Information Assurance & Auditing

4thyear 1st semester

Mini project-2020

Department of Information Technology

Sri Lanka Institute of Information Technology
Sri Lanka

Registration no – IT17059732

Name – S.G.V.S Tharaka

Batch – CSNE-WE

Table of content:

Figure of table:

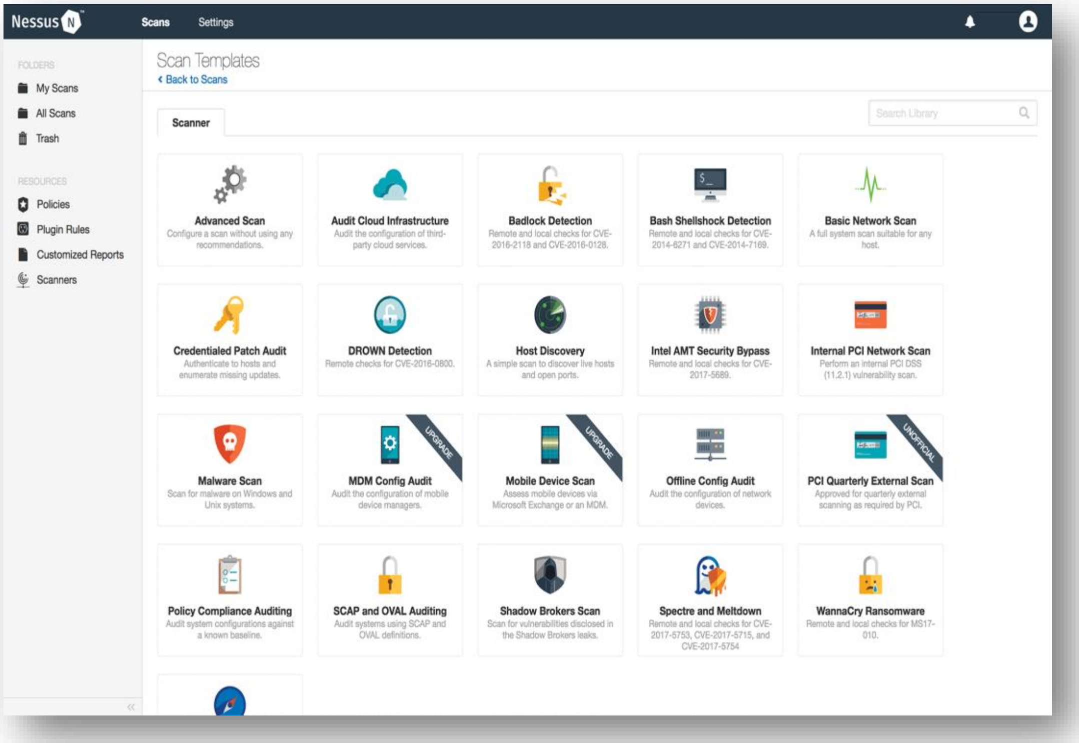
Introduction:

Security audit is auditing of the information of the organization based on the position of the information. So, we met several kind of auditing methods. The security auditing performs a final desired result for meet their organizational objectives. The security auditing shows the vulnerabilities that your sensitive data can be face and it shows us way to ignore that vulnerabilities. Most of the organizations use several type of scanning tools for auditing process. The main security auditing tools are Nessus, Nmap, OpenVAS. Acunetix, Kaseya VSA, Netwrix auditor, Metasploit. In this assessment, we are using the Nessus auditing tool for search vulnerabilities on windows 10 with in the same internal network. Nessus is the free auditing tool. The Nessus can enter the 450 type of templates for scan several types of vulnerabilities according to your requirement. For example, there is a range of scan templates including Basic Network Scan, Advanced Scan, Malware Scan, Host Discovery, WannaCry Ransomware, and more. You can also generate report with your vulnerabilities using Nessus. We can also create summary report and vulnerability report with more detail and save as a PDF, html, csv and xml etc. security auditing produces some important benefits to organization. it shows the current security strategy, check the security efforts are working, reduce the cost, provide the new technology or process, Prove the organization is compliant with regulations. There are several steps in the security auditing process. Initially we must decide the assessment criteria. Secondly, we prepare the security audit. Next conduct the audit and finally complete and share the audit results. We must consider the following things to define the assessment criteria. Maintain the threat catalog and search vulnerabilities, involve the stockholders to that process, industry and the geographic standards are the process of the assessment of criteria. During second step, select the instruments and techniques required to meet the trade goals. Discover or make a suitable survey or study to accumulate the right information for your audit. During third step, lookout to supply suitable documentation and perform due constancy throughout the method. Monitor the progress of the review additionally the information focuses collected for precision. Utilize past audits and unused data as well as the guidance of your examining group to carefully select which rabbit holes in which you slip. You may reveal details that require advance examination but prioritize those unused things with the group to begin with.

There are several challenges that happen during the auditing process. These are avoiding the fly assessments, validity of the audit, discover the scope of the requirement in the audit. Stay focus on risk. There are several security audits types in the in the process. These are one-time assessment. Tollgate assessment and portfolio assessment. This is the things that security scanning focus on. First insufficient password, over permissive ACLS on folders, data retention policies followed, inconsistence ACLs on folders, non-existence or insufficient file activity auditing, disaster recovery plans updated and tested, change management procedures followed, Correct security software and security configurations on all systems[4].

1. Security auditing tool that using for following assessment criteria.

- Nessus



Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

MDM Config Audit
Audit the configuration of mobile device managers.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration of network devices.

PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Figure: 1.1-Nessus tool [5]

- ➢ In this auditing process, we use the Nessus tool as the audit tool. We install the Nessus too in the kali Linux environment. Test the windows 10 operating pc using Nessus tool and find the vulnerabilities on it.

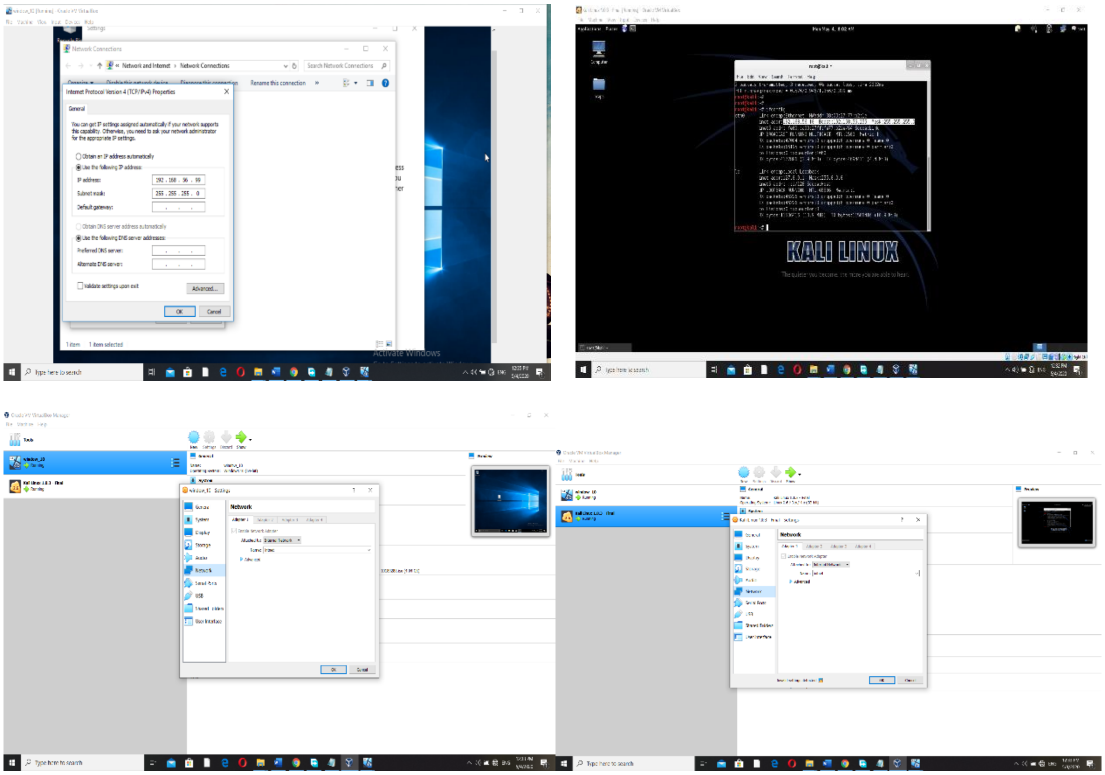
2. Other auditing instruments and operating systems

Figure: 2.1-operating systems [6]

- We use the kali Linux and the windows 10 operating system in this audit
- We are going to test the windows 10 virtual machine using the kali Linux operating system in the virtual box environment.
- All operating systems install into the oracle virtual box and Nessus audit tool install into the kali Linux operating system.
- We are using internal network scan with the Nessus.
- Scan vulnerabilities in the windows 10 pc and generate the report.

3. Scanning process with procedure:

- Select the internal network adapter in both virtual machines and enter the ip address in the same subnet range. After starting the network service in both window 10 and kali Linux virtual machines.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 56 . 99

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

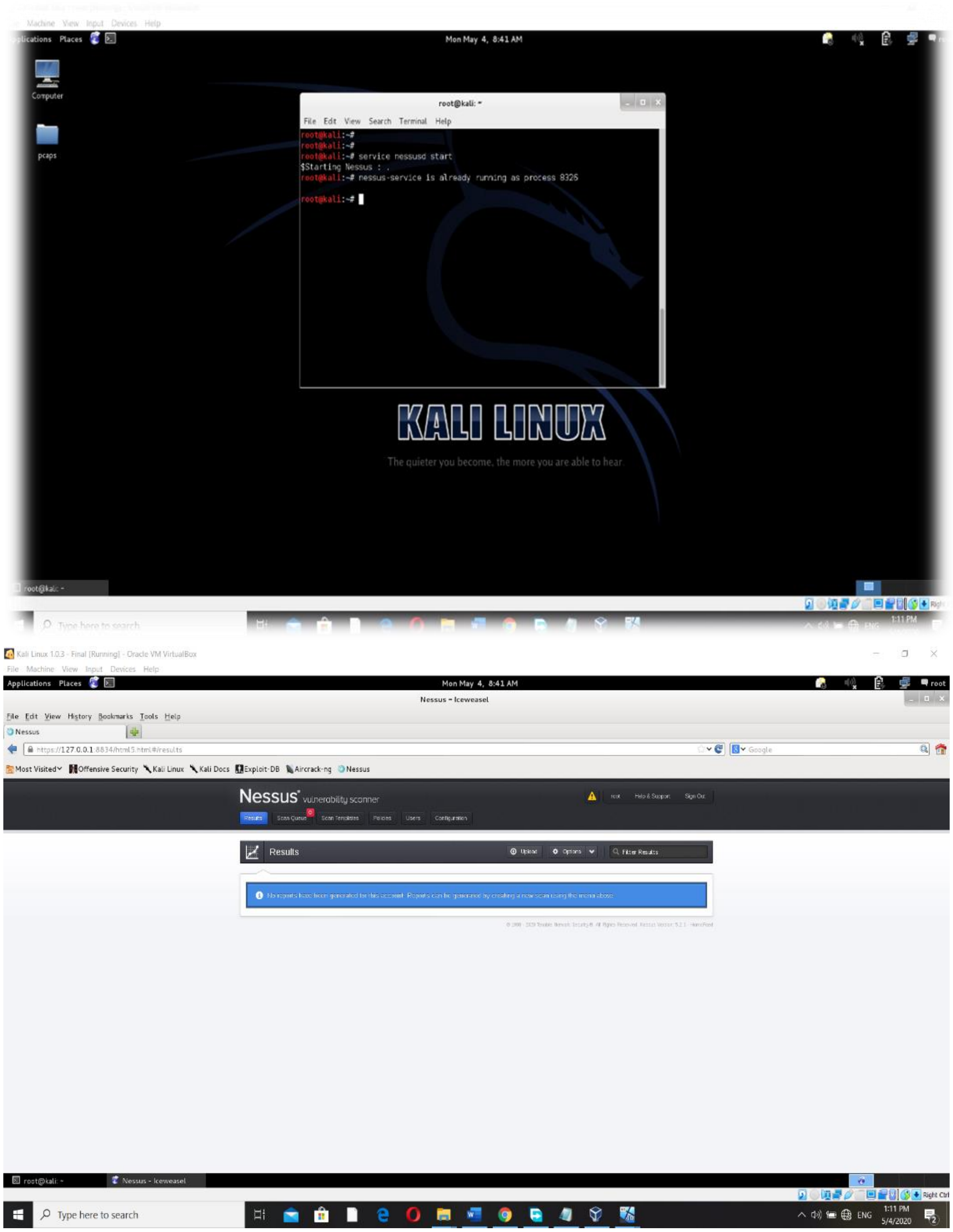
Alternate DNS server: . . .

□ Validate settings upon exit

Figure: 3.1-initial state

- ➢ Interconnect the two pcs (kali Linux and the Window 10)
- ➢ disable the firewall in the windows 10
- ➢ Ping kali to windows 10 machine. (check the connection between two virtual machine).
- ➢ Check the IP address of the windows 10 machine.

- Start the Nessus



```
root@kali:~#
root@kali:~#
root@kali:~# service nessusd start
$Starting Nessus : .
root@kali:~# nessus-service is already running as process 8326

root@kali:~# 
```

No reports have been generated for this account. Reports can be generated by creating a new scan using the menu above.

Figure: 3.2-start Nessus

➢ Login to the Nessus by providing username and password.

- Scan the window 10 using Nessus

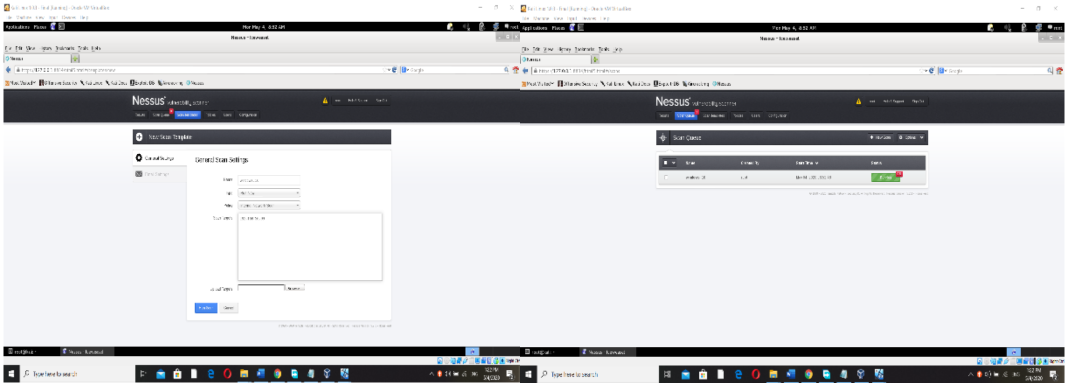
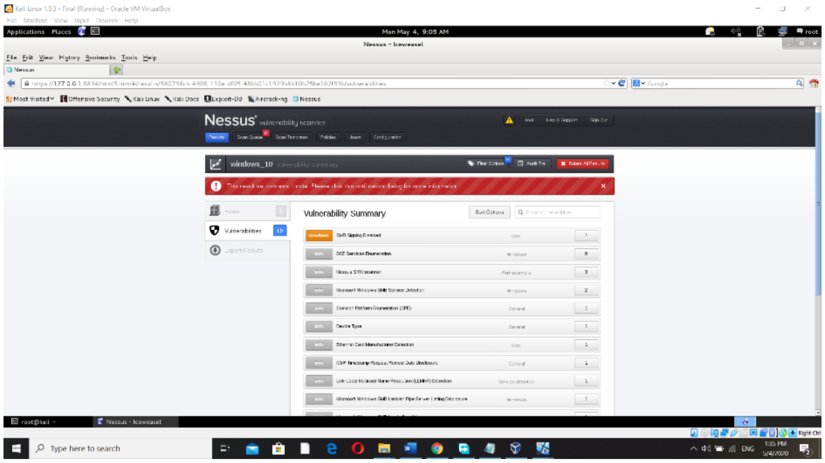


Figure: 3.3- scan using Nessus

- ➢ Create new scan template by giving name
- ➢ Select run now type and select internal network scan policy and after entering the window 10 virtual machine IP address in below scan target box.
- ➢ Finally click on the Run scan button.

- View the Results



windows_10 Vulnerability Summary

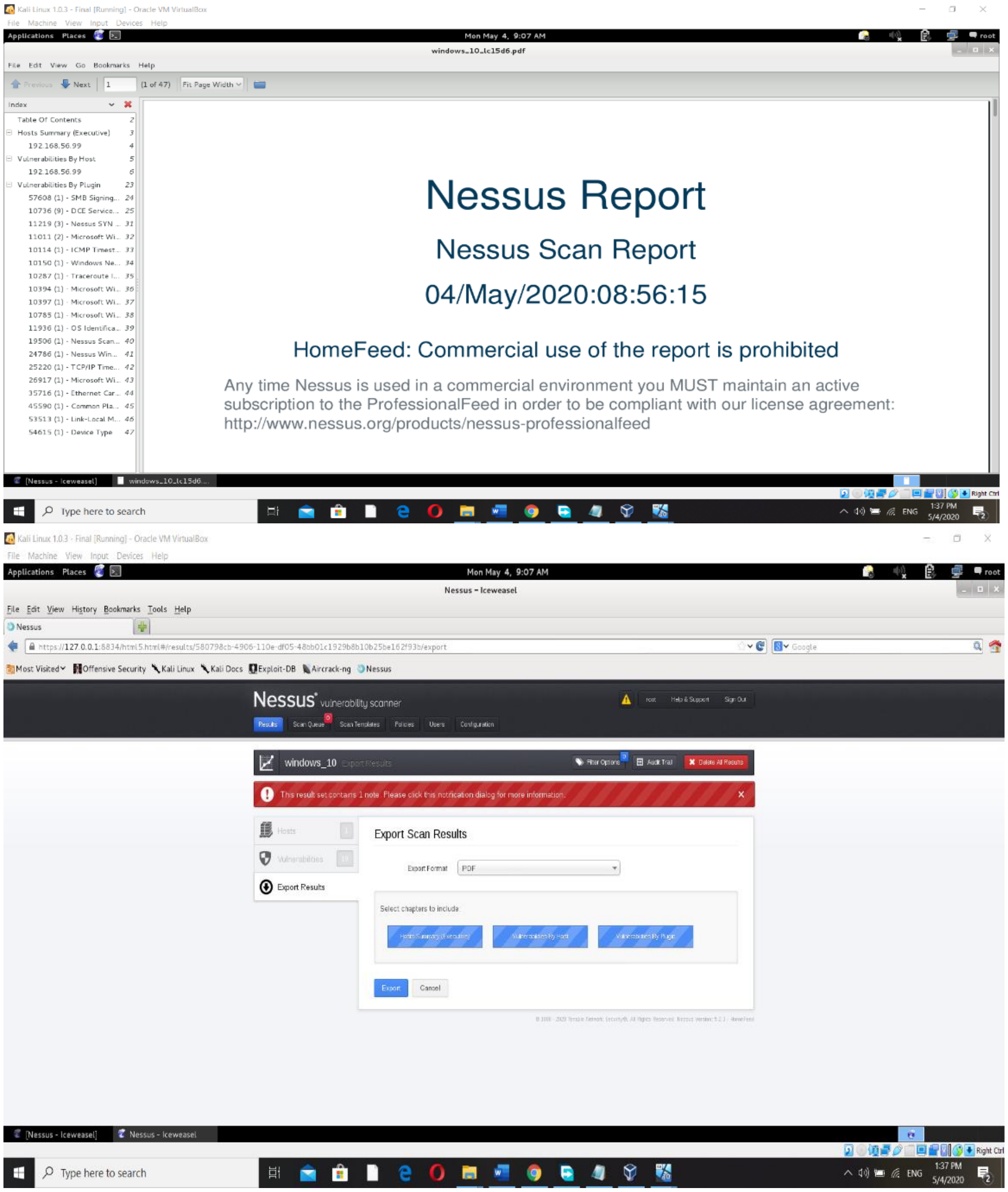
Vulnerability Summary

medium	SMB Signing Disabled	Misc.	1
info	DCE Services Enumeration	Windows	9
info	Nessus SYN scanner	Port scanners	3
info	Microsoft Windows SMB Service Detection	Windows	2
info	Common Platform Enumeration (CPE)	General	1
info	Device Type	General	1
info	Ethernet Card Manufacturer Detection	Misc.	1
info	ICMP Timestamp Request Remote Date Disclosure	General	1
info	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
info	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Windows	1

Figure:3.4- view results

- ➢ View all vulnerabilities

- Export a report of summary of the Result


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Mon May 4, 9:07 AM
root
windows_10_lc15d6.pdf
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 47) Fit Page Width
Index
[Nessus - Iceweasel]
windows_10_lc15d6...
Type here to search
1:37 PM
5/4/2020
ENG
Right Ctrl

Nessus Report

Nessus Scan Report

04/May/2020:08:56:15

HomeFeed: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the ProfessionalFeed in order to be compliant with our license agreement: http://www.nessus.org/products/nessus-professionalfeed

Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Mon May 4, 9:07 AM
root
Nessus - Iceweasel
File Edit View History Bookmarks Tools Help
Nessus
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng Nessus
Nessus vulnerability scanner
root Help & Support Sign Out
Results Scan Queue Scan Templates Policies Users Configuration
Filter Options Audit Trail Delete All Results
Hosts
Vulnerabilities
Export Results
Export Cancel
[Nessus - Iceweasel] Nessus - Iceweasel
Type here to search
1:37 PM
5/4/2020
ENG
Right Ctrl

https://127.0.0.1:8834/html5.html#/results/580798cb-4906-110e-df05-48bb01c1929b8b10b25be162f93b/export

windows_10 Export Results

This result set contains 1 note. Please click this notification dialog for more information.

Export Scan Results

Export Format: PDF

Select chapters to include

Hosts Summary (Executive) | Vulnerabilities By Host | Vulnerabilities By Plugin

© 1998 - 2020 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1 - HomeFeed

Figure: 3.5-report of summary results PDF

- Export the summary result PDF of the scan. (Nessus report).
- We can view all results of the Nessus scan using generated report.

4. Vulnerability declaration:

- It has medium type vulnerability called SMB signing disabled. We are going to describe this vulnerability with more details.

❖ Synopsis

➢ This vulnerability in medium state and it cannot exploit. So, their synopsis shows signing disabled on the SMB server. The synopsis describes about the vulnerability in short form. SMB Marking Disabled may be a Medium risk powerlessness that's one of the foremost regularly found on networks around the world. ... Marking is crippled on the inaccessible SMB server. This will permit man-in-the-middle assaults against the SMB server. SMB servers ought to both require marks as well as support them.

❖ Description

➢ Description provide the more details of the vulnerability and what is the risk also. This shows the attack can be happen to the server. In this scan, it shows man-in-the-middle-attack against the SMB server.

❖ Solution

➢ Solution provide the description to mitigate or ignore this vulnerability. So, it shows the solution for mitigate this problem. So, it shows Enforce message signing in the hosts configuration, on windows this is found in the local security policy on Samba, the setting is called “server signing” And it provides the links to get more details.

❖ See also

➢ It provides the more details to ignore these problems using three links.
➢ Microsoft link, Nessus link Samba link.

❖ Plugin information

➢ It provides plugin ID
➢ Plugin version
➢ Plugin type
➢ Publication date
➢ Modification date
➢ ID -57608, version – 1.7 version, type – remote

- Risk information

- It shows Risk factor. It shows type of the Risk. This is a medium risk.
- it shows risk factor value per the risk type and the danger of risk. It provides 1- 10 value as the factor rate. It shows 5 factor value per the medium type.
- CVSS is well suited as a standard estimation framework for businesses, organizations, and governments that require precise and reliable powerlessness seriousness scores. Vector score provide as vector string.

- Vulnerability information

- CPE is an industry standard that's utilized to supply a uniform way to appear data on Working Frameworks, equipment, and program. It can be utilized for program and equipment stock, and superior defenselessness administration when utilizing the comes about from one item to be followed in a diverse item.
- It also provides vulnerability publication data as a 2012/01/17

We found 19 vulnerabilities from the windows 10 server scan report. It includes one medium type vulnerability and the 18 other general vulnerabilities. The vulnerabilities prioritize from critical to low. Critical vulnerabilities can be exploit. So this report did not contain any critical vulnerability.

References:

1. **Oracle 2020, "Virtual box", Viewed 26th April 2020, <www.virtualbox.org>**

2. **Tenable 2020, "Run your first scan with Nessus, online", viewed 25th April 2020,** <https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus>

3. **Technux 0 2018, YouTube, 'Getting start with Nessus vulnerability scanner", 26th April 2020,** <https://www.youtube.com/watch?v=rdENa32eVvY >

4. **Veronis team, Veronis.com, "what is IT security Audit? The basics", viewed 2nd May 2020,** <https://www.varonis.com/blog/security-audit/>

5. **Tenable, "Nessus professional", 2nd May 2020,** <https://www.tenable.com/products/nessus/nessus-professional>

6. **Mark Gibbs, NETWORKWORLD, "The top Wi-Fi pen testing tools in Kali Linux 2.0" 2nd May 2020,** <https://www.networkworld.com/article/3035566/the-top-wi-fi-pen-testing-tools-in-kali-linux-20.html>

7. **Get wall papers 2018, " HD Windows 10 Logo Wallpapers", viewed 2nd May 2020,** <http://getwallpapers.com/collection/hd-windows-10-logo-wallpapers>

8. **Shubh Malviya 2017 oct 29, YouTube, "Connecting Two Virtual Machines using Virtual Box", viewed 25th April 2020,** <https://www.youtube.com/watch?v=JgMFQcM3Tis>