Shram Sadhana Bombay Trust's
COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI POST BOX NO. 94, JALGAON – 425001. (M.S.)
Included under section 2 (f) & 12 (B) of the UGC Act, 1956
ISO 9001: 2008 certified
Phone No. (0257) 2258393, Fax No. (0257) 2258392
Website- www.sscoetjalgaon.ac.in
Email: sscoetjal@gmail.com

ISO 9001:2008

DEPARTMENT OF COMPUTER ENGINEERING

Laboratory Manual

Class: B.E. Computer

Subject: Cyber Security Lab

Academic Year: 2023-24 **Semester: VIII**

DEPARTMENT OF COMPUTER ENGINEERING

Vision of the Department

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

Mission of the Department

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

DEPARTMENT OF COMPUTER ENGINEERING

Program Educational Objectives (PEOs)

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 industries as 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.

DEPARTMENT OF COMPUTER ENGINEERING

Program Outcomes (POs)

Engineering Graduates will be able to:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change

DEPARTMENT OF COMPUTER ENGINEERING

Program Specific Outcomes (PSOs)

Computer Engineering Graduates will be able to:

1. **Software Systems Development:** Apply the theoretical concepts of computer engineering and practical knowledge in analysis, design and development of software systems.

2. **Open Source Software:** Demonstrate familiarity and practical competence with a broad range of programming languages and open source platforms.

3. **Computer Proficiency:** Exhibit proficiency through latest technologies in demonstrating the ability for work efficacy to the industry &society.

DEPARTMENT OF COMPUTER ENGINEERING

Course Objectives for Cyber Security Lab

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

Course Outcomes (CO) for Cyber Security Lab

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

DEPARTMENT OF COMPUTER ENGINEERING

Cyber Security Lab

Mapping of CO to PO

CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
To describe Information Technology Act of India		2	3	3		3	3	3				3
Describe Cyber Security	3	2	3	3	3	3	3	3				3
Demonstrate Offensive Cyber Security Tools	3	2	3	3	3	3	3	3				3
Demonstrate Defensive Cyber Security Tools	1	1	1	1		3	3	3				3
Demonstrate Security Testing Tools for Web Applications	3	2	3	3	3	3	3	3				3
Average	2.5	1.8	2.6	2.6	3	3	3	3				3

Mapping of CO to PSO

CO	PSO 1	PSO 2	PSO 3
To describe Information Technology Act of India	3		
Describe Cyber Security	3	3	3
Demonstrate Offensive Cyber Security Tools	3	3	3
Demonstrate Defensive Cyber Security Tools	3	2	2
Demonstrate Security Testing Tools for Web Applications	3	3	3
Average	3	2.75	2.75

DEPARTMENT OF COMPUTER ENGINEERING

Cyber Security Lab

List of Experiments

Experiment No.	Title of Experiment
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 sniffing and spoofing tools in Kali Linux
8	Study of forensics tools in Kali Linux
9	Study of reporting tools in Kali Linux

Cyber Security Lab

Guidelines: Students should prepare web pages (computer typed document) for following Lab experiments in their own English language based on their understanding of the topics.

EXPERIMENT NUMBER – 1

Aim: Study of Information Technology Act – Indian Perspective.

References:

1. Section 65 to Section 78, CHAPTER XI, OFFENCES, Page Number 25 - 31
   https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf

2. Acts/Rules/Regulations
   https://www.cert-in.org.in/
   a. Information Technology Act 2000, Section 65 to Section 78, CHAPTER XI, OFFENCES, Page Number 19 - 21
      https://www.cert-in.org.in/PDF/itbill2000.pdf

   b. Information Technology (Amendment) Act 2008, Section 65 to Section 78, Page Number 9 - 15
      https://www.cert-in.org.in/PDF/it_amendment_act2008.pdf

Description: Write Section 65 to Section 78 with description of the offence and its penalties as per Information Technology Act 2000. Write only the amendments of respective sections as per Information Technology (Amendment) Act 2008.

EXPERIMENT NUMBER – 2

Aim: Study of recent Cyber Incidents / Vulnerability.

References:

1. Latest Security Alerts, Virus Alerts in the Home Page
   https://www.cert-in.org.in/
2. VULNERABILITY NOTES (Vulnerability Notes of the year 2021, 2020, 2019)
   https://www.cert-in.org.in/
3. Reporting of Security Incident and Vulnerability
   https://www.cert-in.org.in/
4. National Cyber Crime Reporting Portal
   https://cybercrime.gov.in/

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.

EXPERIMENT NUMBER – 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
```

References:

1. https://diarium.usal.es/pmgallardo/2020/10/16/hping3-syntax/
2. https://www.youtube.com/watch?v=lFpDnPGXNwk
3. https://www.youtube.com/watch?v=WigO82OO9jM
4. https://www.tutorialspoint.com/kali_linux/index.htm

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 sscoetjalgaon.ac.in
```

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 the TCP three-way 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

References:

1. https://tools.kali.org/information-gathering/dnsenum
2. https://www.youtube.com/watch?v=mCbz92LdEfY
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 their key 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

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

References:

1. https://tools.kali.org/information-gathering/p0f
2. https://www.youtube.com/watch?v=t6SWtnfYqQg
3. https://www.tutorialspoint.com/kali_linux/index.htm

EXPERIMENT NUMBER – 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

References:

1. https://tools.kali.org/vulnerability-analysis/bed
2. https://www.youtube.com/watch?v=2Q4QJYMZptc
3. https://www.youtube.com/watch?v=WDtaRfpKJ-s
4. https://www.tutorialspoint.com/kali_linux/index.htm

EXPERIMENT NUMBER – 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**.

In this case, the proxy IP will be 127.0.0.1 with port 8080.

Then configure the browser proxy which is the IP of burpsuite machine and the port.

To start interception, in Burpsuite go to Proxy → Intercept → click "Intercept is on".

Continue to navigate on the webpage that you want to find the parameter to test for vulnerabilities.

In Burpsuite, Go to "HTTP History". The line marked in red arrow shows the last request. In Raw and the hidden parameter such as the Session ID and other parameter such as user name and password has been underlined in red.

References:

1. https://portswigger.net/burp/documentation/desktop/getting-started/proxy-setup/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

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.

References:

1. https://www.zaproxy.org/getting-started/
2. https://www.youtube.com/watch?v=2kaha1J-cQo
3. https://www.tutorialspoint.com/kali_linux/index.htm

EXPERIMENT NUMBER – 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/

References:

1. https://tools.kali.org/vulnerability-analysis/sqlmap
2. https://sqlmap.org/
3. https://www.youtube.com/watch?v=QsMkQMKsIII
4. https://www.tutorialspoint.com/kali_linux/index.htm

EXPERIMENT NUMBER – 7

Aim: Study of Sniffing and Spoofing Tools in Kali Linux

wireshark

Wireshark analyzes deeply the packets in frame level. In Kali, it is found using the following path - Applications → Sniffing & Spoofing → wireshark.
Under Capture menu, Click "Start" and the packet capturing will start

References:

1. https://tools.kali.org/information-gathering/wireshark
2. https://www.youtube.com/watch?v=TkCSr30UojM
3. https://www.youtube.com/watch?v=-rSqbgI7oZM
4. https://en.wikipedia.org/wiki/Wireshark
5. https://www.tutorialspoint.com/kali_linux/index.htm

EXPERIMENT NUMBER – 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 it later at the same point. The mapfile is an essential part of ddrescue's effectiveness.

dd_rescue infilepath outfilepath

References:

1. https://www.linux.com/topic/desktop/gnu-ddrescue-best-damaged-drive-rescue/
2. https://www.tutorialspoint.com/kali_linux/kali_linux_forensics_tools.htm
3. https://www.gnu.org/software/ddrescue/manual/ddrescue_manual.html
4. https://www.youtube.com/watch?v=jwMoIuLCfLE
5. https://www.youtube.com/watch?v=ddrPnuvFV6E
6. https://www.tutorialspoint.com/kali_linux/index.htm

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.

References:

1. https://tools.kali.org/forensics/pdf-parser
2. https://www.youtube.com/watch?v=E0oxxJn7sLM
3. https://www.youtube.com/watch?v=ywyFJ_jAqyE
4. https://www.tutorialspoint.com/kali_linux/index.htm

EXPERIMENT NUMBER – 9

Aim: Study of Reporting Tools in Kali Linux

Dradis framework

Step 1 − To start Dradis, type **"service dradis start"**.in terminal

Step 2 − To open, go to Applications → Reporting Tools → dradis.

The web URL will open. Anybody in LAN can open it in the following URL **https://IP of kali machine:3004** (check the port number)

Log in with the username and password that was used for the first time.

Step 3 − After logging in, you can import files from NMAP, NESSUS, NEXPOSE. To do so, go to "Import from file" → click "new importer(with real-time feedback)".

Step 4 − Select the file type that you want to upload. In this case, it is "Nessus scan" → click "Browse".

If you go to the home page now, on the left panel you will see that the imported scans have are in a folder with their host and port details.

References:

1. https://tools.kali.org/reporting-tools/dradis
2. https://dradisframework.com/ce/documentation/
3. https://www.youtube.com/watch?v=LANOeTvYtaY
4. https://www.youtube.com/watch?v=fA3ky-JV9EE
5. https://www.tutorialspoint.com/kali_linux/index.htm