FACULTY OF COMPUTER APPLICATIONS

MASTER OF SCIENCE – CYBER SECURITY AND CYBER LAW

- **Sem.** : 1
- **Subject Code** : 05CS3105
- **Subject** : Shell Scripting
- **Course Objectives** :

1. Understand command-line fundamentals and bash scripting.
2. Apply bash for cybersecurity operations.
3. Perform data collection and log analysis.
4. Use CLI tools for penetration testing.
5. Develop automation scripts.

- **Prerequisites**: Using Windows OS, Cyber Security Fundamentals, Internet, HTML

Unit No	Topics Covered	No of lectures required
1	Command-Line and Bash foundation Command Line Basics, Running Linux and bash on Windows, Output, Input, Variables, Conditionals, Looping, Functions, Pattern matching in bash, Script to detect OS type	**06**
2	Regular Expressions grep, egrep, Regular Expression Meta characters, Grouping, Brackets and Character Classes, Back References, Quantifiers, Anchors and Word Boundaries	**06**

FACULTY OF COMPUTER APPLICATIONS

MASTER OF SCIENCE – CYBER SECURITY AND CYBER LAW

3	Defensive Security Operations with bash Data Collection Commands (cut, file, head, reg, wevtutil), Gathering System Information, Searching the File System, Transferring Data Data Processing Commands (awk, join, sed, tail, tr), Processing Delimited files, Processing XML, Processing JSON, Aggregating Data Data Analysis Commands (sort, uniq), Web Server Access Log Familiarization, Sorting and Arranging Data, Counting Occurrences in Data, Totaling Numbers in Data, Displaying Data in a Histogram, Finding Uniqueness in Data, Identifying Anomalies in Data	**06**
4	Monitoring Real-Time Log Monitoring Monitoring Test Logs, Monitoring Windows Log, Generating Real-Time Histogram Network Monitoring Commands (crontab, schtasks), create a Port Scanner, Compare to Previous Output, Automation and Notification File System Monitoring Commands (sdiff), Baseline the File System, Detect changes in Baseline, Automation and Notification	**06**
5	Offensive Security & Penetration Testing : Bash for penetration testing, scripting obfuscation techniques, command line fuzzing, remote access tools and techniques, privilege escalation basics	**06**

Course Outcomes :

CO1: Explain CLI and bash scripting fundamentals.

CO2: Apply bash commands for system analysis.

CO3: Analyze cybersecurity incidents.

FACULTY OF COMPUTER APPLICATIONS

MASTER OF SCIENCE – CYBER SECURITY AND CYBER LAW

CO4: Develop automation scripts.

CO5: Evaluate security techniques

Text Book :

1. **Cybersecurity Ops with bash – Attack, Defend and Analyze from the Command Line, Paul Troncone & Carl Albing, O'REILLY , First Edition**

Reference Books :

1. **Linux Command Line and Shell Scripting Bible, Richard Blum & Chistine Bresnahan , Wiley, Fourth Edition**
2. **Mastering Linux Shell Scripting, Mokhtar Ebrahim & Andrew Mallett, Packt>, Second Edition**
3. **Bash Cookbook, Carl Albing & JP Vossen, O'reilly, Second Edition**

Web References:

1. **https://tutorials.cyberaces.org**
2. **https://javatpoint.com/bashs**

App References:

1. **Learn Bash commands – Bash by example**
2. **Advanced Bash Scripting Guide**

Syllabus Coverage from text /reference book & web/app reference:

Unit #	Chapter Numbers
1	Chapter 1, 2
2	Chapter 3
3	Chapter 5, 6, 7
4	Chapter 8, 9, 10
5	Chapter 13,14,15