SEMESTER-V

COURSE 14: CYBER SECURITY

Theory Credits: 3 3 hrs/week

Course Objectives:

The aim of this course is to help the learner to understand key terms and concepts in cyber security. The Learner will learn to secure clean and corrupted systems, protect personal data, and secure computer networks. The Learner will be able to examine secure software development practices and gain an understanding of cryptography, how it has evolved, and some key encryption techniques used today.

Learning Outcomes:

The students will be able to:

Analyze and evaluate the cyber security needs of an organization. Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation. Measure the performance and troubleshoot cyber security systems. Implement cyber security solutions and use of cyber security, information assurance, and cyber / computer forensics software/tools. The Learner will develop an understanding of security policies (such as confidentiality, integrity, and availability) and protocols to implement such policies and will gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.

Unit 1: Cyber Security Fundamentals: Network Security Concepts: Information Assurance Fundamentals, Basics of Cryptography: Symmetric and Asymmetric, DNS, Firewalls, Virtualization, Radio-Frequency Identification Microsoft Windows Security Principles: Windows Tokens, Window Messaging, Windows Program Execution, Windows Firewall

Case Study: Install any Virtualization Software and perform various tasks

Unit 2: Attacker techniques and motivations: Anti forensics, Tunneling Techniques, Fraud Techniques, and Threat Infrastructure

Case Study: Working with Free and commercial proxies available from web-hack.ru.

Unit 3: Exploitation: Techniques to gain a Foothold, Misdirection, Reconnaissanse, and Disruption Methods

Case Study: Working with SQL Injection attacks and DDoS attacks

Unit 4: Malicious Code: Self-Replicating Malicious Code, Evading Detection and Elevating Privileges, Stealing Information and Exploitation.

Case Study: Identify latest Malwares and differentiate different types of malwares

Unit 5: Defense and Analysis Techniques: Memory Forensics, Honeypots, Malicious Code Naming, Automated Malicious Code Analysis Systems, Intrusion Detection Systems

Case Study: Identify latest Anti-Virus Softwares in the market and compare the functionality of each Anti-Virus

Text Books:

1. Cyber Security Essentials by James Graham, Richard Howard, Ryan Olson, CRC Press
2. Introduction to Cyber Security by Jeetendra Pandey
3. Cryptography and Network Security by William Stallings

References:

Cyber Security for Beginners by Heimdal® Security - Proactive Cyber Security Software (heimdalsecurity.com)

SEMESTER-V

COURSE 14: CYBER SECURITY

Practical Credits: 1 2 hrs/week

Assignment 1:

1. What is the command used for finding host/domain name and IP address?
2. What is the command will display the assigned IP address of ETHERNET adapter?
3. What is the command used for checking the network connectivity?
4. What is the command used for finding all the ip addresses of a given domain name?
5. What is the command used for finding connection to and from the host?
6. What is the command used to view user information, user's login name, real name terminal name and write status ?
7. What is the command used for mapping name to IP addresses?
8. What is the command used for connecting to a host on a particular port?
9. What is the command used to make a connection to a remote machine and execute programs as if one were physically present ?
10. What are the text based web browsers available through command line?

Assignment 2:

1. What is the command used for downloading a website for off-line view ?
2. What is the command used for displaying or manipulating the ARP (Address Resolution Protocol) information on a network device or computer. ?
3. What is the command used for checking/starting/stopping networking services, users, messaging, configuration and so on...?
4. What is the command a packet filtering configuration program used for manipulating net filter kernel based firewall?
5. What is the command used for showing network statistics?
6. What is the command used for displaying and manipulating routing table ?
7. What is the command used to monitor access control for supported services ?
8. What is the command used to view network traffic?
9. What is the command used to change your hostname ?
10. What is the command used for an interface IP address ?

Assignment 3:

1. What is the command used for controls access to daemons at the application level, rather than at the IP level?

2. What is the command used for connecting to a host with encryption?

3. In what is the file, we can find the local look up server used by the browser. 4. Command used to find out the intermediate nodes between the host and the server is.

5. What is the command used to find out the intermediate domain name nodes between the host and the server?
6. Command used to follow all the information a DNS server has about a particular domain
7. The command get documents/files from or send documents to a server
8. How to check if a particular interface is up and running?
9. This command used to list info about machines that respond to SMB name queries (for example windows based machines sharing their hard disks).
10. This command used to look up the contact information from the "who is" databases, the servers are only likely to hold major sites. Note that contact information is likely to be hidden or restricted as it is often abused by crackers and others looking for a way to cause malicious damage to organizations.
11. It allows you to send and receive files between two computers.
12. Another part of the ssh package. This command similar to ftp but uses an encrypted tunnel to connect to an ftp server and is therefore more secure than just plain ftp.
13. Part of the ssh package. Allows you to copy files from one computer to another computer.
14. nfs - nfsfstab format and options
15. where to look to find out the services What is the are available to the system .
16.where to look to find out the list of protocols What is the are available to the system along with their port numbers .
17. To listing the iptables of your linux system.
18. How to know if a service is running or not.
19. How to Enable IP Forwarding in Linux

Assignment 4:

1. Study of Wireshark Manual.

Assignment 5 :

Perform the following using Wireshark

1. Identify the first 2 packets (i.e. their packet numbers) containing HTTP GET request.
2. What webpage was visited in the above 2 packets?
3. What version of HTTP was used?
4. What is the destination IP address in the above packets?
5. List the source and destination ports of the packets travelling from the client to this server in the above packets?
6. In the HTTP server's response, look at the information sent about the server. What server software was used?
7. What are the IP addresses of the server?

Assignment 6:

Perform the following using Wireshark.

1. What are the MAC addresses of the client and server?
2. How many WebPages (not websites) have been opened?
3. What is the time difference between first HTTP GET and the first HTTP response (OK)?
4. Count the total number of HTTP GET requests.
5. What is the time difference between the first and last HTTP GET requests? Hint: Follow a similar procedure as mentioned previously.
6. How may packets were exchanged between the server (corresponding to the both IP addresses) and the client?

(Note: Their sum must be equal to the total no. of packets)

7. Find the total no. of HTTP requests sent by the host spongebob.wikia.com.

Assignment 7:

1. SQL Injection Implementation and Execution.

Assignment 8:

1. Give a short note on OSSEC?
2. What are the components of OSSEC
3. List the few key features of OSSEC.
4. What are the types of agent in OSSEC?
5. What are the roles of Manager (server) and an Agent in OSSEC?
6. What is Syscheck in OSSEC?
7. What is LIDS and HIDS?

Assignment 9:

1. What is the type of log used by pflogsumm?
2. What is the type of log used by webalizer?
3. What are the different types of logs used by AWStats?
4. Pflogsumm analyzes is a mail/weblog or both?
5. Webalizer analyzes is a mail/weblog or both?
6. Command line option used for increment log analysis, mention domain name and squid log file with webalizer.
7. AWStats tools written in What is the language?

Assignment 10:

1. Steps for setting up Cyber Security in organization.

References for All Assignments:

1. http://www.ossec.net/
2. www.linuxmanpages.com/man1/pflogsumm.1.php
3. www.webalizer.org/
4. http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/