

Course Code	Course Title	L	T	P	C
1156EC419	SECURED NETWORKED SYSTEM WITH FIREWALL AND IDS	0	0	0	2

**a) Course Category**

Independent Learning – Self Learning Course

**b) Preamble**

This course provides how network systems are secured using firewalls and IDS. This will include understanding the basic components of network security, constructing a dual-firewall DMZ, and defining security policies to implement and enforce these rules. Building upon these lessons we will go in-depth on the popular Linux firewall

**c) Prerequisite**

Nil

**d) Related Courses**

Network Security

**e) Course Outcomes**

On successful completion of this course the student will be able to

CO Nos.	Course Outcomes	Knowledge Level (Based on Revised Bloom's Taxonomy)
CO1	Explain security concepts, services and design principles	K2
CO2	Describe the data access procedures, trust and check their authentication	K2
CO3	Explain Firewall concepts, critical security policies, Enforcement procedures and design principles.	K2
CO4	Describe the procedure for implementing firewall for filtering packets, address ports and policies	K2
CO5	Explain evaluation and performance of firewall and host IDS	K2

**f) Course Content**

**UNIT I CYBER SECURITY CONCEPTS AND SECURITY PRINCIPLES**

Introduction to basic cyber security concepts, root causes of vulnerabilities in a network system - Recent cyber attack incidences and the basic security services for their defense and triage. Risk management framework in a network system, basic security design principles -protect the data and secure the computer systems

## **UNIT II      PROTECT DATA ACCESS AND VERIFY SOURCE OF TRUST**

Principles of least privileges for controlling the proper access given to users and system process. Access control by using an example using the UNIX file access mechanism. Trust -the source and authenticity of the programs and data installed in systems -Ways to check their integrity, and verify their authentication

## **UNIT III      SECURE NETWORK DEFENCE**

Firewall system with dual firewalls to protect site- critical security policies,-Enforcement procedures - security design principles for the firewall system

## **UNIT IV      IMPLEMENT FIREWALL WITH LINUX IP TABLE**

Linux IP tables to implement firewall rules for filtering packets, and SNAPT or DNAT address port-translation, and the security policies

## **UNIT V      INTRUSION DETECTION SYSTEMS**

Introduction to the Snort IDS-Evaluation and performance of network firewalls, Host IDS

### **g)    Learning Resources**

#### **Online Resources**

1. <https://www.coursera.org/learn/design-secure-networked-systems>
2. <https://www.coursera.org/learn/secure-networked-system-with-firewall-ids>