KAVIYATRI BAHINABAI CHAUDHARI,
NORTH MAHARASHTRA UNIVERSITY, JALGAON

NES's

GANGAMAI COLLEGE OF ENGINEERING

ISO 9001:2008

COMPUTER ENGINEERING DEPARTMENT

Laboratory Manuals

Class: B.E. Computer (60-40 Pattern).

Semester: VIII

Subject: Cyber Security Laboratory.

Academic Year:2023-24.

Institute Vision

- Empowering first generation engineers to excel in technical education based on human values

Institute Mission

- To import affordable and quality education in order to meet needs of industry and to achieve excellence in teaching learning process.
- To achieve excellence in application oriented research inselected area of Technology to contribute to thedevelopment of the region.
- To collaborate with industries to promote innovation capabilities of budding engineers.
- To develop responsible citizens to awareness and acceptance of ethical values.
- To build a support system of all stakeholders to develop the institute.

Nagaon Education Society's
GANGAMAI COLLEGE OF ENGINEERING,
NAGAON,DHULE-05
Computer Department

DEPARTMENT OF COMPUTER ENGINEERING

Vision

To emerge as the leading Computer Engineering department forinclusive development of students.

Mission

To provide student-centered conducive environment for preparingknowledgeable, competent and value-added computer engineers.

A Laboratory Manual

For

Cyber Security – Lab

For the Bachelor of Engineering in the Computer Engineering

BE Computer

Semester – VIII

2023-2024

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

Roll No:…………………………………………………Batch:…………………………………..

PRN NO:………………………………………………………………………………………

Nagaon Education Society's
GANGAMAI COLLEGE OF ENGINEERING,
NAGAON,DHULE-05
Computer Department

CERTIFICATE

This is to certify that

Mr./Miss.____

Having Roll No. _

Of VIII Semester for the course Bachelor of Computer Engineering

Of the institute **Gangamai College of Engineering, Nagaon, Dhule**,has completed the term work satisfactorily of the subject

Engineering Cyber Security - Lab

for the academic year 2023 – 2024

as prescribed in the curriculum

Date:_______________ PRN No:____________________

Place: Nagaon, Dhule Exam Seat No: ________________

Subject Teacher **HOD** **Principal**

Seal of the Institute

PRACTICAL-COURSE OUTCOMES

COURSE OUTCOMES(COS)

1. To describe Information Technology Act of India.
2. Describe Cyber Security.
3. Demonstrate Offensive Cyber Security Tools.
4. Demonstrate Defensive Cyber Security Tools.
5. Demonstrate Security Testing Tools for Web Applications.

Expt No.	Name of Experiment	Page No.	Starting Date	Ending Date	Remark
1.	Study of Information Technology Act – Indian Perspective				
2.	Study of recent Cyber Incidents / Vulnerability				
3.	Study of Information Gathering Tools in Kali Linux				
4.	Study of Vulnerability Analysis Tools in Kali Linux				
5.	Study of Web Application Analysis Tools in Kali Linux				
6.	Study of Database Assessment Tools in Kali Linux.				
7.	Study of Snipping and Spoofing Tools in Kali Linux.				
8.	Study of Forensics Tools in Kali Linux.				

DEPARTMENT OF COMPUTER ENGINEERING

Objectives

1. To learn Information Technology Act of India.
2. To understand the importance of Cyber Security.
3. To learn Offensive Cyber Security Tools.
4. To learn Defensive Cyber Security Tools.
5. To learn Security Testing Tools for Web Applications.

DEPARTMENT OF COMPUTER ENGINEERING

Programme Educational Objectives

PEO 1.Core Knowledge

Computer engineering graduates will have the knowledge of basic science and Engineering skills, Humanities, social science, management and conceptual and practical understanding of core computer engineering area with project development.

PEO 2.Employment

Computer engineering graduates will have the knowledge of Industry-based technical skills to succeed in entry level engineering position at various industriesas well as in academics.

PEO 3. Professional Competency

Computer engineering graduates will have the ability to communicate effectively in English, to accumulate and disseminate the knowledge and to work effectively in a team with a sense of social awareness.

Gangamai College of Engineering, Nagaon, Dhule

Department of Computer Engineering

Name :___________________________________

Date of Performance: _ _/_ _/20_ _

Class : B.E. Computer

Date of Completion : _ _/_ _/20_ _

Div :____________ **Batch:**___________

Grade :_________

Subject : Cyber Security Lab

Sign. of Teacher

Experiment No-1

Aim :- Study of Information Technology Act – Indian Perspective.

Section 65. Tampering with computer source documents.

Description:

Anyone who is purposely or intentionally covers up, obliterates or changes or purposefully or purposely causes another to stow away, annihilate, or modify any PC source code utilized for a PC, PC program, PC framework or PC organization, when the PC source code is needed to be kept or kept up by law.

Penalty:

Imprisonment as long as three years, or with fine which may stretchout up to two lakh rupees, or with both

Section 66. Computer related offences.

Description:

On the off chance that any individual, unscrupulously or falsely, does any demonstration alluded to in section 43.

Penalty:

Imprisonment for a term which may stretch out to three years or with fine which may reach out to five lakh rupees or with both.

Amendment:

66A. Punishment for sending offensive messages through communication service, etc.

66B. Punishment for dishonestly receiving stolen computer resource or communication device.

66C. Punishment for identity theft.

66D. Punishment for cheating by personation by using computer resource.

66E. Punishment for violation of privacy.

66F. Punishment for cyber terrorism.

Section 67. Punishment for publishing or transmitting obscene material in electronic form.

Description:

Whoever distributes or sends or causes to be distributed or communicated in the electronic structure, any material which is scurrilous or claims to the lecherous interest.

Penalty:

Imprisonment for a term which may stretch out to three years and with fine which may reach out to five lakh rupees and in case of second or resulting conviction with detainment of one or the other portrayal for a term which may stretch out to five years and furthermore with fine which may reach out to tenlakh rupees.

Amendment:

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

67B. Punishment for publishing or transmitting of material depicting children in

sexually explicit act, etc., in electronic form.

67C. Preservation and retention of information by intermediaries.

Section 68. Power of Controller to give directions.

Description:

The Controller may, by request, direct a Certifying Authority or any worker of such Authority to take such measures or stop continuing such exercises as indicated in the request if those are important to guarantee.

Penalty: Imprisonment for a term not surpassing two years or a fine not surpassing one lakh rupees or with both.

Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

Description:

This Section of the Information Technology Act empowers the Central or State Government or any other competent authority to direct any agency of the appropriate government to monitor, intercept or decrypt any information transmitted, generated, received or stored in any computer resource.

Penalty :

Imprisonment for a term which may reach out to seven years and will likewise be responsible to fine.

Amendment:

69A. Power to issue directions for blocking for public access of any information through any computer resource.

69B. Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

Section 70. Protected system.

Description:

The appropriate Government may, by notification in the Official Gazette declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Penalty:

Imprisonment of one or the other depiction for a term which may reach out to ten years and will likewise be obligated to fine.

Amendment:

70A. National nodal agency.

Section 71. Penalty for misrepresentation.

Description:

Whoever makes any distortion to, or smothers any material reality from the Controller or the Certifying Authority for acquiring any permit or Certificate, by and large.

Penalty:

Imprisonment for a term which may stretch out to two years, or with fine which may reach out to one lakh rupees, or with both.

Section 72. Penalty for Breach of confidentiality and privacy.

Description:

It provides for a criminal penalty where a government official discloses records and information accessed in the course of his or her duties without the consent of the concerned person, unless permitted by other laws.

Penalty:

Imprisonment for a term which may stretch out to two years, or with fine which may reach out to one lakh rupees, or with both.

Amendment:

72A. Punishment for disclosure of information in breach of lawful contract.

Section 73. Penalty for publishing Certificate false in certain particulars.

Description:

It is for publishing electronic Signature Certificate false in certain particulars. Any person who contravenes the provisions of sub-section 1 shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalty:

Imprisonment for a term which may stretch out to two years, or with fine which may reach out to one lakh rupees, or with both.

Section 74. Publication for fraudulent.

Description:

Whoever intentionally makes, distributes or in any case makes accessible a Certificate for any fake or unlawful reason.

Penalty:

Imprisonment for a term which may reach out to two years, or with fine which may stretch out to one lakh rupees, or with both.

Section 75. Act to apply for offence or contravention committed outside India.

Description:

If any person have committed an offence, or contravention committed outside India, and if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India, then the provisions of this Act shall apply also to any offence or contravention.

Section 76. Confiscation.

Description:

Any PC, PC framework, floppies, reduced plates, tape drives orsome other frill related thereto, in regard of which any arrangement of this Act,rules, requests or guidelines made thereunder has been or is being contradicted, will be obligated to seizure:

Section 77. Compensation, penalties or confiscation not to interfere with other punishment.

Description:

No remuneration granted, punishment forced or seizure made under this Act will forestall the honor of pay or inconvenience of some other punishment or discipline under some other law for the time being in power.

Amendment:

77A. Compounding of offences.

77B. Offences with three years imprisonment to be bailable.

Section 78. Power to investigate offences.

Description:

Despite anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a cop not underneath the position of will explore any offense under this Act

Questions for Viva:

1. What is the punishment as per IT Act 2000 section 67?

2. What is the Proposed punishment for identity theft in IT Act?

3. What is the penalty for destroying computer source code, as per section 65 of IT Act?

4. What is the proposed punishment for cyber terrorism in IT Act?

Gangamai College of Engineering, Nagaon, Dhule
Department of Computer Engineering

Name :______________________________ **Date of Performance:** _ _/_ _/20_ _

Class : B.E. Computer **Date of Completion** : _ _/_ _/20_ _

Div :__________ **Batch**:__________ **Grade :**________

Subject : Cyber Security Lab **Sign. of Teacher**

Experiment No-2

Aim: Study of recent Cyber Incidents / Vulnerability

Description: Write at least FIVE recent Security Alerts and Vulnerability Notes each of the year 2021, 2020 & 2019. Write at least THREE recent Virus Alerts. Write about how to report Security Incident and Vulnerability. Write about Filing a Complaint on National Cyber Crime Reporting Portal.

Three recent Virus Alerts

1. "Siloscape" Malware

i. **Original Issue Date :-** June 14, 2021

ii. **Virus Type :-** Malware Targeting Windows Containers

iii. **Description :-** It has been reported that a new category of malware is targeting misconfigured Kubernetes clusters through Windows containers to compromise cloud environments. The malware variant gains initial access by exploitingvulnerabilities in common cloud applications or vulnerable web page or databaseand then utilizes windows container escape techniques, executes code on underlying node and then spreads in poorly configured Kubernetes clusters to open a backdoor in order to run/deploy malicious containers. Once cluster is compromised, the attacker might be able to steal critical information such a usernames and passwords, an organizationis confidential and internal files or even entire databases hosted in the cluster. This malware can leverage the computing resources in Kubernetes cluster for crypto king and potentially exfiltrate Sensitive data from hundreds of applications running in the compromised clusters.

iv. **Behaviour :-**
- Uses Windows container escape techniques to escape the container and gain code execution on the underlying node.
- Attempts to abuse the node's credentials to spread in the cluster.
- Siloscape uses the Tor proxy and an onion" domain to anonymously connect to its command and control (C2) server

v. **Best practices and Countermeasures :-**
- Kubernetes cluster configuration should restrict need privileges such that creation of new deployments is not possible. (It means that any process running in Windows Server containers should not have the same privileges as admin).
- Malware is ineffective in this case. It is advised to follow Microsoft's recommendation of discarding use of Windows containers 95 security feature.
- Hyper-V containers should be employed for operations that rely on containerization as a security boundary and it is recommended to move applications running in Windows Server containers to Hyper-V containers.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process.
- Ideally, this data should be kept on a separate device, and backups should be stored offline. Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- If not required consider disabling, PowerShell / windows script hosting. Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations. Enable Windows Defender Application Guard with designated the trusted sites as whitelisted, so that rest all sites will be open in container to block the access to memory local storage other installed applications or any other resources of to memory, local storage, other installed applications or any other resources of interest to the attacker.
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers.
- Repeat audits at regular intervals. Maintain updated Antivirus software on all systems.

2. Sarbloh Ransomware

i. **Original Issue Date :-** March 12, 2021

ii. **Virus Type :-** Ransomware

iii. **Description :-** It has been reported that a new ransomware named "Sarbloh" is spreading via specially crafted malicious documents sent as spear phishing email attachments. Malicious document is embedded with Marco with a heavily obfuscated VBA code, which downloads original payload (Sarbloh Ransomware)from an AWS URL silently. Once executed, it encrypts files on affected system

(Audio, images, video, databases, and other document files) and renames the encrypted files with the "Sarbloh" extension to make them unusable. The ransomnote ("README_SARBLOH.txt") states that the user's files are encrypted and will not be recovered until Sarbloh's creator's demands are fulfilled. Best Practices and remedial measures Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/attacks.

iv. **Best Practice and Remedial Measures :-**

- Maintain updated Antivirus software on all systems Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.o not open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on URL contained in an unsolicited e-mail, even if the link seems benign.
- In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser. Do not enable Macros if prompted by document received from untrusted sources.
- Follow safe practices when browsing the web.
- Ensure the web browsers are secured enough with appropriate content controls. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process.
- Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Check regularly for the integrity of the information stored in the databases Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- If not required consider disabling, PowerShell / windows script hosting Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Enabled Windows Defender Application Guard with designated the trusted sites 25 whitelisted, so that rest all sites will be open in container to block the access to memory, local storage, other installed applications or any other resources of interest to the attacker.
- Enable Exploit Protection (Successor to EMET] that includes several client side mitigation steps. Detailed configuration steps can be seen in https://docs.microsoft.com/en-us/windows/security/threat rotection/microsoftdefender-atp/enable-exploit-protection.
- Turn on attack surface reduction Rules, including rules that block credential theft, ransom were activity, and suspicious use of PsExec and WMI. Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption. Consider installing Enhanced Mitigation Experience Toolkit, or similar hest-level anti-exploitation tools.
- Block the attachments of file types, exepiftmp/url|vb|VDserreg cerpstemd combat|ll|dathipha wst Carry out vulnerability Assessment and Penetration

Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors.

- Repeat audits at regular intervals. Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released.

3. Adrozek Malware

i. **Original Issue Date :-** December 11, 2020

ii. **Virus Type :-** Browser Modifiers

iii. **Description :-** The malware is distributed via classic drive-by download schemes. Users are typically redirected from legitimate sites to shady domains where they are tricked into installing malicious software. The software installs the Adrozek malware, which then proceeds to obtain reboot persistence with the help of a registry key. The malware looks for locally installed browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox, Yandex Browser and attempts to force install an extension by modifying the browser's App Data folders. It also modifies some of the browsers' DLL files to change browser settings and disable security features to make sure that browser's security features doesn't detect unauthorized modifications, modifications performed by Virus.

iv. **Adrozek include :-**

- Disabling browser updates.
- Disabling file integrity checks.
- Disabling the Safe Browsing feature.
- Registering and activating the extension they added in a previous step.
- Allowing their malicious extension to run in incognito mode.
- Allowing the extension to run without obtaining the appropriate permissions.
- Hiding the extension from the toolbar.
- Modifying the browser's default home page.
- Modifying the browser's default search engine.

❖ VULNERABILITY NOTES 2021

1) CIVN-2021-0146 Multiple Vulnerabilities in Intel Products

Overview-Multiple vulnerabilities have been reported Intel products which could be exploited by an attacker to escalate privileges or cause denial of service conditions on a targeted system

Description- These vulnerabilities exist in Intel products due to improper control of resource, improper input validation improper access control, improper conditions check, insufficient control flow management, uncontrolled resource consumption, protection mechanism failure out-of-bounds write error, incomplete cleanup improper authentication, buffer overflow, path traversal improper resolution and uncontrolled search path element. Successful exploitation of these vulnerabilities could allow the attacker to escalate privileges or cause denial of service conditions cat a targeted system.

2) CIVN-2021-0145 Multiple Vulnerabilities in SAP Products

Overview- Multiple vulnerabilities have been reported in SAP products which could allow a remote CNN attacker to execute arbitrary code, access sensitive information and perform other attacks on a targeted system.

Description-These vulnerabilities exist in SAP products due to missing authorization check, improper input validation, improper authentication, memory corruption and other flaws in the affected software. Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code, access sensitive information: and perform other attacks on the targeted system.

3) CIVN-2021-0144 Privilege Escalation Vulnerabilities in Intel NUC Firmware

Overview- Privilege escalation vulnerabilities have been reported in Intel NUC Firmware that could allow a privileged user to potentially enable escalation of privilege via local access on the targeted system.

Description-These vulnerabilities exist in Intel Products due to improper access control and buffer restrictions in system firmware for some Intel(R) NUCS. Successful exploitation of these vulnerabilities could allow a privileged user to potentially enable escalation of privilege via local access on the targeted system.

4) CIVN-2021-0143 Multiple vulnerabilities in Google Android

Overview-Multiple Vulnerabilities have been reported in Google Android which could be exploited by an attacker to execute arbitrary code, obtain sensitive information or gain elevated privileges on the targeted system.

Description- These vulnerabilities exist in Google Android due to flaws in the Framework components, Media Framework components, System components, Kernel components, MediaTek components, Qualcomm components, Qualcomm closed-source components. An attacker' could exploit these vulnerabilities by hosting a specially crafted file. Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code to disclose sensitive information, gain elevated privileges on the targeted system.

5) CIVN-2021-0142 Multiple Vulnerabilities in Linux Kernel

Overview-Multiple vulnerabilities were found in the Linux kernel which may result in privilege escalation and cause a denial of service (system crash) attack on the targeted system.

Description-

1. Privilege Escalation Vulnerability (CVE-2021-3489 CVE-2021-3490) These vulnerabilities exists in the Linux kemels eBPF verification code due to improper handling of user supplied eBPF programs prior to executing them. An attacker could exploit this vulnerability by executing low-privileged code in the context of the kernel. Successful exploitation of these vulnerabilities may allow an attacker to escalate privileges, execute code in the context of the kernel and poses a threat to data confidentiality and integrity.

2. Buffer overflow vulnerability (CVE-2021-3491) This vulnerability exists due to improper handling of buffers in louring and improper enforcement of the MAX_RW_COUNT limit in some situations. Successful exploitation of this vulnerability may allow an attacker to create a heap overflow (a type of buffer overflow) leading to arbitrary code execution in the context of the kernel and cause denial of service (system crash) attack on the targeted system.

❖ VULNERABILITY NOTES 2020

1) CIVN-2020-0450 Multiple Vulnerabilities in Google Android

Overview- Multiple vulnerabilities have been reported in Google Android operating system (OS) which could enable a remote attacker to perform arbitrary code execution, gain elevated privileges, obtain sensitive information and cause denial of service condition on the targeted system.

Description -These vulnerabilities exists in Google Android due to flaws in the Media Framework, System component, Kernel component, Broadcom components, MediaTek components, Qualcomm components and Qualcomm closed-source components. A remote attacker could exploit these vulnerabilities by hosting a specially crafted file designed to exploit the vulnerabilities. Successful exploitation of these vulnerabilities could allow remote attacker to perform arbitrary code execution within the context of a privileged process, gain elevated privileges, allow the attacker to access sensitive information from the targeted device and cause denial of service conditions on the targeted system.

2) CIVN-2020-0449 Multiple Vulnerabilities in Foxit Reader and Phantom PDF

Overview-Multiple vulnerabilities have been reported in Foxit Reader and Phantom PDF which could allow a remote attacker to cause Out of-Bounds Write Remote Code Execution, Type Confusion Memory Corruption, denial of service condition or execute arbitrary code on the target system.

Description-These vulnerabilities exist due to insufficient validation of objects, incorrect processing of PDF files, lack of proper validation when an incorrect argument is passed to he app.media.openPlayer function, access or use of a deleted pointer and array overflow issue. A remote attacker could exploit these vulnerabilities by sending specially crafted malicious file on the target system Successful exploitation of these vulnerabilities could allow the attacker to cause Out target system Successful exploitation of these vulnerabilities could allow the attacker to cause Out of-Bounds Write Remote Code Execution, Type Confusion Memory Corruption, denial of service condition or execute arbitrary code on the target system.

3) CIVN-2020-0448 Multiple Vulnerabilities in Treck TCP/IP Stack

Overview- D Multiple vulnerabilities have been reported in Treck TCP/IP software, which could be exploited by a remote attacker to perform Denial of Service (DoS) attack or execute arbitrary code and take control of an affected system.

Description- Treck TCP/IP stack software is designed for and used in a variety of tot and embedded systems. The software can be licensed and integrated in various ways, including compiled from source, licensed for modification and reuse and finally as a dynamic or static linked library. These vulnerabilities exist due to buffer overflow in the Treck HTTP Server component, out of-bounds write in the IPV6 component, out-of-bound read in the DHCPv6 A remote attacker could exploit these vulnerabilities by sending specially crafted packets to the targeted system. Successful exploitation of these vulnerabilities allows a remote attacker to perform denial of service (DoS) attackor execute arbitrary code on the targeted system.

4) CIVN-2020-0447 Multiple Vulnerabilities in Mozilla Products

Overview-Multiple vulnerabilities have been reported in Mozilla products which could allow a remote attacker to execute arbitrary code, perform spoofing attacks, disclose potentially sensitive information, or cause denial of service conditions on the targeted system.

Description- These vulnerabilities exist in Mozilla products due to uninitialized memory error in Bigint, heap buffer overflow error or use-after free in WebGL, improper unitization of CSS Sanitizer, use-after-free in StyleGenericFlexBasis, improper security restrictions, improper processing of user supplied input, error while using proxy on Request callback request for viewsource URLS, improper processing of downloaded files without extensions. Successful exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code perform spoofing of these vulnerabilities could allow a remote attacker to execute arbitrary code, perform spoofing attacks, disclose potentially sensitive information, or cause denial of service conditions on the targeted system.

5) CIVN-2020-0446 Information Disclosure Vulnerabilities in GE Healthcare Products

Overview-A vulnerability has been reported in GE Imaging and Ultrasound Products which could allow a remote attacker to gain access or modify the sensitive information on the targeted system,

Description-

1. Information Disclosure Vulnerability (CVE-2020-25125) This vulnerability exists in GE Healthcare Imaging and Ultrasound Products due to unprotected transport of credentials A remote attacker could exploit this vulnerability by gaining access to the network Successful exploitation of this vulnerability could allow attacker to gain access to sensitive information on the targeted system

2. Information Disclosure Vulnerability (CVE-2020-25179) This vulnerability exists in GE Healthcare Imaging and Ultrasound Products because they allow exposed/default credentials to be utilized to access the system. An attacker could exploit this vulnerability by gaining access to the network Successful exploitation of this vulnerability could allow attacker to gain access or modify the sensitive information on the targeted system.

❖ VULNERABILITY NOTES 2019

1) CIVN-2019-0202 TP-Link Router Remote Code Execution Vulnerability

Overview- A vulnerability has been reported in TP-Link routers which could be exploited by a remote attacker to take complete control of the router.

Description-This vulnerability exists in TP Link routers due to improper handling of HTTP requests. A remote attacker could exploit this vulnerability by sending an HTTP request including a character string longer than the allowed number, resulting in the user password being with a value zero. Successful exploitation of this vulnerability could allow the attacker to take complete control of the router

2) CIVN-2019-0199 Multiple Vulnerabilities in Microsoft Window

Overview-Multiple vulnerabilities have been reported in Microsoft Windows which could allow an attacker to bypass security restrictions, access sensitive information, cause denial of service (DoS) condition and execute arbitrary code on the targeted system.

Description-

1. Microsoft Windows Win32k Privilege Escalation Vulnerability (CVE-2019-1458) This vulnerability exists in Microsoft windows due to improper handling of objects in memory. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the targeted system.
2. Microsoft Windows Win32k Information Disclosure Vulnerability (CVE-2019-1469) This vulnerability exists when the win32k component improperly provides kernel information. A local attacker could exploit this vulnerability by running a specially rafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to access sensitive information on the targeted system.
3. Microsoft Windows Hyper-V Information Disclosure Vulnerability (CVE-2019- 470) This vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to access sensitive information on the targeted system.
4. Microsoft Windows Hyper-V Remote Code Execution Vulnerability (CVE-2019- 471) This vulnerability exists when Windows Hyper-V on a host operating system fails properly validate input from an authenticated user on a guest operating system. A remote attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute remote code on the targeted system.
5. Microsoft Windows Kernel Information Disclosure Vulnerability (CVE-2019-1474) This vulnerability exists in Microsoft windows due to the improper handling of objects in memory. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the targeted system.
6. Microsoft Windows Printer Service Privilege Escalation Vulnerability (CVE-2019-1477) This vulnerability exists in Microsoft windows due to a boundary error when the Windows Printer Service improperly validates file paths while loading printer drivers. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the targeted system.
7. Microsoft Windows COM Server Privilege Escalation Vulnerability (CVE-2019-1478) This vulnerability exists in Microsoft windows due to the improper handling of COM object creation. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the targeted system.
8. Microsoft Windows GDI Information Disclosure Vulnerability (CVE-2019-1466 CVE-2019-1465 CVE-2019-1467) These vulnerabilities exist when the Windows GDI component improperly discloses the contents of its memory. A remote attacker

could exploit this vulnerability by convincing a user to open a specially crafted document on the affected system. Successful exploitation of this vulnerability could allow the attacker to access sensitive information on the targeted system.

9. Microsoft Windows Kernel Information Disclosure Vulnerability (CVE-2019-1472) This vulnerability exists when the Windows kernel improperly handles objects in memory. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to access sensitive information on the targeted system.
10. Microsoft Win32k Graphics Remote Code Execution Vulnerability (CVE-2019- 468) This vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. A remote attacker could exploit this vulnerability by hosting a specially crafted weside on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute remote code on the targeted system.
11. Microsoft Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability (CVE-2019- 1453) This vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. A remote attacker could exploit this vulnerability by sending a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to cause denial of service on the targetedsystem.
12. Privilege escalation vulnerability in Microsoft Windows AppX Deployment Server (CVE-2019- 1476 CVE-20191483) These vulnerabilities exist in Microsoft windows due to an error in junctions handling within the Windows Appx Deployment Server. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the targeted system.
13. Microsoft Defender Security Feature Bypass Vulnerability (CVE-2019-1488) This vulnerability exists in Microsoft windows due to the Microsoft Defender improperly handles specific buffers. A remote attacker could exploit this vulnerability by bypassing certain security restrictions and perform unauthorized actions on the affected system. Successful exploitation of this vulnerability could allow the attacker to bypass security features on the targeted system.
14. Microsoft Windows Media Player Information Disclosure Vulnerability (CVE-2019-1481 CVE-2019-1480) These vulnerabilities exist in Microsoft windows due to improper handling of objects in memory A remote attacker could exploit this vulnerability by creating a specially crafted media file memory. A remote attacker could exploit this vulnerability by creating a specially crafted media file, trick the victim into opening it, trigger out-of-bounds read error and read contents of memory on the system. Successful exploitation of these vulnerabilities could allow the attacker to access sensitive information on the targeted system.
15. Microsoft Windows OLE Remote Code Execution Vulnerability (CVE-2019-1484) This vulnerability exists in Microsoft windows due to insufficient validation of user-supplied input in Microsoft Windows OLE implementation. A remote attack could exploit this vulnerability by opening a specially crafted file on the affected system. Successful exploitation of this vulnerability could allow the attacker to execute remote code on the targeted system.

3) CIVN-2019-0198 Microsoft SQL Server Reporting Services XSS Vulnerability

Overview-A Vulnerability has been reported in Microsoft SQL Server Reporting Services which could allow an authenticated attacker to perform Cross-site Scripting (XSS) attack on the targeted system.

Description- This vulnerability exists in Microsoft SQL Server Reporting Services due to improper sanitization of a specially crafted web request to an affected SSRS server. An attacker could exploit this vulnerability by convincing an authenticated user to click a specially crafted link to an affected SSRS server. Successful exploitation of this vulnerability could allow an authenticated attacker to run scripts in the context of the targeted user.

4) CIVN-2019-0200 Multiple Vulnerabilities in Intel Products

Overview-Multiple vulnerabilities have been reported in Intel products which could allow a local attacker to escalate privileges, cause denial of service (DoS) conditions or access sensitive information on a targeted system

Description-

1. Escalation of Privilege Vulnerability in Intel RST (CVE-2019-14568) This vulnerability exists in the Intel Rapid Storage Technology (RST) due to improper handling of permissions by the affected software. An authenticated attacker could exploit this vulnerability through local access to the system, Successful exploitation of this vulnerability could allow the attacker to get escalated privileges on the targeted system.
2. Vulnerability in multiple Intel Processors (CVE-2019-14607) This vulnerability exists in multiple Intel Processors due to improper checking of conditions by the firmware. An attacker could exploit these vulnerabilities through local access to the targeted system. Successful exploitation of these vulnerabilities could allow the attacker to get escalated privileges, cause denial of service (DoS) conditions or access sensitive information on a targeted system.

5) CIVN 2019-0201 Microsoft SharePoint Server Information Disclosure Vulnerability

Overview- A Vulnerability has been reported in Microsoft SharePoint which could allow information from the targeted system. remote malicious user to obtain sensitive.

Description- This vulnerability exists in Microsoft SharePoint. By sending a specially crafted request to a susceptible SharePoint Server instance, a remote attacker could exploit this vulnerability to read arbitrary files on the server.

➢ How to report Security Incident and Vulnerability.

CERT-In shall operate an Incident Response Help Desk on 24 hours basis on all days including Government and other public holidays to facilitate reporting of cyber security incidents.

Reporting of incidents :- Any individual, organisation or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action. The details regarding methods and formats for reporting cyber security incidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cyber security shall be published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.

➢ How to report a cybercrime

1. For online reporting of cybercrime, visit the Cybercrime reporting portal.
2. You can either report a complain pertaining to online Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content either anonymously (i.e. without revealing your identity) or by revealing your identity. However, as a responsible citizen you should use “Report and Track” option for reporting the incident/ crime, since it would help the Law enforcement agencies to contact you for further details.
3. To report anonymously, click here. In this case, a user need not provide any personal information. However, information related to the incident / complaint should be complete for the police authorities to take necessary action. It is recommended that a user uploads the evidence with the complaint which would help police authorities for prompt action. However, a complaint can also be reported by providing information like website address, e-mail address, WhatsApp number etc. Please note that False information provided by complainant may lead to penal action as per law.
4. To report a crime revealing your identity, click the "Report and track option". Register by giving your details such as Name and Mobile number. You will receive a One Time Password (OTP) that will be used to verify your phone number. The OTP is valid for 30 minutes. Once you successfully register register your mobile number on the portal, you will be able to report the compliant. Fill all the details related to the crime and submit.

Questions for Viva:

1. What is cyber security?
2. What are the elements of cyber security?
3. Define cryptography?
4. What are the advantage of cyber security?

Gangamai College of Engineering, Nagaon, Dhule

Department of Computer Engineering

Name :____________________________________ **Date of Performance:** _ _ /_ _/20_ _

Class : B.E. Computer **Date of Completion** : _ _ /_ _/20_ _

Div :____________ **Batch**: ____________ **Grade** :_________

Subject : Cyber Security Lab **Sign. of Teacher**

Experiment No-3

Aim: Study of Information Gathering Tools in Kali Linux

Live host identification:

Hping3 Hping3 is nearly similar to ping tools but is more advanced, as it can bypass the firewall filter and use TCP, UDP, ICMP and RAW-IP protocols. It has a traceroute mode. hping3 172.16.0.7 hping3 --scan 1-30,70-90 -S sscoetjalgaon.ac.in.

hping commands for scanning methods

ICMP ping

hping3 -1 10.0.0.25

Hping performs an ICMP ping scan by specifying the argument -1 on the command line. You may use –ICMP of -1 argument in the command line. By issuing the above command, hping sends ICMP-echo request to 10.0.0.25 and receives ICMP-reply, the same as with a ping utility.

ACK scan on port 80

hping3 –A 10.0.0.25 –p 80 Hping can be configured to perform an ACK scan by specifying the argument -A in the command line. Here, you are setting ACK flag in the probe packets and performing the scan. You perform this scan when a host does not respond to a ping request. By issuing this command, Hping checks if a host is alive on a network. If it finds a live host and an open port, it returns an RST response.

UDP scan on port 80

hping3 -2 10.0.0.25 –p 80

Hping uses TCP as its default protocol. Using the argument -2 in the command line specifies that Hping operates in UDP mode. You may use either --udp of -2 arguments in the command line. By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed, and does not respond with a message if the port is open.

Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -p 139 –s
```

By using the argument -Q in the command line, Hping collects all the TCP sequence numbers generated by the target host (192.168.1.103).

Firewalls and Time Stamps

```
hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
```

Many firewalls drop those TCP packets that do not have TCP Timestamp option set. By adding the –tcp-timestamp argument in the command line, you can enable TCP timestamp option in Hping and try to guess the timestamp update frequency and uptime of the target host (72.14.207.99).

SYN scan on port 50-60

```
hping3 -8 50-60 –S 10.0.0.25 –V
```

By using the argument -8 (or) --scan in the command, you are operating Hping in scan mode in order to scan a range of ports on the target host. Adding the argument -S allows you to perform a SYN scan. Therefore, the above command performs a SYN scan on ports 50-60 on the target host.

FIN, PUSH and URG scan on port 80

```
hping3 –F –P –U 10.0.0.25 –p 80
```

By adding the arguments –F, -P, and –U in the command, you are setting FIN, PUSH, and URG packets in the probe packets. By issuing this command, you are performing FIN, PUSH,and URG scans on port 80 on the target host (10.0.0.25). If port 80 is open on the target, you will not receive a response. If the port is closed, Hping will return an RST response.

Scan entire subnet for live host

```
hping3 -1 10.0.1.x --rand-dest –I eth0
```

By issuing this command, Hping performs an ICMP ping scan on the entire subnet 10.0.1.x; in other words, it sends ICMP-echo request randomly (--rand-dest) to all the hosts from 10.0.1.0 – 10.0.1.255 that are connected to the interface eth0. The hosts whose ports are open will respond with an ICMP-reply. In this case, you have not set a port, so Hping sends packets to port 0 on all IP addresses by default.

Intercept all traffic containing HTTP signature

hping3 -9 HTTP –I eth0

The argument -9 will set the Hping to listen mode. So, by issuing the command -9 HTTP, Hping starts listening on port 0 (of all the devices connected in the network to interface eth0), intercepts all the packets containing HTTP signature, and dump from signature end to the packet's end. For example, on issuing the command hping2 -9 HTTP, if Hping reads a packet that contains data 234-09sdflkjs45-HTTPhello_world, it will display theresult as hello_world.

SYN flooding a victim

hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 –flood

The attacker employs TCP SYN flooding techniques by using spoofed IP addresses to perform DoS attack.

Determine number of pings

hping3 -c 3 10.10.10.10

Here, **-c 3** means that we only want to send three packets to the target machine

Use random source address

--rand-source

Set data size

Set data packet size in bytes --data <size>

Spoof source address

hping3 -S <IP address attacked> -a <spoofed IP address>

or
hping3 S <IP address attacked> spoof <spoofed IP address>

Examples

hping3 <Target IP> -Q -p 139 -s

By using the argument -Q in the command line, Hping collects all the TCP sequence numbers generated by the target host.

hping3 –A <Target IP> –p 80

By issuing this command, Hping checks if a host is alive on a network. If it finds a live host and an open port, it returns an RST response.

hping3 -S <Target IP> -p 80 --tcp-timestamp

By adding the –tcp-timestamp argument in the command line, Hping enable TCP timestamp option and try to guess the timestamp update frequency and uptime of the target host.

hping3 –F –P –U 10.0.0.25 –p 80

By issuing this command, an attacker can perform FIN, PUSH, and URG scans on port 80 on the target host.

hping3 –scan 1-3000 -S 10.10.10.10

Here, **–scan** parameter defines the port range to scan and **–S** represents SYN flag

hping3 10.10.10.10 --udp --rand-source --data 500

Perform UDP packet crafting.

Network and Port Scanner:

NMAP NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

Step 1 - To open, go to Applications → 01-Information Gathering → nmap or zenmap.

Step 2 - The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable "-O". nmap -O 172.16.0.7 nmap -O

Step 3 - Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command - nmap -p 1-65535 -T4 172.16.0.7 Where the parameter "–p" indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and "-T4" is the speed of scanning at which NMAP has to run.

References:

1. https://www.jigsawacademy.com/blogs/cyber-security/nmap-commands/
2. https://www.youtube.com/watch?v=5Q1wFDS3iOo
3. https://www.tutorialspoint.com/kali_linux/index.htm

NMAP Stealth Scan

Stealth scan or SYN is also known as half-open scan, as it doesn't complete theTCP threeway handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn't active or is closed.

nmap -sS 172.16.0.7

nmap -sS -T4 sscoetjalgaon.ac.in

References:

1. https://nmap.org/book/synscan.html
2. https://www.tutorialspoint.com/kali_linux/index.htm

DNS Analysis:

dnsenum Dnsenum helps to get MX, A, and other records connect to a domain.

dnsenum sscoetjalgaon.ac.in

Multithreaded perl script to enumerate DNS information of a domain and to discovernon-contiguous ip blocks.

OPERATIONS:

- Get the host's addresse (A record).
- Get the namservers (threaded).
- Get the MX record (threaded).
- Perform axfr queries on nameservers and get BIND VERSION (threaded).
- Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").
- Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).
- Calculate C class domain network ranges and perform whois queries on them (threaded).
- Perform reverse lookups on netranges (C class or/and whois netranges) (threaded).
- Write to domain_ips.txt file ip-blocks.

Source: https://github.com/fwaeytens/dnsenum

- Author: Filip Waeytens, tix tixxDZ
- License: GPLv2.

References:

1. https://tools.kali.org/information-gathering/dnsenum
2. https://www.youtube.com/watch?v=mCbz92LdEfY3.
3. https://www.tutorialspoint.com/kali_linux/index.htm

SSL Analysis : tlssled

TLSSLed is a Linux shell script used to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. The current tests include checking if the target supports the SSLv2 protocol, the NULL cipher, weak ciphers based on theirkey length (40 or 56 bits), the availability of strong ciphers (like AES), if the digital certificate is MD5 signed, and the current SSL/TLS renegotiation capabilities.

To start testing, open a terminal and type “tlssled URL port“. It will start to test the certificate to find data, where the port is 443.

tlssled sscoetjalgaon.ac.in 443

References:

1. https://tools.kali.org/information-gathering/tlssled
2. https://www.youtube.com/watch?v=D6PuHT6sVQI
3. https://www.tutorialspoint.com/kali_linux/index.htm

Dmitry:

Perform a whois lookup on the IP address or domain name of a host. It also searches for possible subdomains.

dmitry -w sscoetjalgaon.ac.in

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line program coded purely in C with the ability to gather as much information as possible about a host.

DMitry has a base functionality with the ability to add new functions. Basic functionality of Dmitry allows for information to be gathered about a target host from a simple who is lookup on the target to Up Time reports and TCP port scans.

The application is considered a tool to assist in information gathering when information is required quickly by removing the need to enter multiple commands and the timely process of searching through data from multiple sources.

To get straight into DMitry without reading this document, you can initially type "dmitry target", this will perform the majority of functions on the target.

References:

1. https://github.com/jaygreig86/dmitry
2. https://www.youtube.com/watch?v=z2EUhV11QB4
3. https://www.tutorialspoint.com/kali_linux/index.htm

p0f:

p0f is a tool that can identify the operating system of a target host simply by examining captured packets even when the device in question is behind a packet firewall.

Type the command: **“p0f –i eth0 –p -o filename”**.

Where the parameter "-i" is the interface name as shown above. "-p" means it is in promiscuous mode.

"-o" means the output will be saved in a file.

Open a webpage with the address 172.16.0.7 From the results, you can observe that the Webserver is using apache version and the OS.

p0f -i eth0 -p -o abc.

Questions for Viva:

1. What is mean by data leakage?
2. What is port scanning?
3. Explain SSL.
4. What is a VPN?

Gangamai College of Engineering, Nagaon, Dhule

Department of Computer Engineering

Name :___________________________________ **Date of Performance:** _ _/_ _/20_ _

Class : B.E. Computer **Date of Completion** : _ _/_ _/20_ _

Div :____________ **Batch**: ____________ **Grade :**_________

Subject : Cyber Security Lab **Sign. of Teacher**

Experiment No-4

Aim: Study of Vulnerability Analysis Tools in Kali Linux

Fuzzing Tools: BED

BED is a program designed to check daemons for potential buffer overflows, format strings, et. al.

bed -s HTTP -t 172.16.0.7

BED simply sends the commands to the server and checks whether it is still alive afterwards.

Of course this will not detect all bugs of the specified daemon but it will (at least it should) help you to check your software for common vulnerabilities.

BED Package Description

BED stands for Bruteforce Exploit Detector. It is designed to check daemons for potential buffer overflows, format strings et. al.

- Author: mjm, eric
- License: GPLv2

Tools included in the bed package

bed – A network protocol fuzzer

```
root@kali:~# bed


BED 0.5 by mjm ( www.codito.de )

eric ( www.snake-basket.de )


Usage:


./bed.pl -s <plugin> -t <target> -p <port> -o <timeout> [ depends on the plugin ]

<plugin> =

FTP/SMTP/POP/HTTP/IRC/IMAP/PJL/LPD/FINGER/SOCKS4/SOCKS5

<target> = Host to check (default: localhost)

<port> = Port to connect to (default: standard port)


<timeout> = seconds to wait after each test (default: 2 seconds)

use "./bed.pl -s <plugin>" to obtain the parameters you need for the plugin.

Only -s is a mandatory switch.
```

bed Usage Example

Use the HTTP plugin ***(-s HTTP)*** to fuzz the target server ***(-t 192.168.1.15)***:

```
root@kali:~# bed -s HTTP -t 192.168.1.15
```

```
BED 0.5 by mjm ( www.codito.de ) & eric ( www.snake-basket.de
)


+ Buffer overflow testing:


          testing: 1 HEAD XAXAX HTTP/1.0
```

Questions for Viva:

1. What are white hat hackers?
2. Explain botnet.
3. What is MITM attack?
4. Define ARP & its working process.

Gangamai College of Engineering, Nagaon, Dhule
Department of Computer Engineering

Name :________________________________ **Date of Performance:** _ _/_ _/20_ _

Class : B.E. Computer **Date of Completion** : _ _/_ _/20_ _

Div :__________ **Batch**: __________ **Grade :**________

Subject : Cyber Security Lab **Sign. of Teacher**

Experiment No-5

Aim: Study of Web Application Analysis Tools in Kali Linux

Web Application Proxies: Burpsuite

Burpsuite can be used as a sniffing tool between your browser and the web servers to find the parameters that the web application uses.

To open Burpsuite, go to Applications → Web Application Analysis → burpsuite. To make the setup of sniffing, configure burpsuite to behave as a proxy. Go to Proxy → Options; Check the box under Running for interface 127.0.0.1.

Using Burp Proxy

The Proxy tool lies at the heart of Burp's user-driven workflow, and gives you a direct view into how your target application works "under the hood". It operates as a web proxy server, and sits as a man-in-the-middle between your browser and destination web servers. This lets you intercept, inspect, and modify the raw traffic passing in both directions.

If the application employs HTTPS, Burp breaks the TLS connection between your browser and the server, so that even encrypted data can be viewed and modified within Burp's tools.

Configuring your external browser to work with Burp

Once you have confirmed that the proxy listener is up and running, you need to configure your browser to use it as its HTTP proxy server. To do this, you change your browser's proxy settings to use the proxy host address (by default, 127.0.0.1) and port (by default, 8080) for both HTTP and HTTPS protocols, with no exceptions. This ensures that all HTTP and HTTPS traffic will pass through Burp. The details of how to do this vary by rowser and version. Please refer to the relevant section below based on which browser you intend to use with Burp.

- Configuring Firefox to work with Burp
- Configuring Chrome to work with Burp
- Configuring Safari to work with Burp
- Configuring Internet Explorer to work with Burp.

Check your browser proxy configuration

When you've configured your browser, you need to test that it is working properly by performing the following steps. If anything does not happen in the way described below, there is a problem with your browser configuration. In this case, please refer to the troubleshooting page.

1. Make sure you have checked that the proxy listener is active and have configured your chosen browser.

2. With Burp running, open the browser that you configured and go to any HTTP URL (don't use HTTPS for the moment). Your browser should sit waiting for the request to complete, hat is, it should look like it is stuck trying to load a page. This is because Burp has intercepted the HTTP request that your browser is trying to send.

3. In Burp, go to the "Proxy" tab and open the "Intercept" sub-tab. Both of these tabs should be highlighted. On the "Intercept" tab, you should see the intercepted HTTP request in the main panel.

4. Notice the button that says "Intercept is on". If you click it, it will change to "Intercept is off" and the request will be released from Burp.

5. Go back to your browser. You should now see the requested page loading as it would during normal browsing.

If everything went as described above, you have finished the mandatory configuration steps for using an external browser with Burp Suite. However, at the moment you will only be able to test web applications that exclusively use HTTP.If you try and access an HTTPS URL using your external browser, you will notice that the connection is blocked. Therefore, we strongly recommend that youperform the final additional step to install Burp's CA certificate so that you canalso test applications using HTTPS.

Getting set up

Burp Proxy works in conjunction with the browser that you are using to access the target application. You can either:

- **Use Burp's embedded browser**, which requires no additional configuration.Go to the "Proxy" > "Intercept" tab and click "Open Browser". A new browser session will open in which all traffic is proxied through Burp automatically. You can even use this to test over HTTPS without the need to install Burp's CA certificate.
- **Use an external browser** of your choice. For various reasons, you mightnot want to use Burp's embedded browser. In this case, you need to perform some additional steps to configure your browser to work with Burp, and install Burp's CA certificate in your browser.

When you have things set up, visit any URL in your browser, then go to the "Proxy" > "Intercept" tab in Burp Suite. If everything is working, you should see an HTTP request displayed for you to view and modify. You will need to forward HTTP messages as they appear in order to continue browsing. You should alsosee entries appearing on the "HTTP history" tab.

Intercepting requests and responses

The Intercept tab displays individual HTTP requests and responses that have been intercepted by Burp Proxy for review and modification. This feature is a key part of Burp's user-driven workflow:

- Manually reviewing intercepted messages is often key to understanding theapplication's attack surface in detail.
- Modifying request parameters often allows you to quickly identify common security vulnerabilities.

By default, Burp Proxy intercepts only request messages, and does not intercept requests for URLs with common file extensions that are often not directly interesting when testing (images, CSS, and static JavaScript). You can change this default behavior in the interception options. For example, you can configure Burp to only intercept in-scope requests containing parameters, or to intercept all responses containing HTML.

You may often want to turn off Burp's interception altogether, so that all HTTP messages are automatically forwarded without requiring user intervention. Youcan do this using the master interception toggle in the Intercept tab.

Using the Proxy history

Burp maintains a full history of all requests and responses that have passed through the Proxy. This enables you to review the browser-server conversation to understand how the application functions, or carry out key testing tasks. Sometimes you may want to completely disable interception in the Intercept tab,and freely browse a part of the application's functionality, before carefully reviewing the resulting requests and responses in the Proxy history. Burp provides the following functions to help you analyze the Proxy history: The history table can be sorted by clicking on any column header (clicking a header cycles through ascending sort, descending sort, and unsorted). This lets you quickly group similar items and identify any anomalous items.

Burp Proxy testing workflow

A key part of Burp's user-driven workflow is the ability to send interesting items between Burp tools to carry out different tasks. You can do this using the context menus that you can access by right-clicking in various locations throughout Burp. For example, having observed an interesting request in the proxy, you might wantto quickly perform a vulnerability scan of just that request, using Burp Scanner.

- You could send the request to Repeater to manually modify the request and reissue it over and over.
- You could send the request to Intruder to perform various types of automated customized attacks.
- You could send the request to Sequencer to analyze the quality of randomness in a token returned in the response.
- You can perform all these actions and various others from the context menus that appear in both the Intercept tab and the Proxy history.

Key configuration options for Burp Proxy

For more specialized testing tasks, or when working with unusual applications, you may need to modify some of Burp Proxy's numerous options:

- You might need to modify the Proxy listener, to bind to different interfaces, redirect requests to different hosts, handle server TLS certificates differently,or support invisible proxying for non-proxy-aware clients.
- You can configure the Proxy to automatically modify HTTP responses in various systematic ways; for example, to unhide hidden form fields, remove JavaScript form validation, etc.
- You can configure match / replace rules to automatically change the content of requests and responses.

References:

1. https://portswigger.net/burp/documentation/desktop/getting-started/proxysetup/browser
2. https://portswigger.net/burp/documentation/desktop/penetration-testing
3. https://www.youtube.com/watch?v=1O-xOTp96d8
4. https://www.tutorialspoint.com/kali_linux/index.htm

ZapProxy

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.

At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.

ZAP-OWASP Zed Attack Proxy is an easy-to-use integrated penetration testing tool for finding vulnerabilities in web applications. It is a Java interface.

Step 1 - To open ZapProxy, go to Applications → 03-Web Application Analysis → ZAP.

Step 2 - Click “Accept”. ZAP will start to load.

Step 3 - Choose one of the Options and click “Start”.. Preferably select “No, I do not want to persist this session at this moment in time” .

Step 4 - Enter URL of the testing web at “URL to attack” → click “Attack”. After the scan is completed, on the top left panel you will see all the crawled sites. In the left panel “Alerts”, you will see all the findings along with the description.

Step 5 - Click “Spider” and you will see all the links scanned.

Install and Configure ZAP

ZAP has installers for Windows, Linux, and Mac OS/X. There are also Docker images available on the download site listed below.

Install ZAP

The first thing to do is install ZAP on the system you intend to perform pentesting on. Download the appropriate installer from the Download page. Note that ZAP requires Java 8+ in order to run. The Mac OS/X installer includes an appropriate version of Java but you must install Java 8+ separately for Windows, Linux, and Cross-Platform versions. The Docker versions do not require you to install Java.Once the installation is complete, launch ZAP and read the license terms. Click **Agree** if you accept the terms, and ZAP will finish installing, then ZAP will automatically start.

Persisting a Session

When you first start ZAP, you will be asked if you want to persist the ZAP session. By default, ZAP sessions are always recorded to disk in a HSQLDB database with a default name and location. If you do not persist the session, those files are deleted when you exit ZAP. If you choose to persist a session, the session information will be saved in the local database so you can access it later, and you will be able to provide custom names and locations for saving the files.

The Burp tools you will use for particular tasks are as follows:

Scanner - This is used to automatically scan websites for content and security vulnerabilities.

Intruder - This allows you to perform customized automated attacks, to carry out all kinds of testing tasks.

Repeater - This is used to manually modify and reissue individual HTTP requests over and over.

Collaborator client - This is used to generate Burp Collaborator payloads and monitor for resulting out-of-band interactions.

Clickbandit - This is used to generate clickjacking exploits against vulnerable applications.

Sequencer - This is used to analyze the quality of randomness in an application's session tokens.

Decoder - This lets you transform bits of application data using common encoding and decoding schemes.

Comparer - This is used to perform a visual comparison of bits of application data to find interesting differences.

Questions for Viva:

1. Explain WAF.
2. What is the full form of XSS?
3. Who are hackers?
4. What is hacking?

Gangamai College of Engineering, Nagaon, Dhule
Department of Computer Engineering

Name :___________________________________ **Date of Performance:** _ _ /_ _/20_ _

Class : B.E. Computer **Date of Completion** : _ _ /_ _/20_ _

Div :____________ **Batch**: ____________ **Grade :**__________

Subject : Cyber Security Lab **Sign. of Teacher**

Experiment No-6

Aim: Study of Database Assessment Tools in Kali Linux

Sqlmap

Sqlmap automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Step 1 - To open sqlmap, go to Applications → 04-Database Assessment → sqlmap.

Step 2 - To start the sql injection testing, type "sqlmap – u URL of victim".

Step 3 - From the results, you will see that some variable are vulnerable.

sqlmap -u http://172.16.0.7/admission/

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and abroad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Features:

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access,
  IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB database management systems.
- Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.

  Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.
- Support to dump database tables entirely, a range of entries or specific columns as per user’s choice. The user can also choose to dump only a range of characters from each column’s entry.
- Support to search for specific database names, specific tables across all databases or specific columns across all databases’ tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns’ names contain string like name and pass.
- Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to execute arbitrary commands and retrieve their standard output on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user’s choice.
- Support for database process’ user privilege escalation via Metasploit’s Meterpreter getsystem command.

Source: https://github.com/sqlmapproject/sqlmap

Author: Bernardo Damele Assumpcao Guimaraes, Miroslav Stampar

License: GPLv2

Tools included in the sqlmap package

sqlmap – automatic SQL injection tool

```
root@kali:~# sqlmap -help


____
___H___
____ ____[)]_______ ____ ____ {1.2.11#stable}
```

```
|_ -| . [(] | .'| . |
|___|_ [,]_|_|_|__,| _|
|_|V |_| http://sqlmap.org

Usage: python sqlmap [options]


Options:

-h, --help          Show basic help message and exit

-hh                 Show advanced help message and exit

--version           Show program's version number and exit

-v VERBOSE          Verbosity level: 0-6 (default 1)

Target:

At least one of these options has to be provided to
define the
    target(s)

    -u URL, --url=URL Target URL (e.g.
"http://www.site.com/vuln.php?id=1")

-g GOOGLEDORK       Process Google dork results as target
URLs

Request:
These options can be used to specify how to connect to
the target URL
```

```
--data=DATA       Data string to be sent through POST
(e.g. "id=1")
--cookie=COOKIE HTTP Cookie header value (e.g.
"PHPSESSID=a8d127e..")
--random-agent    Use randomly selected HTTP User-Agent
header value
--proxy=PROXY     Use a proxy to connect to the target
URL
--tor             Use Tor anonymity network
--check-tor       Check to see if Tor is used properly


Injection:
These options can be used to specify which parameters
to test for,
provide custom injection payloads and optional
tampering scripts
-p TESTPARAMETER      Testable parameter(s)
--dbms=DBMS           Force back-end DBMS to provided
value

Detection:


    These options can be used to customize the
detection phase


--level=LEVEL     Level of tests to perform (1-5,
    default 1)


--risk=RISK       Risk of tests to perform (1-3,default
1)
Techniques:
```

These options can be used to tweak testing of specific SQL injection

Techniques

```
--technique=TECH SQL injection techniques to use

(default "BEUSTQ")
```

Enumeration:

These options can be used to enumerate the back-end

Database

management system information, structure and data

contained in the

tables. Moreover you can run your own SQL statements

```
-a, --all          Retrieve everything
-b, --banner       Retrieve DBMS banner
--current-user     Retrieve DBMS current user
--current-db       Retrieve DBMS current database
--passwords        Enumerate DBMS users password hashes
--tables           Enumerate DBMS database tables
--columns          Enumerate DBMS database table columns
--schema           Enumerate DBMS schema
--dump             Dump DBMS database table entries
--dump-all         Dump all DBMS databases tables entries
-D DB              DBMS database to enumerate
-T TBL             DBMS database table(s) to enumerate
-C COL             DBMS database table column(s) to

Enumerate
```

```
Operating system access:
These options can be used to access the back-end
Database management
    system underlying operating system
--os-shell        Prompt for an interactive operating
system shell
--os-pwn          Prompt for an OOB shell, Meterpreter
or VNC

General:
These options can be used to set some general working
parameters
--batch           Never ask for user input, use the
default behavior
--flush-session   Flush session files for current target

Miscellaneous:

--sqlmap-shell    Prompt for an interactive sqlmap shell

--wizard          Simple wizard interface for beginner
Users
```

Features

- Full support for **MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid,**

InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB and Virtuoso database management systems.

- Full support for six SQL injection techniques: **boolean-based blind, timebased blind, error-based, UNION query-based, stacked queries and outof-band**.
- Support to **directly connect to the database** without passing via a SQLinjection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate **users, password hashes, privileges, roles, databases, tables and columns**.
- Automatic recognition of password hash formats and support for **cracking them using a dictionary-based attack**.
- Support to **dump database tables** entirely, a range of entries or specificcolumns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
- Support to **search for specific database names, specific tables across all databases or specific columns across all databases' tables**. This is useful,for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
- Support to **download and upload any file** from the database serverunderlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to **execute arbitrary commands and retrieve their standard output** on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to **establish an out-of-band stateful TCP connection between the attacker machine and the database server** underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.
- Support for **database process' user privilege escalation** via Metasploit's Meterpreter get system command.

Questions for Viva:

1. What is network sniffing?
2. What is the importance of DNS monitoring?
3. What is Black box testing and White box testing?
4. What is SSH?

Gangamai College of Engineering, Nagaon, Dhule
Department of Computer Engineering

Name :________________________________ **Date of Performance:** _ _/_ _/20_ _

Class **:** B.E. Computer **Date of Completion :** _ _/_ _/20_ _

Div **:**____________ **Batch**: ____________ **Grade :**_________

Subject : Cyber Security Lab **Sign. of Teacher**

Experiment No-7

Aim: Study of Sniffing and Spoofing Tools in Kali Linux

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions. Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

Wireshark has a rich feature set which includes the following:

Deep inspection of hundreds of protocols, with more being added all the time

Live capture and offline analysis

Standard three-pane packet browser

Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others

Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility

The most powerful display filters in the industry

Rich VoIP analysis

Capture files compressed with gzip can be decompressed on the fly

Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)

Coloring rules can be applied to the packet list for quick, intuitive analysis

Output can be exported to XML, PostScript®, CSV, or plain text

Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network * General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime,WildPackets EtherPeek/TokenPeek/AiroPeek, and many others

Source: http://www.wireshark.org/about.html

wireshark – network traffic analyzer

```
root@kali:~# wireshark -h


Wireshark 2.6.4 (Git v2.6.4 packaged as 2.6.4-1)

Interactively dump and  analyze  network  traffic.
See https://www.wireshark.org for more information.


Usage: wireshark [options] ... [ <infile> ]



Capture interface:


-i <interface> name or idx of interface (def:

first non-loopback)

-f <capture filter> packet filter in libpcap filter

Syntax

-s <snaplen>          packet snapshot length (def:

appropriate maximum)
-p                    don't capture in promiscuous
mode
```

```
-k                     start capturing immediately
(def:

do nothing)
-S                     update packet display when new

packets are captured
-l                     turn on automatic scrolling
while -

S is in use
-I                     capture in monitor mode, if

available
-B <buffer size>       size of kernel buffer (def: 2MB)
-y <link type>         link layer type (def: first

appropriate)

--time-stamp-type <type> timestamp method for
interface
-D                     print list of interfaces and
exit
-L                     print list of link-layer types
of

iface and exit
--list-time-stamp-types   print list of timestamp
types for

iface and exit

Capture stop conditions:

-c <packet count>      stop after n packets (def:
infinite)
-a <autostop cond.> ...   duration:NUM - stop after
NUM
seconds
                       filesize:NUM - stop this file after
NUM KB
                       files:NUM - stop after NUM files

Capture output:
```

```
-b <ringbuffer opt.> ... duration:NUM - switch to next
file
after NUM secs
                     filesize:NUM - switch to next file

after NUM KB
                     files:NUM - ringbuffer: replace

after NUM files

Input file:



-r <infile>          set the filename to read from (no
pipes or stdin!)

Processing:
-R <read filter>     packet filter in Wireshark display
filter syntax
                     disable all name resolutions (def:

all enabled)

-N <name resolve flags>   enable specific name resolution(s):
"mnNtdv"

-d <layer_type>==<selector>,<decode_as_protocol> ...

                     "Decode As", see the man page for

Details

                     Example: tcp.port==8888,http

--enable-protocol <proto_name>

                     enable dissection of proto_name

--disable-protocol <proto_name>

                     disable dissection of proto_name

--enable-heuristic <short_name>

                     enable dissection of heuristic

protocol

--disable-heuristic <short_name>

                     disable dissection of heuristic
```

```
protocol


User interface:

-C <config profile>       start with specified
configuration

profile

-Y <display filter>       start with the given display
filter

-g <packet number>        go to specified packet
number after

"-r"
-J <jump filter>          jump to the first packet
matching
the (display)

                          filter
-j                        search backwards for a
matching
packet after "-J"

-m <font>                 set the font name used for
most
Text

-t a|ad|d|dd|e|r|u|ud     output format of time stamps
(def:
r: rel. to first)

-u s|hms                  output format of seconds
(def: s:
seconds)

-X <key>:<value>          eXtension options, see man
page for
Details

-z <statistics>           show various statistics, see
man
page for details
```

```
Output:

-w <outfile|->              set the output filename (or
'-' for
stdout)

Miscellaneous:

-h                          display this help and exit
-v                          display version info and
exit
-P <key>:<path>             persconf:path - personal
configuration files


                            persdata:path - personal data files
-o <name>:<value> ...       override preference or recent
setting
-K <keytab>                 keytab file to use for kerberos
decryption
--display=DISPLAY           X display to use
--fullscreen                start Wireshark in full screen
```

Wireshark is a packet sniffing program that administrators can use to isolate and troubleshoot problems on the network. It can also be used to capture sensitive data like usernames and passwords. It can also be used in wrong way (hacking) to ease drop.

Packet sniffing is defined as the process to capture the packets of data flowing across a computer network. The Packet sniffer is a device or software used for the process of sniffing.

Below are the steps for packet sniffing:

- Open the Wireshark Application.
- Select the current interface. Here in this example, interface is Ethernet that we would be using.
- The network traffic will be shown below, which will be continuous. To stop or watch any particular packet, you can press the red button below the menu bar.

Apply the filter by the name 'http.' After the filter is applied, the screen will look as:

The above screen is blank, i.e.; there is no network traffic as of now.

Open the browser. In this example, we have opened the 'Internet Explorer.' You can choose any browser.

As soon as we open the browser, and type any address of the website, the traffic will start showing, and exchange of the packets will also start. The image for this is shown below:

The above process explained is called as packet sniffing.

Questions for Viva:

1. Define Exfiltration.

2. What is exploit in network security?

3. What do you mean by penetration testing?

4. Explain TCP three way handshake.

Gangamai College of Engineering, Nagaon, Dhule
Department of Computer Engineering

Name :_________________________________

Date of Performance: _ _/_ _/20_ _

Class : B.E. Computer

Date of Completion : _ _/_ _/20_ _

Div :____________ **Batch**: ___________

Grade :_________

Subject : Cyber Security Lab

Sign. of Teacher

Experiment No-8

Aim: Study of Forensics Tools in Kali Linux.

Forensic image tools:

ddrescue It copies data from one file or block device (hard disc, cdrom, etc.) to another, trying to rescue the good parts first in case of read errors.

The basic operation of ddrescue is fully automatic. That is, you don't have to wait for an error, stop the program, restart it from a new position, etc.

If you use the mapfile feature of ddrescue, the data is rescued very efficiently (only the needed blocks are read). Also, you can interrupt the rescue at any time and resume itlater at the same point. The mapfile is an essential part of ddrescue's effectiveness.

Linux system with GNU ddrescue (gddrescue on Ubuntu), the drive you are rescuing, and a device with an empty partition at least 1.5 times as large as the partition you are rescuing, so you have plenty of headroom. Run out of room, even if it’s just a few bytes,GNU ddrescue will fail at the very end.

There are a couple of ways to set this up. One way is to mount the sick drive on your Linux system, which is easy if it’s an optical disk or USB device. For SATA and SDDdrives, USB adapters are inexpensive and easy to use. I prefer bringing the sick device to my good reliable Linux system and not hassling with bootloaders and strange hardware. I keep a spare SATA drive in a portable USB enclosure for storing the rescued data.

Another way is to boot up the system that hosts the dying drive with your SystemRescueCD (or whatever rescue distro you prefer), and connect your rescue storage drive.

Identify Drive Names:

As of two 1.8TB drives. One has the root filesystem and my home directory, and theother is an extra data storage drive. lsblk accurately identifies the Compact Flash drive, an SD card, and the optical drive (sr0, iHAS424 identifies a Lite-On optical drive).If this doesn’t help you identify your drives then try findmnt:

```
$ findmnt -D

SOURCE    FSTYPE    SIZE      USED      AVAIL     USE% TARGET
udev      devtmpfs  7.7G      0         7.7G      0%   /dev
tmpfs     tmpfs     1.5G      9.6M      1.5G      1%   /run
/dev/sda3 ext4      36.6G     12.2G     22.4G     33%  /

tmpfs     tmpfs     5M        4K        5M        0%
     /run/lock
tmpfs     tmpfs     7.7G      0         7.7G      0%
     /sys/fs/cgroup
/dev/sda4 ext2      18.3G     46M       17.4G     0%   /tmp
/dev/sda2 ext2      939M      119.1M    772.2M    13%  /boot

/dev/sda6 ext4      1.8T      505.4G    1.2T      28%  /home
tmpfs     tmpfs     1.5G      44K       1.5G      0%
     /run/user/1000
gvfsd-fuse   fuse.gvfsd-fuse 0         0         0         -
/run/user/1000/gvfs
/dev/sdd1 vfat      14.6G     8K        14.6G     0%
/media/carla/100MB
/dev/sdc1 vfat      243.8M    40K       243.7M    0%
/media/carla/50MB
/dev/sdb4 ext4      1.8T      874G      859.3G    48%
/media/carla/8c670f2e-

     dae3-4594-9063-07e2b36e609e
```

This shows that /dev/sda3 is my root filesystem, and everything in /media is external to my root filesystem.

/media/carla/100MB2 and /media/carla/50MB have labels instead of UUIDs like /media/carla/8c670f2e-dae3-4594-9063-07e2b36e609e because I always give my USB sticks descriptive filesystem labels. You can do this for any filesystem, for example I could label the root filesystem this way:

```
$ sudo e2label /dev/sda3 rootdonthurtmeplz
```

The easy way is to use GParted; unmount the filesystem and then you can apply or change the label without having to look up the command for each filesystem.

Basic Rescue

The first command copies as much as possible, without retries. The second command goes over the damaged filesystem again, and makes three retries to copy everything. The logfile is on the root filesystem, which I think is a better place than the removable media,

```
$ sudo ddrescue -f --no-split /dev/sdb1 /dev/sdc1 logfile

$ sudo ddrescue -f -r3 /dev/sdb1 /dev/sdc1 logfile
```

To copy an entire drive use just the drive name, for example /dev/sdb and don't specify a partition.

If you have any damaged files that ddrescue could not completely recover you'll need other tools to try to recover them, such as Testdisk, Photorec, Foremost, or Scalpel. The Arch Linux wiki has a nice overview of file recovery tools.

PDF Forensics Tools:

pdf-parser pdf-parser is a tool that parses a PDF document to identify the fundamental elements used in the analyzed pdf file. Generally, this is used for pdf files that you suspect has a script embedded in it.

pdf-parser -o 10 filepath where "-o" is the number of objects.

pdf-parser – Parses PDF files to identify fundamental element

```
root@kali:~# pdf-parser -h

Usage: pdf-parser [options] pdf-file|zip-file|url

pdf-parser, use it to parse a PDF document


Options:
--version                 show program's version number and exit
-h, --help                show this help message and exit
-s SEARCH, --search=SEARCH

                          string to search in indirect objects
                          (except streams)
-f, --filter             pass stream object through
                         filters(FlateDecode,
                          ASCIIHexDecode, ASCII85Decode, LZWDecode
                          And RunLengthDecode only)

-o OBJECT, --object=OBJECT

                          id of indirect object to select (version
independent)

-r REFERENCE, --reference=REFERENCE

                          id of indirect object being referenced
                          (version independent)
-e ELEMENTS, --elements=ELEMENTS

                          type of elements to select (cxtsi)

-w, --raw                 raw output for data and filters

-a, --stats               display stats for pdf document

-t TYPE, --type=TYPE      type of indirect object to select
```

```
-v, --verbose            display malformed PDF elements

-x EXTRACT, --extract=EXTRACT

                         filename to extract malformed content to


-H, --hash               display hash of objects

-n, --nocanonicalizedoutput
                         do not canonicalize the output

-d DUMP, --dump=DUMP     filename to dump stream content to

-D, --debug              display debug info

-c, --content            display the content for objects
without streams

or

                         with streams without filters


--searchstream=SEARCHSTREAM


                         string to search in streams

--unfiltered             search in unfiltered streams

--casesensitive          case sensitive search in streams

--regex                  use regex to search in streams
```

Questions for Viva:

1. List out some of the common cyber attack.
2. How to protect email message?
3. Define forward security.
4. Explain the concept of cross site scripting.