|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Course Code:** | **Course Title: Network Security** | | | | **TPC** | **3** | **2** | **3** |
| **Version No.** | **2.0** | | | | | | | |
| **Course Pre-requisites/ Co-requisites/ anti-requisites (if any).** | **Computer Networks, Cryptography, Operating Systems, Secure Coding** | | | | | | | |
| **Objectives:** | 1. Identify computer and network security threats, classify the threats and develop a security model to prevent, detect and recover from the attacks. | | | | | | | |
| **Expected Outcome:** | On completion of the course, students will have the ability to   1. Understanding the factors driving the need for network security 2. Identify and classify particular examples of attacks 3. Define the terms vulnerability, threat and attack 4. Identify physical points of vulnerability in simple networks and systems 5. Identify attack pattern and characteristics of malicious software. | | | | | | | |
| **Module No. 1** | **Basic network security** | | **8** | | | | | |
| The OSI security architecture: A model for network security, Secure network system design, design principles, security best practices. | | | | | | | | |
| **Module No. 2** | **Web security** | | **8** | | | | | |
| Web security, Secure Socket layer, Transport layer security, and secure electronic transaction, web vulnerabilities, Introduction to XSS. | | | | | | | | |
| **Module No. 3** | **Secure VPN solutions** | | **6** | | | | | |
| Virtual Private Networks – Configuring VPNs, Tunneling, TOR, Port mapping, Network traffic analysis | | | | | | | | |
| **Module No. 4** | **Secure Email and browser solutions** | | **8** | | | | | |
| Sign-on solutions – Secure login to desktop, Inactivity Control, Secure Email implementation, browser security, Intruders, Intrusion Detection, and Password Management. | | | | | | | | |
| **Module No. 5** | **Firewall** | | | **8** | | | | |
| Malicious software programs: Viruses and related Threats, Virus Countermeasures, Firewall Design Principles, Trusted Systems | | | | | | | | |
| **Module No. 6** | **Smart Phone Security** | **6** | | | | | | |
| Attack vector: rooting and repackaging mobile apps, collusion attacks, disk encryption, Hardware protection: Trust Zone | | | | | | | | |
| **Text Books**   1. Cryptography and network Security. William Stalling, Pearson Education | | | | | | | | |
| **References**   1. Cryptography and network Security, Behrouz A Forouzan, TMH | | | | | | | | |
| **Mode of Evaluation** | **Practice Tests-20%, Continuous Assessment Tests-60%, Practical Assesment-20%**  Practice Tests - Cumulative for 16 Weeks 20%  Continuous Assessment Test-1 20%  Continuous Assessment Test-2 20%  Continuous Assessment Test-3 20%  Practical Assessment 20% | | | | | | | |
| **Recommended by the Board of Studies on** | xx-xx-xxxx | | | | | | | |
| **Date of Approval by the Academic Council** | Xxth Academic Council held on xx-xx-xxxx | | | | | | | |

**List of Laboratory Experiments**

1. Configuring and working with Real-time Intrusion detection System using SNORT.

2. Network packet and protocol analysis using Wireshark.

3. Port scanning, OS fingerprinting and network reconnaissance using Nmap.

4. Study of poisoning attacks and prevention using Ettercap

5. Hands-on Network security tools using Kali Linux.

6. Study on security certificates, SSL, TLS, HTTPS.

7. Mini project