Date: _____ Name: _____

Station Number: _____ Email: _____

Installation and Configuration

Total Duration:	3.0 hours
Goal:	To demonstrate the ability to install and configure a Red Hat Enterprise Linux system and implement network services and security.

You have been instructed to install Red Hat Enterprise Linux on a system within your organization. The system must be configured with a set of locally-defined administrators and bound to an NIS domain, `RHCE`, for additional user accounts. Your machine will be a member of the DNS domain `example.com`. All systems in the `example.com` DNS domain are in the `172.24.0.0/255.255.0.0` subnet, and all systems in that subnet are in `example.com`.

Perform the tasks listed below. You should read the entire list before you begin. In order to fulfill the printing requirement, you will probably need to install the X Window System.

Your system will be rebooted before it is graded, so make sure that all changes you implement are persistent across reboots. You should also be aware the scoring items will be evaluated by whether they work as specified. Consequently, a correctly configured networking service will earn no points if networking itself is broken.

`station249.example.com` is accessible by `ssh` for testing the availability of network services on your system. If your hostname is `station1.example.com`, then you can log in to this system with the username `guest1` and the password of `password`. If `station2.example.com`, then you can log in as `guest2` with the same password, and so on. You will not be able to log in successfully to any other account on that system. Additional information on how you might use this system may be included with specific requirements below.

The requirements for this section include configuration of security restrictions on various network services. You should be aware that making the services available for permitted hosts and networks is a higher priority than restricting any prohibited networks, because you will not receive credit for successful configuration of services if the implemented restrictions block access to permitted hosts and networks. If you choose to use kernel level firewalling, you must `REJECT` rather than `DROP` unwanted packets.

Be aware that you are not permitted to communicate with other examinees during the course of this exam. You are also prohibited from connecting to the hosts of other examinees. The testing system and the network will be monitored, and misuse of either will result in a grade of zero on this section.

Installation Instructions

- Install Red Hat Enterprise Linux on the examination system using the following source for the installation media:

  NFS `server1.example.com:/var/ftp/pub`

- Once your system is installed the distribution is available via YUM:

  YUM `http://server1.example.com/pub/Server`

The examiner will provide a suitable boot medium to begin the installation.

- Installation options should be chosen as follows:
  - Use DHCP to configure networking for eth0.
  - Install the boot loader to the Master Boot Record (MBR) – do not include any additional options for the bootloader to pass to the kernel unless instructed to do so by the examiner
  - Set the root password to `rW9ySX`.
  - The timezone should be appropriate for your locale, and the system clock should be set to UTC.
  - Skip entering an Installation Number.
  - Do not attempt to register the system with Red Hat Network.
  - Consult the instructions concerning parititioning in the next section before you begin your installation

RHCT (Local) Requirements

Perform all of the following steps. When you receive your results, these items will be reported as a single score identified as *RHCT*. You must score 70 or higher on these RHCT requirements in order to earn certification.

- Complete the form at `http://server1.example.com/cgi-bin/enroll`. Provide your name as you wish to have it appear on your certificate (should you earn it) and the email address you wish for us to use when contacting you with your results. Red Hat Global Learning Services requires this information to process and report your results.
- Install the *dialog* RPM package.
- Partition the system's primary hard drive using the following scheme:

```
/boot    256 MB
/        1024 MB
/home    512 MB
/usr     2048 MB
/var     512 MB
swap     1.5 - 2 times memory reported in /proc/meminfo
/shared  Use the remaining space to create a RAID 0 set on /dev/md0
```

  If you do not know how to create the RAID 0 set for /shared, you must create it as a separate directory. You may create the RAID 0 set at install time or post-installation as you prefer.
- SELinux must be running in the Enforcing mode.
- Create the following users, groups, and group memberships:
  - A group named `sysusers`
  - A user `andrew` who belongs to `sysusers` as a secondary group
  - A user `susan` who also belongs to `sysusers` as a secondary group
  - A user `brad` who does not have access to an interactive shell on the system, and who is not a member of `sysusers`
  - `andrew`, `susan`, and `brad` should all have the password of `password`
- Create a collaborative directory `/shared/sysusers` with the following characteristics:

  - Group ownership of `/shared/sysusers` is `sysusers`
  - The directory should be readable, writable, and accessible to members of `sysusers`, but not to any other user. (It is understood that root has access to all files and directories on the system.)
  - Files created in `/shared/sysusers` automatically have group ownership set to the `sysusers` group

- Install the appropriate kernel update from `ftp://server1.example.com/pub/updates`. The following criteria must also be met:
  - The updated kernel is the default kernel when the system is rebooted
  - The original kernel remains available and bootable on the system

- Enable IP forwarding on your machine.

- Set up the default local print queue to forward jobs to the IPP (CUPS) print queue `station`x on `server1.example.com`, where x is your station number. Configure this printer as a "Generic – text-only" print queue.

  Note: The queue `station`x on `server1` dumps print jobs into the file `http://server1/printers/station`x. This file can be examined to confirm that you have configured the print queue correctly.

- The user `andrew` must configure a cron job that runs daily at `15:25` local time and executes
  - `/bin/echo hello`

- Bind to the NIS domain `RHCE` provided by 172.24.254.254 for user authentication. Note the following:
  - nisuser$x$ should be able to log into your system, where x is your station number, but will not have a home directory until you have completed the `autofs` requirement below
  - All NIS users have a password of `password`

- Configure `autofs` to automount the home directories of NIS users. Note the following:
  - `server1.example.com (172.24.254.254)` NFS-exports `/rhome/station`x to your system, where x is your station number
  - `nisuser`x's home directory is `server1.example.com:/rhome/station`x`/nisuser`x
  - `nisuser`x's home directory should be automounted locally beneath `/rhome` as `/rhome/nisuser`x
  - home directories must be writable by their users
  - While you are able to log in as any of the users `nisuser1` through `nisuser20`, the only home directory that is accessible from your system is nisuser$x$.

  Example: `station100` would configure the automounter such that `nisuser100`'s home directory `/rhome/nisuser100` gets mounted automatically upon login. The NFS share would be `server1.example.com:/rhome/station100/nisuser100`.

- Copy the file `/etc/fstab` to `/var/tmp`. Configure the permissions of `/var/tmp/fstab` so that:
  - the file `/var/tmp/fstab` is owned by the `root` user.
  - the file `/var/tmp/fstab` belongs to the group `root`.
  - the file `/var/tmp/fstab` should not be executable by anyone.
  - the user `andrew` is able to read and write `/var/tmp/fstab`.
  - the user `susan` can neither write nor read `/var/tmp/fstab`.
  - all other users (current or future) have the ability to read `/var/tmp/fstab`.

- Configure your system so that it is an NTP client of server1.example.com.

RHCE (Network Services and Security) Requirements

Perform all of the following steps. When you receive your results, these items will be reported as a single score identified as *RHCE*. You must score 70 percent on the RHCE requirements in order to earn RHCE.

You will note that some requirements specify that a service should not be available from the DNS domain `my133t.org` (that's m-y-one-three-three-t). All systems in that domain are in the `172.25.0.0/255.255.0.0` subnet, and all systems in that subnet are in `my133t.org`.

- Configure SSH access as follows:
  - `susan` has remote SSH access to your machine from within `example.com`
  - Clients within `my133t.org` should NOT have access to ssh on your system
- Configure POP3 email on your system according to these criteria:
  - `brad` must be able to retrieve email from your machine using POP3 from within `example.com`
  - Clients within the `my133t.org` domain should not have access to your POP3 service
- Configure FTP access on your system:
  - Clients within the `example.com` domain should have anonymous FTP access to your machine
  - Clients outside `example.com` should NOT have access to your FTP service
- Share the `/shared` directory via SMB:
  - Your SMB server must be a member of the `SMBGROUP` workgroup
  - The share's name must be `shared`
  - The `shared` share must be available to `example.com` domain clients only
  - The `shared` share must be browseable
  - `susan` must have read access to the share, authenticating with the same password `password`, if necessary
- Implement a web server for the site `http://stationX.example.com`, then perform the following steps:
  - Download `ftp://server1.example.com/pub/rhce/station.html`
  - Rename the downloaded file to `index.html`
  - Copy this `index.html` to the `DocumentRoot` of your web server
  - Do NOT make any modifications to the content of `index.html`
- Export your `/shared` directory via NFS to the `example.com` domain only.

  Note: because you will not have root access, you will not be able to directly mount your exported `/shared` *directory using your guest account on the system provided for testing. However, the automounter on the system has been configured such that it will automount your* `/shared` *directory under* `/home/guest`*x*`/nfs/station`*x, where x is your station number. Consequently, successful execution of* `ls /home/guest`*x*`/nfs/station`*x indicates that the automounter was able to automount your NFS share.*
- Configure an email alias for your MTA such that mail sent to `acctmgr` is received by the local user `andrew`.

- Configure SMTP mail service according to the following requirements:
  - Your mail server should accept mail from remote hosts and localhost
  - `susan` must be able to receive mail from remote hosts
  - Mail delivered to `susan` should spool into the default mail spool for `susan`, `/var/spool/mail/susan`.

Additional RHCE Requirements

Perform any two of the following steps. Completion of more than two will not result in extra credit. If time allows, you may wish to complete more than the minimum just in case one of your tasks does not meet our specifications. Please note that these additional items are part of your RHCE-specific score.

- Provide SSL-encapsulated IMAP access (IMAPS):
  - IMAPS must be available to `brad` from `example.com`
  - IMAPS must NOT be available to other networks or domains.
  - The SSL certificate for the IMAPS server must be created as follows:
    - Use the defaults for `Country`, `State`, `Locality`, and `Organization Name`
    - Set `Organizational Unit` to `GLS`
    - Set `Common Name` to `station`x`.example.com`
    - Set `Email Address` to `root@station`x`.example.com`
- Implement a web proxy server bound to port `8080`.
  - Clients within `example.com` should have access to your proxy server
  - Clients outside of `example.com` should NOT have access to your proxy server
- Extend your web server to include a virtual host for the site `http://www`x`.example.com/`, where x is your station number, then perform the following steps:
  - Set the `DocumentRoot` to `/var/www/virtual`
  - Download `ftp://server1.example.com/pub/rhce/www.html`
  - Rename the downloaded file to `index.html`
  - Place this `index.html` in the `DocumentRoot` of the virtual host
  - Do NOT make any modifications to the content of `index.html`
  - Ensure that `susan` is able to create content in `/var/www/virtual`

  Note: The original web site `http://stationX.example.com` must still be accessable. DNS resolution for the hostname `www`x`.example.com` is already provided by the name server on `server1.example.com`.