Cyber Defence Technique:
Firewalls,
Intrusion Detection System (IDS)

Instructor: Sarada Prasad Gochhayat
Office: ECSB 1310
Phone:
E-mail: sgochhay@odu.edu

Lectures: Wednesday, 7:10 pm – 9:50 pm
Textbook: Internet Security, A Hands-on Approach, Wenliang Du
Class webpage: www.blackboard.odu.edu

COURSE DESCRIPTION: We will discuss about asymmetric encryption

1) Check iptables in Linux machine all the parameters
    a) sudo iptables -h
2) Check all the list
    a) sudo iptables -L --line-numbers
3) Logging icmp packets
    a) Iptables -A INPUT -p icmp -j LOG --log-prefix “PING IDENTIFIED”
4) Add a rule to iptable:
    a) Sudo iptables -A INPUT -p icmp -j ACCEPT
    b) USE “sudo iptables -L” to check the rule added to the list
5) Store a rule to iptable:
    a) Sudo -i
    b) iptables-save > /etc/iptables.conf
6) Check the stored iptable:
    a) Gedit /etc/rc.local

b) Iptables-restore < /etc/iptables.conf

1. Installing Snort
    a. sudo apt-get install snort
2. Then, to run snort:
    a. sudo snort -c /etc/snort/snort.conf -l /var/log/snort/ -A full
3. Dependencies installation:
    a. sudo apt-get install flex bison build-essential checkinstalllibpcap-dev libnet1-dev libpcre3-dev libmysqlclient15-dev libnetfilter-queue-dev iptables-dev