

Lab 03 Linux Configuration

💡 It is very rare that you will find an enterprise that is either fully Windows, Mac or Linux. You will likely find a heterogeneous environment where many different operating systems are leveraged to accomplish the organization's mission. In this lab, you will configure an operating system called CentOS. This particular operating system is open source and has been pre-built for you. Your job will be to complete the configuration steps to make it useful and manageable in your growing enterprise.

Networking dhcp01

Find dhcp01 Virtual Machine in your vsphere environment, & configure the network so that it is using your internal LAN segment. And don't forget the Snapshot prior powering dhcp01 on, if you like to have a backup.

 SYS255-02-LAN-rubeus.hagrid

💡 Its default root password is with the other default passwords in Canvas.

<https://sites.google.com/a/champlain.edu/cncs-wiki/home/operating-systems/linux/network-configuration> describes the process of setting a hostname and IP address, though many students appreciate the **nmtui** application. For those having trouble, the following [video tutorial](#) shows the process of setting the networking configuration.

dhcp01 network settings:

Setting	Value
IP Address and Netmask	10.0.5.3/24
Gateway	10.0.5.2
DNS	10.0.5.5
Search Domain	yourname.local
Hostname	dhcp01-yourname



LET US DARE

Adding a privileged user

Figure out how to add a named user who is a member of the wheel group (Linux's local admin group on Centos). Hint: The linked video also shows how to do this.

Networking Test

If you did everything right, then you should be able to ping systems inside 10.0.5.0/24 and outside (SYS255-WAN) of your network.

Deliverable 1. Login as the named user (**not root!**) and attempt to ping google.com, ad01 and fw01. Provide a screenshot similar to the one below that shows the three successful pings.

```
dhcp01-rubeus.hagrid Enforce US Keyboard Layout View Fullscreen

lrubeus@dhcp01-rubeus ~]# ping -c1 google.com
PING google.com (142.250.64.110) 56(84) bytes of data.
64 bytes from lga34s31-in-f14.1e100.net (142.250.64.110): icmp_seq=1 ttl=115 time=12.7 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.771/12.771/12.771/0.000 ms
lrubeus@dhcp01-rubeus ~]# ping -c1 ad01-rubeus
PING ad01-rubeus.rubeus.local (10.0.5.5) 56(84) bytes of data.
64 bytes from ad01-rubeus.rubeus.local (10.0.5.5): icmp_seq=1 ttl=128 time=0.369 ms

--- ad01-rubeus.rubeus.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.369/0.369/0.369/0.000 ms
lrubeus@dhcp01-rubeus ~]# ping -c1 fw01-rubeus
PING fw01-rubeus.rubeus.local (10.0.5.2) 56(84) bytes of data.
64 bytes from fw01-rubeus.rubeus.local (10.0.5.2): icmp_seq=1 ttl=64 time=0.378 ms

--- fw01-rubeus.rubeus.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.378/0.378/0.378/0.000 ms
lrubeus@dhcp01-rubeus ~]# _
```


DNS

Take a look at last week's lab, and figure out how to add A and PTR records for dhcp01 to the DNS configuration on ad01. Test this by issuing a ping from wks01 to dhcp01 using the undistinguished hostname.



LET US DARE

Deliverable 2. Using WKS01, Provide a screenshot showing the successful ping using dhcp01's hostname only (leave off yourname.local).

 Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\rubeus.hagrid-adm> ping -n 1 dhcp01-rubeus


Pinging dhcp01-rubeus.rubeus.local [10.0.5.3] with 32 bytes of data:
Reply from 10.0.5.3: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.5.3:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\rubeus.hagrid-adm> █
```

Remote Access from ad01

Systems Administrators will typically manage linux systems remotely via SSH (Secure Shell). An application called PuTTY was popular for this purpose and can still be optionally installed. Fortunately, Windows 10 now ships with an SSH client and we'll use this.

Deliverable 3. Provide a screenshot that shows a successful ssh session as your named Linux user from wks01:

 rubeus@dhcp01-rubeus:~

```
PS C:\Users\rubeus.hagrid-reg> hostname
wks01-rubeus
PS C:\Users\rubeus.hagrid-reg> ssh rubeus@dhcp01-rubeus
The authenticity of host 'dhcp01-rubeus (10.0.5.3)' can't be established.
ECDSA key fingerprint is SHA256:O+dCwnBorBonuqINT6nBU+GYQGHw6gby36cIalxVsMU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'dhcp01-rubeus,10.0.5.3' (ECDSA) to the list of known hosts.
rubeus@dhcp01-rubeus's password:
Last login: Wed Sep  8 11:37:31 2021
Last login: Wed Sep  8 11:37:31 2021
[rubeus@dhcp01-rubeus ~]$ █
```

Getting around and sudo

When you login via SSH or locally, you land in the logged-in users home directory (~). The pwd command shows you this.



LET US DARE

Show the present working directory	<pre> rubeus@dhcp01-rubeus:~ [rubeus@dhcp01-rubeus ~]\$ pwd /home/rubeus [rubeus@dhcp01-rubeus ~]\$ </pre>
Navigate up to the /home directory and list the contents	<pre> rubeus@dhcp01-rubeus:/home [rubeus@dhcp01-rubeus ~]\$ cd /home [rubeus@dhcp01-rubeus home]\$ ls rubeus [rubeus@dhcp01-rubeus home]\$ </pre>
Navigate up to the parent directory using a relative <code>cd ..</code> command. It is relative to where you are in the directory structure.	<pre> rubeus@dhcp01-rubeus/ [rubeus@dhcp01-rubeus home]\$ cd .. [rubeus@dhcp01-rubeus /]\$ ls bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var [rubeus@dhcp01-rubeus /]\$ </pre>
long listing of files and directories with <code>ls -l</code> .	<pre> rubeus@dhcp01-rubeus:/ [rubeus@dhcp01-rubeus /]\$ ls -l total 16 lrwxrwxrwx. 1 root root 7 Jul 20 08:50 bin -> usr/bin dr-xr-xr-x. 5 root root 4096 Jul 20 14:27 boot drwxr-xr-x. 19 root root 3140 Aug 24 14:32 dev drwxr-xr-x. 84 root root 8192 Aug 24 15:52 etc drwxr-xr-x. 3 root root 20 Aug 24 13:57 home lrwxrwxrwx. 1 root root 7 Jul 20 08:50 lib -> usr/lib lrwxrwxrwx. 1 root root 9 Jul 20 08:50 lib64 -> usr/lib64 drwxr-xr-x. 2 root root 6 Apr 11 2018 media drwxr-xr-x. 2 root root 6 Apr 11 2018 mnt drwxr-xr-x. 3 root root 16 Jul 20 08:51 opt dr-xr-xr-x. 174 root root 0 Aug 24 14:32 proc dr-xr-xr-x. 4 root root 164 Jul 20 09:01 root drwxr-xr-x. 29 root root 860 Aug 24 14:35 run lrwxrwxrwx. 1 root root 8 Jul 20 08:50 sbin -> usr/sbin drwxr-xr-x. 2 root root 6 Apr 11 2018 srv dr-xr-xr-x. 13 root root 0 Aug 24 14:32 sys drwxrwxrwt. 9 root root 206 Aug 24 15:52 tmp drwxr-xr-x. 13 root root 155 Jul 20 08:50 usr drwxr-xr-x. 20 root root 282 Jul 20 08:58 var [rubeus@dhcp01-rubeus /]\$ </pre>
show the manual page indicating what each directory in the file hierarchy is used for. <code>man hier</code> . Read the description of the first level directories.	<pre> rubeus@dhcp01-rubeus/ Linux Programmer's Manual HIER(7) NAME hier - description of the file system hierarchy DESCRIPTION A typical Linux system has, among others, the following directories: / This is the root directory. This is where the whole tree starts. /bin This directory contains executable programs which are needed in single user mode and to bring the system up or repair it. /boot Contains static files for the boot loader. This directory holds only the files which are needed during the boot process. The map installer and configuration files should go to /sbin and /etc. /dev Special or device files, which refer to physical devices. See mknod(1). /etc Contains configuration files which are local to the machine. Some larger software packages, like X11, can have their own subdirectories below /etc. Site-wide configuration files may be placed here, or in /usr/etc. Nevertheless, programs should always look for these files in /etc and you may have links for these files to /usr/etc. /etc/opt Host-specific configuration files for add-on applications installed in /opt. /etc/sgml This directory contains the configuration files for SGML and XML (optional). /etc/skel When a new user account is created, files from this directory are usually copied into the user's home directory. </pre>



<p>Use the "tilde" shortcut to go to the home directory ~</p>	 <pre> rubeus@dhcp01-rubeus:~ [rubeus@dhcp01-rubeus /]\$ cd ~ [rubeus@dhcp01-rubeus ~]\$ pwd /home/rubeus [rubeus@dhcp01-rubeus ~]\$ </pre>
<p>Create and navigate to a directory called sys255 in your home directory</p>	 <pre> rubeus@dhcp01-rubeus:~/sys255 [rubeus@dhcp01-rubeus ~]\$ mkdir sys255 [rubeus@dhcp01-rubeus ~]\$ cd sys255/ [rubeus@dhcp01-rubeus sys255]\$ pwd /home/rubeus/sys255 [rubeus@dhcp01-rubeus sys255]\$ </pre>
<p>Try to install the "tree" package as the named non root user. This should fail because your named account does not have privileges to install software.</p>	 <pre> rubeus@dhcp01-rubeus:~/sys255 [rubeus@dhcp01-rubeus sys255]\$ yum install -y tree Loaded plugins: fastestmirror, langpacks You need to be root to perform this command. [rubeus@dhcp01-rubeus sys255]\$ </pre>
<p>Elevate privileges using the sudo command. This will only work if you set your named user to be an administrator. The sudo command run this way will execute a single command as a privileged user then drop you back down to normal permissions.</p>	 <pre> rubeus@dhcp01-rubeus:~/sys255 [rubeus@dhcp01-rubeus sys255]\$ sudo yum install tree [sudo] password for rubeus: Loaded plugins: fastestmirror, langpacks Determining fastest mirrors * base: mirror.umd.edu * extras: mirror.steadfastnet.com * updates: mirrors.umflint.edu base 3.6 kB 00:00:00 extras 2.9 kB 00:00:00 updates 2.9 kB 00:00:00 (1/2): extras/7/x86_64/primary_db 286 kB 00:00:00 (2/2): updates/7/x86_64/primary_db 3.8 MB 00:00:02 Resolving Dependencies --> Running transaction check --> Package tree.x86_64 0:1.6.0-10.el7 will be installed --> Finished Dependency Resolution Dependencies Resolved ===== Package Arch Version Repository Size ===== Installing: tree x86_64 1.6.0-10.el7 base 46 k Transaction Summary ----- Install 1 Package Total download size: 46 k Installed size: 87 k Is this ok [y/d/N]: </pre>
<p>Show the groups your user has been assigned to. In this case, the wheel group is analogous to the Administrator's group in Windows.</p>	 <pre> rubeus@dhcp01-rubeus:~/sys255 [rubeus@dhcp01-rubeus sys255]\$ groups rubeus wheel [rubeus@dhcp01-rubeus sys255]\$ </pre>



Become root for an extended time with `sudo -i`. This is necessary if you have a lot to do in a privileged state, be sure to "exit" the root shell when you are done. A second exit will probably close your SSH session.

The `whoami` command will show what user you are logged in as.

```
rubeus@dhcp01-rubeus:~/sys255
[rubeus@dhcp01-rubeus sys255]$ pwd
/home/rubeus/sys255
[rubeus@dhcp01-rubeus sys255]$ sudo -i
[root@dhcp01-rubeus ~]# whoami
root
[root@dhcp01-rubeus ~]# pwd
/root
[root@dhcp01-rubeus ~]# exit
logout
[rubeus@dhcp01-rubeus sys255]$ whoami
rubeus
[rubeus@dhcp01-rubeus sys255]$ pwd
/home/rubeus/sys255
[rubeus@dhcp01-rubeus sys255]$
```

History

Sometimes it is useful to see the history of those things you've typed at the command line (this works in powershell too!). Type `history` to see what commands have been typed.


Deliverable 4: Provide the first 10 commands recorded in your history file:

```
rubeus@dhcp01-rubeus:~/sys255
rubeus@dhcp01-rubeus sys255]$ history | head -n 10
 1 sudo ls -la /root
 2 exit
 3 ping -c1 google.com
 4 ping -c1 fw01-rubeus
 5 clear
 6 ping -c1 google.com
 7 ping -c1 ad01-rubeus
 8 ping -c1 fw01-rubeus
 9 ip a
10 exit
rubeus@dhcp01-rubeus sys255]$
```

Hidden Files: Go to your home directory and do a normal `ls`. Follow that by the `ls -la` command. This command lists those hidden files (those that start with a period.)




LET US DARE

 rubeus@dhcp01-rubeus:~/sys255

```
[rubeus@dhcp01-rubeus sys255]$ ls ~
sys255
[rubeus@dhcp01-rubeus sys255]$ ls -la ~
total 16
drwx-----. 5 rubeus rubeus 126 Aug 24 15:59 .
drwxr-xr-x. 3 root   root   20 Aug 24 13:57 ..
-rw-----. 1 rubeus rubeus 290 Aug 24 15:52 .bash_history
-rw-r--r--. 1 rubeus rubeus  18 Mar 31 22:17 .bash_logout
-rw-r--r--. 1 rubeus rubeus 193 Mar 31 22:17 .bash_profile
-rw-r--r--. 1 rubeus rubeus 231 Mar 31 22:17 .bashrc
drwxrwxr-x. 3 rubeus rubeus  18 Aug 24 13:58 .cache
drwxrwxr-x. 3 rubeus rubeus  18 Aug 24 13:58 .config
drwxrwxr-x. 2 rubeus rubeus   6 Aug 24 15:59 sys255
[rubeus@dhcp01-rubeus sys255]$
```

View .bash_history (if it is missing, logout of ssh and log back in again).

 rubeus@dhcp01-rubeus:~

```
PS C:\Users\rubeus.hagrid-reg> ssh rubeus@dhcp01-rubeus
rubeus@dhcp01-rubeus's password:
Last login: Wed Sep  8 11:50:34 2021 from wks01-rubeus.rubeus.local
[rubeus@dhcp01-rubeus ~]$ ls .bash_history
.bash_history
[rubeus@dhcp01-rubeus ~]$ cat .bash_history
ls .bash_history
ping -c1 google.com
ping -c1 ad01-rubeus
ping -c1 fw01-rubeus
ls .bash_history
cat .bash_history
exit
ping -c1 google.com
exit
ping -c1 ad01-rubeus
ping -c1 fw01-rubeus
ls .bash_history
cat .bash_history
exit
clear
exit
[rubeus@dhcp01-rubeus ~]$
```

Deliverable 5. This is a two part question:

- a. What security implications does this file represent? List at least one pro and one con.
- b. What command is used to clear bash history?



LET US DARE

Deliverable 6. This is the final reminder for specs, and is expected for the remaining labs.

Deliverable 7. Tech Journal entry reminder. There are loads of Linux commands, so go exploring for at least 3 new ones. Also, their *man* page is your new BFF.



LET US DARE