Aim Algo and Result

1.Image Steganography

Aim: To hide a secret message within a cover-media in such a way that others cannotdiscern the presence of the hidden message.

Algorithm:
Step 1:Start
Step 2:Input: Cover_Image, Secret_Message, Secret_Key; Step 3:TransferSecret_Message into Text_File;
Step 4:ZipText_File;
Step 5:ConvertZip_Text_File to Binary_Codes; Step 6:ConvertSecret_Key into Binary_Codes; Step 7:SetBitsPerUnit to Zero;
Step 8:Encode Message to Binary_Codes; Step 9:Add by 2 unit for bitsPerUnit; Step 10:Output: Stego_Image;
Step 11:End

Result: Thus the program to implement image steganography was verified andexecuted Successfully.

2.Configuration of Network – commands
Description:

3. WIRELESS AUDIT

Aim: To perform wireless audit on Access Point and decrypt WPA keys using aircrack-ngtool in Kalilinux OS.

Algorithm:
1. Check the current wireless interface with iwconfig command.
2. Get the channel number, MAC address and ESSID with iwlist command.
3. Start the wireless interface in monitor mode on specific AP channel with airmon-ng.
4. If processes are interfering with airmon-ng then kill those process.
5. Again, start the wireless interface in monitor mode on specific AP channel with airmon- ng.
6. Start airodump-ng to capture Initialization Vectors (IVs).
7. Capture IVs for atleast 5 to 10 minutes and then press Ctrl + C to stop the operation.
8. List the files to see the captured files
9. Run aircrack-ng to crack key using the IVs collected and using the dictionary file rockyou.txt
10. If the passphrase is found in dictionary then Key Found message displayed; else print Key Not Found.

Result:Thus wireless audit on Access Point and decrypt WPA keys using aircrack-ngtool in Kalilinux OS has been implemented successfully.

4. LINUX AUDITING USING LYNIS

Aim:
To audit the currently installed Linux operating system and then increase the hardening
index by installing rootkit hunter and clamav antivirus scanner.

Description:
Lynis is an open-source and much powerful auditing tool for Unix/Linux-like operating systems. It scans the system for security information, general system information, installed and available software information, configuration mistakes, security issues, user accounts without a password, wrong file permissions, firewall auditing, etc. Since Lynis is flexible, it is used for various different purposes that include:

- Security auditing
- Compliance testing
- Penetration testing
- Vulnerability detection
- System hardening

Algorithm:

1. Using yum or dnf install lynis tool.
2. To list out all options available type show options
3. Audit the Linux operating system by using audit system option in lynis
4. Find out the current hardening index
5. To increase hardening index, install rkhunter and clamav software
6. Again run lynis audit system command to observe that the hardening index has increased

Result: Thus, the auditing of a currently installed Linux operating system and then increment of hardening index by installing rootkit hunter and clamav antivirus scanner has been executed successfully.

5. SNORT IDS

Aim:
To demonstrate Intrusion Detection System (IDS) using snort tool.

Description:
Snort is a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. It uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity. Using snort, network admins can spot denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks, Common Gateway Interface (CGI) attacks, buffer overflows, and stealth port scans. Snort creates a series of rules that define malicious network activity, identify malicious packets, and send alerts to users.

Algorithm:

1. Download and extract the latest version of daq and snort
2. Install development packages - libpcap and pcre.
3. Install daq and then followed by snort.
4. Verify the installation is correct.
5. Create the configuration file, rule file and log file directory
6. Create snort.conf and icmp.rules files
7. Execute snort from the command line
8. Ping to yahoo website from another terminal
9. Watch the alert messages in the log files

Result:
Thus demonstration of Intrusion Detection System (IDS) using snort tool has been implemented successfully.

6. LINUX OS HARDENING

Aim:
To harden the Linux operating system through various configurations and reducing the attack surface.

Algorithm:

1. Check unwanted services are running and remove it
2. Update the system packages using yum or dnf
3. Disable USB stick by adding to no-usb file the following- install usb-storage /bin/true
4. Turn on SELinux and put in permissive/enforcing mode
5. Lock account not currently in use
6. Check accounts for empty password
7. Enable iptables
8. Lockdown cron jobs by putting the name into the cron.deny file
9. Turn off IPv6 by putting the entry no for IPV6INIT and NETWORKING_IPV6

Result: Thus, the implementation harden the Linux operating system through various configurations and reducing the attack surface has been executed successfully.

7. LIVE DATA ACQUISITION OF A FOLDER

Aim: To do live acquisition of a folder and take it’s disk image.

Algorithm:

1. Open the AccessData FTKImager-4.5 applicaton.
2. Click the File option in the menu and choose Create Disk Image
3. Then choose the contents of a folder option
4. Click yes to generate the logical image of the folder
5. Enter the path details of the source folder
6. Click the add button
7. Fill the case number, evidence number, unique description and Examiner name.
8. Click the next button
9. Fill the destination folder path and the name to be given to the captured folder image
10. Click Finish button to create the folder image

11.Now open the text file Case001 Evidence.ad1 to know details about the captured evidence folder

Result:
Thus, live acquisition of a folder and it's disk image has been recorded successfully.

8. WEB VULNERABILITES USING O-SAFT

Aim:
To test the vulnerabilities in SSL connection with various options in o-saft tool.

Description;
O-Saft is an easy-to-use tool to show information about SSL certificates and tests the SSL connection according to a given list of ciphers and various SSL configurations. It's designed to be used by penetration testers, security auditors or server administrators. The idea is to show the important information or the special checks with a simple call of the tool. However, it provides a wide range of options so that it can be used for comprehensive and special checks by experienced people.

Algorithm:
1. Download o-saft.tgz from the website https://github.com/OWASP/O-Saft/raw/master/o- saft.tgz
2. Unpack o-saft.tgz using the tar command
3. Change the directory to O-Saft
4. Run the o-saft command with +info option and tld as rajalakshmi.org
5. Run the o-saft command with +cipher option to show the supported ciphers of rajalakshmi.org

Result: Thus, the experiment to test the vulnerabilities in SSL connection with various options in o-saft tool has been implemented successfully.

9. MALWARE ANALYSIS

Aim:
To write a yara script to detect spyeye, a type of malware file.

Description:
YARA is the name of a tool primarily used in malware research and detection.It provides a rule-based approach to create descriptions of malware families based on textual or binary patterns. A description is essentially a YARA rule name, where these rules consist of sets of strings and a boolean expression. The language used has traits of Perl compatible regular expressions. YARA by default comes with modules to process PE, ELF analysis, as well as support for the open-source Cuckoo sandbox.

Algorithm:

1. Fill the meta section with author name, description of file and version of script
2. In strings section, fill either text strings or hexadecimal string
3. Specify condition for detecting the malware based on the strings and filesize
4. If no output comes then spyeye is not found
5. Else spyeye malicious file detected by yara.

Result: Thus, yara script to detect spyeye has been implemented successfully.

10. N-STALKER

Aim:To find out the web application security using N-Stalker tool.

Description:
N-Stalker is a leader on Web Application Security Assessment technology. It currently develops and maintains N-Stalker Web Application Security Scanner suite, a software product aimed on scanning and finding security vulnerabilities in Web Applications. It can play significant role in application security testing. This is trusted when it comes to browser level vulnerabilities. Some of the features are-

- HTTP Fingerprinting
- Parallel Web Crawling
- Server-side technology discoverer
- Automatic False Positive Prevention Engine
- Component-oriented Web Crawler
- Component-oriented Scanning Engine
- IDS Evasion Fuzzing Test
- Web form autocomplete mechanism

Algorithm:
1. Open the N-Stalker application
2. Click New Scan
3. Type the web application URL as www.rajalakshmi.org
4. Choose scan policy as manual test and click Next button
5. Click Optimize button
6. Click Start Session button
7. Next press Start Scan button
8. Save the scan results.

Result: Thus, web application security using N-Stalker tool has been implemented successfully.

11.OWASP VULNERABILITY TEST

Aim: To identify web vulnerablites, using OWASP project using tool like OWASP ZAP.

Description:

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

Top 10 vulnerabilities 2021 are listed below:
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection.
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failuers
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request

Algorithm:

1. Start ZAP and click the Quick Start tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the URL to attack text box, enter the full URL of the web application you want to attack.
4. Click the Attack
5. Click the Alerts tab in the Information Window.
6. Click each alert displayed in that window to display the URL and the vulnerability detected in the right side of the Information Window.
7. In the Workspace Windows, click the Response tab to see the contents of the header and body of the response. The part of the response that generated the alert will be highlighted.
8. Click Reports on the menu tab to generate report of the attack which will describe each attack and its vulnerabilities.

Result:
Thus, the implementation of testing for OWASP vulnerability has been executed successfully.

12.WEBSITE AUDIT

Aim: To implement website audit and generate a report.

Description:
A website audit is an examination of page performance prior to large-scale search engine optimization (SEO) or a website redesign. Auditing your website can determine whether or not it's optimized to achieve your traffic goals and give you a sense of how you can improve it to to reach those goals.
Types of website Audits are Competitive website audits, SEO link Audit, Lead Conversion Optimization Audit, Social Meadia Audit and SEO Website Audit.

Algorithm:

1.Go to www.semrush.com
2. Enter the domain to be audited
3. Click on start campaign.
4.The process will generate a list of test and check for vunerablites and malware.
5. Once process is complete you can view the site health and the errors prone.
6.Generate a PDF of the report.

Result:
Thus, the implementation of the wesite audit and generation of reportss has been executed successfully.