KALASALINGAM
ACADEMY OF RESEARCH & EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A" Grade

SCHOOL OF COMPUTING

Department of Computer Science and Engineering

IT PHYSICAL SECURITY & SYSTEM SECURITY

Lab Manual (213CSE2309)

Student Name : …………………………………….. ……………………………….

Register Number : ……………………………………….

Section : ……………………………………………...

KALASALINGAM
ACADEMY OF RESEARCH & EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A" Grade

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Bonafide record of work done by____

of________________ in ___________IT Physical security and System Security___________

during odd semester in academic year 2023-2024.

Staff In-charge Head of the Department

Submitted to the practical Examination held at Kalasalingam University, Krishnankoil on

____

REGISTER NUMBER

INTERNAL EXAMINER **EXTERNAL EXAMINER**

EXPERIMENT EVALUATION SUMMARY

Name: **Reg No:**

Class: Slot 1 (10203) **Faculty: Dr. T. Manikumar**

S.No	Date	Experiment	Marks (100)	Faculty Signature
1		Installation of MBSA (Microsoft Baseline Security Analyzer)		
2		How to scan the computer by using Microsoft Baseline Security Analyzer (MBSA)		
3		How to scan by computer by using IP address		
4		How to install the trip wire		
5		How to configure the trip wire		
6		Secure check scanning using tripwire		
7		Nikto Web analysis		
8		Unix Private security check		

INTRODUCTION

IT Physical security and System Security (213CSE2309)

Information security, sometimes abbreviated as InfoSec, encompasses the tools and processes organizations use to protect their information. This includes setting policies to ensure unauthorized persons cannot access business or personal information. InfoSec is a constantly growing and evolving field with many areas of specialization ranging from network and infrastructure security to testing and auditing.

Information security prevents the inspection, recording, modification, disruption, or destruction of sensitive information like account details or biometrics. Repercussions of security incidents can include identity theft, tampering with information, or data wiping. From a business perspective, security disruptions interrupt workflow and cost money while damaging a company's reputation. Organizations need to allocate funds for security and ensure that their personnel are equipped to detect and deal with threats from software attacks like phishing, malware, viruses and malicious insiders.

Information security goals

Information security focuses on the three objectives, confidentiality, integrity, and availability, which are collectively known as CIA:

Confidentiality—preventing the disclosure of information to unauthorized users. This requires implementing access restrictions to protect personal privacy and proprietary information. Failure to maintain confidentiality, whether as a result of an accident or an intentional breach, can have severe consequences for businesses or individuals, who often cannot undo the damage. For example, a compromised password is a breach of confidentiality, and once it has been exposed, there is no way to make it secret again. The most publicized security incidents often involve a breach of confidentiality.

Data integrity—ensuring the accuracy and authenticity of data. Only authorized persons may edit data, and they need to follow procedures to prevent former employees from retaining the ability to alter company data. A failure of integrity could, for example, allow a malicious attacker to redirect traffic from your website, or to edit or delete the content on your website.

Availability—authorized users should have reliable access to information when they need it. This often requires collaboration between departments, such as development teams, network operations, and management. An example of a common threat to availability is a denial of service (DoS) attack, where an attacker overloads or crashes the server to prevent users from accessing a website.

Types of Information Security

Application Security

Application security involves protecting software applications by preventing, detecting, and fixing bugs and vulnerabilities. Software vulnerabilities often affect web and mobile applications, as well as application programming interfaces (APIs). They provide an entry point for malicious attacks, so you need to be able to find and fix them. Specialized tools for security testing and application shielding provide protection for various aspects of your application portfolio. Security testing lets you assess coding threats so you can commit code safely. It can be static, involving code analysis at fixed points in the development pipeline; dynamic, involving analysis of running code; or interactive, which combines elements of both. App shielding tools like firewalls make it harder for hackers to carry out attacks.

Much of the security process takes place during the development stage, but efforts to secure your apps must continue after deployment. The responsibility for application security should cut across multiple teams, from network and desktop operations to development.

Cloud Security

Cloud security includes the protection of data, applications, and infrastructures involved in cloud computing. High-level security concerns—unauthorized data exposure and leaks, weak access controls, susceptibility to attacks, and availability disruptions—affect traditional IT and cloud systems alike.

It can be a challenge to safely build and host your software on the cloud. Since cloud computing involves shared environments you have to make sure your process is adequately isolated. You also need to ensure that any third-party cloud applications you use are safe. However, centralization facilitates the management of your cloud security needs.

Some IT departments are reluctant to move mission-critical systems to the cloud. All cloud models, whether public, private, or hybrid, are susceptible to threats. You can apply a set of policies, controls, and tools to help protect your systems and data, maintain compliance with licenses and regulations, and safeguard the privacy of your users. For example, authentication rules limit access to authorized users or devices.

Your cloud provider may offer solutions for cloud security, which is the joint responsibility of your organization and provider. You need to choose the right security solution to protect your organization from threats like unauthorized access and data breaches while reaping the benefits of cloud computing.

Cryptography

Cryptography covers a range of techniques for communicating in a secure manner. Cryptography and encryption are becoming increasingly important as organizations store, edit, and transmit sensitive information online. You can use encryption to protect the confidentiality and integrity of your data while in transit and at rest and digital signatures to validate the authenticity of your data.

Infrastructure Security

Traditional security perimeters protecting digital infrastructures are becoming blurred. As organizations take advantage of information technology and the internet, critical infrastructures like data centers, internal and external networks, servers, desktops, and mobile devices have become highly interconnected. This makes them vulnerable to threats like sabotage by a disgruntled employee or cyber terrorist groups, information warfare waged by private profiteers or rival countries, and natural disasters like earthquakes or hurricanes that can damage physical structures.

The interdependence of infrastructures means that a failure or disruption in one system can spread to others. You can reduce this risk by restricting access points between networks. You should also ensure all your data is backed up, which can mitigate the damage to your infrastructure.

Vulnerability Management

Vulnerability management is a means of reducing the risk of flaws in code or in the design of an application. When you expand your infrastructure, provide access to new users, or add new applications to your system, you are also increasing the potential vectors for attack. You can also find new vulnerabilities in old code.

Build in a schedule to constantly scan your digital environment for potential vulnerabilities so you can apply patches or remove defective code. Having a system in place to assess the risks associated with vulnerabilities will help you find and prioritize remediation. It is important to identify vulnerabilities early on so can save your organization the costs of a breach.

KALASALINGAM
ACADEMY OF RESEARCH & EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A" Grade

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE AN ENGINEERING

COURSE PLAN

Subject with code	IT Physical Security and System Security (213CSE2309)
Degree/Branch	B.Tech/CSE
Year/Semester	II/III
Course Credit	3 (Theory with Practical)
Course Coordinator	Dr.B.Pitchaimanickam
Module Coordinator	Dr.N.C.Brintha
Programme Coordinator	Dr.N.C.Brintha

COURSE PRE-REQUISITE:

Students should have basic knowledge about Information Security.

COURSE DESCRIPTION

This course will discuss the major tools and techniques used for securing the system and information. This course includes the installation of Microsoft Baseline Security Analyzer (MBSA), scanning the computer by using MBSA, scanning of IP address, tripwire installation, tripwire configuration, tripwire secure check, nikto web analysis and Unix private security check. As a result, you will learn how to install and check the systems security with recent tools such as Microsoft Baseline Security Analyzer, Tripwire and Nikto tool.

COURSE OBJECTIVES:

After completing the course, students should be able,

1. To understand the physical security and vulnerability assessment.

2. To understand the different strategies for security surveys and audit.

3. To understand the various approaches to the physical security and Intrusion Detection System (IDS).

4. To understand the video technology, biometric characteristics,control standards and fence standards.

5. To understand the fire safety and standards and guidelins for global resources and security personnel.

COURSE OUTCOMES:

COs	**DESCRIPTION**
CO1	Understand the importance of physical security, to relate between physical and cyber security and perform vulnerability assessment.
CO2	Deep understanding of Physical Security layers, to know what plans and tools are required for a particular environment, and perform survey and audit.
CO3	Understand the approaches to physical security, alarm and intrusion detection system (IDS).
CO4	Enumerate methods employed to mitigate video technology, bio metrics, access control and fence standards for ensuring the physical security.
CO5	Understand the meaning of fire safety inspection, to use the standards, regulations, guidelines and compliance of security personnel to give the solution for future risks.

PROGRAMME SPECIFIC OUTCOMEs

PSOs	DESCRIPTION
PSO1	**Problem-Solving Skills:** The ability to apply mathematics, science and computer engineering knowledge to analyze, design and develop cost effective computing solutions for complex problems with environmental considerations.
PSO2	**Professional Skills**: The ability to apply modern tools and strategies in software project development using modern programming environments to deliver a quality product for business accomplishment.
PSO3	**Communication and Team Skill:** The ability to exhibit proficiency in oral and written communication as individual or as part of a team to work effectively with professional behaviors and ethics.
PSO4	**Successful Career and Entrepreneurship:** The ability to create a inventive career path by applying innovative project management techniques to become a successful software professional, an entrepreneur or zest for higher studies.

PROGRAMME OUTCOMES

POs	DESCRIPTION
PO1	Ability to apply knowledge of mathematics, science and computer engineering to solve computational problems.
PO2	Identify, formulate, analyze and solve complex computing problems.
PO3	Capability to design and develop computing systems to meet the requirement of industry and society with due consideration for public health, safety and environment.
PO4	Ability to apply knowledge of design of experiment and data analysis to derive solutions in complex computing problems and society with due consideration for public health, safety and environment.
PO5	Ability to develop and apply modeling, simulation and prediction tools and techniques to engineering problems.
PO6	Assess and understand the professional, legal, security and societal responsibilities Relevant to computer engineering practice.
PO7	Ability to understand the impact of computing solutions in economic, environmental and societal context for sustainable development.

PO8	Applying ethical principles and commitment to ethics of IT and software profession.
PO9	Ability to work effectively as an individual as well as in teams.
PO10	Effectively communicating with technical community and with society.
PO11	Demonstrating and applying the knowledge of computer engineering and management principles in software project development and in multidisciplinary areas.
PO12	Understanding the need for technological changes and engage in life-long learning.

ABET – CSO STATEMENT

At the end of the programme, the students will be able to:

CSO1 : Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

CSO2 : Design, implement, and evaluates a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.

CSO3 : Communicate effectively in a variety of professional contexts.

CSO4 : Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

CSO5 : Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

CSO6 : Apply Computer Science theory and software development fundamentals to produce computing-based solutions.

ABET – ESO STATEMENT

At the end of the programme, the students will be able to:

ESO1 : Ability to identify, formulate and solve complex engineering problems by applying principles of Engineering, Science, and Mathematics.

ESO2 : Ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.

ESO3 : An ability to communicate effectively with a range of audiences.

ESO4 : Ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.

ESO5 : Ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.

ESO6 : Ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions.

MAPPING OF COURSE OUTCOMES WITH PO, PSO

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CO 1	S	S	S										S	S		S
CO 2	S	S	S										S	S		S
CO 3	S	S	S	S	S		S				S	S	S	S		S
CO 4	S	S	S										S	S		S
CO 5	S	S	S	S	S		S				S	S	S	S		S

S- Strong Correlation M- Medium Correlation L – Low Correlation

WEB RESOURCES

S.No	Topic Name	Website Link
1	Installation of MBSA (Microsoft Baseline Security Analyzer)	https://www.technology.pitt.edu/help-desk/how-to-documents/help-using-microsoft-baseline-security-analyzer-mbsa
2	How to scan the computer by using Microsoft Baseline Security Analyzer (MBSA)	https://www.microsoft.com/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/

3	How to scan by computer by using IP address	https://www.microsoft.com/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/
4	How to install the trip wire	https://medium.com/@Alibaba_Cloud/how-to-install-and-configure-tripwire-ids-on-ubuntu-16-04-d7941c6b4db9
5	How to configure the trip wire	https://medium.com/@Alibaba_Cloud/how-to-install-and-configure-tripwire-ids-on-ubuntu-16-04-d7941c6b4db9
6	Secure check scanning using tripwire	https://tripwire-securecheq.software.informer.com/1.0/
7	Nikto Web analysis	https://null-byte.wonderhowto.com/how-to/scan-for-vulnerabilities-any-website-using-nikto-0151729/#:~:text=Nikto%20is%20a%20simple%2C%20open,exploit%20or%20hack%20the%20site.&text=Any%20site%20with%20an%20intrusion,detect%20that%20it's%20being%20scanned.
8	Unix Private security check	https://phoenixnap.com/kb/linux-ssh-security

LIST OF EXPERIMENTS

S.No	Experiment Details	Number of Periods	Cumulative Number of Periods
1	Installation of MBSA (Microsoft Baseline Security Analyzer)	2	2
2	How to scan the computer by using Microsoft Baseline Security Analyzer (MBSA)	2	4
3	How to scan by computer by using IP address	2	6
4	How to install the trip wire	2	8
5	How to configure the trip wire	2	10
6	Secure check scanning	2	12
7	Nikto Web analysis	2	14

8	Unix Private security check	2	16

ADDITIONAL EXPERIMENTS:

1. Network Intrusion Prevention and Detection systems
2. Network Packet tracer

ASSESSMENT METHOD:

S.No	Assessment	Split up
1	Internal Assessment (50 marks)	Regular Lab Exercises (20)
		Model Lab (30)
2	External Assessment (50 marks)	Algorithm/Procedure(10)
		End Semester program and output(30)
		Viva voce(10)

RUBRICS FOR INDIVIDUAL EXPERIMENTS

Modules	Unacceptable	Fair	Acceptable	Excellent
Level of understanding	Very little background information provided or information is incorrect (1)	Some introductory information, but still missing some major points(4)	Introduction is nearly complete, missing some minor points(7)	Introduction complete, provides all necessary background principles for the experiment(10)
Algorithm/ Procedure	Several major aspects of the exercise are missing, student displays a lack of understanding about how to write an	Algorithm/Procedure misses one or more major aspects	Algorithm /Procedure is nearly complete, missing some minor points	Algorithm/Procedure is complete and well-written; provides all

	algorithm /Procedure (2)	of carrying out the exercise (6)	(10)	necessary background principles for the exercise(15)
Design principles & Logic	Missing several important experimental details are not written in proper logic in program (10)	Written in proper logic, still missing some important details (20)	Written in proper logic, important details are covered, some minor details missing (30)	Design principles and Logic is well written, all details are covered (40)
Output	Output contains errors or are poorly constructed, (2)	Partial output; missing some important output features(4)	Output is good but some minor problems or could still be improved(7)	Output is excellent (10)
Discussion/ Viva	Answered for less than 40% of the questions indicating a lack of understanding of results (2)	Answered for 60% of the questions. but incomplete understanding of results is still evident(4)	Answered for 60% of the questions. Still need some improvements (7)	Answered for more than 90% of the questions correctly, good understanding of results is conveyed(10)

Ex .No 1 INSTALLATION OF Microsoft Baseline Security Analyzer (MBSA)

AIM:-

To install the Microsoft Baseline Security Analyzer (MBSA) for checking the security updates.

THEORY:-

The **Microsoft Baseline Security Analyzer (MBSA)** is a software tool that helps determine **the security of your Windows** computer based on Microsoft's security recommendations. MBSA can be used **to improve your security management process** by analyzing a computer or a group of computers and detecting missing patches/updates and common security misconfigurations. After you run a MBSA scan, the tool will provide you with specific suggestions for remediating security vulnerabilities. An MBSA scan can reduce and eliminate possible threats caused by security configuration problems and missing security updates. This document explains how to use MBSA from the graphical user interface (GUI).

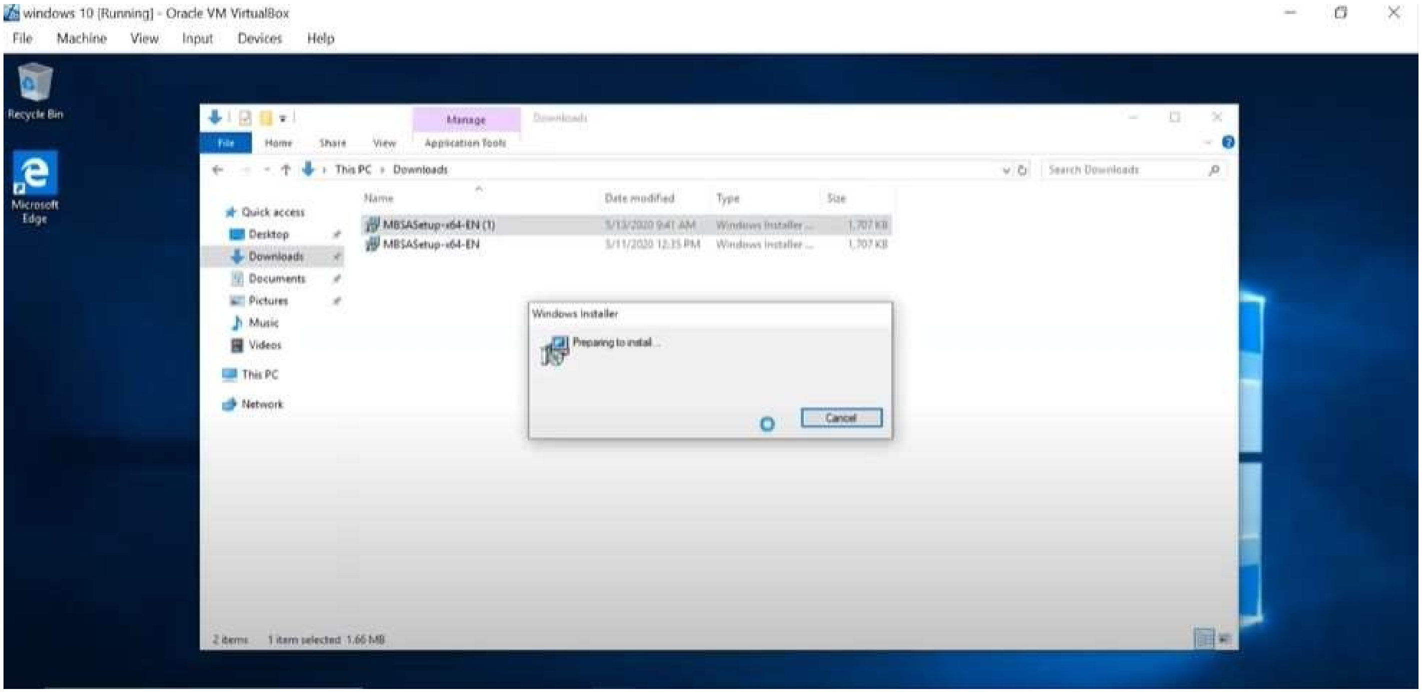
MBSA performs the following actions during a scan:

- Checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server.
- Scans a computer for insecure configuration settings. When MBSA checks for Windows service packs and patches, it includes in its scan Windows components, such as Internet Information Services (IIS) and COM+.
- Uses Microsoft Update and Windows Server Update Services (WSUS) technologies to determine what updates are needed.

Procedure:

1) Open the web browser such as www.google.com
2) Download the Microsoft Baseline Security Analyzer 2.1.1 for IT professional
3) Choose the downloaded file name like as MBSASetup-X64-EN-msi
4) Click next
5) Save the downloaded file.
6) Right click the downloaded file and install.
7) Microsoft Baseline Security Analyzer Setup dialog box will appear and click the option button to agree the license agreement and click next.
8) Set the destination folder by clicking the browse option.
9) Start the installation by clicking the install.
10) By getting acknowledgment for installing the setup file in your device and click "yes"
11) Microsoft Baseline Security Analyzer setup has completed successfully.
12) Open the MBSA
13) Check the computers for common security misconfigurations and MBSA can running Microsoft windows server 2008 R2,Windows 7,Windows server 2003,windows server 2008,Windows vista, Windows XP or Windows 2000 and also have the three options like i) Scan a computer ii) Scan multiple computers iii) view existing security scan reports.

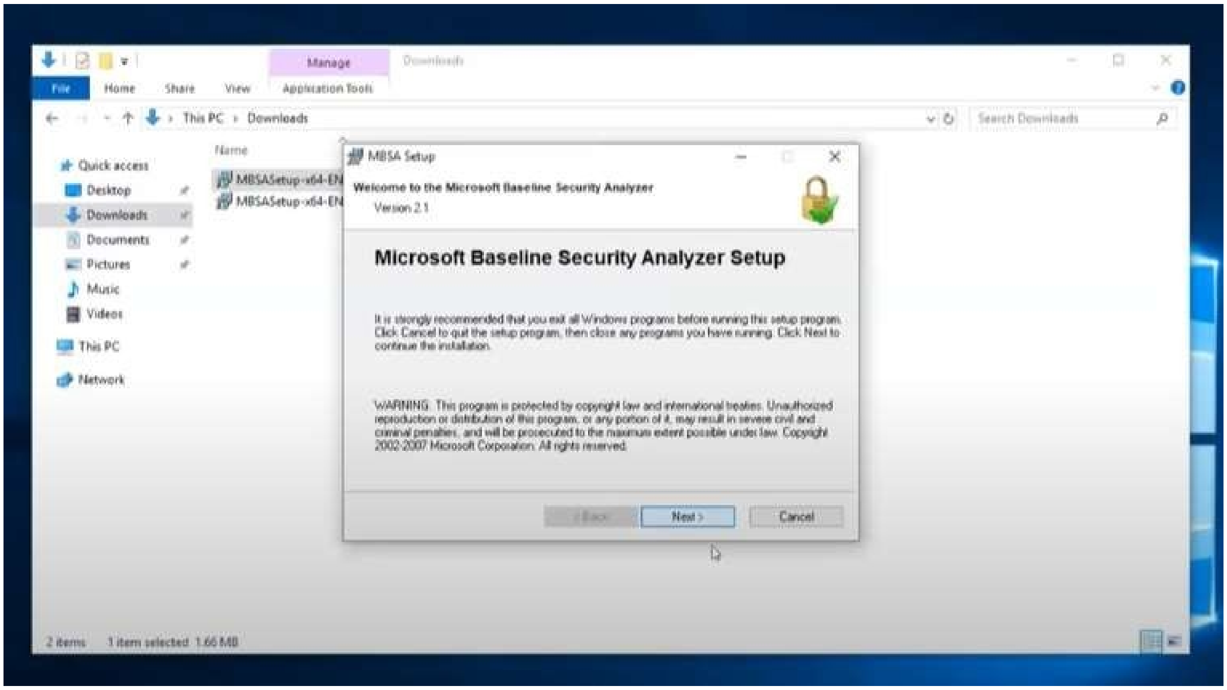
Screen shots:-



Name	Date modified	Type	Size
MBSASetup-x64-EN (1)	5/13/2020 9:41 AM	Windows Installer ...	1,707 KB
MBSASetup-x64-EN	5/11/2020 12:35 PM	Windows Installer ...	1,707 KB

Windows Installer

Preparing to install...



MBSA Setup

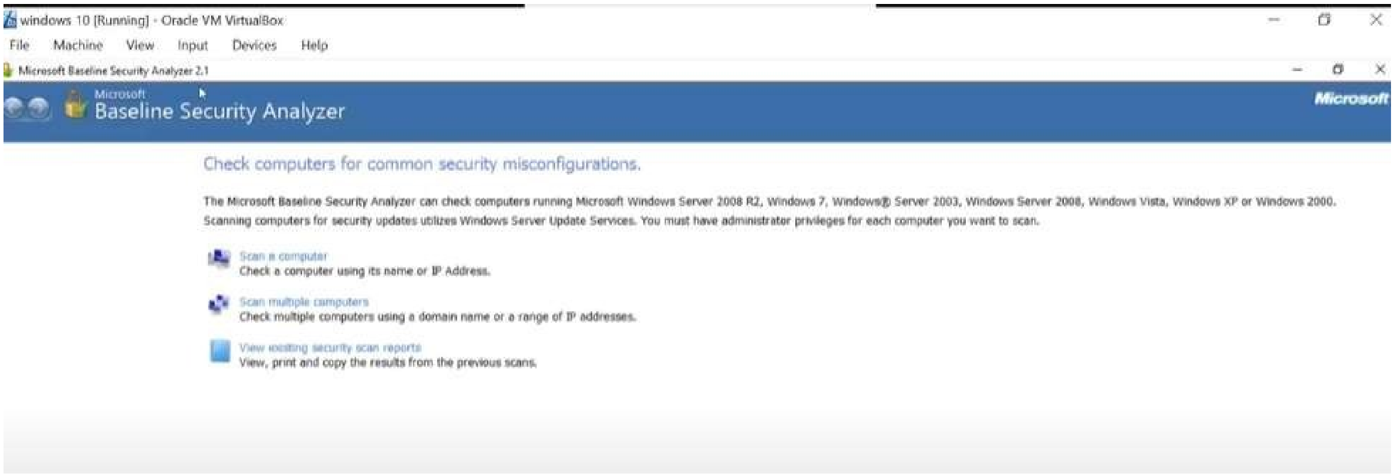
Welcome to the Microsoft Baseline Security Analyzer

Version 2.1

Microsoft Baseline Security Analyzer Setup

It is strongly recommended that you exit all Windows programs before running this setup program. Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law. Copyright 2002-2007 Microsoft Corporation. All rights reserved.



windows 10 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, Windows XP or Windows 2000. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

/

VIVA QUESTIONS: -

1. What is meant by information security?
2. What are the design goals of information security?
3. What is meant by Microsoft Baseline Security Analyzer?
4. What are the actions performed in MBSA during scanning process?

EVALUA+TION:-

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT:-

Thus, the Microsoft Baseline Security analyzer is installed successfully.

Ex .No 2 How to scan the computer by using Microsoft Baseline Security Analyzer (MBSA):-

AIM

To scan the computer by using Microsoft Baseline Security Analyzer (MBSA).

THEORY

The MBSA provides built-in checks to determine if Windows administrative vulnerabilities are present, if weak passwords are being used on Windows accounts, the presence of known IIS and SQL administrative vulnerabilities, and which security updates are required on each individual system. The MBSA provides dynamic assessment of missing security updates. The MBSA can scan one or more computers by domain, IP address range or other grouping. Once complete, the MBSA provides a detailed report and instructions on how to help turn your system into a more secure working environment. The MBSA will create and store individual XML security reports for each computer scanned and will display the reports in the graphical user interface in HTML.

To use the MBSA tool, users will need either Windows Server 2008 R2, Windows 7, Server 2003, Server 2008, Vista, XP or Windows 2000 and will need administrator privileges sufficient to scan the target computers.

After installing MBSA and running the tool, users are taken to the screen seen below which provides quick access to three different sides of the application. Users can scan a computer using its name or IP address, scan multiple computers within a domain name or a range of IP addresses, or view existing security scan reports. There are even more options available through the command-line interface to support scripting and fine-tuned control over MBSA’s scanning and reporting features.

PROCEDURE:-

1. Open the Microsoft Baseline Security Analyzer (MBSA) tool
2. This tool have three options namely i) Scan a computer ii) scan multiple computers iii) viewing existing security scan reports and click the option as scan a computer.
3. Give the name of the computer name and also options to check the security

i) Check for windows administrative vulnerabilities.

ii) Check for weak password

iii) Check for IIS administrative vulnerabilities

iv) Check for SQL administrative vulnerabilities

v) Check for the security updates.

4. Select the options and click the startscan option
5. This will take some time to complete the scan the system.
6. After scanning process, a report detail for the computer is generated with a date and time.
7. The report details includes the computer name, IP Address, Security report name, Scan date and Scanned with MBSA version and also security update catalog.
8. Choose the sort order by selecting the option “Score (worst first)”
9. The red color cross mark is displayed in the administrative vulnerabilities for indicating the problem and the automatic update of the system is not properly configured and warning symbol is occurred while scanning for the security updates.
10. In the window scan results, the green color tick mark has no issues for the administrative vulnerabilities such as File system, Auto logon, Guest account, Restrict Anonymous, Administrators and window firewall.

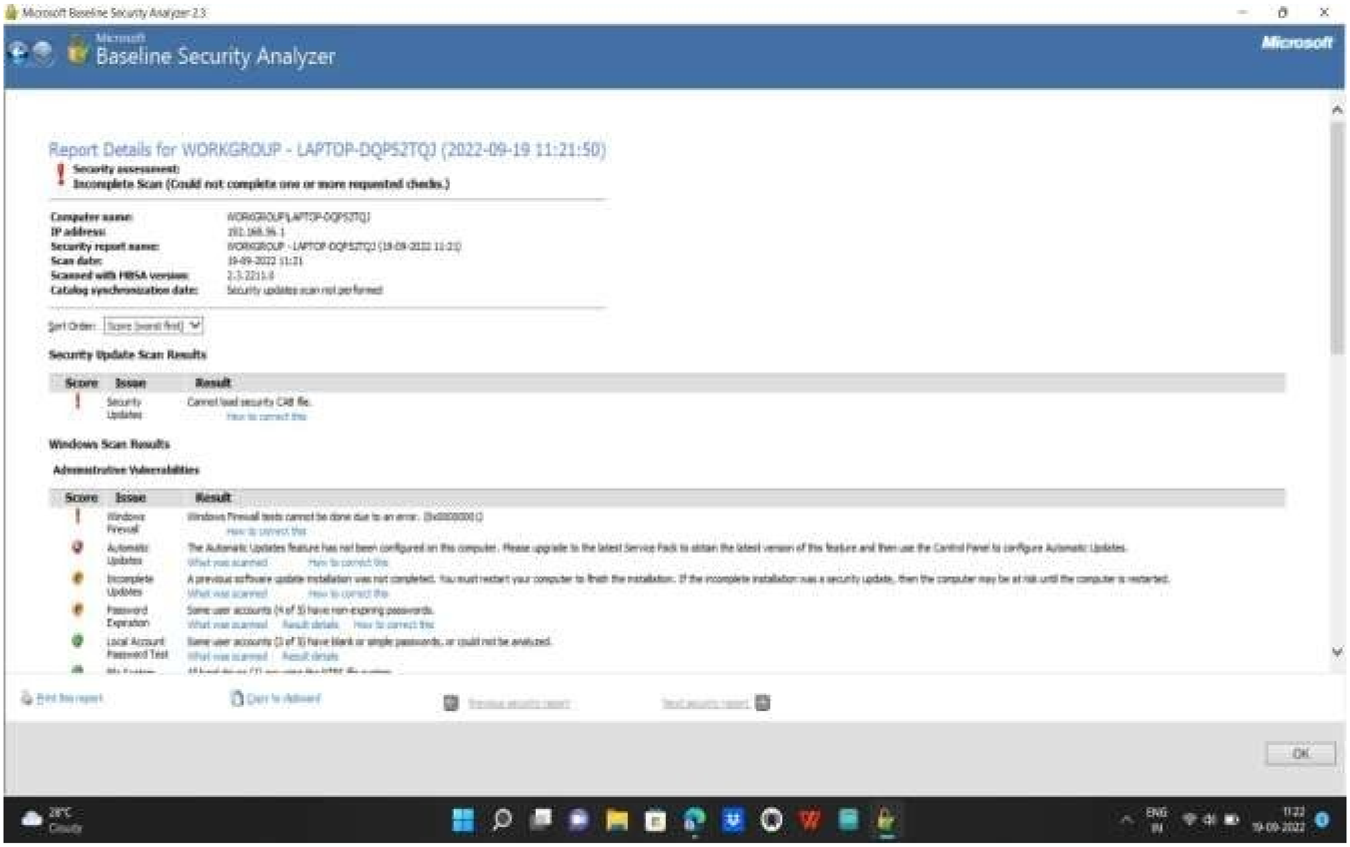
11. Additional information is also considered such as auditing, service, sharing and windows version during the scanning process.

12. Display the IIS (Internet Information Services) scan results but this service is not currently running the computer.

13. Display the SQL server scan results and MSDE status.

14. Display the desktop application scan results for the administrative vulnerabilities.

Screen shots:-



Microsoft Baseline Security Analyzer 2.3

Report Details for WORKGROUP - LAPTOP-DQPS2TQJ (2022-09-19 11:21:50)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	WORKGROUP\LAPTOP-DQPS2TQJ
IP address:	192.168.56.1
Security report name:	WORKGROUP - LAPTOP-DQPS2TQJ (19-09-2022 11:21)
Scan date:	19-09-2022 11:21
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	Security updates scan not performed

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
!	Windows Firewall	Windows Firewall tests cannot be done due to an error. (0x00000001) How to correct this
●	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
●	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
●	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
●	Local Account Password Test	Some user accounts (1 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details

VIVA QUESTIONS

1. What is meant by system security?
2. List the features of System security.
3. Difference between IP address and MAC address.
4. What is the expansion of IIS?

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the computer is scanned successfully by using the Microsoft Baseline Security Analyzer (MBSA).

Ex .No 3 How to scan the computer by using IP address in Microsoft Baseline Security Analyzer (MBSA)

AIM:-

To scan the computer by using IP address in Microsoft Baseline Security Analyzer (MBSA).

THEORY:-

In response to direct customer need for a streamlined method of identifying common security misconfigurations, Microsoft has developed the Microsoft Baseline Security Analyzer (MBSA). It includes a graphical and command line interface that can perform local or remote scans of Windows systems.

MBSA extends previous versions by adding support for Windows Vista. MBSA can be installed on computers running Windows Vista and it can scan Windows Vista computers. More information on the capabilities of MBSA is available on the MBSA Web site.

MBSA runs on Windows Vista, Windows Server 2003, Windows 2000, and Windows XP systems and will scan for common security misconfigurations in the following products: Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 5.0, and 6.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003. MBSA also scans for missing security updates, update rollups and service packs published to Microsoft Update.

PROCEDURE:-

1. Open the Microsoft Baseline Security Analyzer (MBSA) tool

2. This tool have three options namely i) Scan a computer ii) scan multiple computers iii) viewing existing security scan reports and click the option as scan a computer.

3. Get the IP address by opening command prompt and give the command "ipconfig"

4. Obtain the IP address for the Ethernet adapter Ethernet2.

5. Enter the IP address in the MBSA tool and also select the option for "Check for weak password" and select the start scan option.

6. After scanning process, the report will be generated with date and time.

7. The report details includes the computer name, IP Address, Security report name, Scan date and Scanned with MBSA version and catalog synchronization date.

8. Warning message for local account password test in the window scan process. Some of the user accounts have blank or simple passwords or could not be analyzed.

9. Click the result details for user accounts have blank or simple passwords.

10. Click the option "how to correct this" and also give the solution for password policy settings.

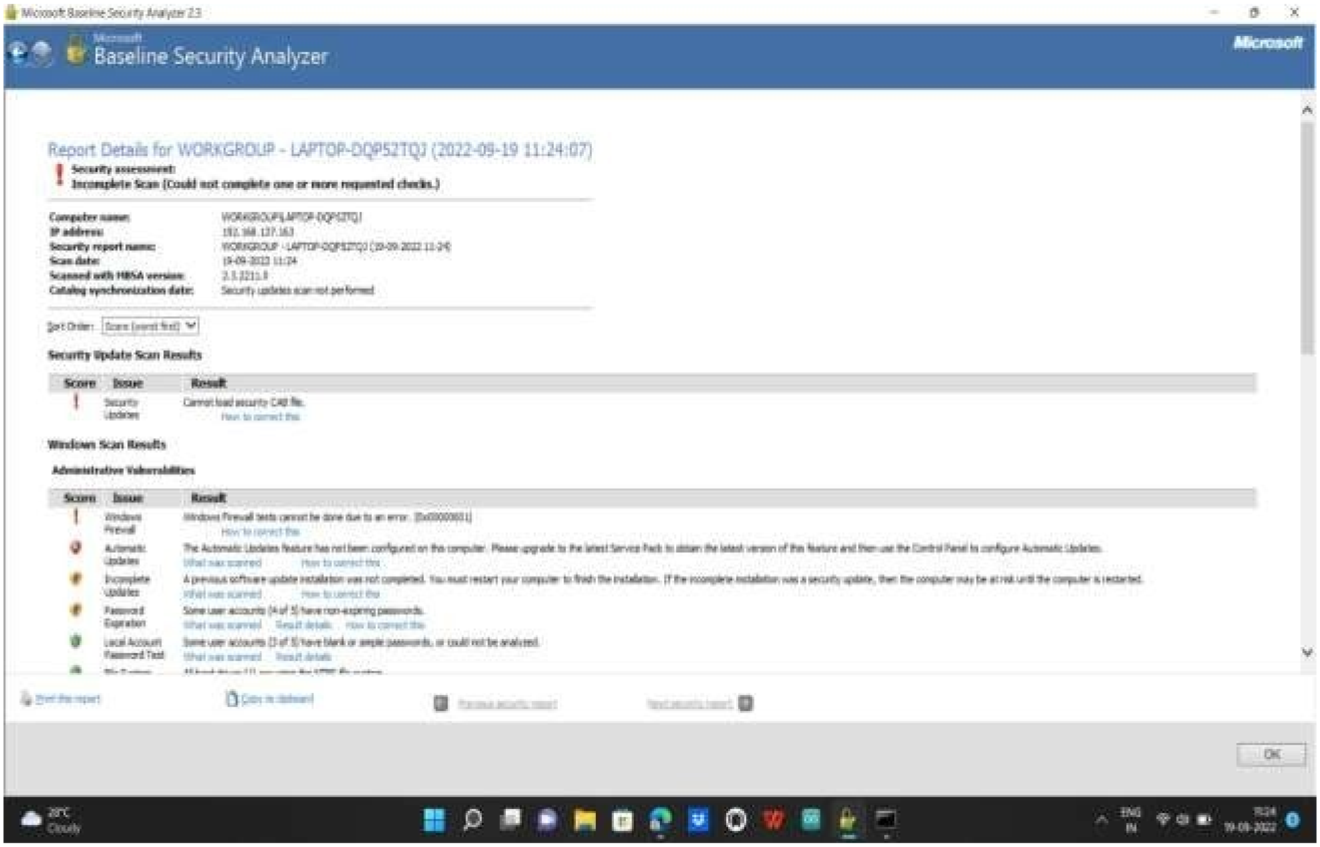
11. Open the control panel and double click the administrative tools and double click the local security policy.

12. Select the password policy from the account policies and display the security setting details of enforce password history, maximum password age, minimum password age, minimum password length.

13. By double clicking the maximum password age to change the number of days.

14. Based on the application demands to enable or disable the "Store passwords using reversible encryption".

Screen shots



Report Details for WORKGROUP - LAPTOP-DQP52TQJ (2022-09-19 11:24:07)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	WORKGROUP\LAPTOP-DQP52TQJ
IP address:	192.168.137.163
Security report name:	WORKGROUP - LAPTOP-DQP52TQJ (19-09-2022 11-24)
Scan date:	19-09-2022 11:24
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	Security updates scan not performed

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
!	Windows Firewall	Windows Firewall tests cannot be done due to an error. (0x00000001) How to correct this
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
⚠	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
⚠	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (2 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system.

VIVA QUESTIONS:-

1. What is meant by IP address?

2. Which command is used to find the IP address of the system?

3. How to set the password policy?

4. Define Encryption and Decryption.

5. What is the use of Ethernet adapter?

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the computer is scanned successfully by using the IP address in the Microsoft Baseline Security Analyzer (MBSA).

Ex.No.4 How to install the tripwire

AIM

To install the tripwire in Linux.

THEORY

Tripwire is a free and open source Intrusion Detection System (IDS). It's a security tool for monitoring and alerting file changes on the system. Tripwire is a powerful IDS that protects your system against unwanted changes. You can monitor your system files, including website files. So when there is any unwanted file change in any of the files that are being monitored, tripwire will check your system and will alert you (if that setup is in place).

PROCEDURE

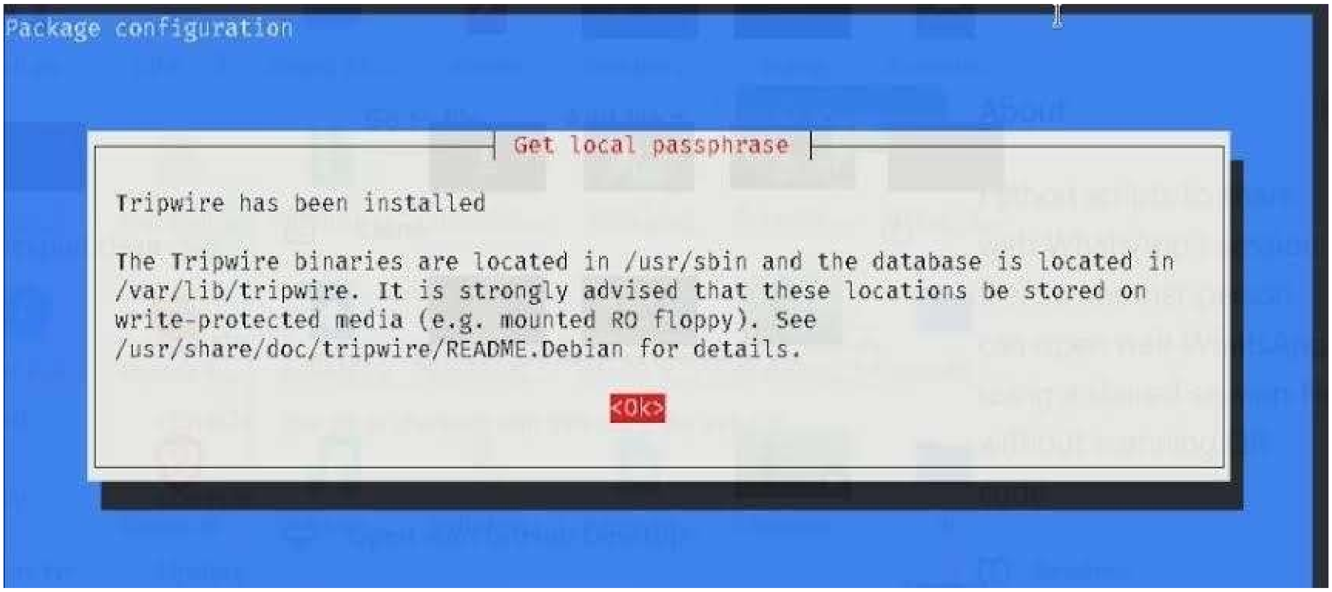
1. Open the onworks.net in the web browser.
2. Open the terminal in Linux.
3. Enter the command like
   a. "apt install tripwire”
4. If you give the command as sudo lsof \var\lib\dpkg\lock-frontend
5. Again you enter the command as **sudo apt install tripwire** .
6. This will take some time for installing based on your internet connection.
7. The configuration window for tripwire will appear and click “Ok” option
8. The package configuration window will appear to create/use your site key passphrase during installation and click the “Yes” option.
9. The package configuration window will ask to rebuild the tripwire configuration and click “yes”.
10. Enter the **site-key passphrase** and it should be remembered. If you forget the site-key passphrase then it will be difficult to recover the site-key passphrase.
11. Again you repeat the site-key passphrase and click “Ok”
12. Enter **the local key passphrase** and click “Ok”.

13. After giving these two values, trip wire has been installed.

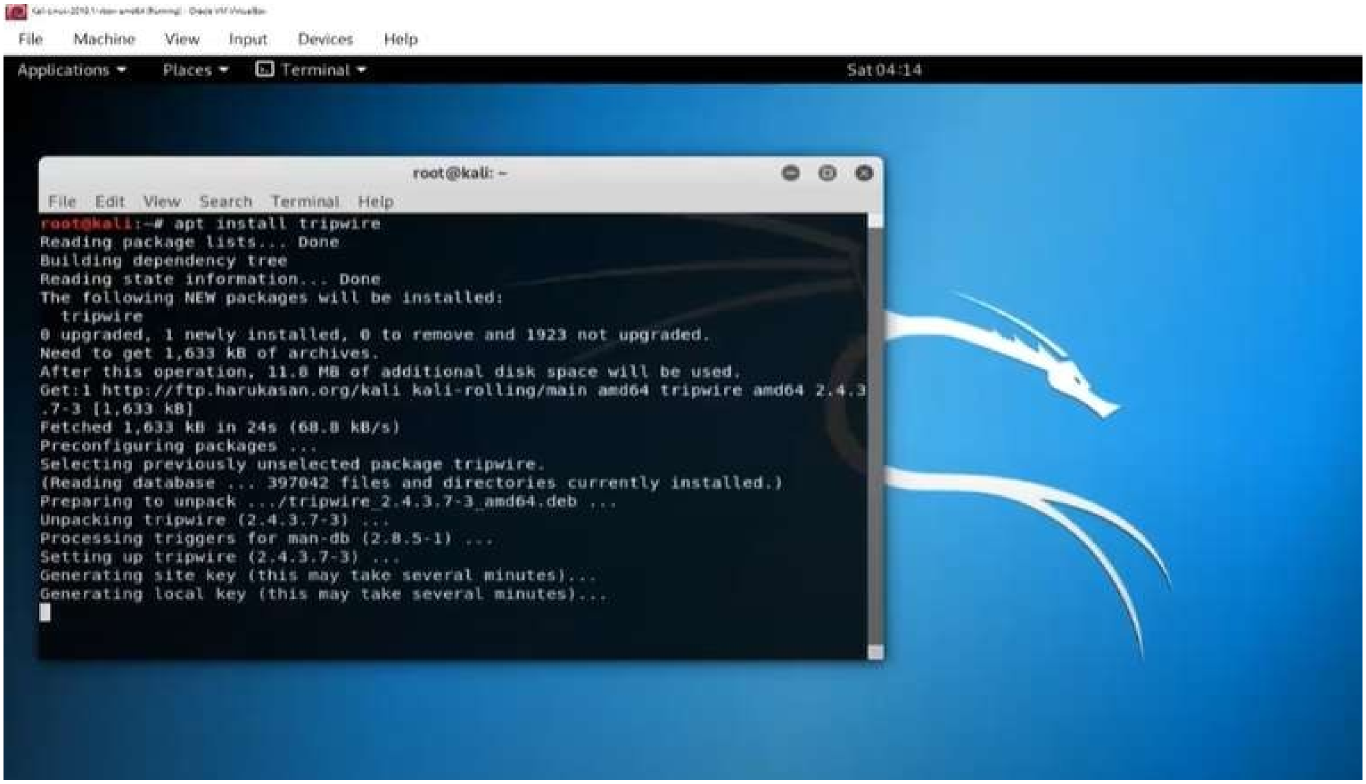
14. Display the location of tripwire.

Give the command as " **sudo tripwire – init**" and ask for the local passphrase

Screen shots



```
Package configuration

                    ┤ Get local passphrase ├

 Tripwire has been installed

 The Tripwire binaries are located in /usr/sbin and the database is located in
 /var/lib/tripwire. It is strongly advised that these locations be stored on
 write-protected media (e.g. mounted RO floppy). See
 /usr/share/doc/tripwire/README.Debian for details.

                              <Ok>
```



```
root@kali:~# apt install tripwire
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  tripwire
0 upgraded, 1 newly installed, 0 to remove and 1923 not upgraded.
Need to get 1,633 kB of archives.
After this operation, 11.8 MB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 tripwire amd64 2.4.3
.7-3 [1,633 kB]
Fetched 1,633 kB in 24s (68.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package tripwire.
(Reading database ... 397042 files and directories currently installed.)
Preparing to unpack .../tripwire_2.4.3.7-3_amd64.deb ...
Unpacking tripwire (2.4.3.7-3) ...
Processing triggers for man-db (2.8.5-1) ...
Setting up tripwire (2.4.3.7-3) ...
Generating site key (this may take several minutes)...
Generating local key (this may take several minutes)...
```

VIVA QUESTIONS

1. Define: Intrusion Detection System (IDS)
2. What is the use of Tripwire tool?
3. How to secure our files using tripwire?
4. List out the security tools for Linux environment.

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the tripwire is successfully installed in Linux.

Ex.No.5 How to configure the tripwire

AIM

To configure the tripwire in Linux

THEORY

Tripwire is a free, open source host-based Intrusion Detection System (IDS) that can be used to detect if unauthorized file system changes occurred over time. Tripwire continuously monitors computer's file system, when an expected change occurs, such as upgrading a package, the baseline database can be updated to the new known-good state. Tripwire works by collecting detail information of your file system and stores this information to reference and validate the current state of the system. If changes are found between the known-good state and the current state, Tripwire will send an alert to you. The baseline and check behavior are controlled by a policy file, which specifies which files or directories to monitor, and which attributes to monitor on them, such as hashes, file permissions, and ownership. Tripwire allows the system admin to know immediately what was compromised and fix it.

PROCEDURE

1. To install the tripwire by using the command sudo tripwire -- init
2. By configuring the tripwire to give the command nano /etc/tripwire/twpol.txt
3. Open the two terminals in kali linux machine.
4. In left side we have received the warning messages for the tripwire installation.
5. To find the warning message in the right of the terminal.
6. In the left side of the terminal, to give the command as tripwire -- init and enter the passphrase.

7. After the modification, to rewrite the twadmin -m P /etc/tripwire/twpol.txt.

8. Enter the passphrase code and policy file is updated now.

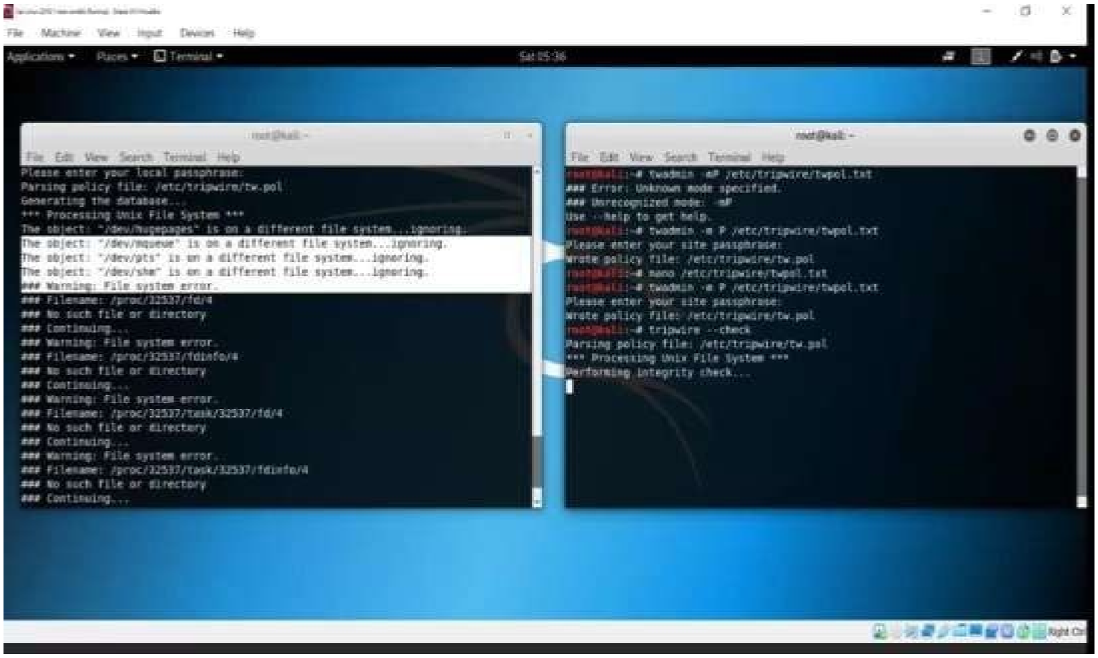
9. Again to perform the sudo tripwire – init command in the left side of the terminal and enter the passphrase and the database was successfully generated.

10. Give the command sudo tripwire –check in the right side of the kali linux machine and performing the integrity check.

11. The following files are ignored during the configuration "/dev/hugepages", "/dev/mqueue", "/dev/pts","/dev/shm".

12. Now the integrity check was completed.

Screen shots



File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾
Sat 05:36
root@kali: ~
File Edit View Search Terminal Help

```
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
The object: "/dev/hugepages" is on a different file system...ignoring.
The object: "/dev/mqueue" is on a different file system...ignoring.
The object: "/dev/pts" is on a different file system...ignoring.
The object: "/dev/shm" is on a different file system...ignoring.
### Warning: File system error.
### Filename: /proc/32537/fd/4
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/32537/fdinfo/4
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/32537/task/32537/fd/4
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/32537/task/32537/fdinfo/4
### No such file or directory
### Continuing...
```

```
root@kali:~# twadmin -mP /etc/tripwire/twpol.txt
### Error: Unknown mode specified.
### Unrecognized mode: -mP
Use --help to get help.
root@kali:~# twadmin -m P /etc/tripwire/twpol.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
root@kali:~# nano /etc/tripwire/twpol.txt
root@kali:~# twadmin -m P /etc/tripwire/twpol.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
root@kali:~# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

VIVA QUESTIONS

1. Why to use the tripwire tool?

2. Give the command to rewrite the tripwire admin file?

3. What is meant by integrity check?
4. Which command is used to configure the tripwire?

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the tripwire is successfully configured.

Ex.No.6 Secure check scanning using tripwire

AIM

To explore the secure check scanning process

THEORY

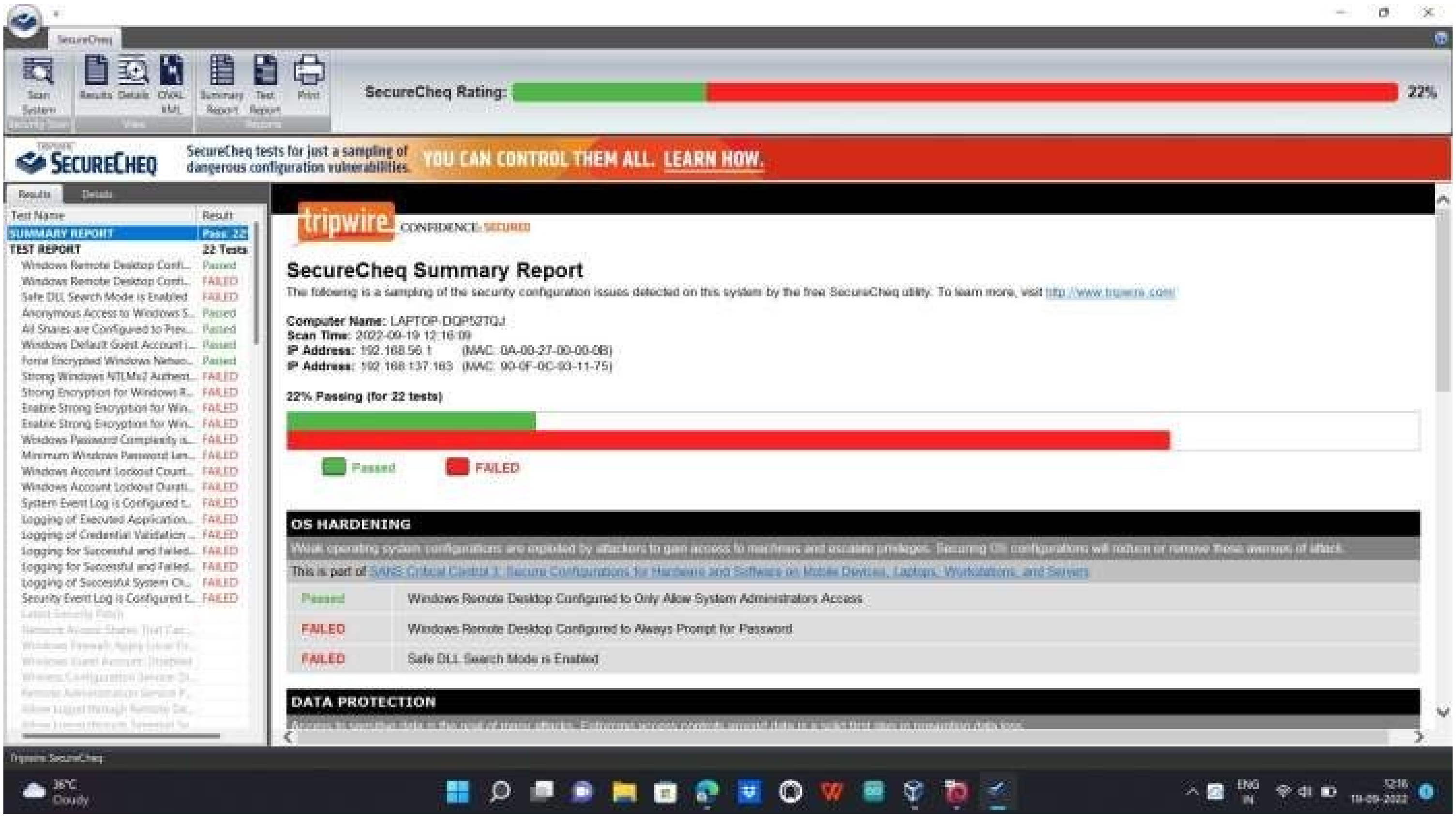
Tripwire Secure Cheq is a free configuration evaluator that tests for a subset of typical (and often dangerous) Windows configuration errors. The program provides detailed remediation and repair advice by demonstrating how systems can be continually hardened against attack. Evaluate and test the sources of errors in your system. Analyze the current state of drives and processes, view detailed remediation, and check the available repair options. Implement specific operations and integrate required files manually, view the results, etc.

PROCEDURE

1. Download the tripwire Secure Cheq in the web browser.
2. Click download.
3. Save the downloaded file in the location.
4. Install the tripwire securecheq by using the right click.
5. Tripwire Secure Cheq setup wizard will appear.
6. By clicking the next option and choose the I agree option.
7. Select the installation folder and click next option.
8. By clicking the next option to install the tripwire secure cheq.
9. Open the tripwire secure cheq tool.
10. This is the free utility will scan your system for a sampling of high priority configuration vulnerabilities.
11. Click the scan option to scan the system.
12. After the scanning process, scan complete dialog box will appear.
13. By clicking the view results the summary report will appear.

14. The summary report includes the computer name, scan time, IP address and MAC address.

Screen shots



Test Name	Result
SUMMARY REPORT	Pass: 22
TEST REPORT	22 Tests
Windows Remote Desktop Confi...	Passed
Windows Remote Desktop Confi...	FAILED
Safe DLL Search Mode is Enabled	FAILED
Anonymous Access to Windows S...	Passed
All Shares are Configured to Prev...	Passed
Windows Default Guest Account i...	Passed
Force Encrypted Windows Netwo...	Passed
Strong Windows NTLMv2 Authent...	FAILED
Strong Encryption for Windows R...	FAILED
Enable Strong Encryption for Win...	FAILED
Enable Strong Encryption for Win...	FAILED
Windows Password Complexity is...	FAILED
Minimum Windows Password Len...	FAILED
Windows Account Lockout Count...	FAILED
Windows Account Lockout Durati...	FAILED
System Event Log is Configured t...	FAILED
Logging of Executed Application...	FAILED
Logging of Credential Validation ...	FAILED
Logging for Successful and Failed...	FAILED
Logging for Successful and Failed...	FAILED
Logging of Successful System Ch...	FAILED
Security Event Log is Configured t...	FAILED
Latest Security Patch	
Network Access Shares That Can...	
Windows Firewall Apply Local Fi...	
Windows Guest Account: Disabled	
Wireless Configuration Service Di...	
Remote Administration Service F...	
Allow Logon through Remote De...	
Allow Logon through Terminal Se...	

SecureCheq Summary Report

The following is a sampling of the security configuration issues detected on this system by the free SecureCheq utility. To learn more, visit http://www.tripwire.com/

Computer Name: LAPTOP-DQP52TQJ
Scan Time: 2022-09-19 12:16:09
IP Address: 192.168.56.1 (MAC: 0A-00-27-00-00-0B)
IP Address: 192.168.137.163 (MAC: 90-0F-0C-93-11-75)

22% Passing (for 22 tests)

🟩 Passed 🟥 FAILED

OS HARDENING

Weak operating system configurations are exploited by attackers to gain access to machines and escalate privileges. Securing OS configurations will reduce or remove these avenues of attack.

This is part of SANS Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Passed	Windows Remote Desktop Configured to Only Allow System Administrators Access
FAILED	Windows Remote Desktop Configured to Always Prompt for Password
FAILED	Safe DLL Search Mode is Enabled

DATA PROTECTION

[illegible]

VIVA QUESTIONS

1. What is the use of tripwire tool?
2. How to check the secure scanning in tripwire tool?
3. List out the any other security scanning tools.
4. What is meant by vulnerabilities?
5.

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the tripwire secure check is successfully installed and scanned the system.

Ex.No.7 Nikto web analysis

AIM

To analyze the vulnerabilities using nikto web tool.

THEORY

Nikto is a simple, open-source web server scanner that examines a website and reports back vulnerabilities that it found which could be used to exploit or hack the site. Also, it's one of the most widely used website vulnerabilities tools in the industry, and in many circles, considered the industry standard.

Although this tool is extremely effective, it's *not* stealthy at all. Any site with an intrusion-detection system or other security measures in place will detect that it's being scanned. Initially designed for security testing, stealth was never a concern.

If you just run Nikto by itself on a targeted website, you may not know what to do with the information from the scan. Nikto is actually more like a laser pointer to call in a much larger strike, and you will see how that plays out in a little bit.

PROCEDURE

1. Open the two different machine such as kali linux machine and vulnerable linux server machine.
2. In the kali linux machine, to clear the contents by using the clear command.
3. By using the command “ifconfig” and get the IP address.
4. By using the ifconfig command and get the IP address for the Kali linux machine.
5. In the kali linux machine to ping the IP address of vulnerable linux server.
6. To ping the IP address of the kali linux machine in linux server machine.
7. Now to check the vulnerability analysis by using nikto tool.
8. Open the firefox browser and give the IP address and choose the option as “DVWA”.

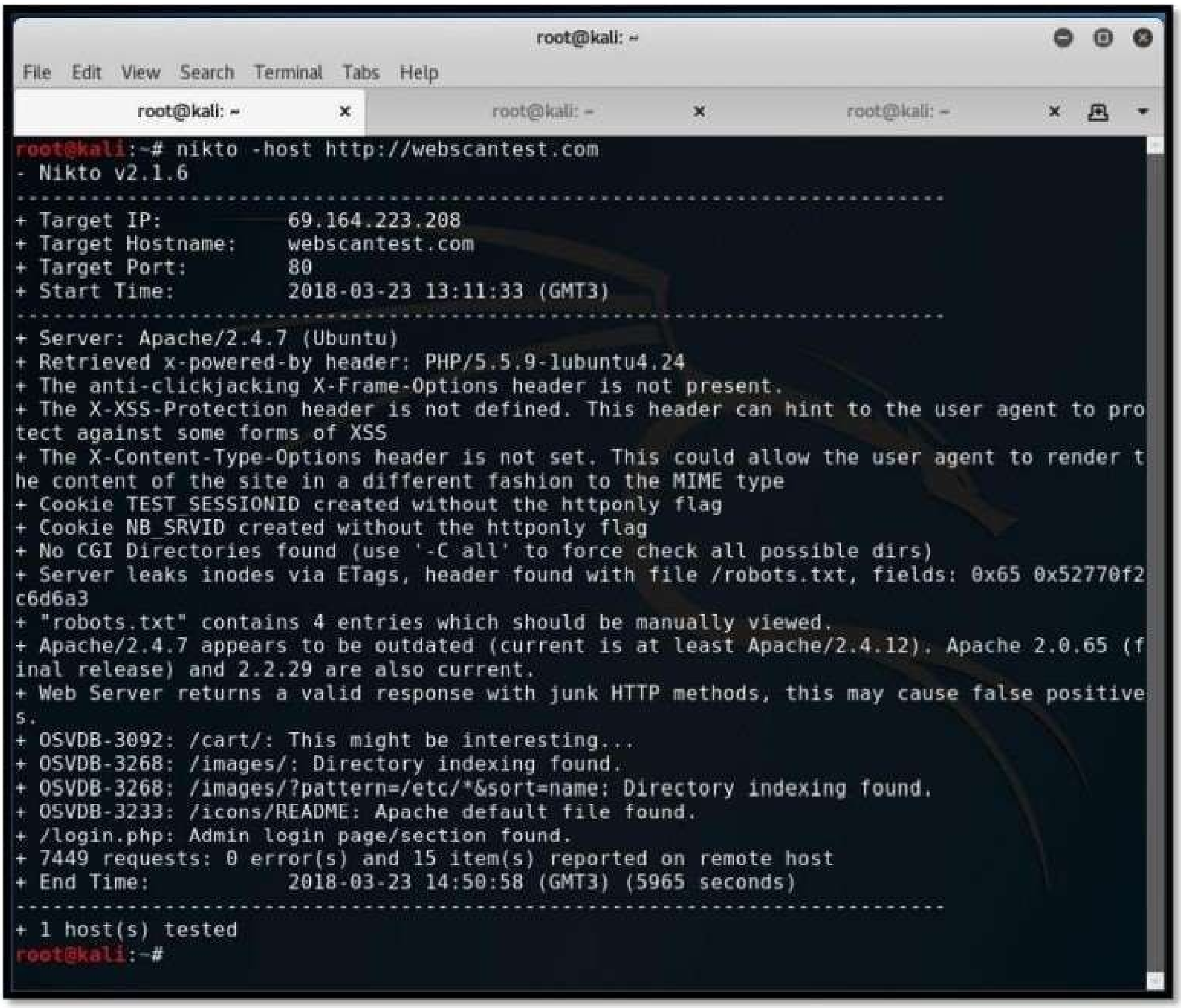
9. Give the username as admin and password.

10. Goto the terminal, and type the command in the kali linux machine

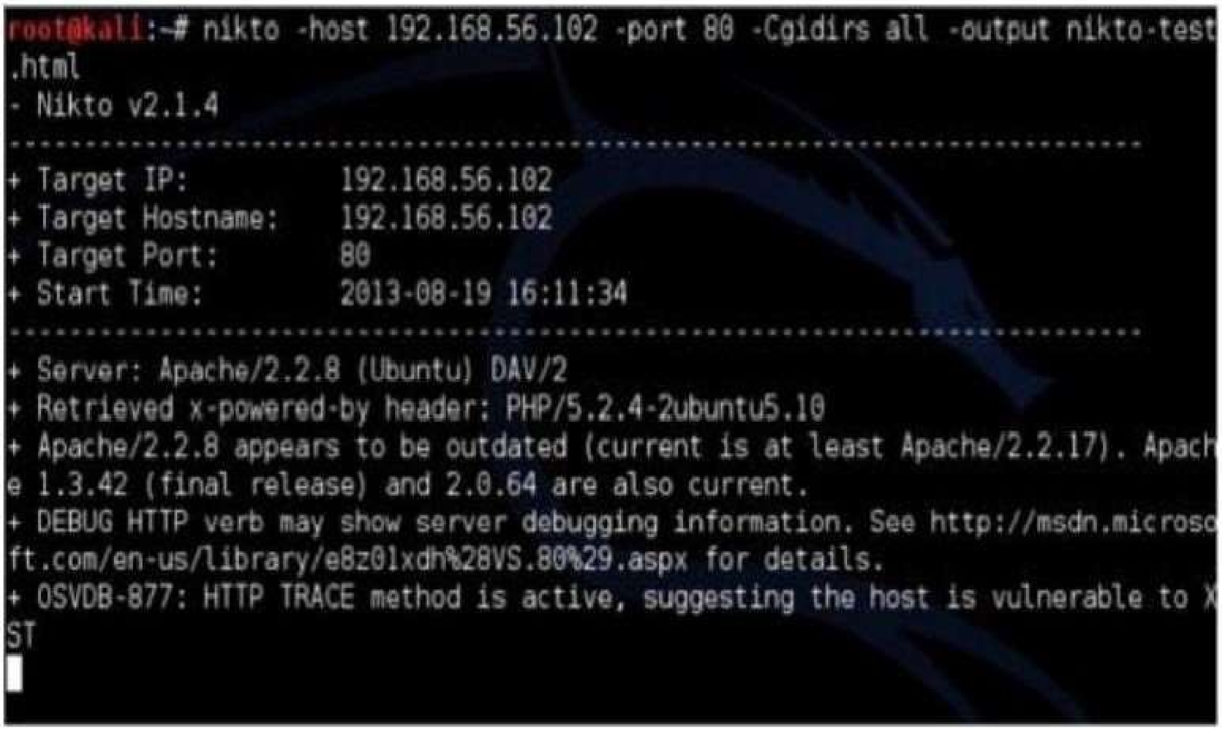
    nikto –h http://192.168.1.9/dvwa/index.php

11. Nikto v2.1.6 version is used and checks the target IP address, Target host name, Target port, start time.
12. Apache servers are running on ubuntu and copy the details of Apache server.
13. Download the Apache HTTP server version 2.2.8 for analyzing the security vulnerabilities.
14. Display the CVE details of ultimate security vulnerability data source.
15. Choose the option Reflected Cross site scripting (XSS) in DVWA.
16. To check the DVWA security by choosing the "low" option for the security level and click submit
17. Now the security level set to low.
18. Type the following command in the reflected Cross site scripting(XSS) <script> alert(0) </script> and click submit then the dialog box will appear for the alert(0).
19. Check the vulnerabilities of the web server and finally it displays the "Hello".

Screen shots



```
root@kali:~# nikto -host http://webscantest.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          69.164.223.208
+ Target Hostname:    webscantest.com
+ Target Port:        80
+ Start Time:         2018-03-23 13:11:33 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to pro
tect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2
c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (f
inal release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positive
s.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2018-03-23 14:50:58 (GMT3) (5965 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```



```
root@kali:~# nikto -host 192.168.56.102 -port 80 -Cgidirs all -output nikto-test
.html
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2013-08-19 16:11:34
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.17). Apach
e 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
```

VIVA QUESTIONS

1. What is the use of nikto web tool?

2. How to check the vulnerabilities of web server by using nikto tool?

3. What is the Apache web server?

4. How the Apache web server works?

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the nikto web tool is successfully analyzed the web server vulnerabilities.

Ex.No.8 Unix Private Security Check

AIM

To analyze the vulnerability check by using the Unix private security check tool.

THEORY

Unix-privesc-checker is a script that runs on Unix systems (tested on Solaris 9, HPUX 11, Various Linuxes, FreeBSD 6.2). It tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases).

It is written as a single shell script so it can be easily uploaded and run (as opposed to un-tarred, compiled and installed). It can run either as a normal user or as root (obviously it does a better job when running as root because it can read more files).

PROCEDURE

1. Open browser with the address http://pentestmonkey.net/tools/audit/unix-privesc-check and to install theunix-privesc-check.
2. In this check, we have two modes such as standard mode and detailed mode. This script check file permissions and other settings that could allow local users to escalate privileges.
3. Go to the oracle VM virtual box and choose the option terminal emulator from applications.
4. Give the command as ifconfig and get the IP address(inet) as 10.0.2.6
5. Open the new terminal in the kali linux machine and give the command as ifconfig and use the ping command with the ip address. Ex: ping 10.0.2.6
6. Open the another terminal to ping the ip address as 10.0.2.7
7. Give the command as unix-privesc-check standard 10.0.2.6 in the kali linux machine.
8. Analyze the behavior of the system with the IP address and give the command to store the content

```
Unix-privesc-check standard 10.0.2.6  >  standard.txt
```

9. Entire details are stored in the standard.txt and goto the text editor and open the standard.txt file.

10. Try to find the “warning” and WARNING: Sudo is configured. Manually check nothing unsafe is allowed.

11. Try to find the next warning, there are SSH agents running on this system.

12. These are the warning in the standard mode of the unix private check.

13. To find the detailed analysis mode by using the command such as:

    unix-privesc-check detailed 10.0.2.6 > detailed.txt

14. After the analysis the detailed information is stored in the detailed.txt file.

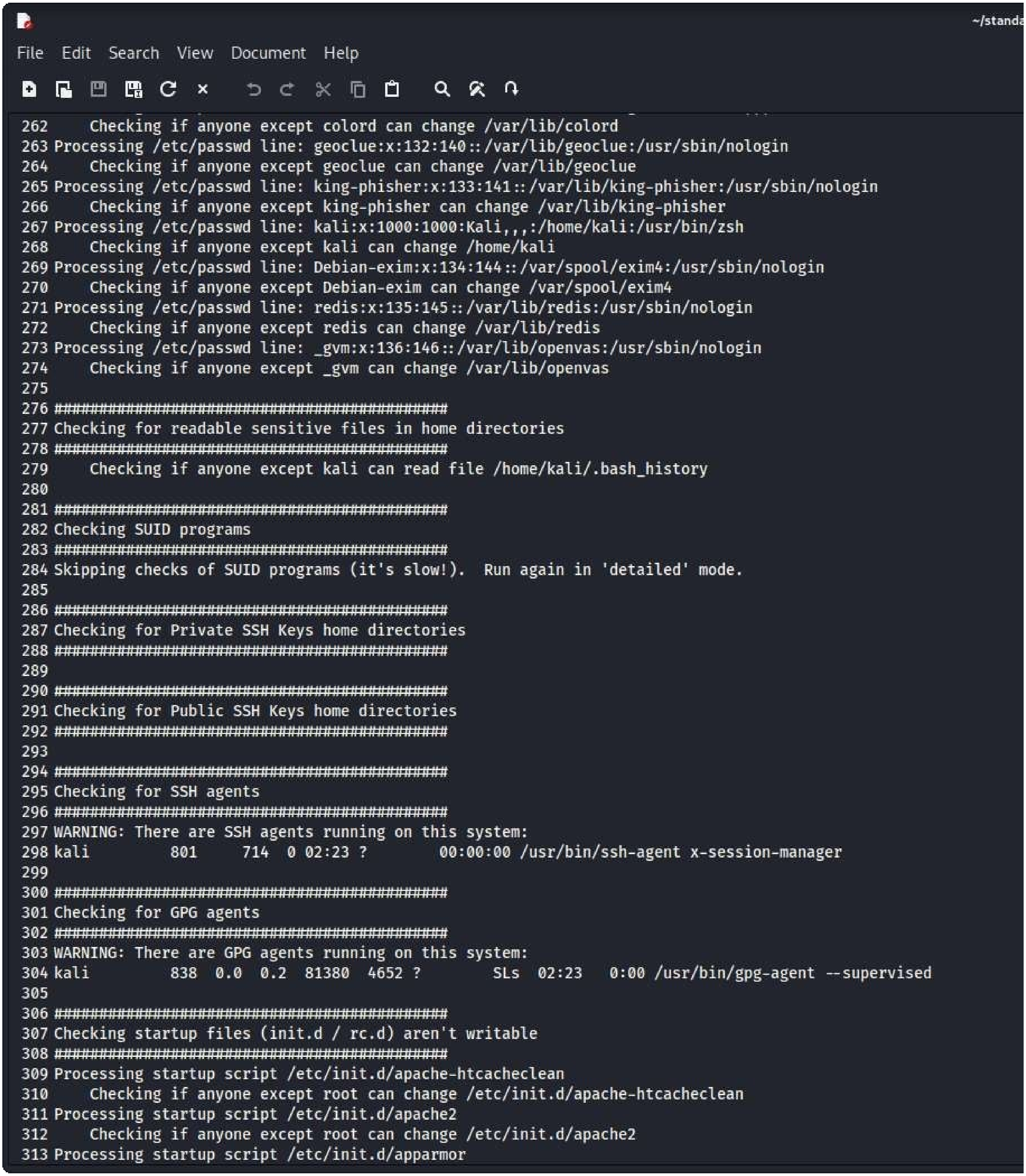
15. Goto the text editor and open the detailed.txt file.

16. To find the warning statement such as sudo is configured, manually check nothing unsafe is allowed.

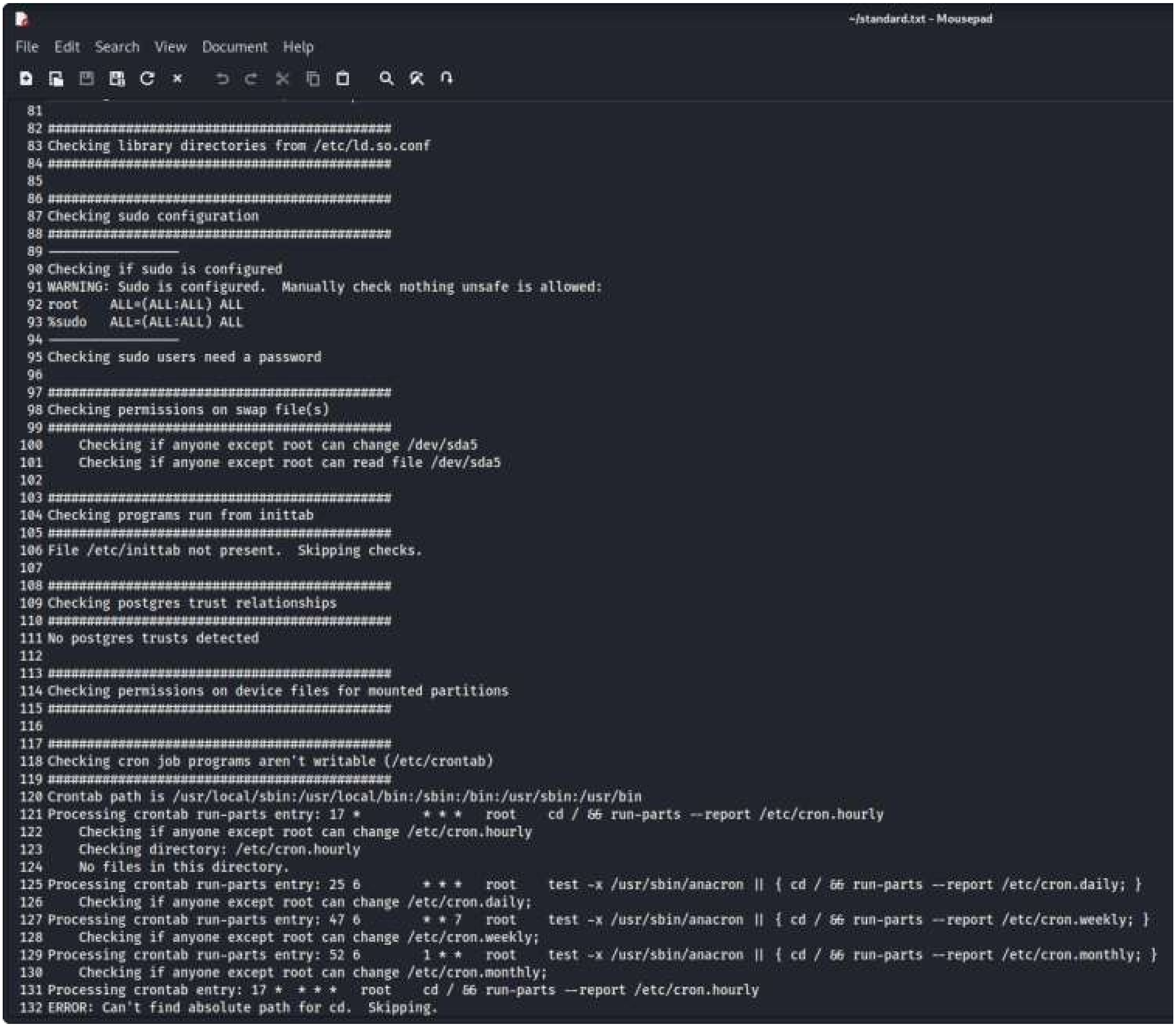
17. To find the warning statement such as /etc/cron.daily/apache2 is run by cron as root. This is the elaborate report.

18 The warning occur at ssh-keysign, kismet_capture, SSh agents avahi-Daemon and darkstat.

Screen shots



```
    Checking if anyone except colord can change /var/lib/colord
Processing /etc/passwd line: geoclue:x:132:140::/var/lib/geoclue:/usr/sbin/nologin
    Checking if anyone except geoclue can change /var/lib/geoclue
Processing /etc/passwd line: king-phisher:x:133:141::/var/lib/king-phisher:/usr/sbin/nologin
    Checking if anyone except king-phisher can change /var/lib/king-phisher
Processing /etc/passwd line: kali:x:1000:1000:Kali,,,:/home/kali:/usr/bin/zsh
    Checking if anyone except kali can change /home/kali
Processing /etc/passwd line: Debian-exim:x:134:144::/var/spool/exim4:/usr/sbin/nologin
    Checking if anyone except Debian-exim can change /var/spool/exim4
Processing /etc/passwd line: redis:x:135:145::/var/lib/redis:/usr/sbin/nologin
    Checking if anyone except redis can change /var/lib/redis
Processing /etc/passwd line: _gvm:x:136:146::/var/lib/openvas:/usr/sbin/nologin
    Checking if anyone except _gvm can change /var/lib/openvas

############################################
Checking for readable sensitive files in home directories
############################################
    Checking if anyone except kali can read file /home/kali/.bash_history

############################################
Checking SUID programs
############################################
Skipping checks of SUID programs (it's slow!).  Run again in 'detailed' mode.

############################################
Checking for Private SSH Keys home directories
############################################

############################################
Checking for Public SSH Keys home directories
############################################

############################################
Checking for SSH agents
############################################
WARNING: There are SSH agents running on this system:
kali         801     714  0 02:23 ?        00:00:00 /usr/bin/ssh-agent x-session-manager

############################################
Checking for GPG agents
############################################
WARNING: There are GPG agents running on this system:
kali         838  0.0  0.2  81380  4652 ?        SLs  02:23   0:00 /usr/bin/gpg-agent --supervised

############################################
Checking startup files (init.d / rc.d) aren't writable
############################################
Processing startup script /etc/init.d/apache-htcacheclean
    Checking if anyone except root can change /etc/init.d/apache-htcacheclean
Processing startup script /etc/init.d/apache2
    Checking if anyone except root can change /etc/init.d/apache2
Processing startup script /etc/init.d/apparmor
```


~/standard.txt - Mousepad
File Edit Search View Document Help

```

############################################
Checking library directories from /etc/ld.so.conf
############################################

############################################
Checking sudo configuration
############################################
-----------------
Checking if sudo is configured
WARNING: Sudo is configured.  Manually check nothing unsafe is allowed:
root    ALL=(ALL:ALL) ALL
%sudo   ALL=(ALL:ALL) ALL
-----------------
Checking sudo users need a password

############################################
Checking permissions on swap file(s)
############################################
    Checking if anyone except root can change /dev/sda5
    Checking if anyone except root can read file /dev/sda5

############################################
Checking programs run from inittab
############################################
File /etc/inittab not present.  Skipping checks.

############################################
Checking postgres trust relationships
############################################
No postgres trusts detected

############################################
Checking permissions on device files for mounted partitions
############################################

############################################
Checking cron job programs aren't writable (/etc/crontab)
############################################
Crontab path is /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
Processing crontab run-parts entry: 17 *        * * *   root    cd / && run-parts --report /etc/cron.hourly
    Checking if anyone except root can change /etc/cron.hourly
    Checking directory: /etc/cron.hourly
    No files in this directory.
Processing crontab run-parts entry: 25 6        * * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
    Checking if anyone except root can change /etc/cron.daily;
Processing crontab run-parts entry: 47 6        * * 7   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
    Checking if anyone except root can change /etc/cron.weekly;
Processing crontab run-parts entry: 52 6        1 * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
    Checking if anyone except root can change /etc/cron.monthly;
Processing crontab entry: 17 *  * * *   root    cd / && run-parts --report /etc/cron.hourly
ERROR: Can't find absolute path for cd.  Skipping.
```

VIVA QUESTIONS

1. What is the use of unix-privesc-check tool?
2. What are the two different modes used for the analysis?
3. How the Vulnerabilities of the system are checked with the standard mode?
4. How the Vulnerabilities of the system are checked with the detailed mode?
5. How to find the IP address of the UNIX system?

EVALUATION

Assessment	Marks Scored
Understanding the Problem (10)	
Efficiency of understanding the algorithm / Procedure (15)	
Efficiency of applying the procedure for solving problem (40)	
Output (15)	
Viva (20) **(Technical – 10 and Communications - 10)**	
Total (100)	

RESULT

Thus, the unix-privesc-check tool is successfully analyzed the vulnerabilities of the system.