



Information Assurance & Auditing

4th year 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:

Introduction.....	4
Security auditing tool that using for following assessment criteria.....	5
Other auditing instruments and operating systems.....	6
Scanning process with procedure.....	7
Reference.....	11

Figure of table:

Figure: 1.1-Nessus tool.....	5
Figure: 2.1-operating systems.....	6
Figure: 3.1-initial state.....	7
Figure: 3.2-start Nessus.....	8
Figure: 3.3- scan using Nessus.....	9
Figure:3.4- view results.....	9
Figure: 3.5-report of summary results PDF.....	10

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

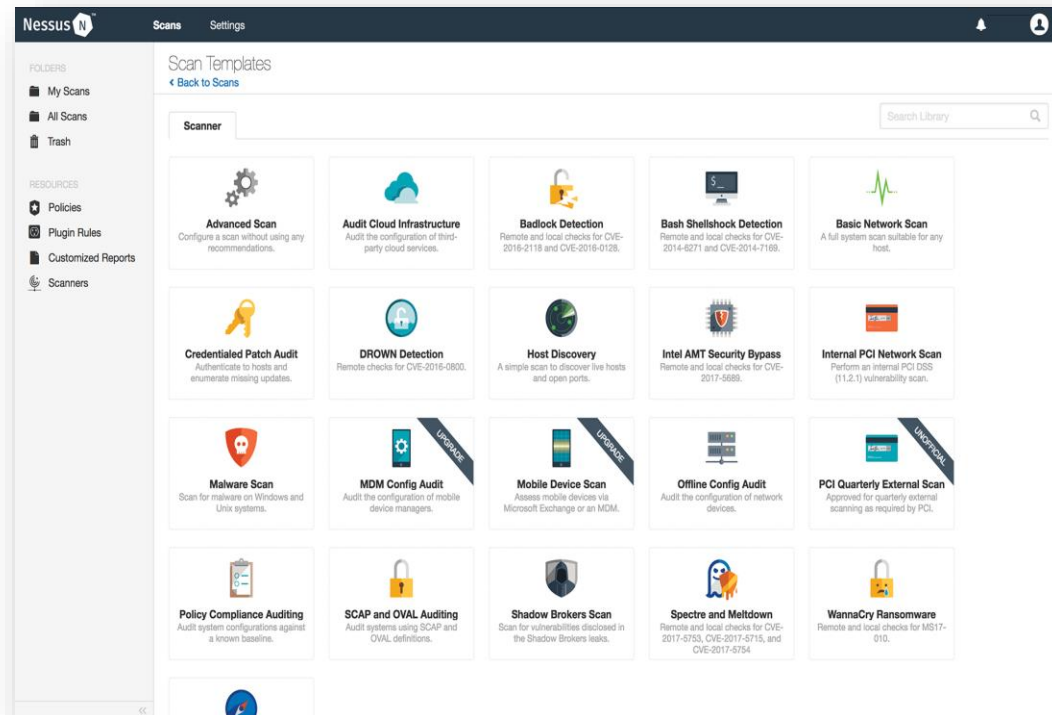


Figure: 1.1-Nessus tool [5]

- 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.

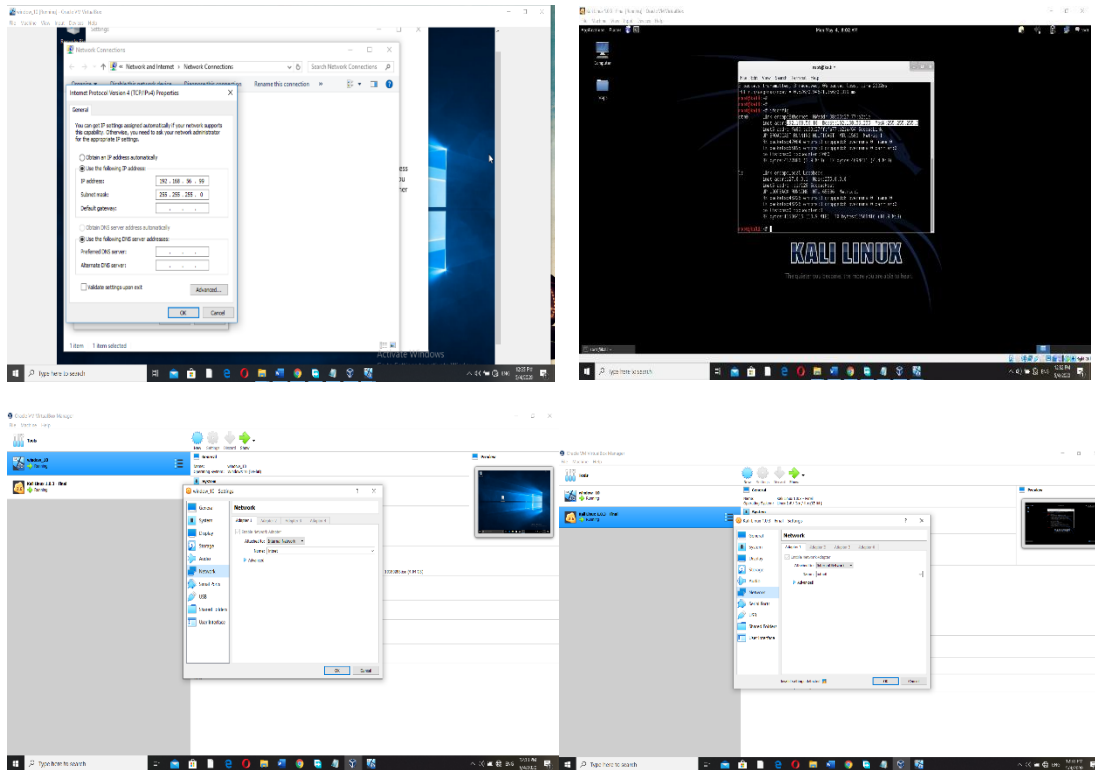


Figure: 3.1-initial state

- 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

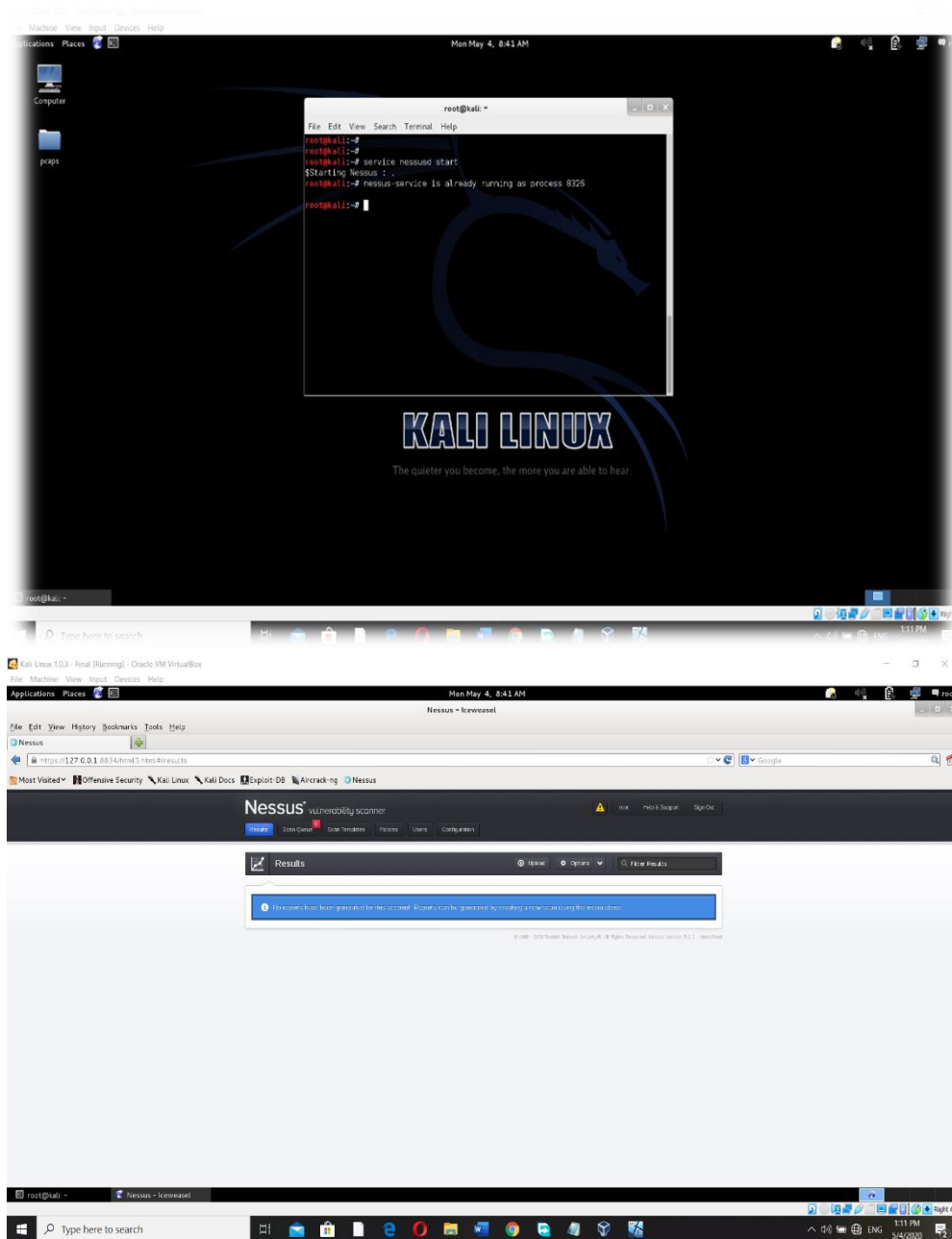


Figure: 3.2-start Nessus

- Login to the Nessus by providing username and password.

-

- 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 all vulnerabilities](#)

- Export a report of summary of the Result

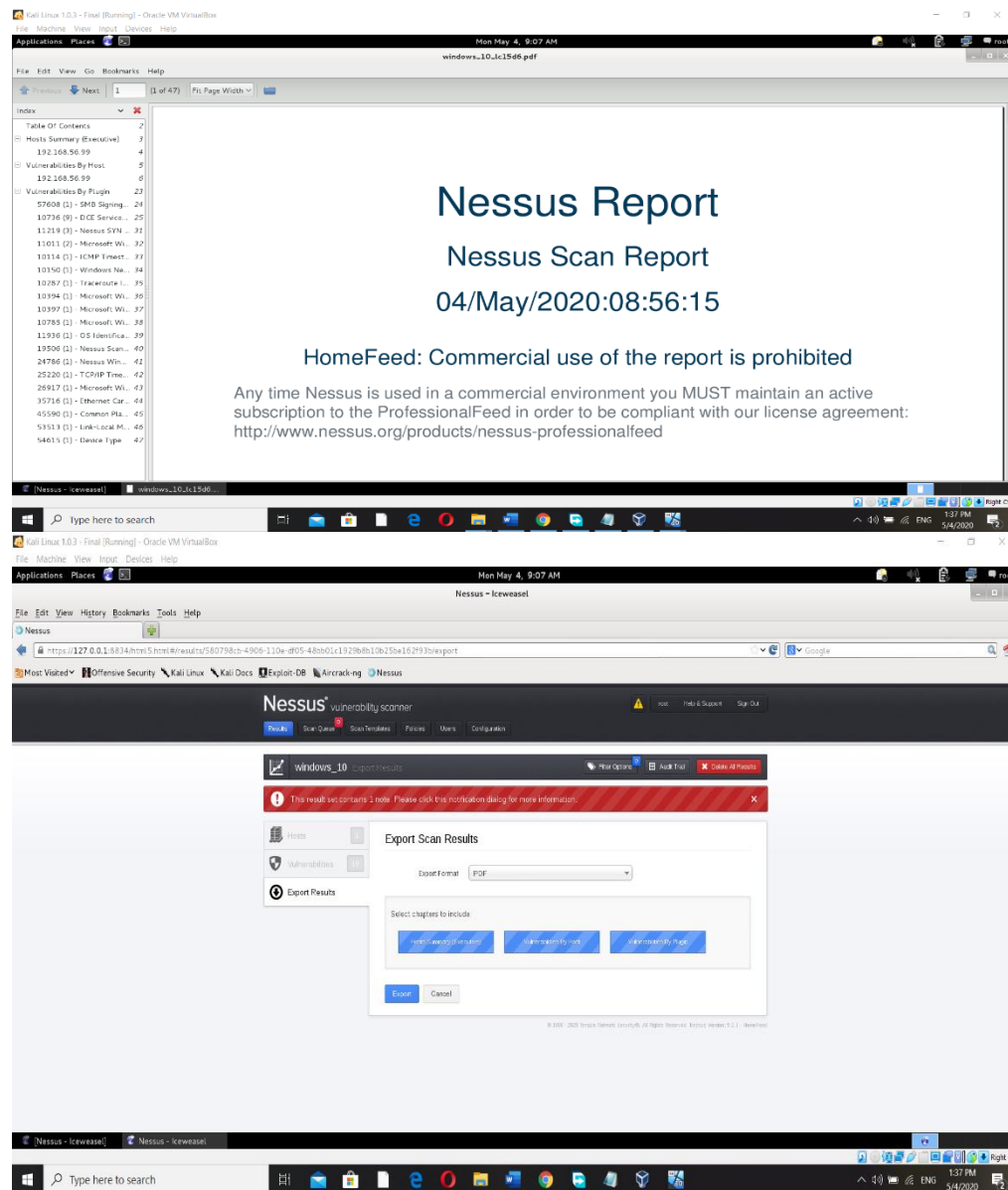


Figure: 3.5-report of summary results PDF

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

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>>

