Security Workshop

Accessing Lab Components

Contents

1 Objectives

This set of instructions is to ensure you have access to the different equipment in your group. Keep in mind that since you are working as a group each one of you potentially needs to be able to access all the equipment in the group but no single equipment is allocated to a particular person. You must all decide on who does what.

In particular after completing this you should have the following setup.

- SSH for accessing the VMS (and later on routers)
- Telnet for console access to routers
- VNC for console access to the VMS

2 SSH

Depending on your operating system, you may already have an SSH client installed. SSH will be discussed in class and gives encrypted console access to the equipment managed by your group.

2.1 Windows

Windows does not come with an SSH client but you can download one. For this course we need more than just the SSH executable we also need an SSH key generator and an SSH agent.

- You can download all the above as the Putty Application. You would need
  - putty.exe - the SSH application
  - puttygen.exe - an SSH Key generator
  - pageant.exe - an SSH Agent
- An alternate SSH application that can work with PUTTY's ssh agent and key generator is Kirby
- See the SSH presentation for others.

These executables will likely be available on the workshop wiki page so you do not have to download them from the Internet.

2.2 Linux

Linux distributions usually ship with SSH clients. To check, open a terminal and type:

```
$ ssh -V
```

How to install one depends on your distribution. For Ubuntu and other Debian based derivatives you can install the OpenSSH client package (and we'd recommend the server package while you're at it).

```
$ sudo apt-get install openssh-client
```

2.3 OS X

Mac OS X comes with an SSH client (OpenSSH). To use it just open the Terminal application located in /Applications/Utilities

3 Router Console access

Each of your groups includes a router. We are using dynamips to emulate CISCO hardware. The instructor will let you know what IP to use to access the console server. Assuming your group number is X and the console server is 1.2.3.4 you can then access your router's console port by using:

```
$ telnet 1.2.3.4 210X
```

Windows does not ship with the telnet application installed by default these days. However, you can use the putty (or Kirby) application downloaded earlier and ensure you use telnet rather than SSH as the protocol - it will select the right port once you switch.

4 Virtual Machine Console access

We are running all your machines in a virtualised environment using KVM. In some cases you may want to access the console of the virtual machine for example when installing software off a CD remotely.

The instructors will give you the ip address of the VNC server(s) and the port used to access particular VMs. However you need a VNC client installed which

depends on your operating system. As an example the firewall on each of your groups will be under VNC port 1000X where X is your group number.

A good opensource VNC server (and client) is TightVNC. If you have java installed you can just use the Java client and not install additional software.

4.1 Windows

Windows does not ship with a VNC client but Tight VNC makes clients for 32 bit and 64 bit versions of windows. Download and install either one (or the Java client mentioned earlier)

4.2 Linux

Most linux distributions come with a VNC client. Ubuntu's default VNC client is vinagre. If you don't have it installed you can get it via apt:

```
$ sudo apt-get install vinagre
```

If you want to install the tightvnc viewer on Ubuntu instead you could type:

```
$ sudo apt-get install xtightvncviewer
```

If you have a JRE installed you can also use the Java Client.

4.3 OS X

Mac OS X comes with an inbuilt VNC client accessible via Finder. However, it does not consistently allow you to connect to an arbituary port on the VNC server. As such you are advised to download a VNC client for OS X such as Chicken