

CTMSDFIS SI P4: Python and Scripting

Teaching Scheme					Evaluation Scheme									
Th	Tu	Pr	C	TCH	Theory					Practical				Total
					Internal Exams				University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs		
					Marks	Hrs	Marks	Hrs						
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To learn the concept of scripting for cyber security
2. To Learn Python basics for scripting
3. To Learn PowerShell scripting for information security concept
4. To learn Bash Scripting for cyber security related task
5. To Learn the concept related secure development and threat hunting

UNIT – I

Scripting Part 1

What Is "The Shell", Understanding the File System Tree and its Navigation, Exploring the System, Manipulating Files and Directories, Manipulating Files and Directories, I/O Redirection, Expansion, Permissions, Job Control, Configuration and The Environment, Introduction To vi, Customizing the Prompt

UNIT – II

Scripting Part 2

Package Management, Storage Media, Networking, Searching for Files, Archiving and Backup, Regular Expressions, Text Processing, Formatting Output, Printing, Compiling Programs. Writing Shell Scripts: Starting A Project, Top-Down Design, Flow Control: Branching With if, Reading Keyboard Input, Flow Control: Looping With while / until & for, Troubleshooting, Strings and Numbers, Arrays

UNIT – III

Basic Python Scripting

Python Setup, Debugging, Variables, String, Lists, Dictionaries, Networking, Selection, Function, Iteration, Classes and Objects (OOP), Inheritance and Composition, Comments and Pound Character, Numbers and Math, Variables and Names, Conditional statements

UNIT – III

Advance Python Scripting

Exception Handling File I/O, Sys Module, OS Module, Long-Tail/Short-Tail Analysis,

Geolocation Acquisition, Blacklists and Whitelists, Packet Analysis, Packet Reassembly, Payload Extraction. **Forensic Python:** Acquiring Images from Disk, Image Forensics and PIL, SQL Queries, HTTP Communications with Python Built in Libraries, Web Communications with the Requests Module.

UNIT – V

PowerShell Essential and Scripting

Overview PowerShell, Environment Setup, PowerShell Integrated Script Environment (ISE), Working with PowerShell scripts, cmdlets, files and folders, dates and timers, file I/O, Advanced Cmdlets, PowerShell Scripting: special variables, operators, looping, conditions, array, hash tables, regex, blackets, alias, WMIC & PowerShell. PowerShell providers and drives, \$Args variable, param statement, Passing data by value and by reference, PowerShell Advance Functions, Using PowerShell remoting capabilities: emoting concepts Invoking remote commands, processing output, Objects in Windows PowerShell: Error handling concepts, terminating and non-terminating errors, Handling errors using \$?, \$Error and \$lastExitCode variables, Error Record object anatomy, Working with textual files : Saving information into textual and csv files, Reading information from textual and csv files, Example implementation of error handling code.

Reference book

1. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers by TJ O' Connor (Author)
2. Shell Scripting: How to Automate Command Line Tasks Using Bash Scripting and Shell Programming by Jason Cannon
3. Mastering PowerShell Scripting - Fourth Edition: Automate and manage your environment using PowerShell by Chris Dent