Security workshop

Tacacs lab

1 getting tacacs configured

```
$ sudo apt-get install tacacs+
$ sudo groupadd -r cisco
$ sudo vi /etc/tacacs+/tac_plus.conf
```

1.0.1 change the following settings

1. we want to set the password for routers who want to use our service to TacacsPassword
2. We also want to limit access for users based on groups. For this example we will use settings in tac_plus.conf

```
# change this line

key = TacacsPassword

# ... then at the end of the file .... add:

group = netops {
        default service = permit
        login = file /etc/passwd
        enable = file /etc/passwd
        service = exec {
                priv-lvl = 15
                }
}

#
# "level 2" users who cannot "debug" or "config"
#
group = l2_tacacs_users {
        default service = permit
        login = file /etc/passwd
        enable = file /etc/passwd
        service = exec {
                priv-lvl = 15
                }
        cmd = configure {
                deny "."
                }
        cmd = debug {
                deny "."
                }
}
```

```
user = sysadm {
    member = netops
}
```

1.0.2 restart tacacs_plus to pick up the new settings

```
$ sudo service tacacs_plus restart
```

2 getting a cisco device to talk to your tacas

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization exec default group tacacs+ if-authenticated
aaa session-id common

aaa accounting delay-start
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+


tacacs-server host 10.10.9.1
tacacs-server key TacacsPassword
```

2.0.3 Now you can verify accounting

```
Router#show accounting
```