



(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Department of Computer Science and Engineering (Cyber Security)

CYBER FORGE 2.0

Date: 12th February 2026

DAYANANDA SAGAR UNIVERSITY

CYSEC 26

**Powered by
CySec
Club**

CYBER FORGE 2.0

Understand Attacks to Build
Effective Defenses

THINGS TO LEARN

- Creation of controlled malware samples
- SQL injection vulnerabilities
- Legacy system (Windows XP) security analysis
- Access gaining techniques in ethical hacking

Venue & Timings
Lecture Hall - 3
12th February 2026
8:30 AM to 10:20 AM

Note
Virtual box with Windows XP and Kali Linux
Bring your laptop to follow along in the hands-on segment!

Resource person

PROF. JOSHE RAJ
Assistant professor
Computer Science and Engineering
(Cyber Security)

Convenors
Dr. Udaya Kumar Reddy K R
Dean, School of Engineering
Dr. Dilip Kumar J. B. Saini
Chairman, CSE(Cyber Security)

Organizers
Prof. Ranjima P
Prof. Joshe Raj
Assistant professor
CSE (Cyber Security)

Tutorial for Installation of requirements

Windows XP
Kali Linux

Organized By:

Dept. of Computer Science Engineering

(Cyber Security),

School Of Engineering,

DAYANANDA SAGAR UNIVERSITY



(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Department of Computer Science and Engineering (Cyber Security)

OBJECTIVE

To introduce the fundamental concepts of ethical hacking and penetration testing. The session aimed to provide a practical understanding of reconnaissance, vulnerability identification, network scanning, SQL injection basics, and gaining system access in a controlled environment. It also focused on understanding attacker mindset, networking fundamentals, and commonly used cybersecurity tools.

EVENT SUMMARY

Cyber Forge 2.0 began at 8:55 AM and was conducted by Mr. Joshe Raj, the resource person for the event. He introduced the fundamentals of ethical hacking and emphasized the importance of thinking like an attacker to identify system vulnerabilities. The session covered the phases of penetration testing, starting with reconnaissance techniques such as Google dorking to uncover publicly exposed information. Basic SQL injection concepts were explained to demonstrate how login pages can be tested for weaknesses.

The practical segment included SSH configuration, use of Linux networking commands, and network scanning using Nmap to identify open ports and services. Mr. Joshe Raj also discussed brute force attack concepts, CVE databases for vulnerability identification, and introduced the Metasploit framework to explain payloads and system access within a controlled environment. The session concluded with an overview of TCP networking fundamentals and the importance of securing systems against potential exploits.

KEY HIGHLIGHTS

- Introduction to the phases of penetration testing, with emphasis on reconnaissance and understanding attacker mindset.
- Demonstration of Google Dorking techniques and basic SQL Injection concepts used to identify exposed login pages and databases.
- Practical exposure to network scanning using Nmap, including port scanning and service detection.
- Overview of SSH configuration and remote access concepts in a controlled Linux environment.
- Introduction to vulnerability identification through CVE databases and payload concepts using the Metasploit framework.



(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Department of Computer Science and Engineering (Cyber Security)

PHOTO GALLERY





DAYANANDA SAGAR
UNIVERSITY

SCHOOL OF ENGINEERING



SCHOOL OF
ENGINEERING

(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Department of Computer Science and Engineering (Cyber Security)





(A State Private University under the Karnataka Act No. 20 of 2013)

Approved by UGC & AICTE, New Delhi, Accredited by NAAC with A+ grade

Department of Computer Science and Engineering (Cyber Security)

