Actionable Sheet - Wiki Server (Ubuntu)

STIG - Follow Brants

Firewall: <https://www.configserverfirewall.com/ufw-ubuntu-firewall/ubuntu-check-firewall-status-ufw/>

1. Basic Commands
   * *“sudo ufw insert 1 allow 80”*, adding a rule using a numbered format
   * *“sudo ufw deny 22”* close an opened port
   * “*sudo ufw delete 4*” deletes rule 4
   * *“sudo ufw logging on”* turns on logging
2. Check the firewall status
   * “*sudo* *ufw status”*
     + If the firewall is enabled then you will see rules. If not you will see, “Status: inactive”
   * *“sudo ufw enable”*
3. Display firewall rule numbers
   * “*sudo ufw status numbered*”
   * Can use this to modify existing firewall rules
4. Filter Firewall status with grep command
   * Display default firewall policy
     + “*sudo ufw status verbose | grep -i default*”
   * Filter by specific port
     + “*sudo ufw status | grep 22*”
     + Will display rules related to the ssh port 22
   * Filter the status to display firewall rules that have configured to deny connections
     + “*sudo ufw status | grep -i deny*”

Service Management:

<https://askubuntu.com/questions/19320/how-to-enable-or-disable-services>

1. Starting or Stopping a service
   1. ***sudo*** [service name] [action]
      1. ***sudo service apache2 stop***  OR ***sudo service apache2 start***
   2. Ubuntu version older than 15.04
      1. Use the upstart commands
         1. ***sudo start mysql***  OR use  ***stop , restart, status***
   3. \*\*Ubuntu version past 15.04
      1. Use SYSTEMD command
         1. ***systemct1 start*** [service]
         2. Can also use ***stop, restart, reload, status, enable, disable, is-enabled, is-active, show, mask, unmask***

How to kick users: <https://unix.stackexchange.com/questions/615/how-do-you-kick-a-benign-user-off-your-system>

1. Commands
   * “*who -u*” See who’s logged into your machine and check their Process ID
   * “*killall -u username*” this will kill all processes by that user
2. Log-out the user
   * *sudo pkill -KILL -u <*username*>*
   * Ex: *sudo pkill -9 -u guest-24whg*

Method 1 - Script (Brants Script)

nano updatessh.sh

#!/bin/bash

sudo sed -i '/^Protocol/s/1/2/' /etc/ssh/sshd\_config

#Insert AllowUsers

#Insert DenyUser

sudo sed -i '/^PermitRootLogin/s/yes/no/' /etc/ssh/sshd\_config

sudo sed -i '/^HostbasedAuthentication/s/yes/no/' /etc/ssh/sshd\_config

sudo sed -i '/^AllowTcpForwarding/s/yes/no/' /etc/ssh/sshd\_config

sudo sed -i '/^X11Forwarding/s/yes/no/' /etc/ssh/sshd\_config

sudo sed -i '/^LogLevel/s/yes/no/' /etc/ssh/sshd\_config

sudo sed -i '/^PermitEmptyPasswords/s/yes/no/' /etc/ssh/sshd\_config

sudo service ssh restart

sudo chmod 755 updatessh.sh

sudo ./updatessh.sh