# Cyber Security Workshop 2015

## "Hardening Network Security"

By

Ashish Belwase

KU SECURITY RESEARCHER

# Automatic Security Updates

- CentOS
  - *Yum install yum-cron*
  - *Vi etc/yum/yum-cron.conf*
  - *update_cmd = default <security>*
- Debian
  - https://help.ubuntu.com/community/AutomaticSecurityUpdates

# SUDO

- *belwase ALL=(ALL)ALL*
- *Strong password*

# Securing SSH

- *vi /etc/ssh/sshd_config*
- ***PermitRootLogin no*** *# This will disable root login. Note → This step is crucial.*
- ***X11Forwarding no*** *# Disable X11 Forward*
- ***AllowUsers belwase test*** *# This will allow only belwase and test users to login*
- *Port xxxx #change the default port number*
-

# Basic Firewall

- *iptables -P INPUT DROP && iptables -P FORWARD DROP && iptables -P OUTPUT DROP*
- *iptables -A INPUT/OUTPUT -i lo -j ACCEPT*
- *iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT  #enabling ssh*
- *iptables -A INPUT -p tcp --dport 80 -j ACCEPT  #Allow port 80*
- *In centos 7  :*
  - *firewall-cmd --permanent --add-service=ssh*
-

# SELINUX

- *Provides  Mandatory Access Control (MAC).*
- *Controls of an application of user to files,sockets,processes.*
- *Keep in Enforcing mode*
- *semanage port -a -t ssh_port_t -p tcp 22 # add port 22 to semanage list*
-

# LOG Analysis

- *Tools : head, tail , grep ,vi*
- *Logs : /var/logs/*
- *Syslog*
- *Messages*
- *Httpd logs*
- *Secure*
- *Auth logs*
- *And many more...*