NWIT 245 – Defending the Network

Hands-on Labs

Lab 11-TightVNC

Background

In this assignment, you have the option to work as a team that we established earlier or as an individual. If you work as an individual, please make sure to have another machine if implemented in Windows instead of VM. However, if you are to install it in your VM, say using the Ubuntu instructions below, you can access your machine from your VM.

Introduction

TightVNC is a free and open-source remote desktop software server and client application for Linux and Windows. TightVNC or VNC (Virtual Network Computing) works as a connection system that allows you to use your keyboard and mouse to interact with a graphical desktop environment on a remote server. It will allow you to remotely connect to a computer (remote sharing system). You can also access your server from any location if needed.

Assignment

In this assignment, you'll set up and configure VNC Server with TightVNC either on your Windows, Kali Linux or Ubuntu VM and connect to it securely through an SSH tunnel. Then, you'll use a VNC Viewer program on your local machine to interact with your Server (your team's machine in a single network) through a graphical desktop environment.

Note: The easiest way to implement TightVNC using the GUI on Windows 10/11. You also have the option to use any VNC.

Requirements

1. **Windows 10/11**, or Kali Linux (Extra Point), or Ubuntu
    a. Windows:
        i. On Windows, you can use TightVNC, RealVNC, or UltraVNC.
        ii. Download TightVNC from: https://www.tightvnc.com/download.php
        iii. All you have to do is download the installer based on your processor (64-bit / 32-bit) and install on both machines (Client and Server) by following the installer prompt.

            Note: I usually install both the Viewer and the Server on both machines to allow access from both machines.

b. Kali:

i. On Linux, you can choose from many options, including Vinagre, an older version but updated GUI version is included in GNOME 2.22, KRDC, RealVNC, or TightVNC.

NOTE: GNOME is Desktop and Platform release of the latest version of the popular, multi-platform free desktop environment.

GNOME runs on a variety of platforms, including GNU/Linux (commonly called Linux), Solaris, HP-UX, BSD and Apple's Darwin. GNOME includes powerful features such as high-quality smooth text rendering, a first-class internationalization and accessibility infrastructure, including support for bi-directional text.

ii. The minimal version installation of Kali (CLI only) will not allow this installation unless you install GNOME, the GUI version of Kali. Another option is to install the Xfce desktop to function well on VNC.

iii. We will use Xfce4 when we install it on Ubuntu below.

c. Ubuntu:

i. Ubuntu 20.04/22.04 server with a non-root user and a firewall configured with UFW. If you do not have this configured, follow this initial server setup guide for Ubuntu 20.04 from DigitalOcean.com.

ii. A local computer with a VNC client installed (@ the Extra Point Client-Side Installation).

d. MacOS:

i. On macOS, you can use the built-in Screen Sharing program.
ii. You can also a similar VNC server called RealVNC.

2. Any Browser to Download

3. A VirtualMachine (if installed on Ubuntu or Kali of our VM instances)
NOTE: Remember that installing on VM is optional.

Instruction:

One of the best installations is done on a VM. Although I'm installing this on Ubuntu, you can install it anywhere you'd like to, including Kali, MacOS, Windows 10/11 on your machine etc…

There are two components to the installation.

- **VNC Server**: Installed on the target machine. You need an IP address of that machine.
- **VNC Viewer**: Installed on the machine you are going to use to access or "view" the computer (VNC Server) with.

NOTE: You can install both the Server and Viewer on each machine so that you can access each machine from the other client machine.

Server Side - Installing VNC Server on Ubuntu VM.

1. Update your Ubuntu installation [***sudo apt update***]
   If issues arise, make sure to close any running app and review the below screenshot's 3 command lines.

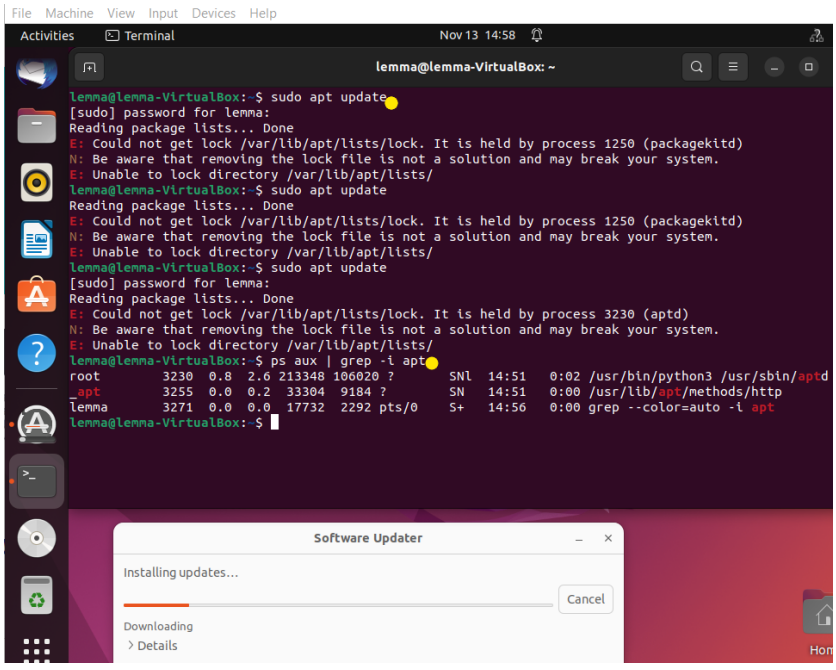

Fig. 1-While Software is updating, the command line to update will complain.


```
lemma@lemma-VirtualBox:~$ ps aux | grep -i apt
root        3230  0.8  2.6 213348 106020 ?       SNl  14:51   0:02 /usr/bin/python3 /usr/sbin/aptd
_apt        3255  0.0  0.2  33304  9184 ?        SN   14:51   0:00 /usr/lib/apt/methods/http
lemma       3271  0.0  0.0  17732  2292 pts/0    S+   14:56   0:00 grep --color=auto -i apt
lemma@lemma-VirtualBox:~$ ps aux | grep -i apt
root        3230  0.3  2.6 213348 106036 ?       SNl  14:51   0:02 /usr/bin/python3 /usr/sbin/aptd
lemma       3289  0.0  0.0  17732  2344 pts/0    S+   15:03   0:00 grep --color=auto -i apt
lemma@lemma-VirtualBox:~$ sudo apt update
Ign:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Ign:3 https://www.kismetwireless.net/repos/apt/git/focal focal InRelease
Ign:4 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Ign:5 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease
Ign:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Ign:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Ign:3 https://www.kismetwireless.net/repos/apt/git/focal focal InRelease
Ign:6 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
```

Fig. 2-Once update is completed, or other running apps are closed, the issue is resolved.

Notice the _apt issue is not showing once the "Software Update" is closed. The apt update is properly functioning.

2. Install Xfce4 for desktop enhancements (improved GUI, image, artwork, etc. views) This will allow you to have an enhanced GUI when you view the client machine.

   [***sudo apt install xfce4 xfce4-goodies***]

3. Type "y" when prompted. This may take several minutes as it will install several xfce4 related tools.

```
Setting up libthunarx-3-0:amd64 (4.16.10-1) ...
Setting up xfce4-whiskermenu-plugin:amd64 (2.7.1-1) ...
Setting up xfce4-xkb-plugin:amd64 (1:0.8.2-1) ...
Setting up xfce4-verve-plugin:amd64 (2.0.1-1) ...
Setting up libgarcon-gtk3-1-0:amd64 (4.16.1-1) ...
Setting up thunar (4.16.10-1) ...
Setting up xfce4-places-plugin (1.8.1-1build1) ...
Setting up xfce4-clipman-plugin:amd64 (2:1.6.2-1) ...
Setting up xfce4-session (4.16.0-1ubuntu2) ...
Setting up xfce4-panel (4.16.3-1) ...
Setting up thunar-media-tags-plugin (0.3.0-2) ...
Setting up xfdesktop4 (4.16.0-1) ...
Setting up thunar-volman (4.16.0-1) ...
Setting up thunar-archive-plugin (0.4.0-2) ...
Setting up xfce4 (4.16) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for libglib2.0-0:amd64 (2.72.1-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Setting up xfce4-goodies (4.14.0) ...
lemma@lemma-VirtualBox:~$
```

Fig. 3- After proper installation of xfce4-goodies, the above message should appear.

Note: It took approximately 30 minutes for the xfce4-goodies installation to complete.

4. Install the Server using [***sudo apt install tightvncserver***] and type "y".

```
lemma@lemma-VirtualBox:~$ sudo apt install tightvncserver
[sudo] password for lemma:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tightvncpasswd
Suggested packages:
  tightvnc-java
The following NEW packages will be installed:
  tightvncpasswd tightvncserver
0 upgraded, 2 newly installed, 0 to remove and 31 not upgraded.
Need to get 690 kB of archives.
After this operation, 1,827 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Fig. 4-When installing TightVNC, additional disk space is needed for the upgrades.

5. Starting a vncserver requires you to create a password that is between 6-8 chars length. If longer than 8, it'll be truncated to the first 8 chars only.

```
Processing triggers for man-db (2.10.2-1) ...
lemma@lemma-VirtualBox:~$ vncserver

You will require a password to access your desktops.

Password:
```

Fig. 5- To start the server, you'll need to create a password.

6. Make sure to select 'n' when the view-only password creation option appears.
   NOTE: If you only wish to show or demonstrate (without having control to the client machine), select "n" in the "view-only" password selection. Otherwise, select "y"
   - Entering "n" will give the viewer the right to participate actively.
   - The option "y" will only give the right to watch or "view".

```
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
```

Fig. 5a-Viewer installation is complete with option of view-only password being created.

NOTE: If you wish to change your selection for the password (change your password)

i. Enter [vncpasswd] as in the image below.
ii. Enter your Ubuntu password x2.
iii. Change the password selection option to “y” or “n” as in below.
iv. If “n” is selected, VNC will create the default configuration files and other port configuration. In other words, it will setup the default port number to:
   a. 5901 (display port) as :1
   b. 5902 as :2
   c. 5903 as :3

   This means, you don’t need to enter port number after the IP Address (192.168.10.10**:1**) as in other installations.

```
lemma@lemma-VirtualBox:~$ vncpasswd
Using password file /home/lemma/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
```

Fig. 5b-Changing the password selection option from “y” to “n” or vice versa.

7. Enter “y” to have a complete access.

```
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:

Warning: lemma-VirtualBox:1 is taken because of /tmp/.X1-lock
Remove this file if there is no X server lemma-VirtualBox:1

New 'X' desktop is lemma-VirtualBox:2

Creating default startup script /home/lemma/.vnc/xstartup
Starting applications specified in /home/lemma/.vnc/xstartup
Log file is /home/lemma/.vnc/lemma-VirtualBox:2.log

lemma@lemma-VirtualBox:~$
```

Fig. 6-After creating a vnc password, a host name (lemma-virtualBox:2), a log file location and .vnc script are created for the startup.

Configuring VNC Server

As you can imagine, managing a remote desktop using CLI can be challenging. In many cases, it's downright impossible to access it if the remote desktop/client is not equipped with similar options. This is why we installed the xfce4 earlier.

1. Backup the initial startup configuration prior to modifying it.
   [mv ~/.vnc/xstartup ~/.vnc/xstartup.bak]
2. Stop the VNC server
   [**vncserver -kill :1**]
   NOTE: If you encounter an issue, a message stating that "you will have to stop VNC manually", that's because you selected a different desktop.

```
lemma@lemma-VirtualBox:~$ mv ~/.vnc/xstartup ~/.vnc/xstartup.bak
lemma@lemma-VirtualBox:~$ vncserver -kill :2
Killing Xtightvnc process ID 6558
lemma@lemma-VirtualBox:~$
```

   Fig. 7. Stopping the correct machine lemma-virtualBox:**2**
3. Create a new startup file and open it in text editor.
   [***nano ~/.vnc/xstartup***]

4. Adding lines to the nano file.

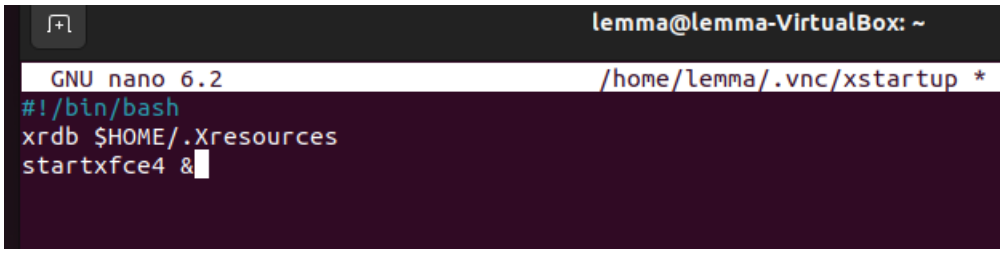

   Fig. 8-In these 3 lines, the first line tells vnc to expect a Bash interpreter (shebang). The second line is telling xfce4 to read the server's resources where a user can make changes using his/her mouse/keyboard in the GUI. The last command is telling the server to start the xfce4. Now, each time you start vnc server, these command lines will be executed automatically.
5. Save and close [CTRL + X]
6. When you get the prompt to "save the modified buffer" select "y", then enter.
7. Create an executable [***chmod +x ~/.vnc/xstartup***]


```
lemma@lemma-VirtualBox:~$ mv ~/.vnc/xstartup ~/.vnc/xstartup.bak
lemma@lemma-VirtualBox:~$ vncserver -kill :2
Killing Xtightvnc process ID 6558
lemma@lemma-VirtualBox:~$ nano ~/.vnc/xstartup
lemma@lemma-VirtualBox:~$ chmod +x ~/.vnc/xstartup
lemma@lemma-VirtualBox:~$
```

Fig. 8- Ent entire process of 1. Creating a backup file, 2. Killing vnc, 3. Creating a new startup file using bash, 4. Creating an executable file of the startup bash file.

8. Restart your VNC Server. [***vncserver -localhost***]

```
lemma@lemma-VirtualBox:~$ vncserver -localhost

Warning: lemma-VirtualBox:1 is taken because of /tmp/.X1-lock
Remove this file if there is no X server lemma-VirtualBox:1

New 'X' desktop is lemma-VirtualBox:2

Starting applications specified in /home/lemma/.vnc/xstartup
Log file is /home/lemma/.vnc/lemma-VirtualBox:2.log

lemma@lemma-VirtualBox:~$
```

Fig. 9-The .exe bash file we created is now working. Your VNC is ready to use (localhost only)
Note: Your machine's output may be different.

9. Connect to your local machine using the below command.
   [*ssh -L 59000:localhost:5901 -C -N -1 lemma-VirtualBox:2 192.168.1.1*]
   Make sure to change the machine's name to your machine's name, and the IP Address.
   - -L: a switch that specifies a given port (59000) on the local machine is to be forwarded to the destination server's local host (5901).
   - -C: Allows compression to minimize resources and speed.
   - -N: No execution to remote commands
   - -1: Lets you identify the user you want to connect to once you connect to the VNC server (lemma-VirtualBox:2 192.168.1.1). Again, your machine name and IP Address will be different.

Extra Point (5 pts):

Two to three students can work together in the Extra Point option.

1. You can use any environment like your machine or your VM, using Windows, MacOS, Ubuntu, Kali, etc.
2. Connect with a different machine (team member's IP address) using your machine.

3. This can't be a single machine installation/configuration. Either it's local, VMs or any other installation on a single device will not count.

Questions:

1. Are you able to access your teammate's machine or VM setup?
2. What concerns should you bring to your organization's IT manager regarding remote connection?
3. How do you protect your network and devices when you have a remote access policy?
4. What would you consider implementing for endpoint protection when you have remote connection policy?
5. Consider the following and associate the benefits they provide with remote connection security.
    a. MFA
    b. Encryption
    c. VPN
    d. IDS/IPS
    e. Antivirus
    f. Your IT department members.

