ETHICAL HACKING AND DIGITAL FORENSIC TOOLS LAB

Course code: 13CS2216	**L**	**P**	**C**
	0	**3**	**2**

Pre requisites : Information Security.

Course Educational Objectives:
The main objective this practical session is that students will get the exposure to various forensic tools and scripting languages.

Course Outcomes:
By the completion of this laboratory session Student

1. Will get the practical exposure to forensic tools.
2. Will gain the knowledge on perl and Unix scripting languages to implement various security attacks.
3. Will get the ideas in various ways to trace an attacker.

The following programs should be implemented preferably on platform Windows/Unix through perl, shell scripting language and other standard utilities available with UNIX systems. :-

Part A :

1. Write a perl script to concatenate ten messages and transmit to remote server
   a) Using arrays
   b) Without using arrays.
2. Write a perl script to implement following functions:
   a) Stack functions
   b) File functions
   c) File text functions
   d) Directory functions
   e) Shift, unshift, Splice functions.
3. Write a Perl script to secure windows operating systems and web browser by disabling Hardware and software units.
4. Write a perl script to implement Mail bombing and trace the hacker.
5. Write a shell script to crack UNIX login passwords and trace it when breaking is happened.

6. Write a shell script to send fake mails to the remote servers or web browsers.
7. Write a shell script to crack windows login password and trace it who is the attacker.
8. Write a shell script to implement buffer overflow attacks.
9. Write a shell script to implement formal string Vulnerabilities.
10. Write a shell script to trace an attacker how he is connected to various servers URL's and various processes and services ? (Note: Use Santoku O.S)
11. Write a perl script to handle Bluetooth attacks.
12. Write a perl script to implement Web Data Extractor and Web site watcher
13. Test the Vulnerabilities Using Security Scanner through following packages support
    (a) Zlib (b) libcap (c) MYSQL (d) Apache software products (e) PHP (f) Snort.
14. Test and Show the functionality of secure database through the support of packages
    (a) JPGraph (b) ADOdb (c) ACID

Part B: Exposure on Forensic tools.

1. Backup the images file from RAM using Helix3pro tool and show the analysis.
2. Introduction to Santhoku Linux operating system and features extraction.
3. Using Santoku operating system generates the analysis document for any attacked file from by taking backup image from RAM.
4. Using Santoku operating system generates the attacker injected viewing java files.
5. Using Santoku operating system shows how attackers opened various Firefox URL's and pdf document JavaScript files and show the analysis.
6. Using Santoku operating System files show how an attacker connected to the various network inodes by the specific process.
7. Using exiftool (-k) generate the any picture hardware and software.
8. Using deft_6.1 tool recover the attacker browsing data from any computer.

9. Using Courier tool Extract a hacker secret bitmap image hidden data.
10. Using sg (Stegnography) cyber Forensic tool hide a message in a document or any file.
11. Using sg cyber Forensic tool unhide a message in a document or any file.
12. Using Helix3pro tool show how to extract deleted data file from hard disk or usb device.
13. Using Ghostnet tool hide a message into a picture or any image file.
14. Using kgbkey logger tool record or generate an document what a user working on system
15. Using pinpoint metaviewr tool extract a metadata from system or from image file.
16. Using Bulk Extractor tool extract information from windows file system.