INT242:CYBER SECURITY ESSENTIALS

L:2 T:0 P:2 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: illustrate the concept of information security, threats and vulnerabilities

CO2 :: define the basic concept of cryptography and authentication control

CO3 :: discuss the security appliances and protocols to secure the networks

CO4 :: analyze how to secure the mobile system and application concept

CO5 :: examine the procedures for incident response, cyber security and physical security

CO6 :: apply the port scanning, socket creation and web crawling using python programming

Unit I

Security roles and security controls : information security roles, security control and framework types, threat actor types and attack Vectors, Threat Intelligence Sources.

Performing security assessments : assess organizational security with network reconnaissance tools, security concerns with general vulnerability types, vulnerability scanning techniques, penetration testing concepts

Social engineering and malware : social engineering techniques, indicators of malware-based attacks

Unit II

Basic cryptographic concepts : cryptographic ciphers, cryptographic modes of operation, summarize cryptographic use cases and weaknesses, cryptographic technologies, digital certificates and certificate authorities, PKI management

Authentication controls : authentication design concepts, knowledge-based authentication, authentication technologies, biometrics authentication concepts

Unit III

Secure network designs and protocols : secure network designs, secure switching and routing, secure wireless infrastructure, load balancers, network operations protocols, application protocols, remote access protocols

Network security appliances : firewalls and proxy servers, network security monitoring, use of SIEM

Unit IV

Secure mobile solutions : mobile device management, secure mobile device connections

Secure application concepts : indicators of application attacks, indicators of web application attacks, secure coding practices, secure script environments, deployment and automation concepts

Data privacy and protection concepts : privacy and data sensitivity concepts, privacy and data protection controls

Unit V

Incident response : incident response procedures, utilize appropriate data sources for incident response, apply mitigation controls

Cyber security Resilience : redundancy strategies, implement backup strategies, cyber security resiliency strategies, physical site security controls, physical host security controls

Unit VI

Network security programming with python : introduction to python and working on linux, windows, raw socket basics, socket libraries and functionality, programming server and clients, port scanner program in python, identifying live host over a network using python, creating backdoor using python, web crawler program in python, wireless packet sniffer in python

List of Practicals / Experiments:

Setup virtual environment

- Installation of Virtual Workstation (VMware/VirtualBox), Installing a guest OS

Performing basic network commands

- ping, ifconfig,ipconfig, route, netstat,nslookup,tracert/traceroute/pathping,arp, mtr

Performing Reconnaissance and Discovery Tools

- Open Source Intelligence (OSINT) information gathering, theHarvester,shodan

Identifying Port Scanning Threats

- port scanning, service discovery, version detection using nmap and Advanced IP scanner

Conducting Security Analysis

- Use of Netcat for establish connection with remote machines, backdoor, port scanning and fingerprinting

Capturing Network Traffic

- Capturing and monitoring network data with Wireshark

Evaluating security threats

- Social Engineering attacks using SEToolkit, password attacks using hashcat, identifying threats toDNS using nslookup

Cryptographic Ciphers

- Demonstration: RSA ciphertext generation.

Network Security

- Configuring firewall parameters in windows , iptables in linux.Configuration of ACL using Cisco Packet Tracer on routers.Divide large network into subnets by using subnetting and implement in Cisco Packet tracer.

Web Application Attack

- Sqlmap tool of linux to show the real execution of SQL injection on vulnerable website: www.testphp.vulnweb.com

Text Books:

1. INTRODUCTION TO COMPUTER NETWORKS AND CYBERSECURITY by CHWAN-HWA (JOHN) WU, J. DAVID IRWIN, CRC PRESS

References:

1. COMPTIA SECURITY+ STUDY GUIDE: EXAM SY0-601, 8TH EDITION by MIKE CHAPPLE, DAVID SEIDL, WILEY