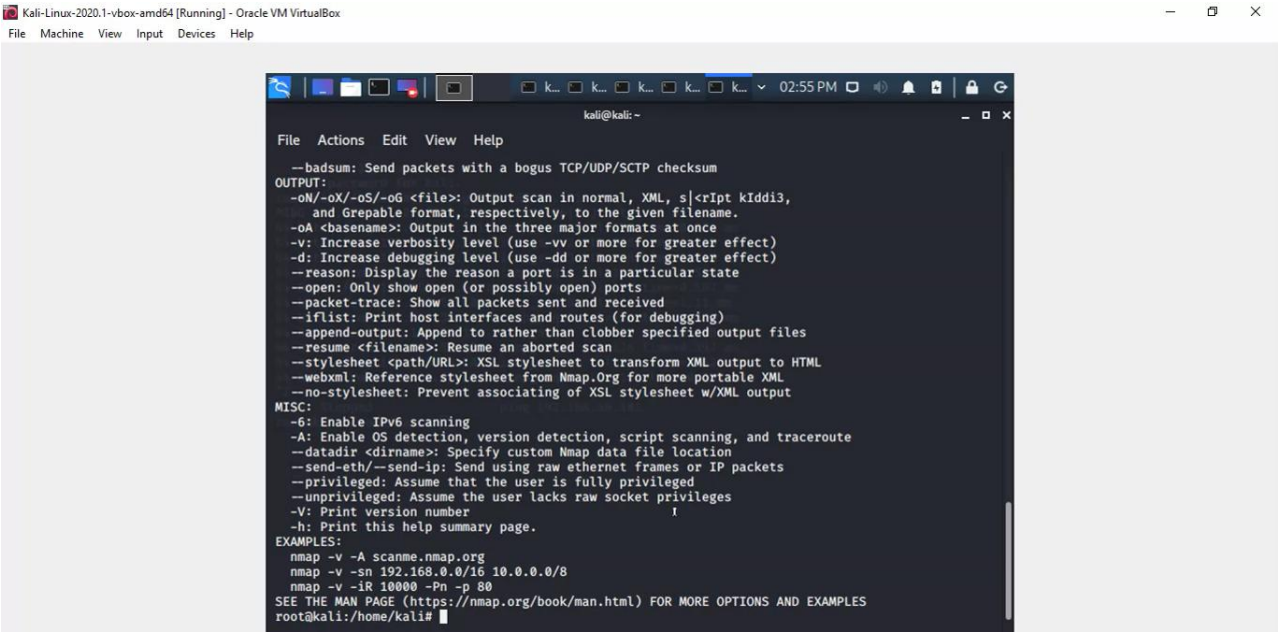

Figure 3.7:Listing down all the available commands under nmap

Then issue the command “ifconfig” to get the IP address of Kali Linux virtual machine.

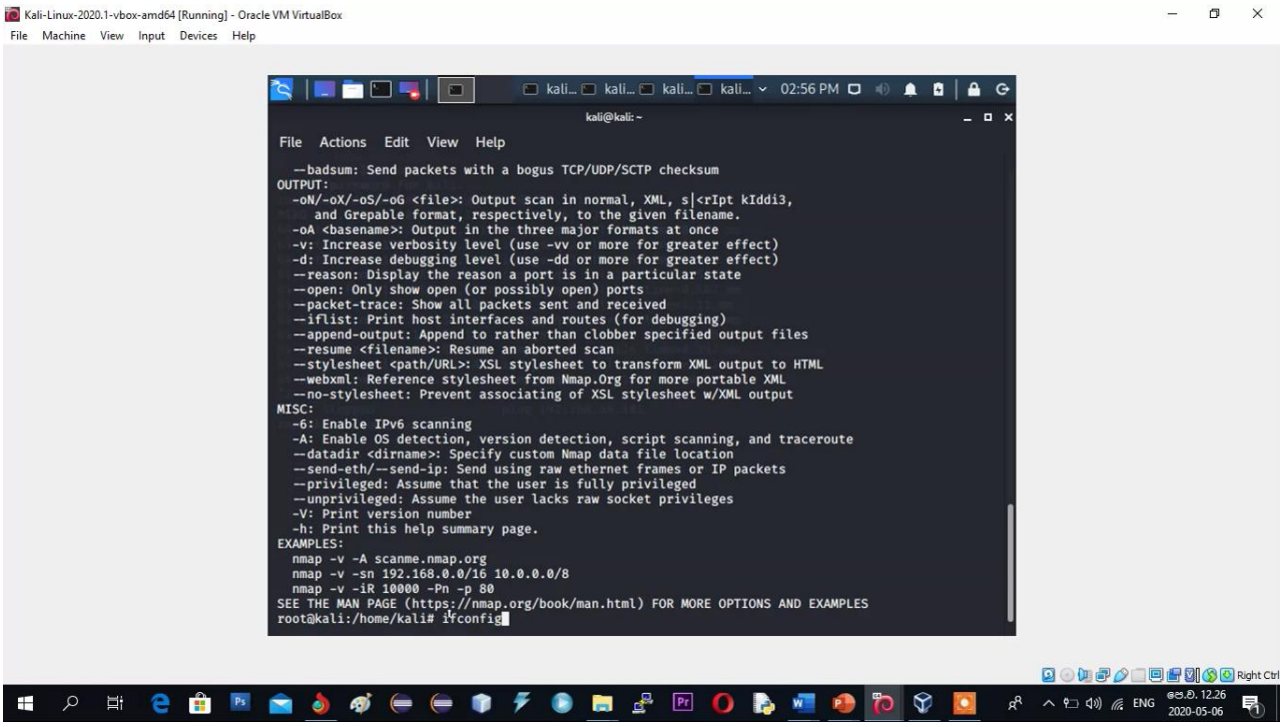

Figure 3.8:Getting the IP address of Kali Linux VM

Then we have to get the IP address of the hosts that are connected to the Kali Linux VM machine.

For that issue the following comand.

nmap -sP 192.168.56.102

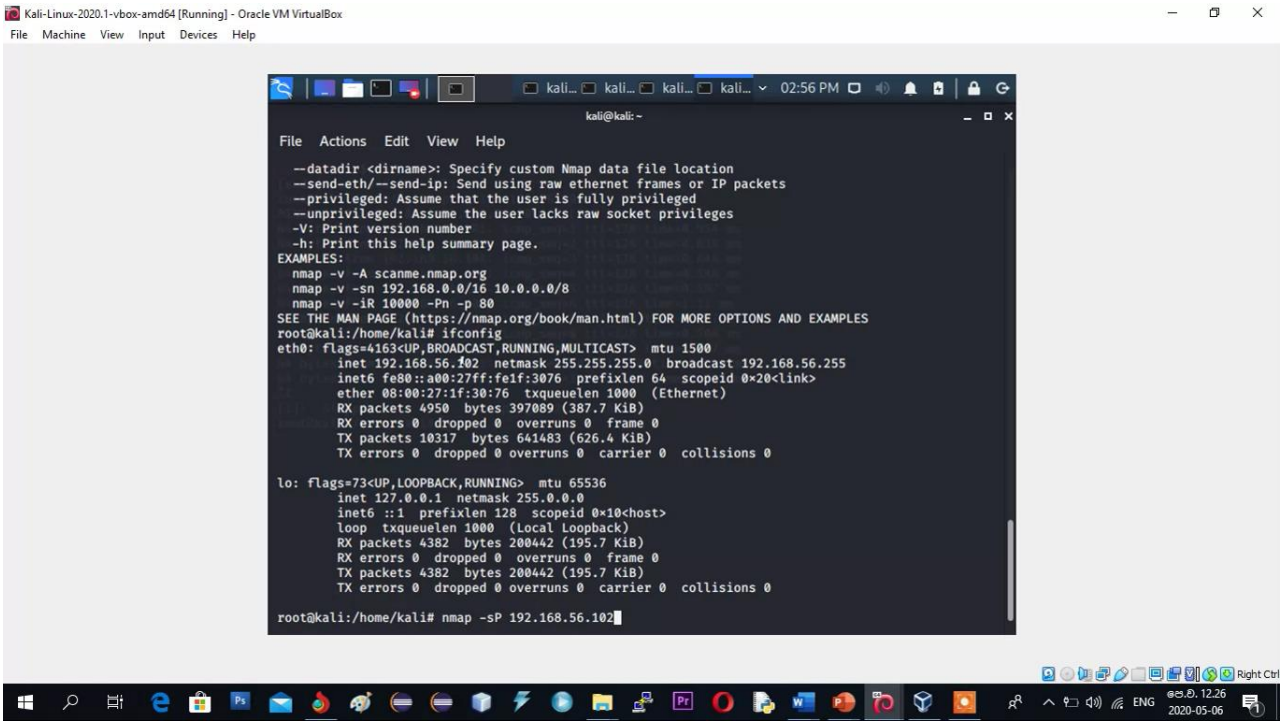

Figure 3.9:Getting the IP addresses of hosts that are connected to the Kali VM

In order to get the information about the TCP ports, issue the below command with the IP address of target, on the terminal. Then it will list down information on TCP ports as mentioned in following figure.

nmap -sS 192.168.56.101

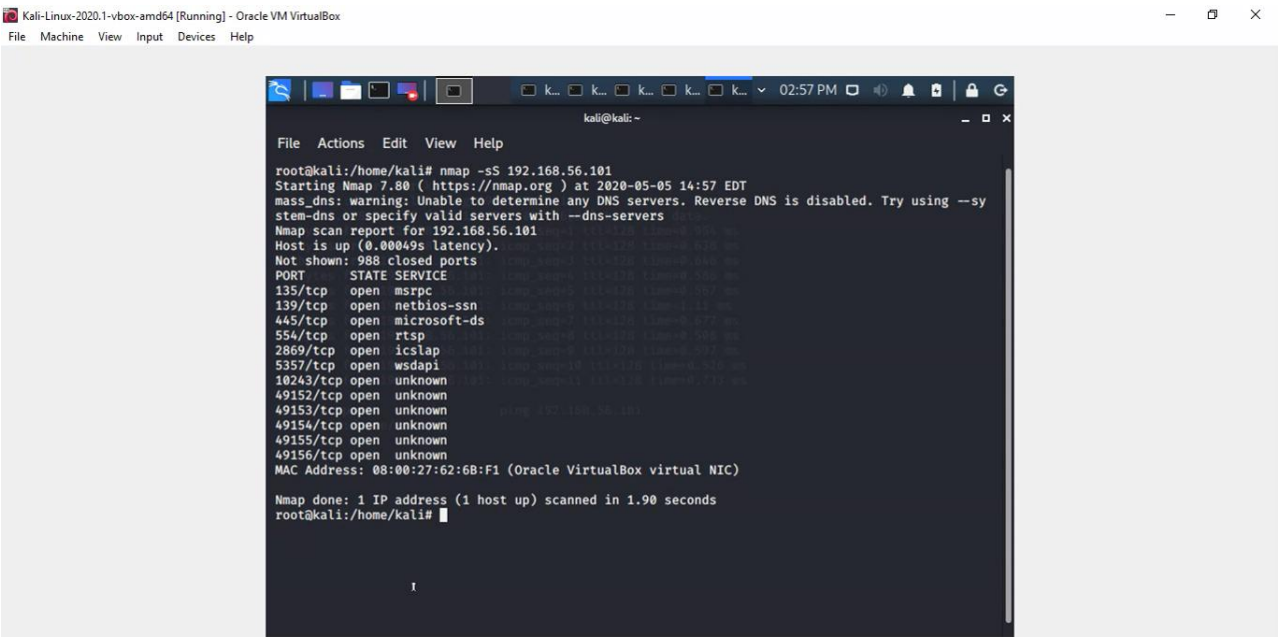

Figure 3.10:Getting information on TCP ports

In order to get the information on UDP ports that are available, issue the following command.

nmap -sU 192.168.56.101

Then it will not display the information until some time as shown in following figure. It happens because, when we issue the abovecommand, it will check for all the available UDP ports.

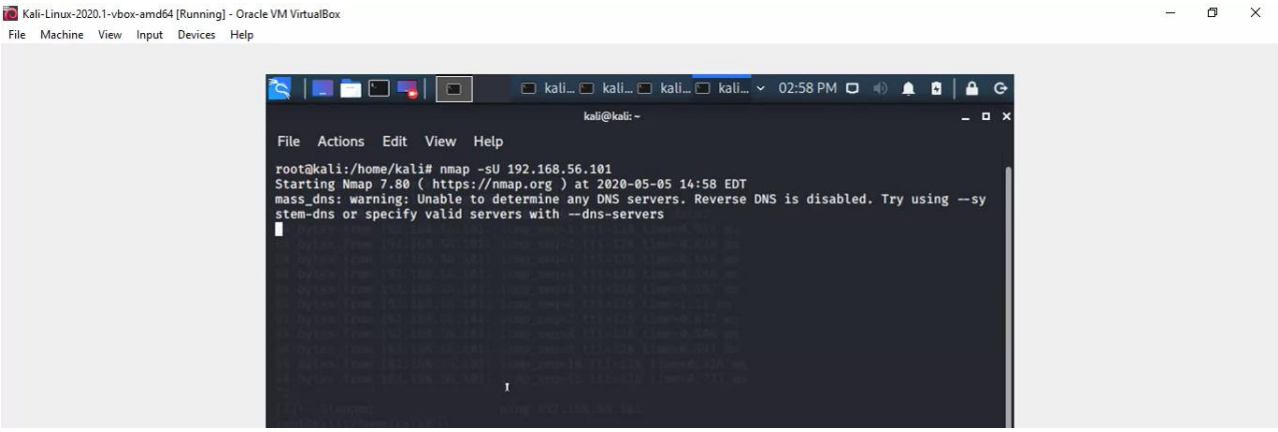

Figure 3.11:Checking for all available UDP ports

Issue the following command to get the information on required UDP ports only.

nmap -sU -p U:130-140 192.168.56.101

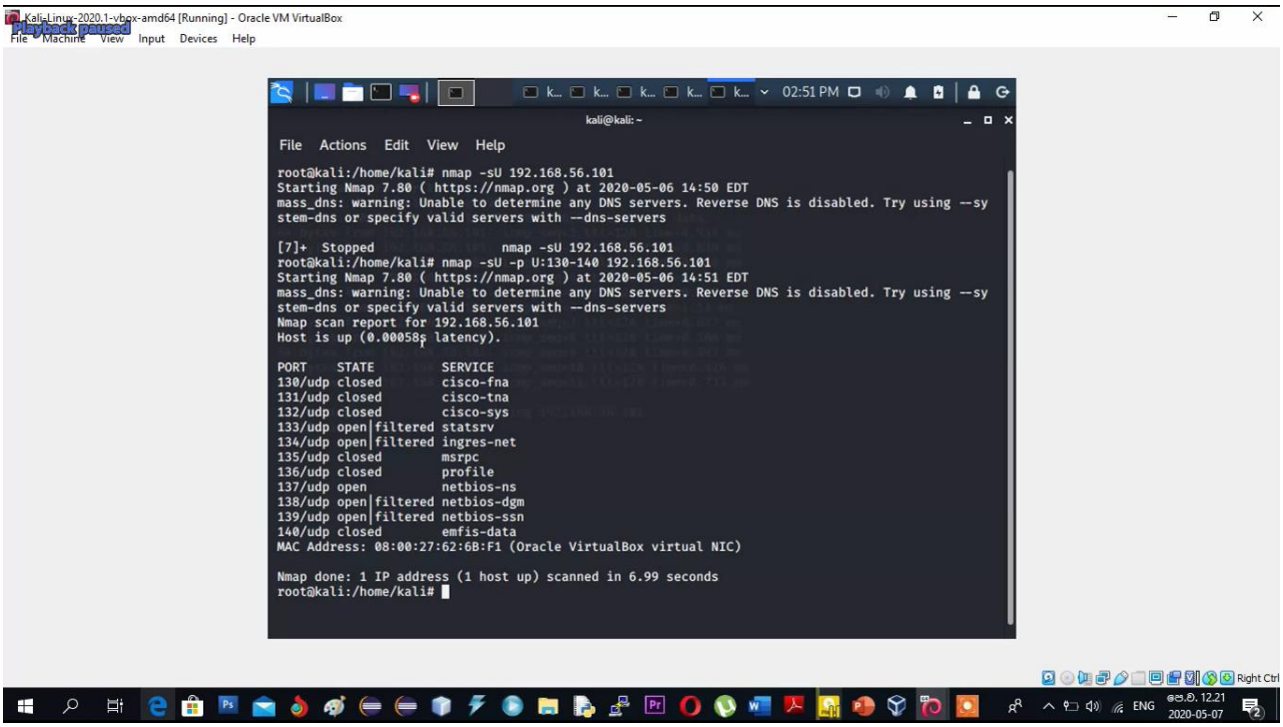

Figure 3.12:Listing down the information about UDP ports.

Now we have gathered all the information using nmap.

4 Vulnerability Scanning Using Nessus

Open a web browser in Kali Linux virtual machine and give https://localhost:8834 on the terminal. Then you will be redirected to a page as shown in following figure and it is a Graphical User Interface of Nessus.

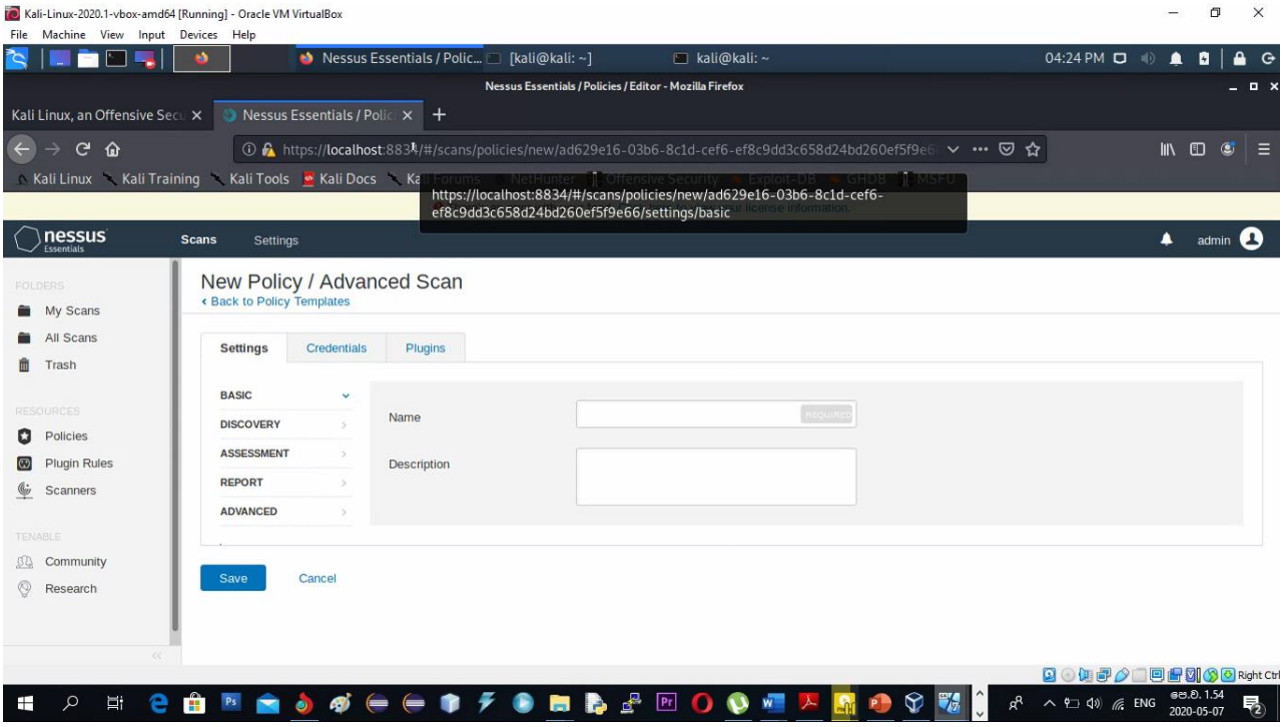

Figure 4.1:GUI of Nessus

Then the GUI of Nessus will be displayed as shown in following figures. Click on “Policies” and it will allow you to create a new policy and display the predefined policies.

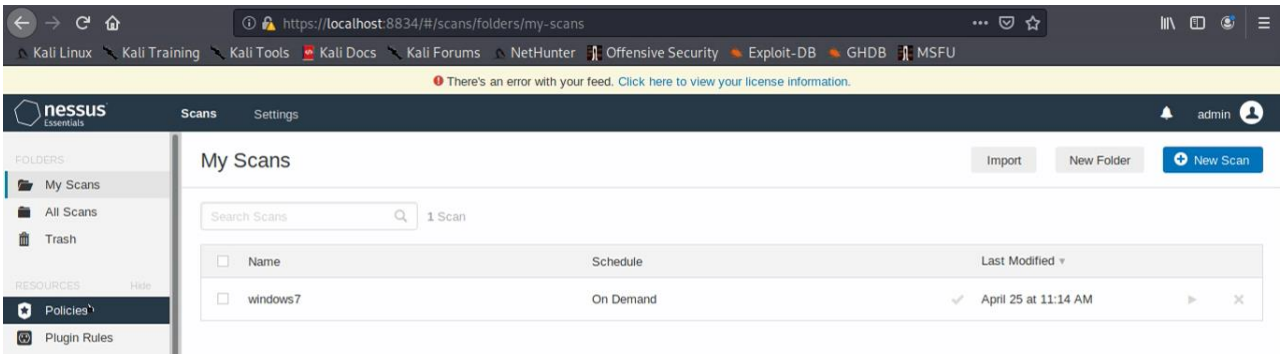

Figure 4.2:Displaying predefined policies

Then click on “Plugin Rules” and then it will allow you to set plugin rules.

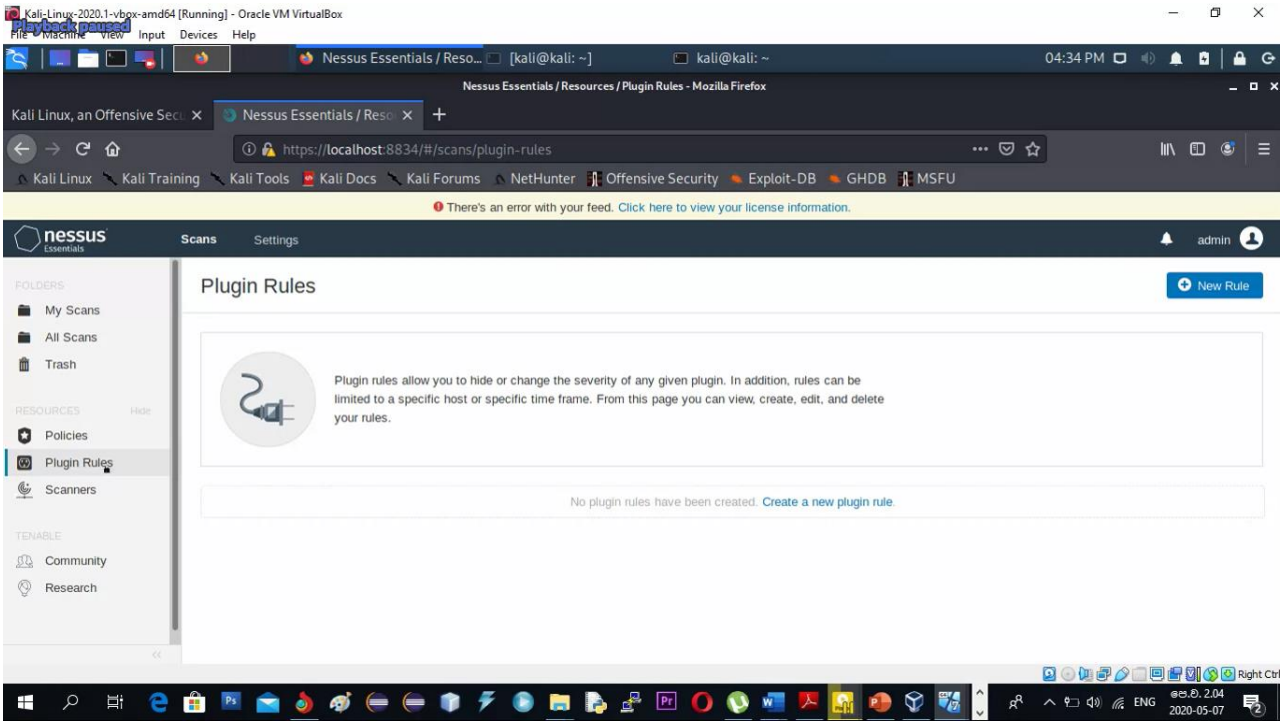

Figure 4.3:Setting plugin rules

Then click on “Scanners” and then it will display the Local Scanner. The status of Local Scanner should be online at every time.

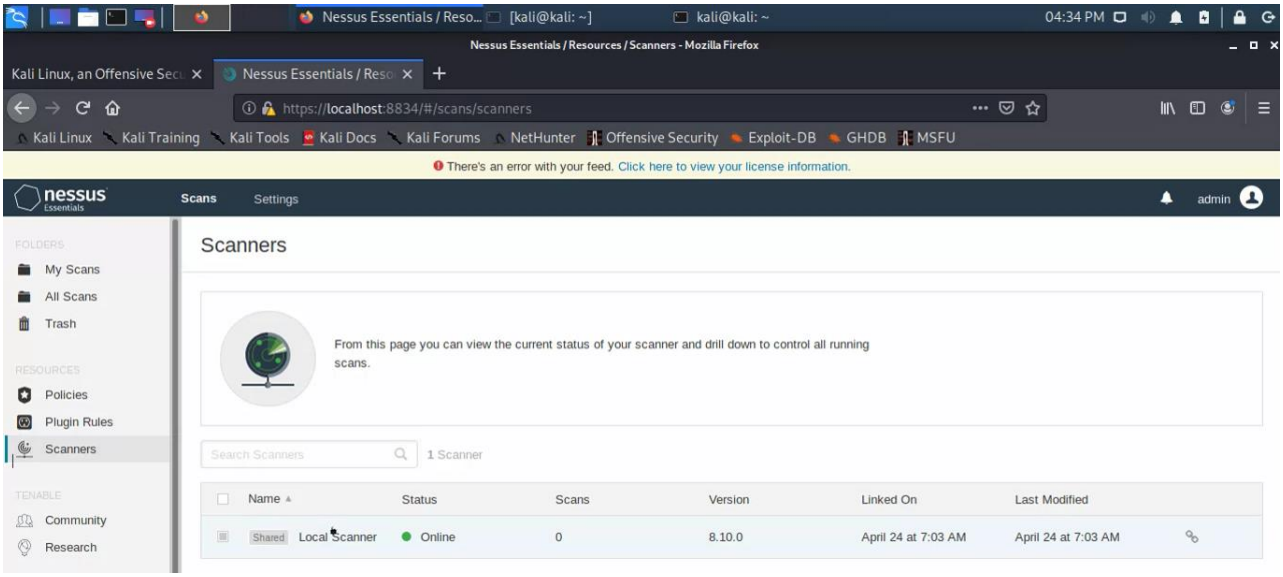

Figure 4.4:Setting scanners

Before starting the vulnerability scanning a new policy should be created. Click on “Policies” and then on “New Policy”.

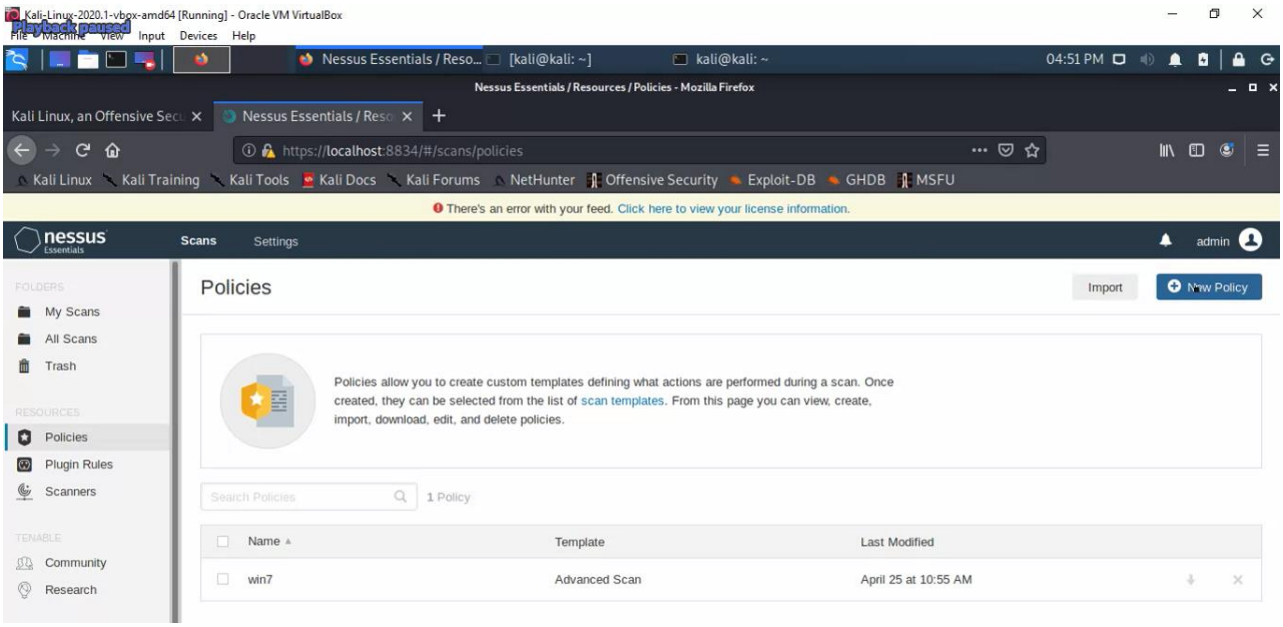

Figure 4.5:Creating a new policy

Then it will show all the options available and then click on “Advanced Scan”.

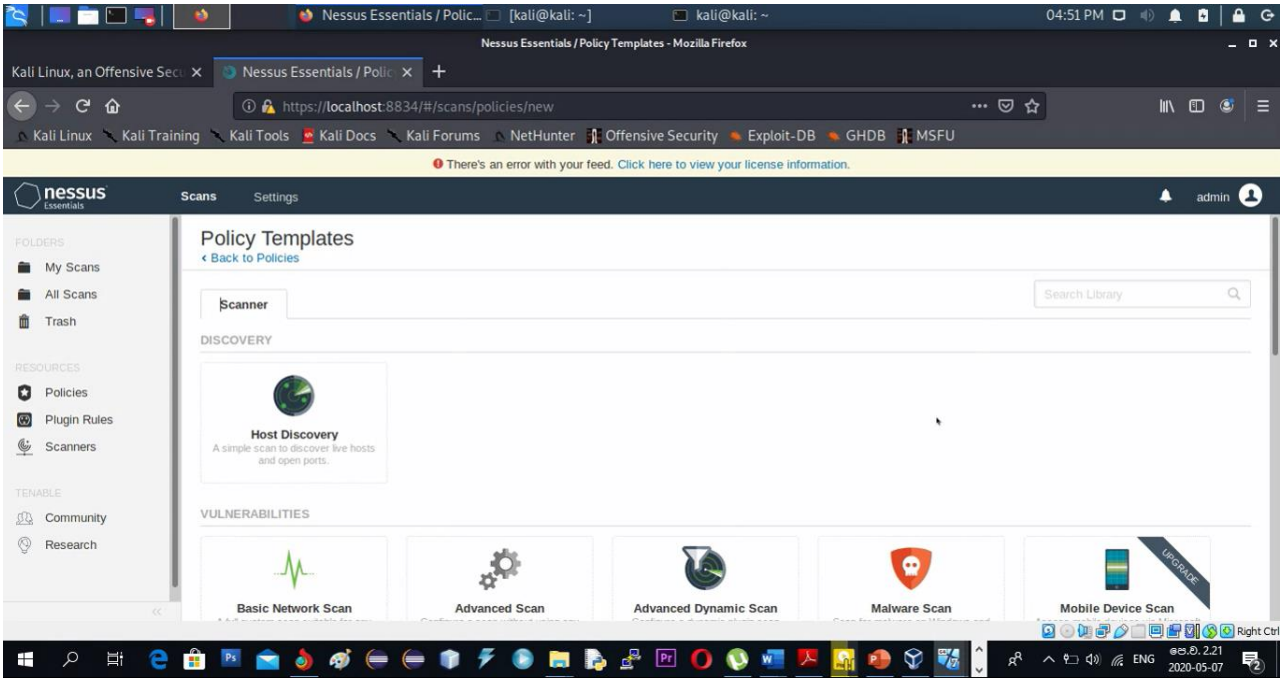

Figure 4.6:Creating a policy for Advanced Scan

Then it will display “Settings”, “Credentials” and “Plugins” as shown in following figure.

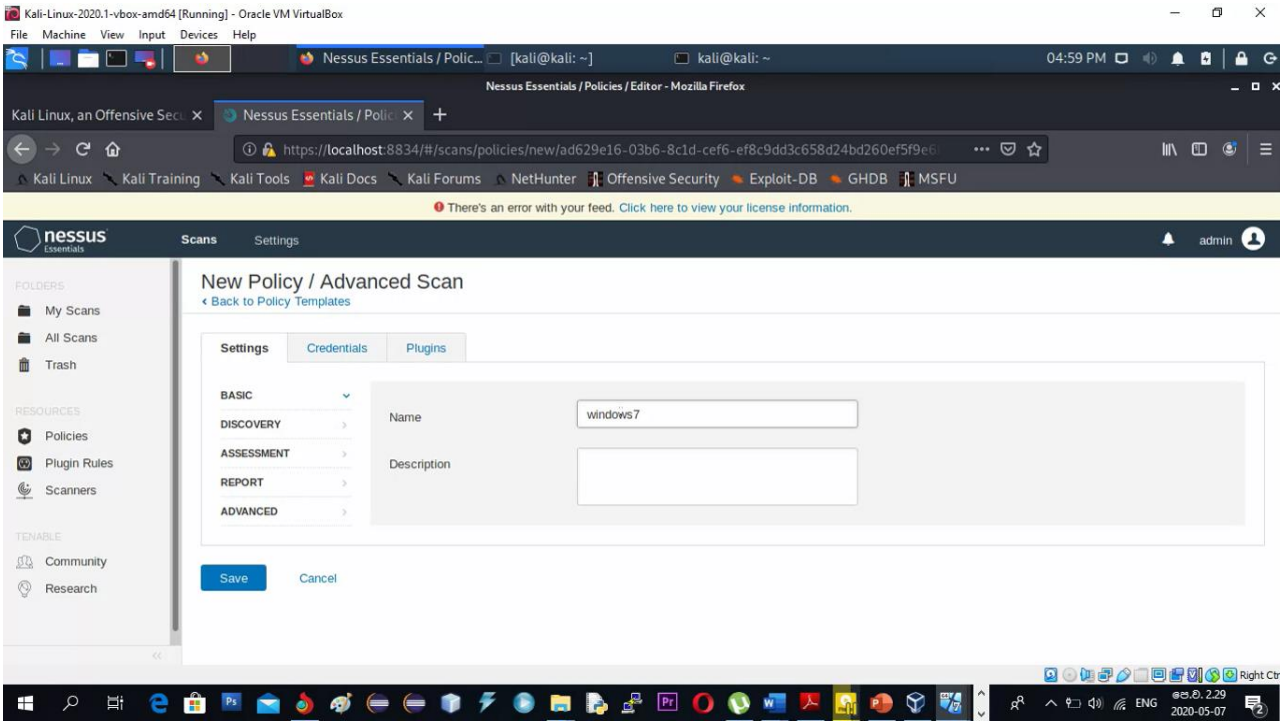

Figure 4.7:Giving information for Settings

Then click on “credentials”.

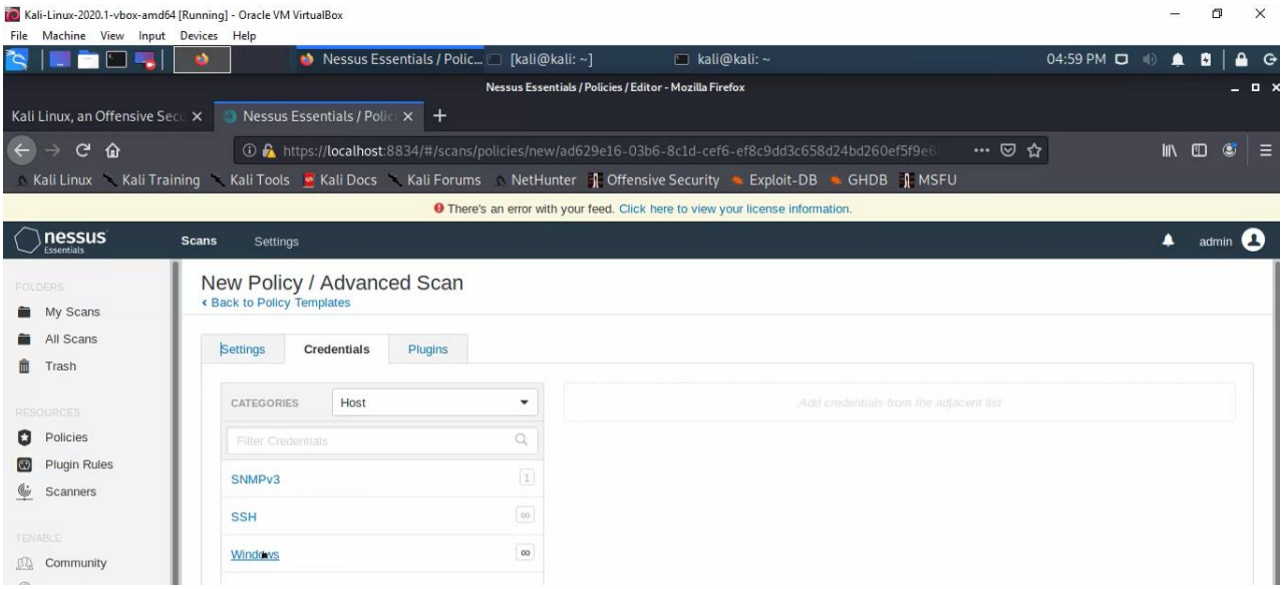

Figure 4.8:Selecting “Windows” under credentials.

Select the “Password” for Authentication method, give the Username a s “administrator” and give a password.

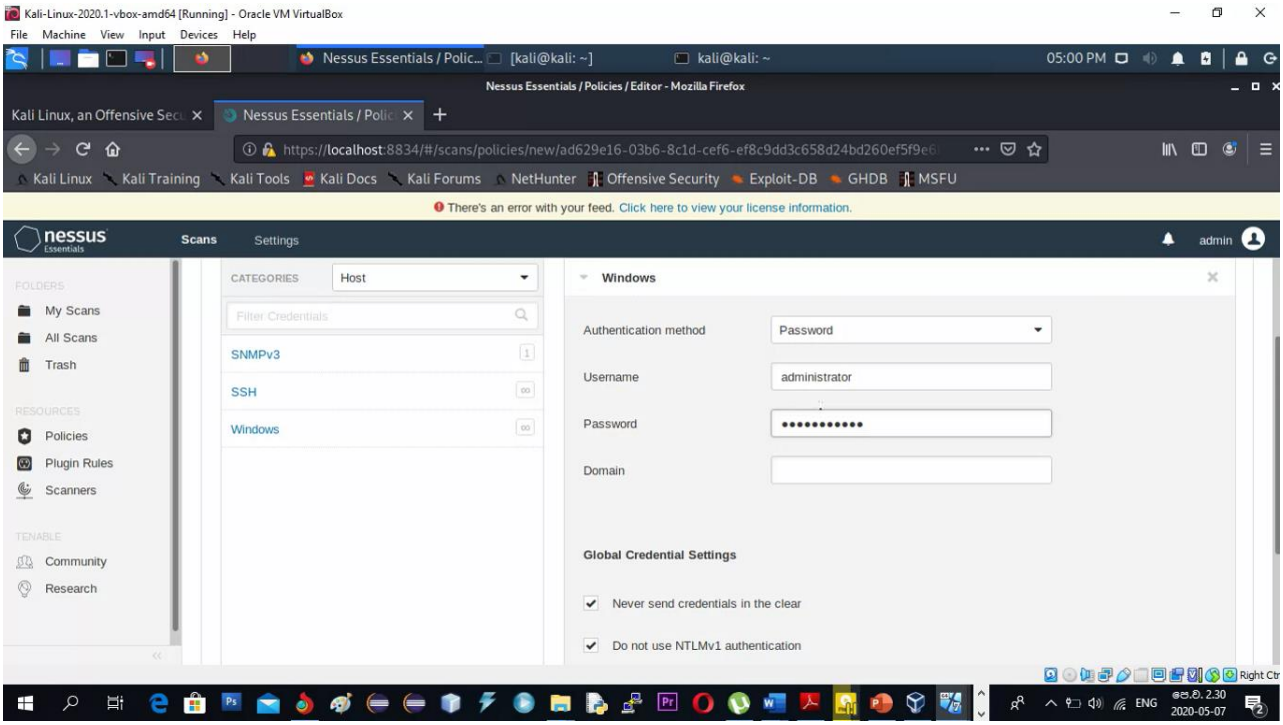

Figure 4.9:Giving required details

Then, enable four Global Configuration Settings.

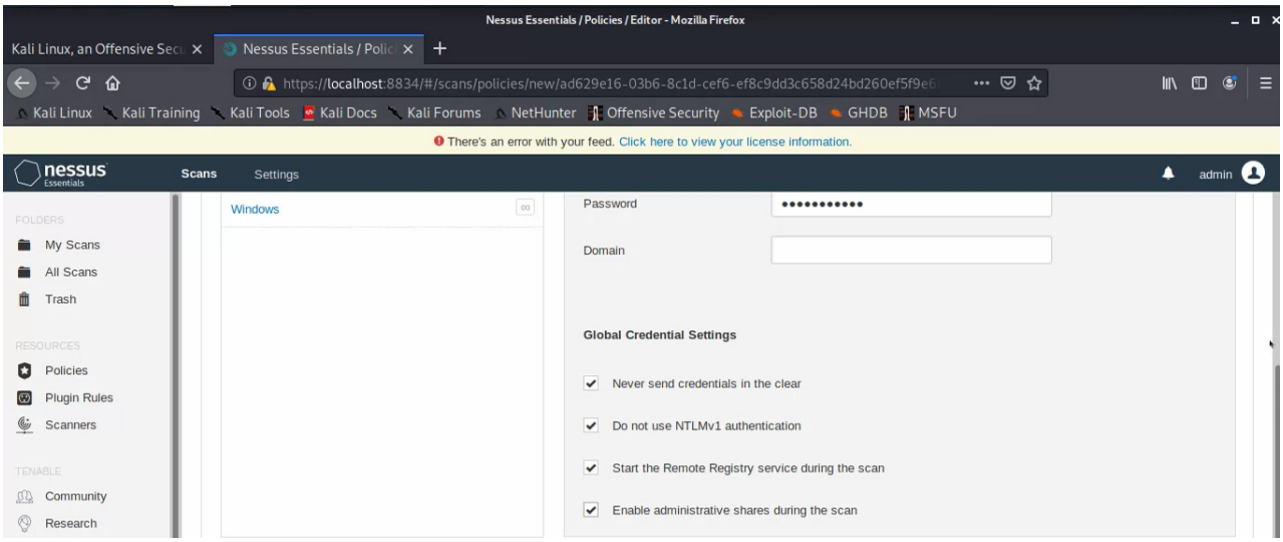

Figure 4.10:Enabling global configuration settings

Then click on “Plugins” and it will list down all plugins.

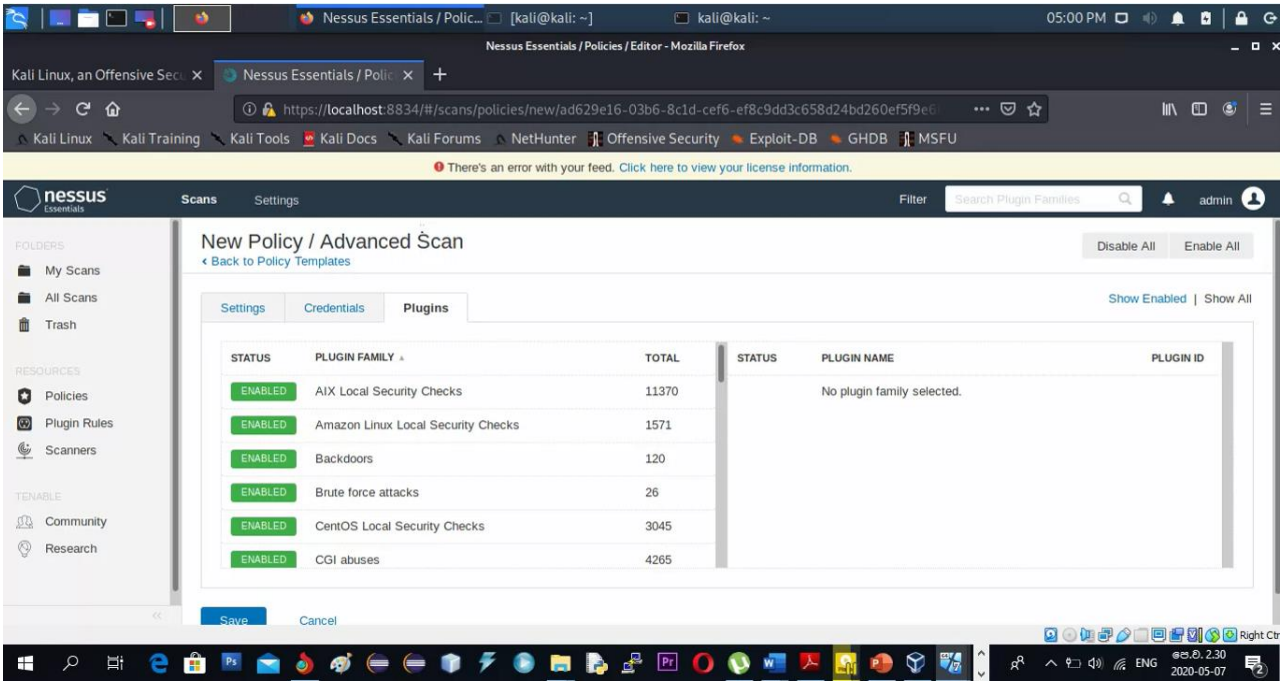

Figure 4.11:List down available plugins

Then enable or disable the plugins according to your requirement.

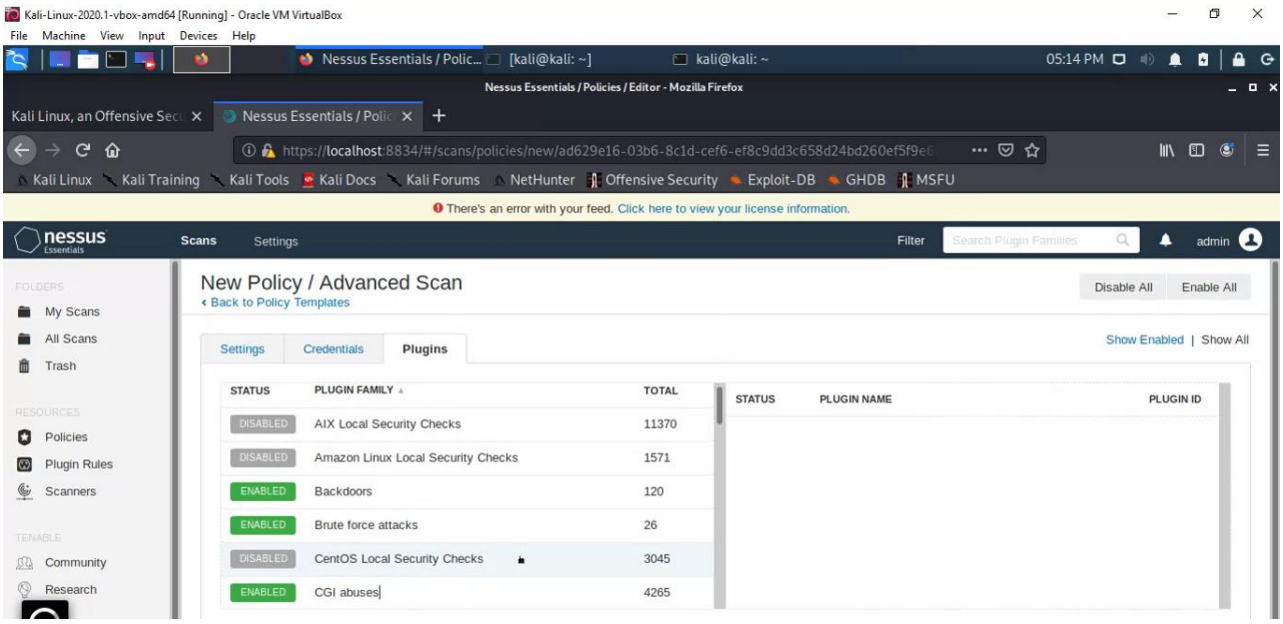

Figure 4.12:Enabling and disabling plugins

These are the enabled and disabled plugins for vulnerability scanning Windows 7 box.

Table 4.1:Enabled and Disabled plugins for vulnerability scanning Windows 7 box

Enabled	Disabled
Windows : User management	Windows : Microsoft Bulletins
Windows	VMware ESX Local Security Checks
Web Servers	Virtuozzo Local Security Checks
SNMP	Ubuntu Local Security Checks
SMTP problems	SuSE Local Security Checks
Settings	Solaris Local Security Checks
Service detection	Slackware Local Security Checks
Policy Compliance	Scientific Linux Local Security Checks
PhotonOS Local Security Checks	SCADA
Peer-To-Peer File Sharing	RPC
NewStart CGSL Local Security Checks	Red Hat Local Security Checks
Huawei Local Security Checks	Palo Alto Local Security Checks
General	OracleVM Local Security Checks
FTP	Oracle Linux Local Security Checks
Denial of Service	Netware
Databases	Misc.
CGI abuses : XSS	Mandriva Local Security Checks
CGI abuses	MacOS X Local Security Checks
Brute force attacks	Junos Local Security Checks
	HP-UX Local Security Checks
	Gentoo Local Security Checks
	Gain a shell remotely
	FreeBSD Local Security Checks
	Firewalls
	Fedora Local Security Checks
	F5 Networks Local Security Checks
	DNS
	Default Unix Accounts
	Debian Local Security Checks
	CISCO
	CentOS Local Security Checks
	Backdoors
	Amazon Linux Local Security Checks
	AIX Local Security Checks

Then click on “Save” to save the plugins.

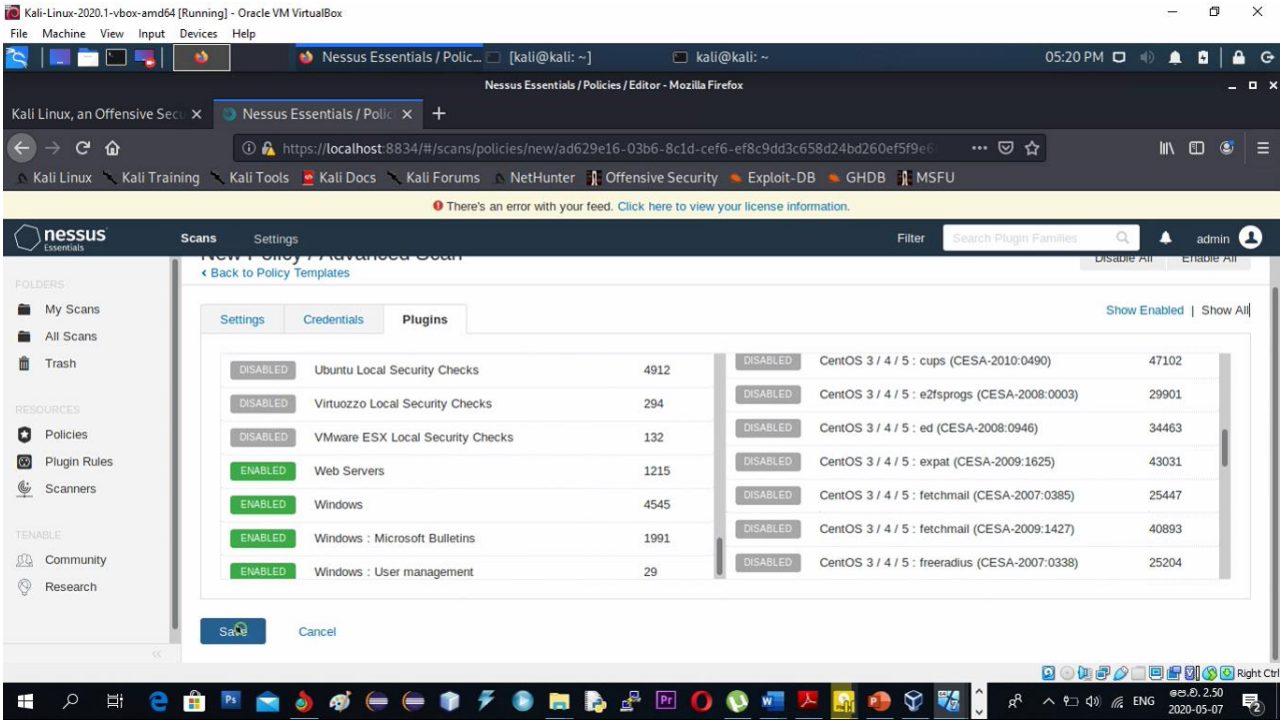

Figure 4.13:Saving the plugins

Then it will display the created policy according to the below figure.

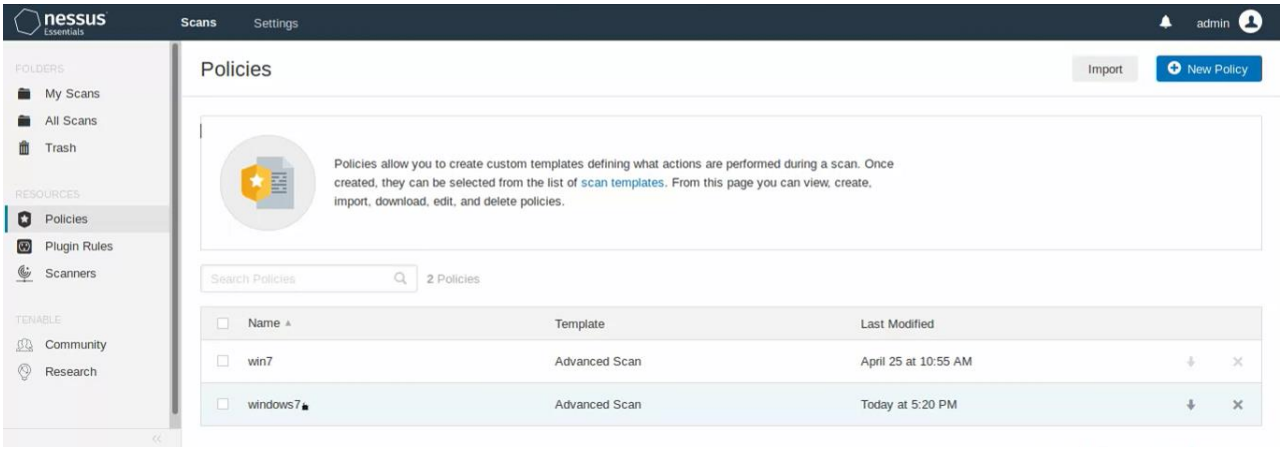

Figure 4.14:Displaying the created policy

Then we can start the vulnerability scan for the target, 192.168.56.101. Click on “My scans” and the “New Scan”. Then you will have two options “Scanner” and “User Defined”.

Click on “User Defined”.

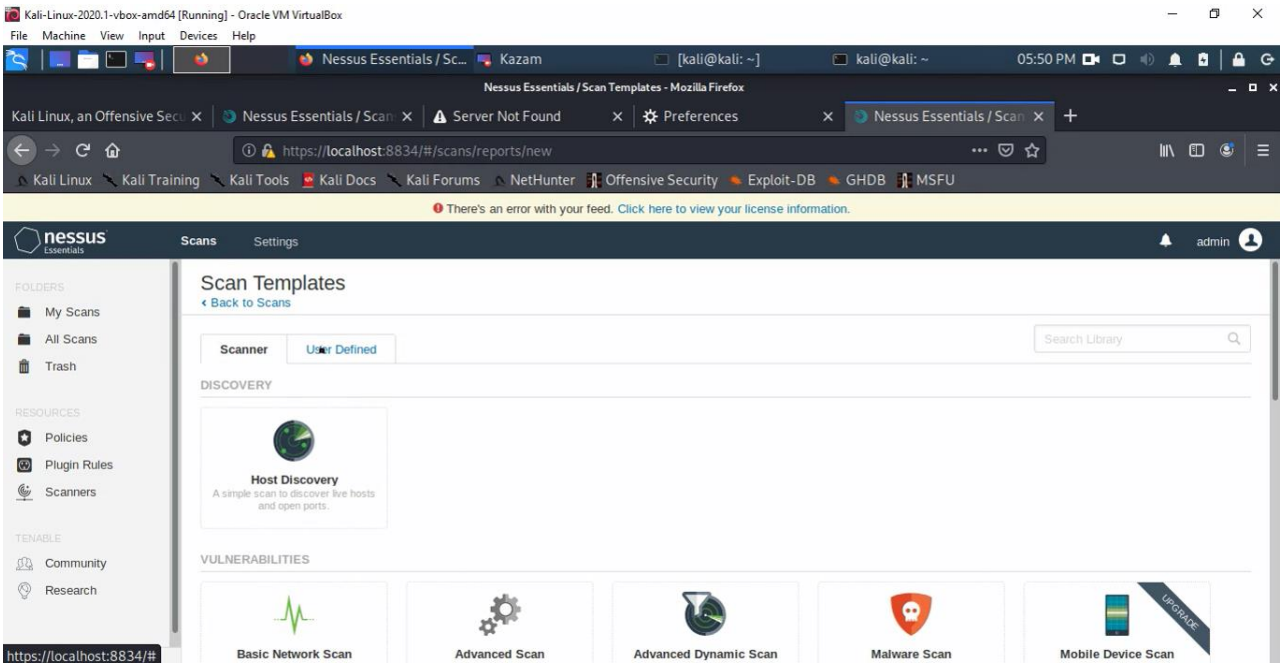

Figure 4.15:Starting the vulnerability assessment

Then the created policies will be displayed under “User Defined” and click on the created policy.

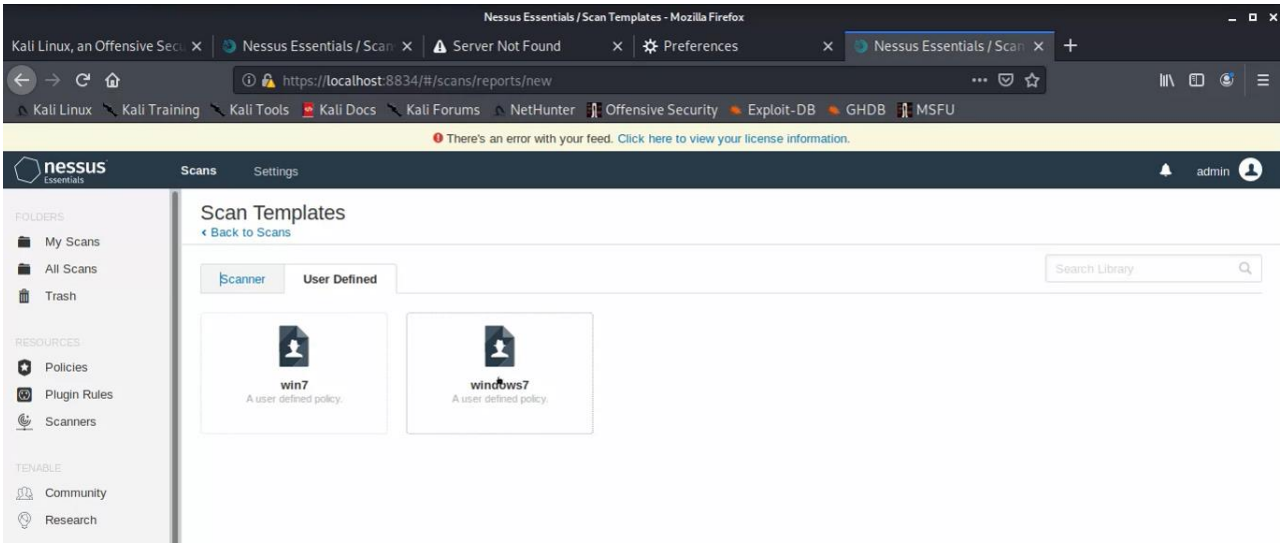

Figure 4.16:Displaying created policies.

Then give a name for the assessment and mention the IP address of target.

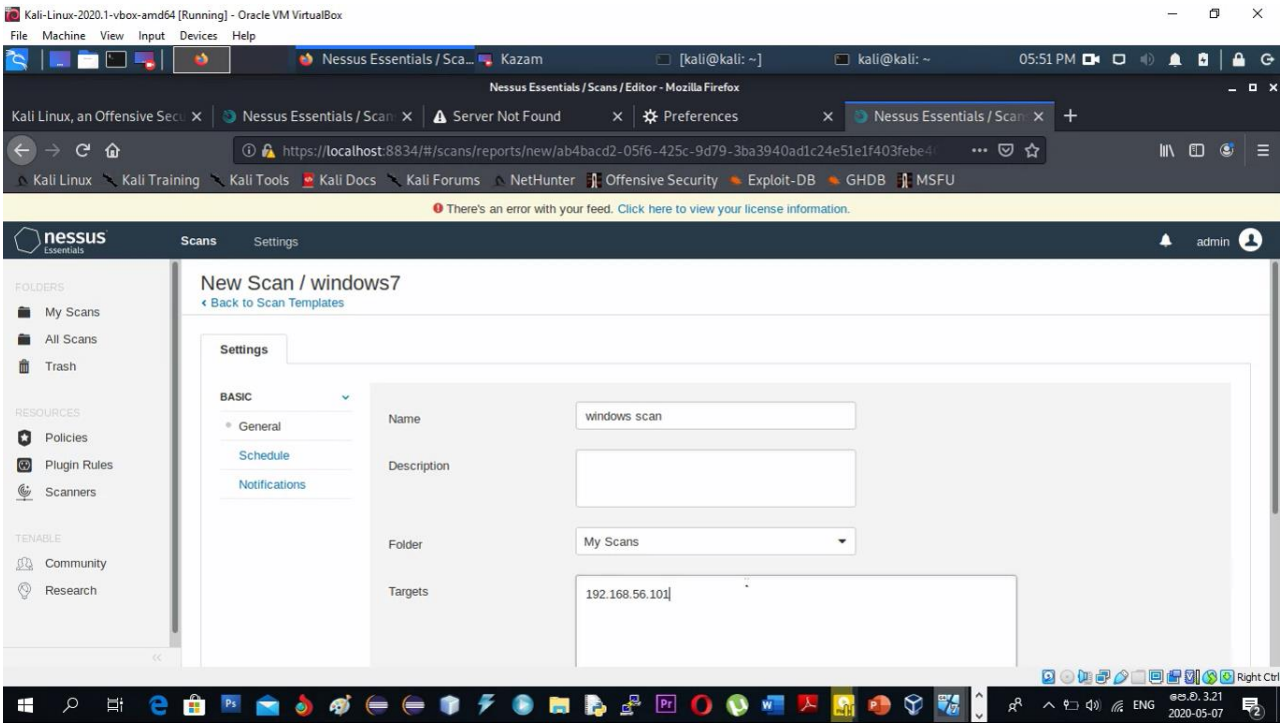

Figure 4.17:Giving the information for vulnerability assessment.

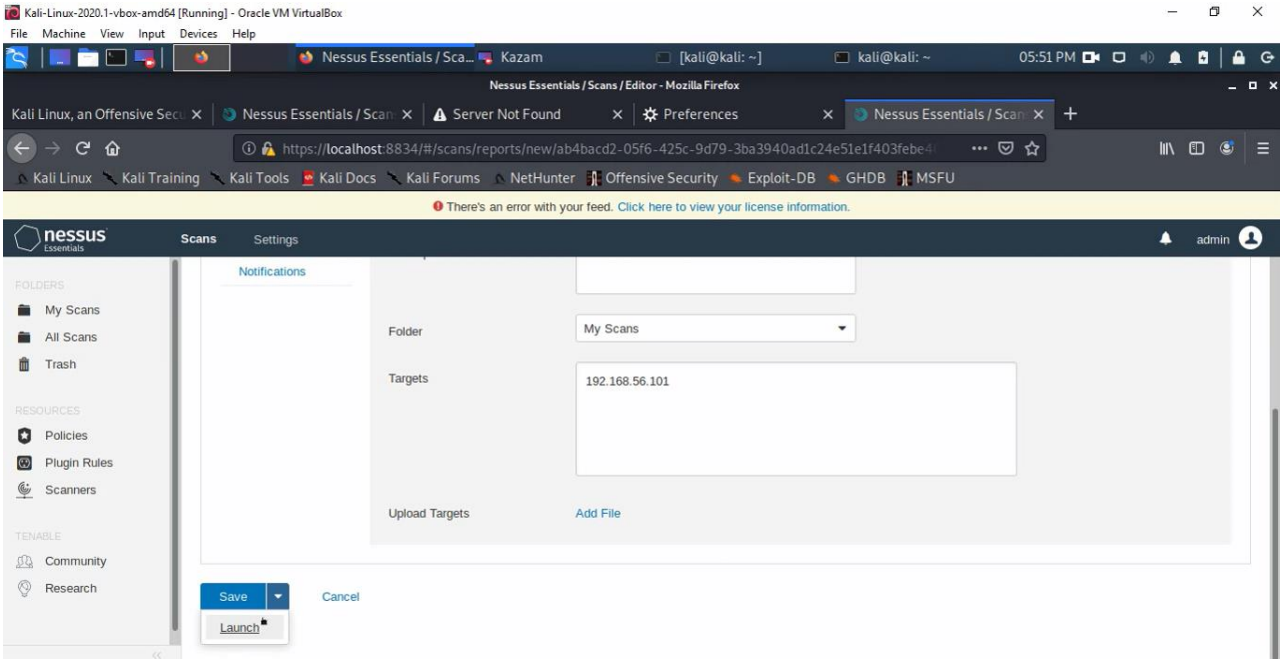

Figure 4.18:Defining the target and launching the scanning.

Then the scan will start to running.

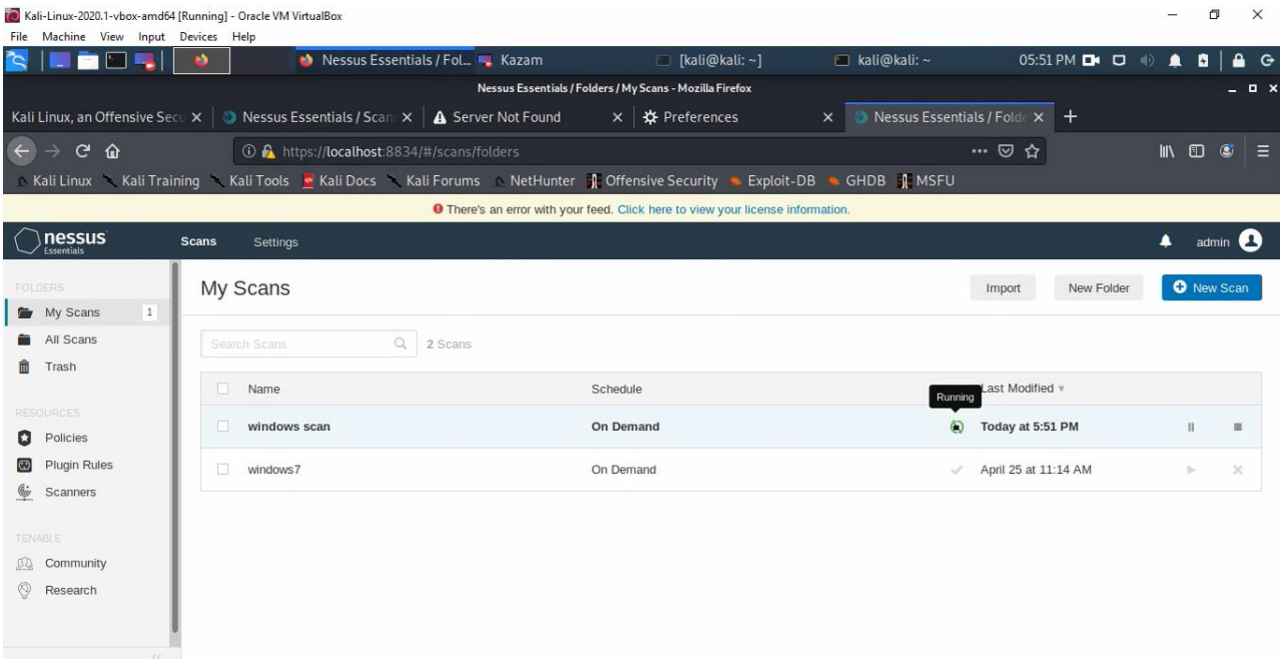

Figure 4.19:Starting the scan

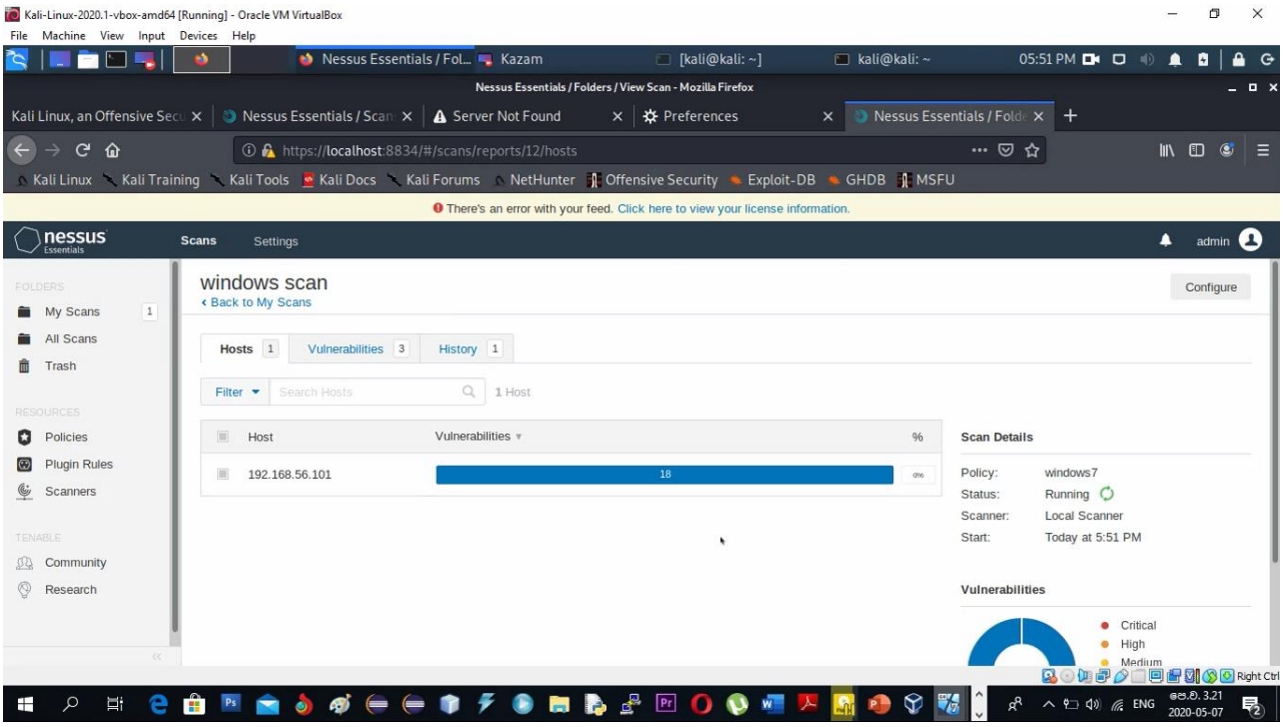

Figure 4.20:Running the scan

Then the completed vulnerability assessment will be displayed as shown in following figure.

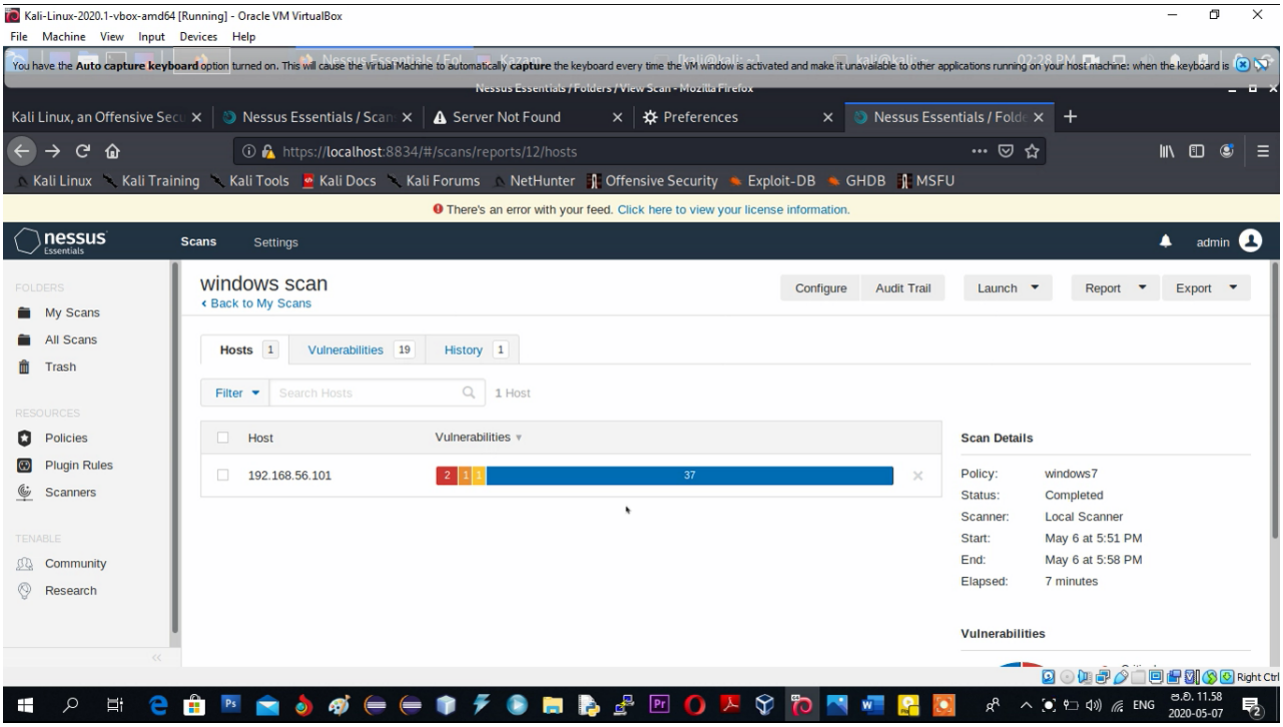

Figure 4.21:Completed vulnerability assessment

According to the following figure, there are,

- Two critical vulnerabilities
- One high vulnerability
- One medium vulnerability
- 37 Information

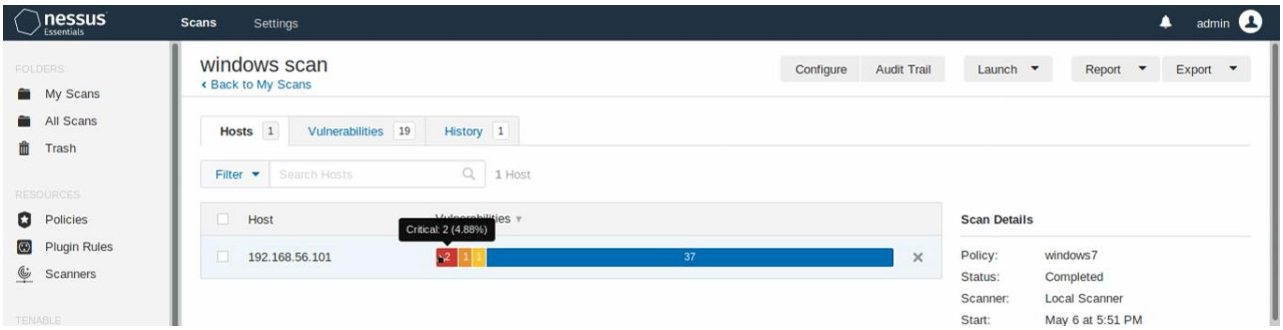

Figure 4.22:Two critical vulnerabilities

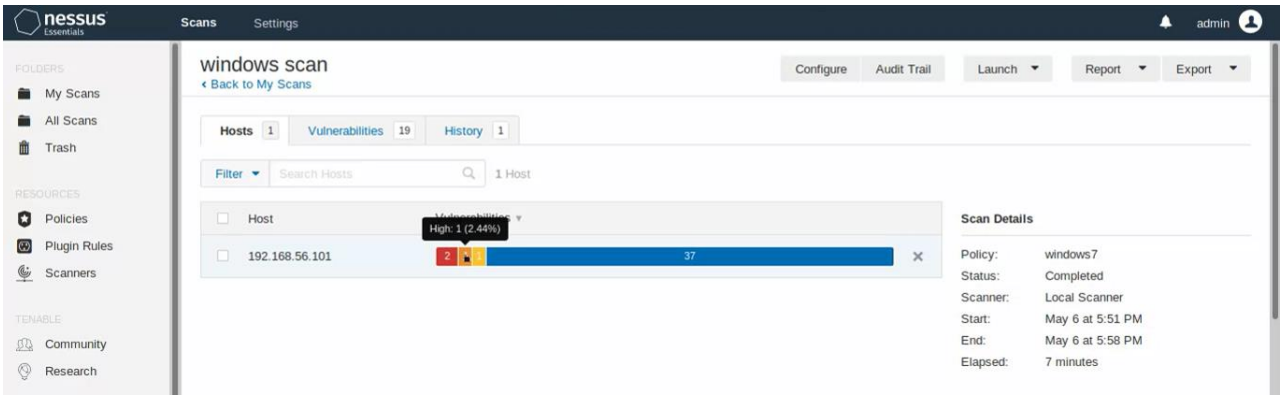

Figure 4.23:One high vulnerability

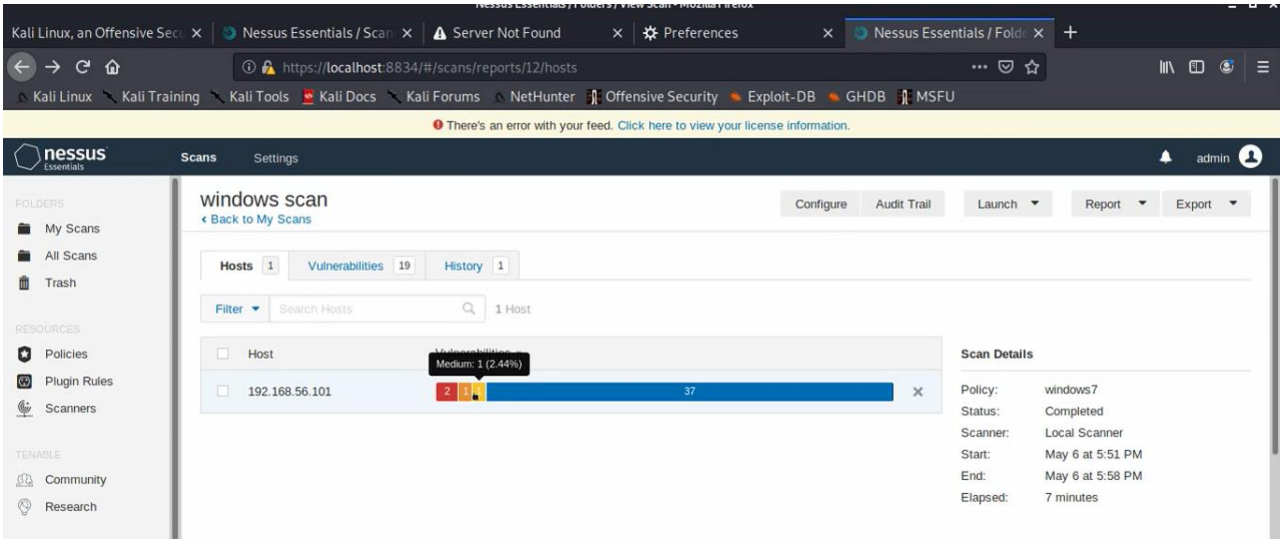

Figure 4.24:One medium vulnerability

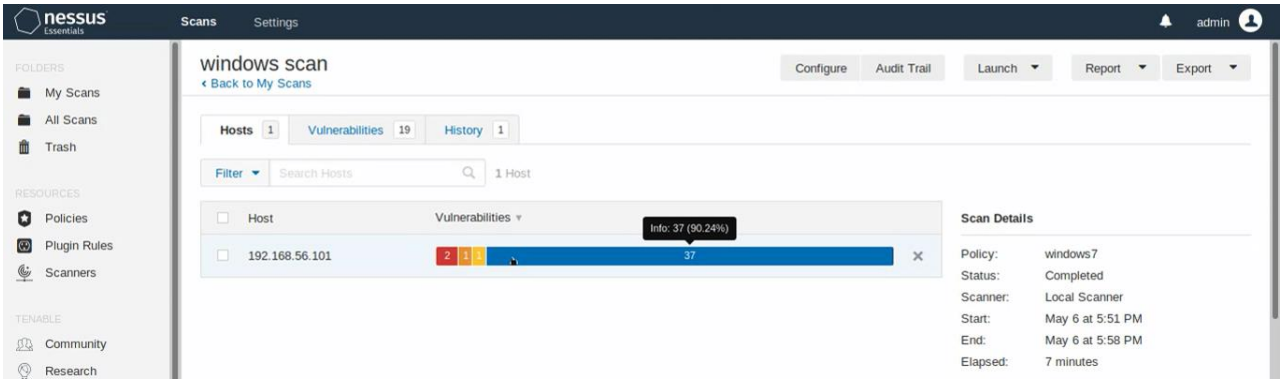

Figure 4.25:37 Information

The pie chart, which is at the bottom, displays the percentage of vulnerabilities. According to the pie chart.

- Critical vulnerabilities = 7%
- High vulnerabilities = 3%
- Medium vulnerabilities = 3%
- Information = 86%

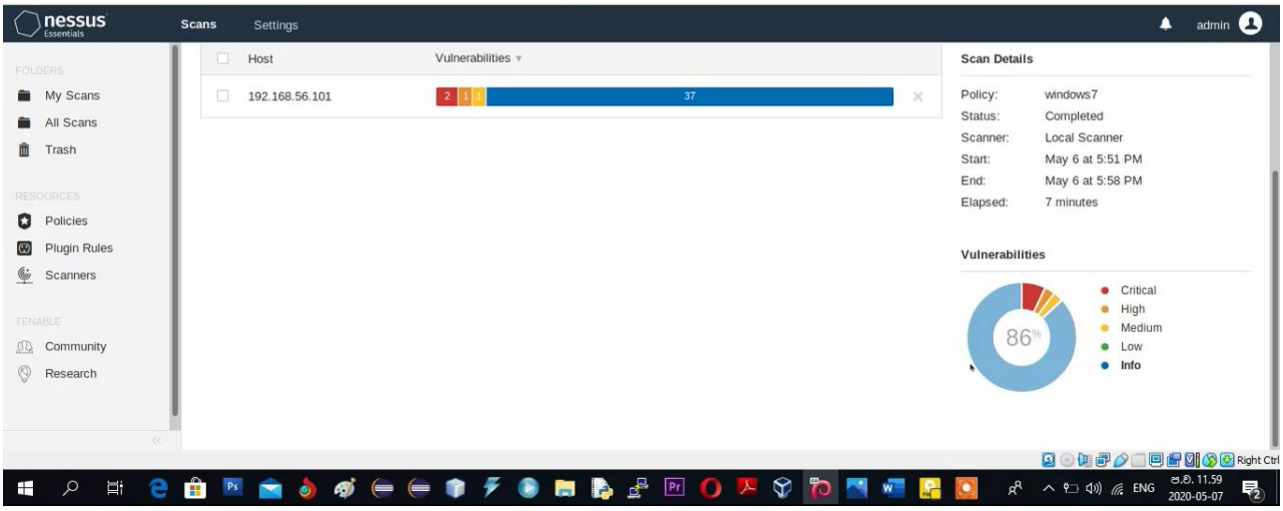

Figure 4.26:Percentage of vulnerabilities from a pie chart

Click on the bar and then it will list down the available vulnerabilities.

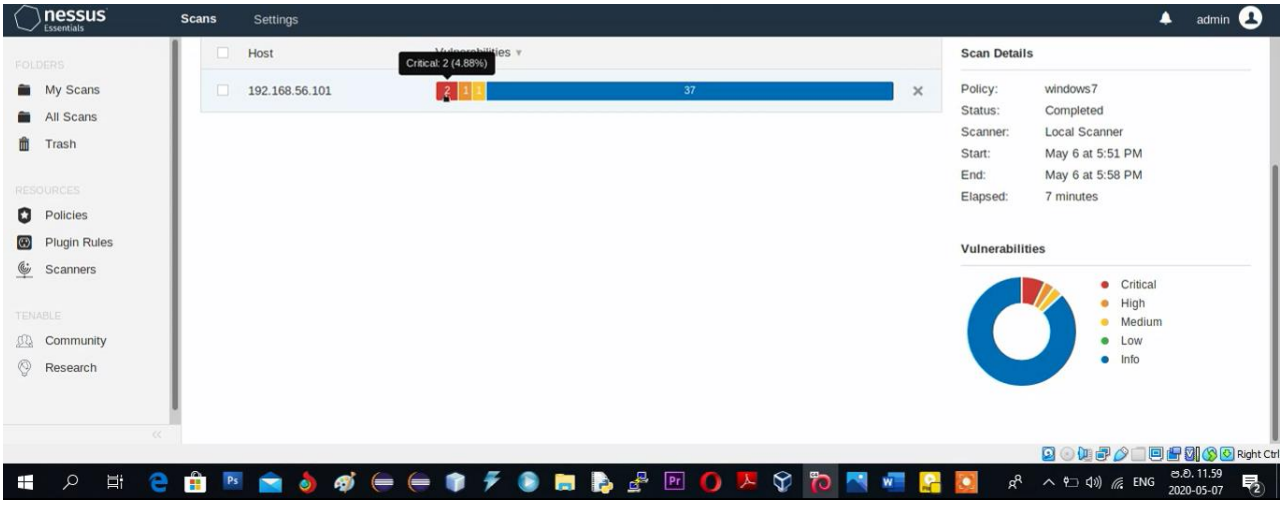

Figure 4.27:Viewing the vulnerabilities.

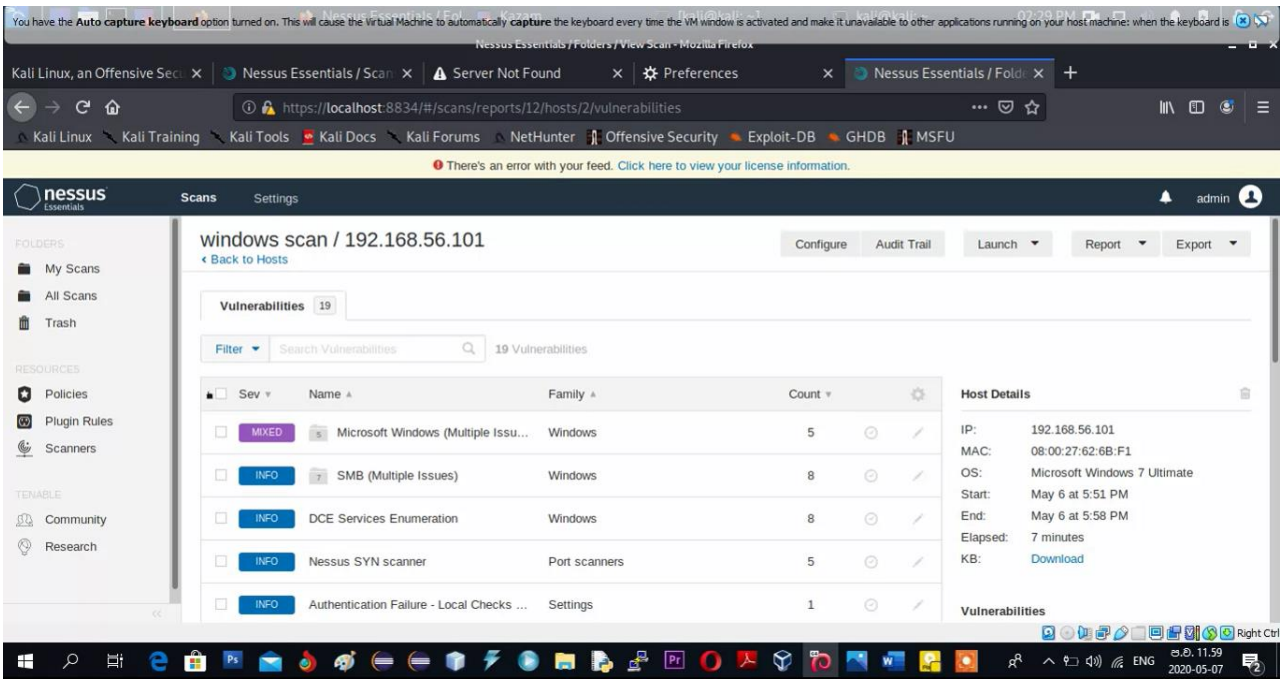

Figure 4.28:Listing down the vulnerabilities

We can get the information in detail, by going inside a vulnerability. Click on “Mixed”and check the details.

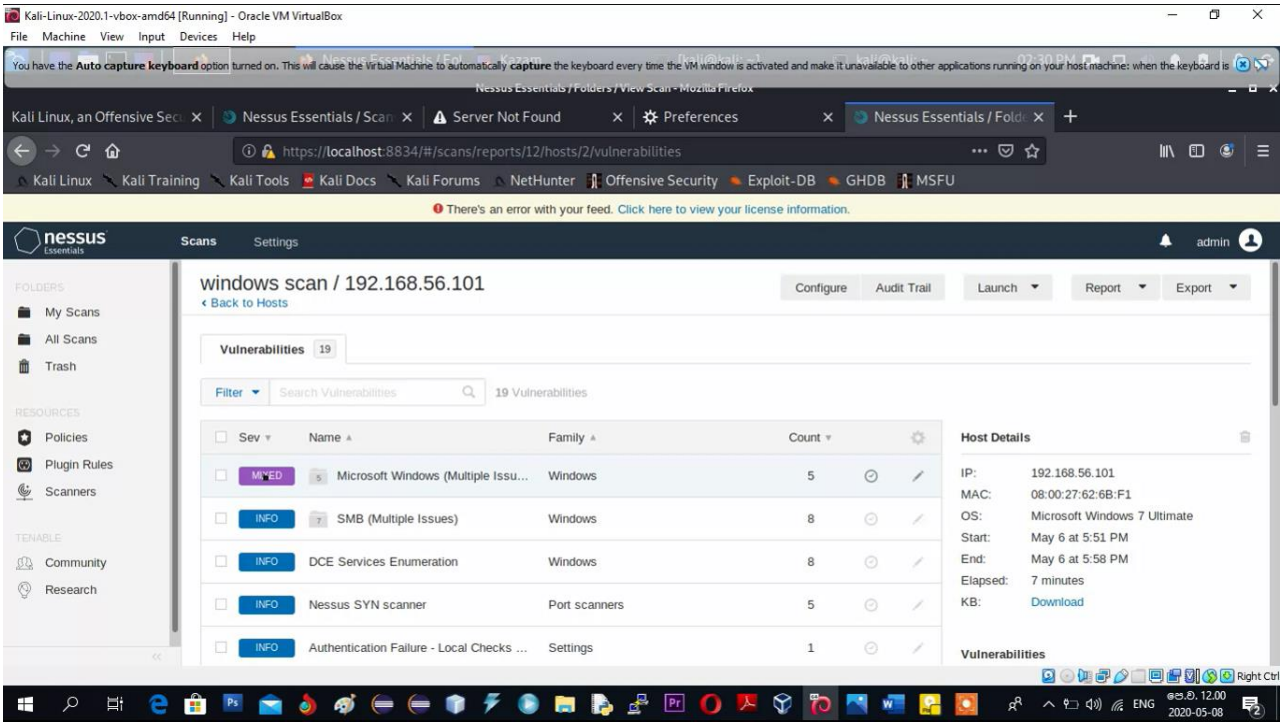

Figure 4.29:Getting information in detail.

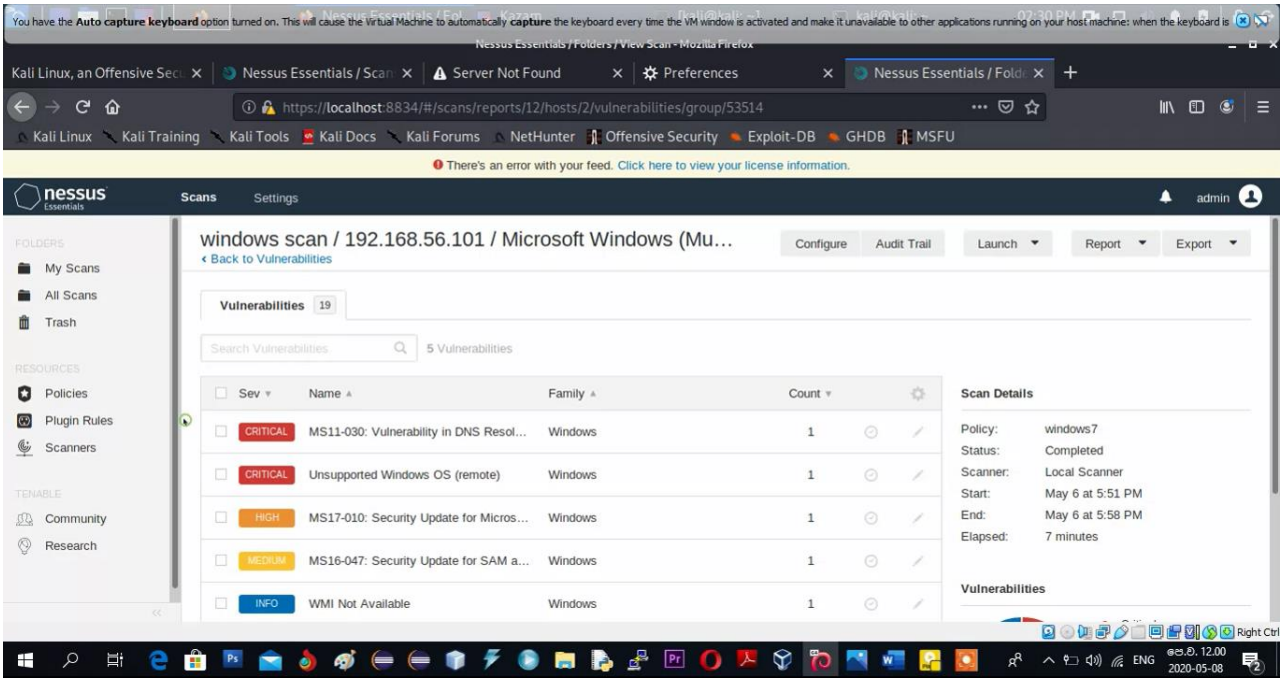

Figure 4.30:Viewing critical vulnerabilities

Then it will display the available critical, high and medium vulnerabilities. Then click on them and go inside the vulnerability. Then it will describe the vulnerability and mention the solution for that.

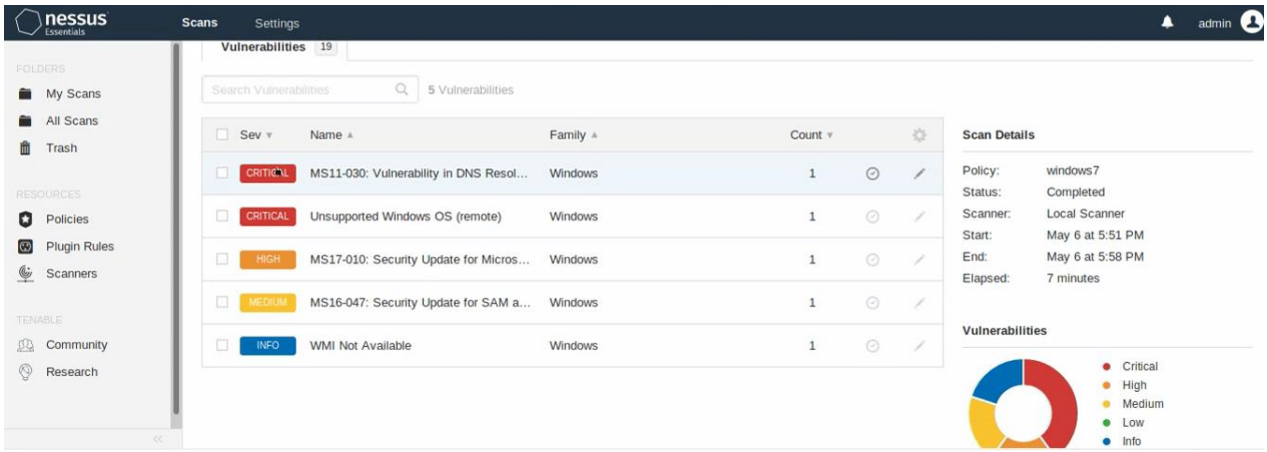

Figure 4.31:Available critical, high and medium vulnerabilities.

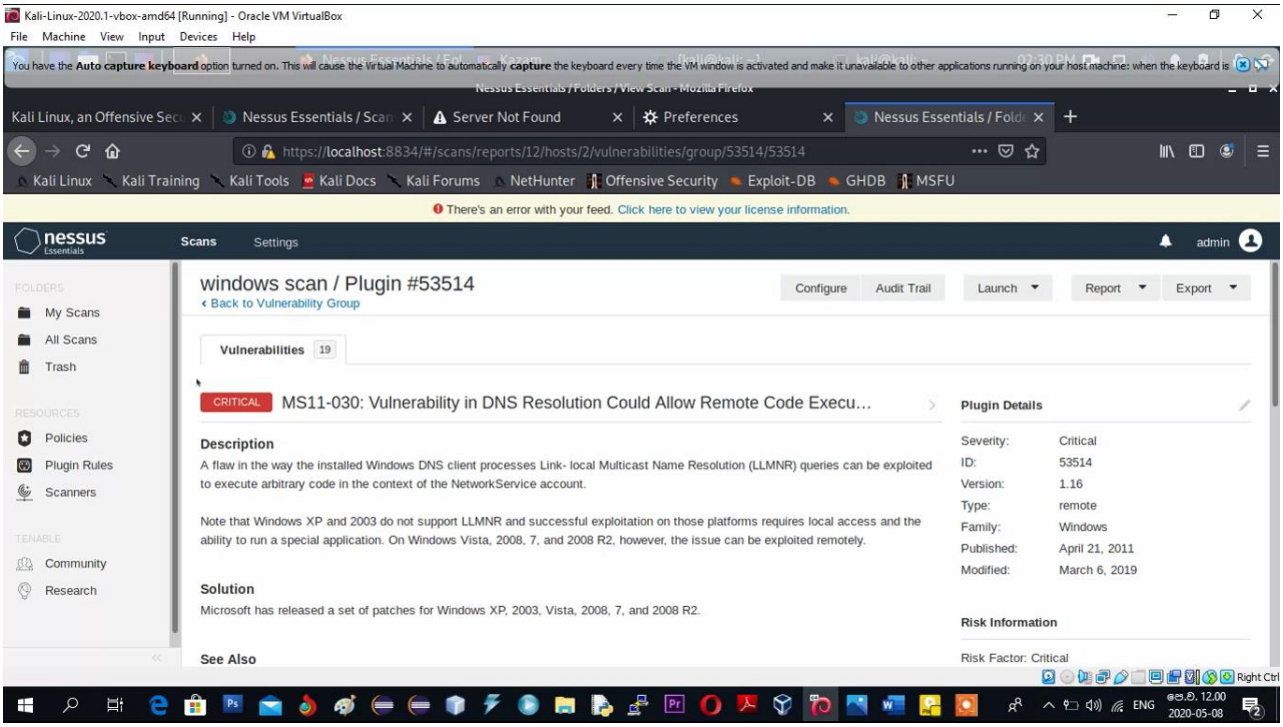

Figure 4.32:MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution

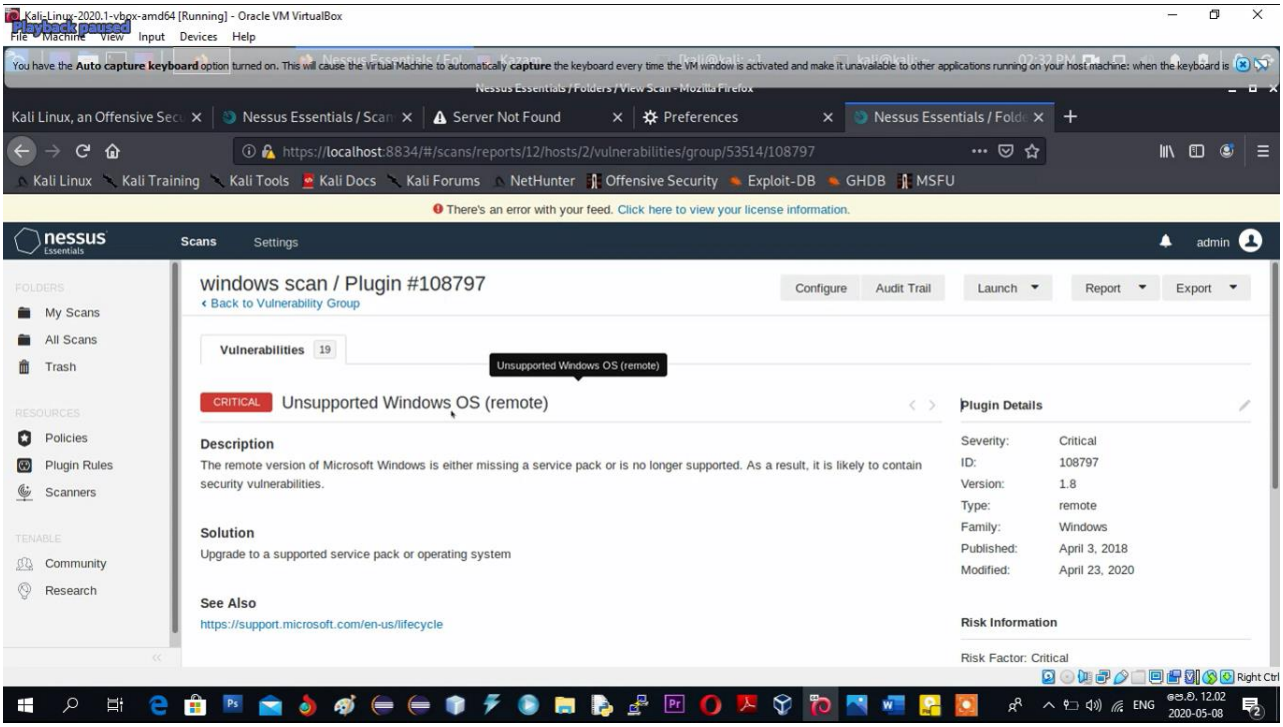

Figure 4.33:Unsupported Windows OS (remote)

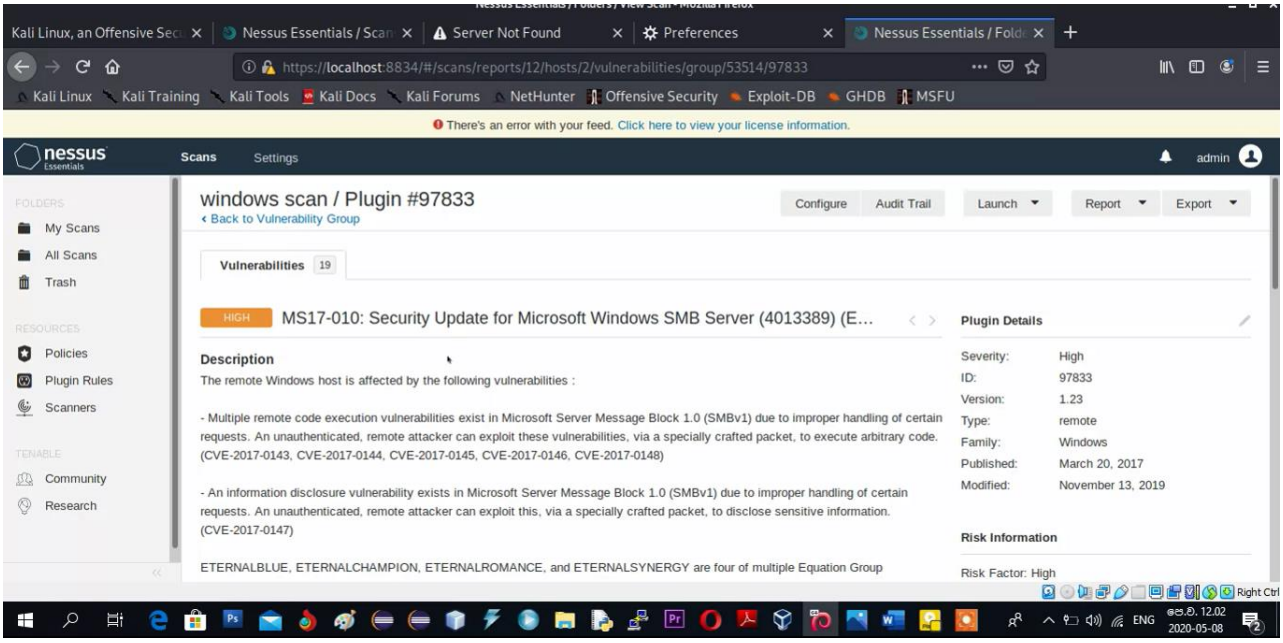

Figure 4.34:MS17-010: Security Update for Microsoft Windows SMB Server

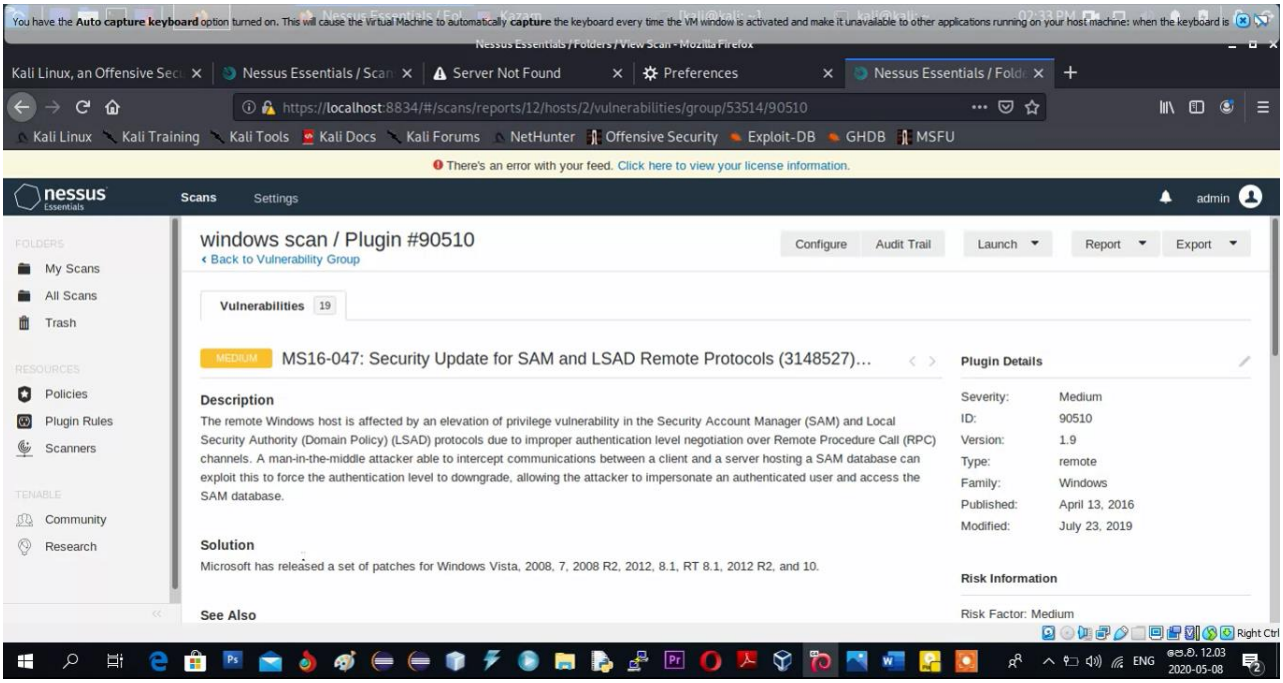

Figure 4.35:Security Update for SAM and LSAD Remote Protocols

The information also are given in detail as mentioned follows.

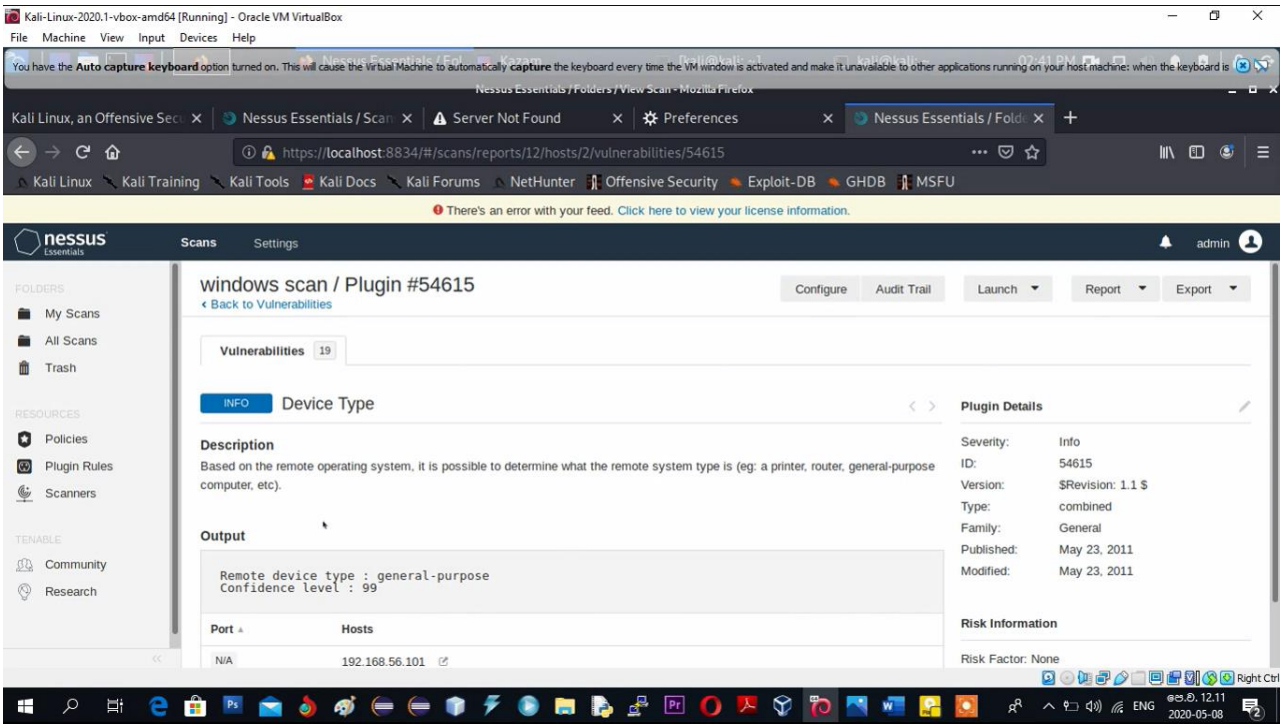

Figure 4.36:Information: Device Type

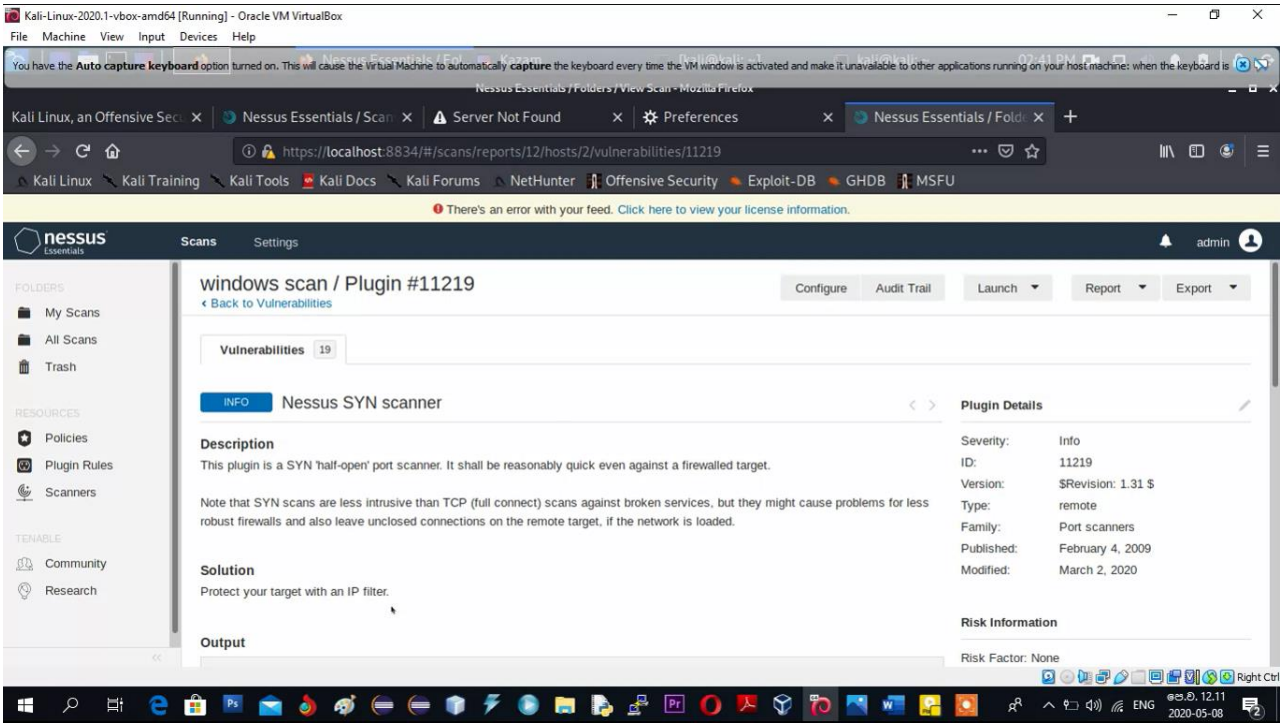

Figure 4.37:Information Nessus SYN scanner

According to vulnerability scanning followings are the critical vulnerabilities of Windows 7 box.

1. MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution

   Description: A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the Network Service Account.

   Solution: Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7 and 2008 R2

2. Unsupported Windows OS (remote)

   Description: Unsupported version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

   Solution: Upgrade to a supported service pack or operating system.

Followings are the high and medium vulnerabilities.

High vulnerability

MS17-010: Security Update for Microsoft Windows SMB Server

Description: The remote Windows host is affected by the following vulnerabilities.

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

Medium Vulnerability

MS16-047: Security Update for SAM and LSAD Remote Protocols

Description: The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

5 Conclusion

According to the audit conducted for Windows 7 box, two critical vulnerabilities, one high vulnerability and one medium vulnerability were identified.

1. MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution
2. Unsupported Windows OS (remote)
3. MS17-010: Security Update for Microsoft Windows SMB Server
4. MS16-047: Security Update for SAM and LSAD Remote Protocols

In order to mitigate above vulnerabilities, required patches need to be updated and new version should be installed.

References

[1] "What is Windows Auditing? A primer to auditing events in Windows Environment", *Petri*. [Online]. Available: https://www.petri.com/windows_auditing. [Accessed: 01- May- 2020].

[2] "Why you should perform regular security audits", *TechRepublic*. [Online]. Available: https://www.techrepublic.com/article/why-you-should-perform-regular-security-audits/. [Accessed: 25- Apr- 2020].

[3] "Nessus Professional", *Tenable*®. [Online]. Available: https://www.tenable.com/products/nessus/nessus-professional. [Accessed: 02- May- 2020].