Apache Lab

Objectives:

- Setup web01
- Install httpd
- Configure httpd
- Join web01 to AD domain

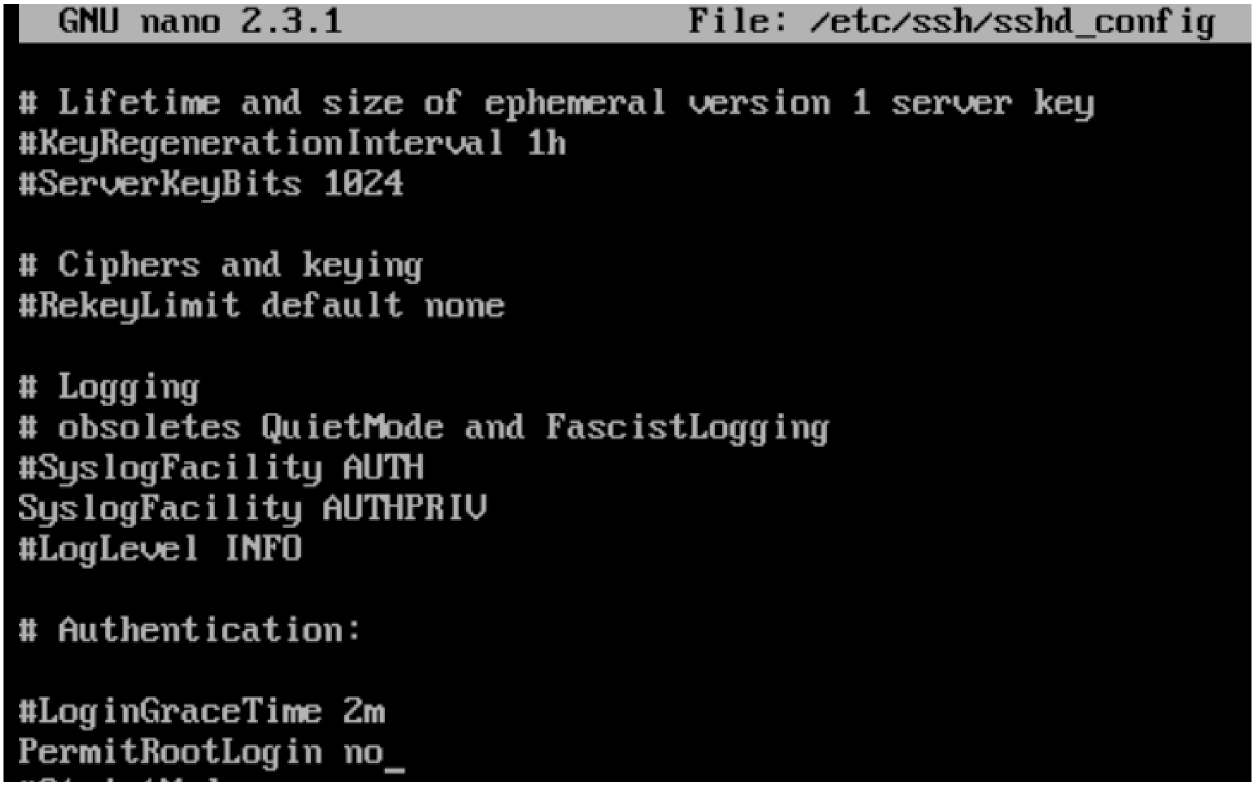
web01

- IP: 10.0.5.4
- Hostname: web01-yourname
- Named sudo user
- You know the rest

SSH Security

> 💣 CentOS and other Redhat based Linux servers ship with SSH turned on. This combined with a known "root" user who is able to attempt login remotely presents a security flaw that must be addressed by the systems administrator before the system is accessible over the internet. The typical solution involves explicitly preventing root from logging in via the sshd_config file.

Disable remote root ssh access within the PermitRootLogin no flag in /etc/ssh/sshd_config file.

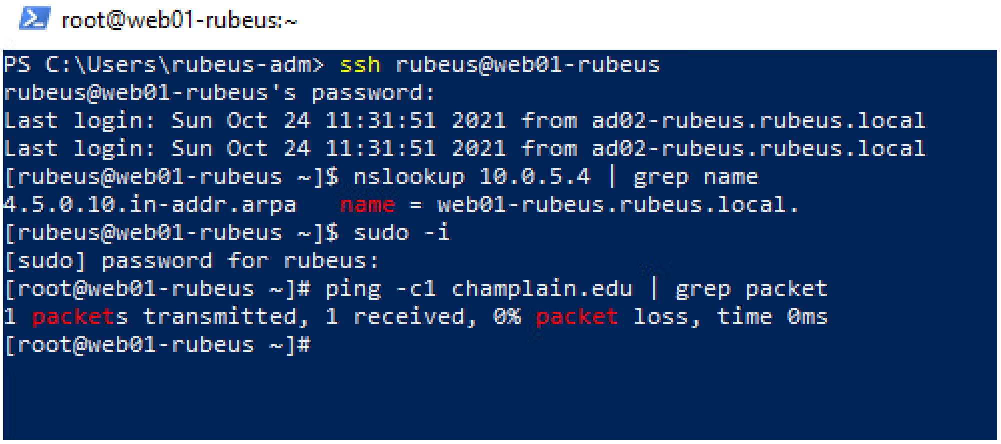


```
  GNU nano 2.3.1                    File: /etc/ssh/sshd_config

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no_
```

Restart sshd, logout and login again via SSH, so that your new hostname takes hold in the active session.

Deliverable 1. Using PuTTY or SSH from AD02 to Web01, provide a screenshot that shows:

- Your console login as a named sudo user and your elevation to root. The hostname should already be set. This implies that wks01 has network connectivity, you have downloaded PuTTY (you may need to work your way around the DHCP outage), and that you have properly configured DNS for web01.
- nslookup to 10.0.5.4, grepping the hostname to target results.
- ping to champlain.edu, grepping the string ‘packet’ to target results.



```
PS C:\Users\rubeus-adm> ssh rubeus@web01-rubeus
rubeus@web01-rubeus's password:
Last login: Sun Oct 24 11:31:51 2021 from ad02-rubeus.rubeus.local
Last login: Sun Oct 24 11:31:51 2021 from ad02-rubeus.rubeus.local
[rubeus@web01-rubeus ~]$ nslookup 10.0.5.4 | grep name
4.5.0.10.in-addr.arpa   name = web01-rubeus.rubeus.local.
[rubeus@web01-rubeus ~]$ sudo -i
[sudo] password for rubeus:
[root@web01-rubeus ~]# ping -c1 champlain.edu | grep packet
1 packets transmitted, 1 received, 0% packet loss, time 0ms
[root@web01-rubeus ~]#
```

Running Apache

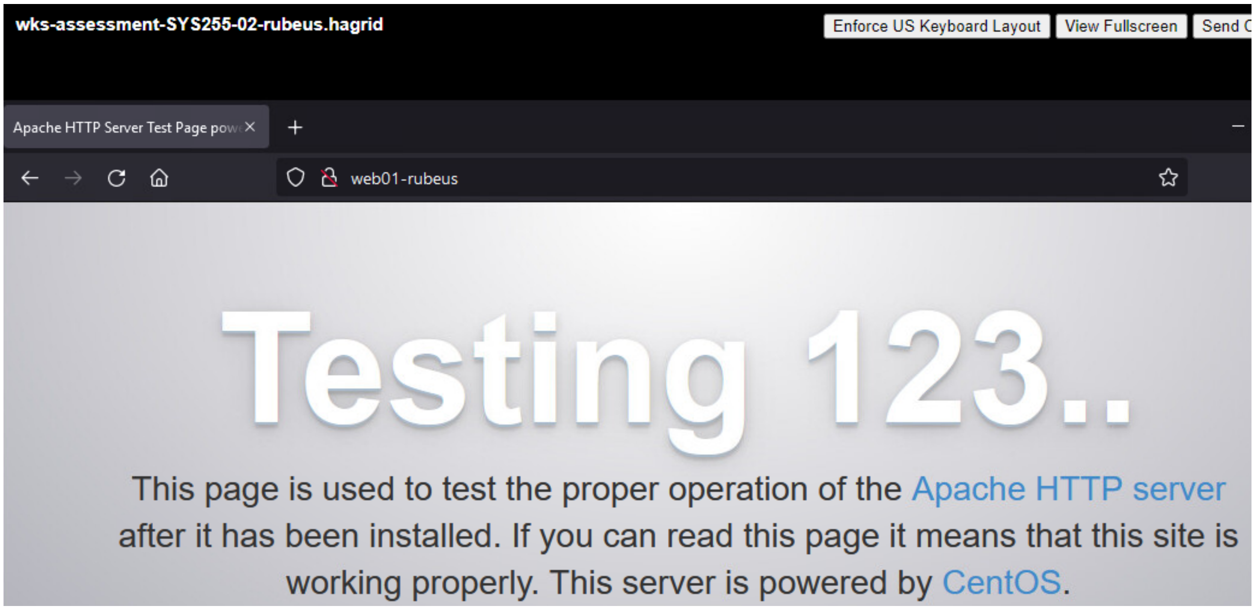
Using yum, install the httpd package.

Add ports 80/tcp & 443/tcp or HTTP and HTTPS defined services to your firewall permanently.

`Deliverable 2.  Provide the output of firewall-cmd --list-all`

Use systemctl to enable and start httpd.

`Deliverable 3.  Provide a screenshot showing wks browsing to web01 by hostname`



wks-assessment-SYS255-02-rubeus.hagrid
Enforce US Keyboard Layout
View Fullscreen
Send C
Apache HTTP Server Test Page pow
web01-rubeus

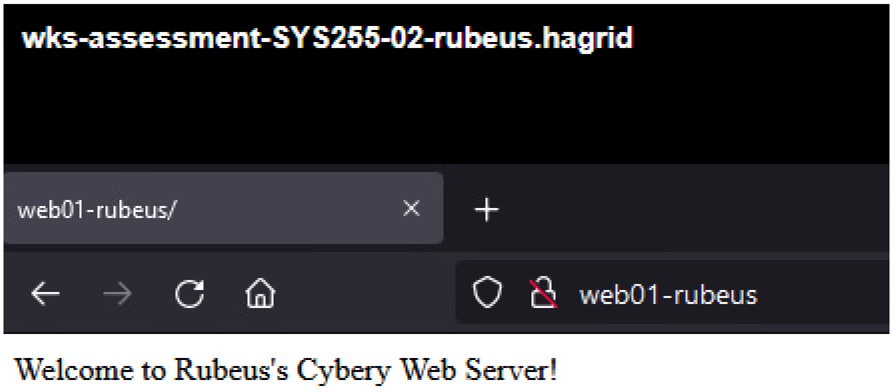
Testing 123..

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by CentOS.

Scroll down and take a look at the message to Administrators.

Go ahead and remove the welcome.conf file referenced in the message, and add a new file to /var/www/html/ called index.html. Add a welcome message including your hostname.

Deliverable 4. Provide a screenshot similar to the one below, displaying VM name and browse by hostname.



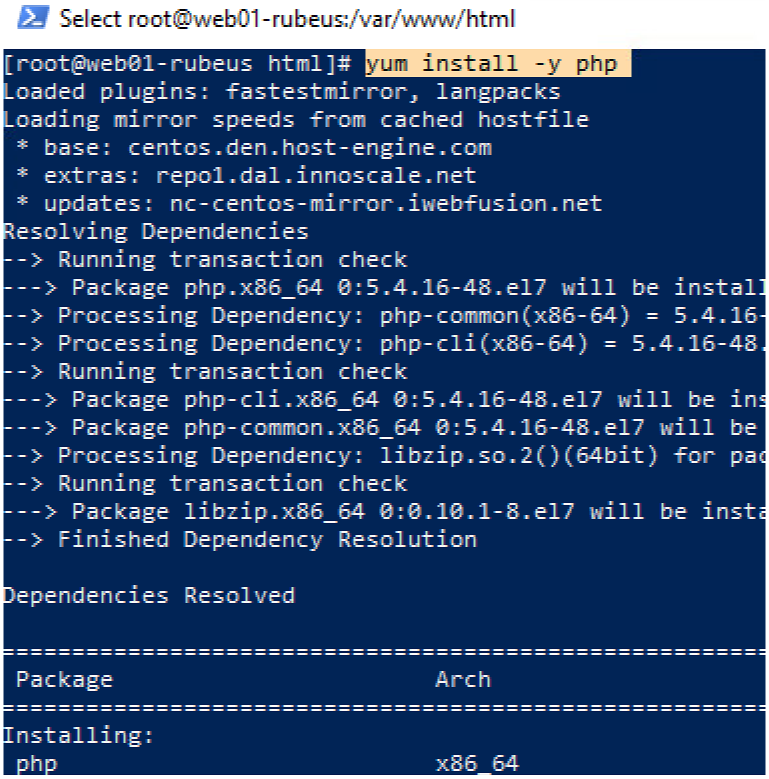
wks-assessment-SYS255-02-rubeus.hagrid

web01-rubeus

Welcome to Rubeus's Cybery Web Server!

PHP

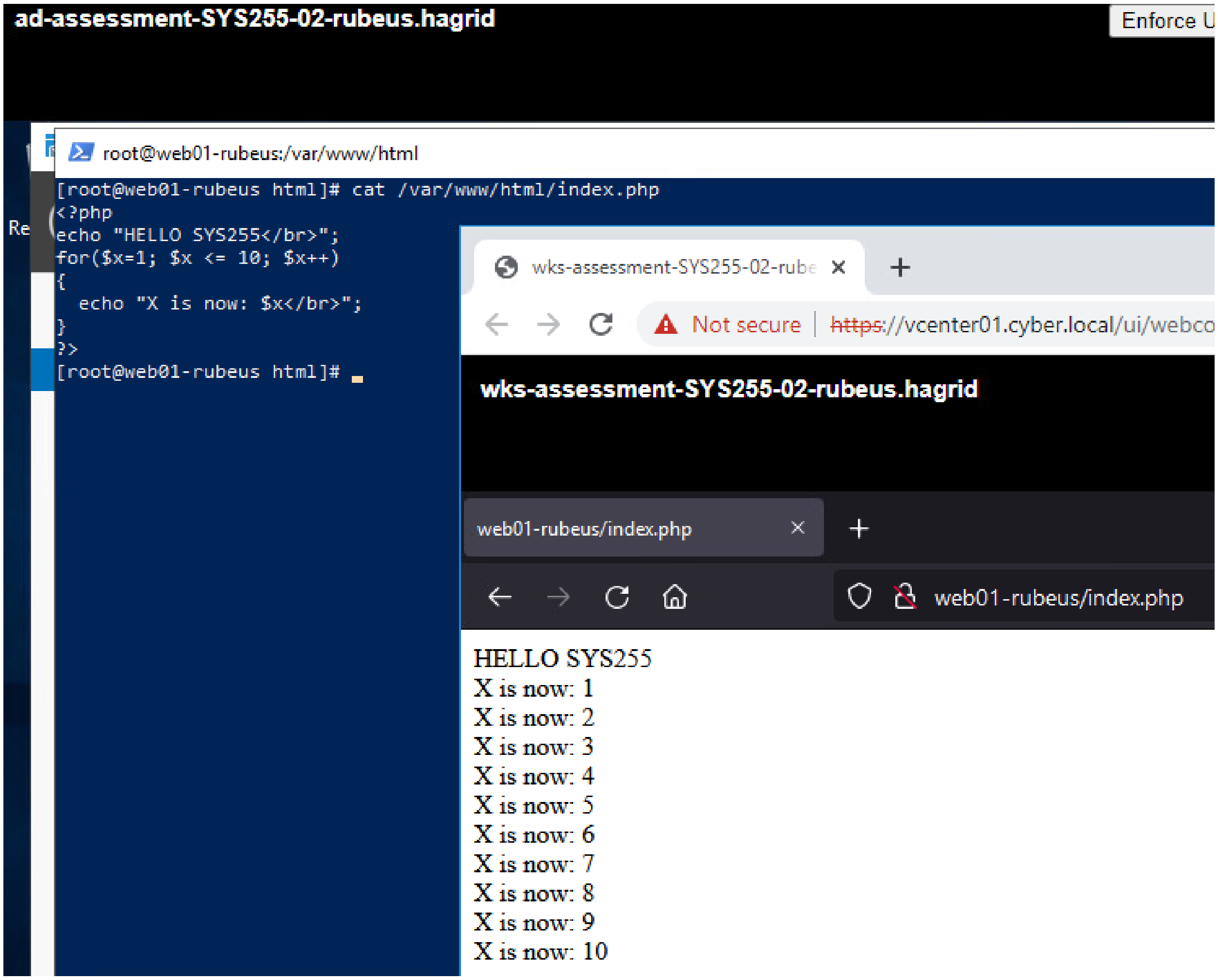
💡Static content is useful, but today's web applications are powered by dynamic data and rendered via scripting languages such as PHP. You will need to restart httpd after installing PHP.



Select root@web01-rubeus:/var/www/html

```
[root@web01-rubeus html]# yum install -y php
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.den.host-engine.com
 * extras: repo1.dal.innoscale.net
 * updates: nc-centos-mirror.iwebfusion.net
Resolving Dependencies
--> Running transaction check
---> Package php.x86_64 0:5.4.16-48.el7 will be install
--> Processing Dependency: php-common(x86-64) = 5.4.16-
--> Processing Dependency: php-cli(x86-64) = 5.4.16-48.
--> Running transaction check
---> Package php-cli.x86_64 0:5.4.16-48.el7 will be ins
---> Package php-common.x86_64 0:5.4.16-48.el7 will be
--> Processing Dependency: libzip.so.2()(64bit) for pac
--> Running transaction check
---> Package libzip.x86_64 0:0.10.1-8.el7 will be insta
--> Finished Dependency Resolution

Dependencies Resolved

=======================================================
 Package                        Arch
=======================================================
Installing:
 php                            x86_64
```

Deliverable 5. You can either use & modify the script shown below, or develop your own. Provide a screenshot showing both the PHP code and how it is rendered similar to the screenshot below. Make sure you access this site by hostname.


ad-assessment-SYS255-02-rubeus.hagrid
Enforce U
root@web01-rubeus:/var/www/html
wks-assessment-SYS255-02-rube
Not secure
https://vcenter01.cyber.local/ui/webco
wks-assessment-SYS255-02-rubeus.hagrid
web01-rubeus/index.php
web01-rubeus/index.php

```
[root@web01-rubeus html]# cat /var/www/html/index.php
<?php
echo "HELLO SYS255</br>";
for($x=1; $x <= 10; $x++)
{
  echo "X is now: $x</br>";
}
?>
[root@web01-rubeus html]#
```

```
HELLO SYS255
X is now: 1
X is now: 2
X is now: 3
X is now: 4
X is now: 5
X is now: 6
X is now: 7
X is now: 8
X is now: 9
X is now: 10
```

Linux Domain Join

We are currently administering systems using multiple credential stores. Each Linux system has their own Local credentials (/etc/passwd and /etc/shadow), while Windows has both Local accounts and centralized AD domain accounts. We are going to leverage Windows ADDS to consolidate our future Linux accounts.

Install realmd

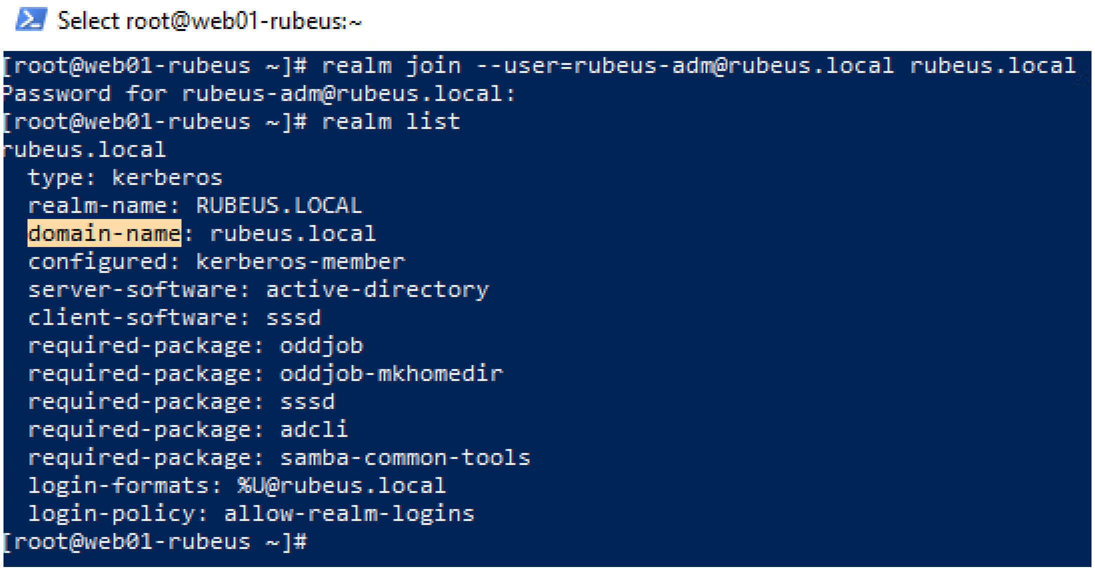
💡The ability to easily join a Linux system to a Windows Active Directory Domain is a huge win for centralized account management and security. We are going to join our web01 server to yourname.local domain.

```
sudo yum install -y realmd samba samba-common oddjob oddjob-mkhomedir
sssd
```

Join the domain

> 💡Note, if your time is not consistent across Windows and Linux, then you will likely have problems. Time zones can sometimes be a problem. So best resolve this now.

```
realm join --user=your-domain-admin-username@yourdomain.local yourdomain.local
realm list
```

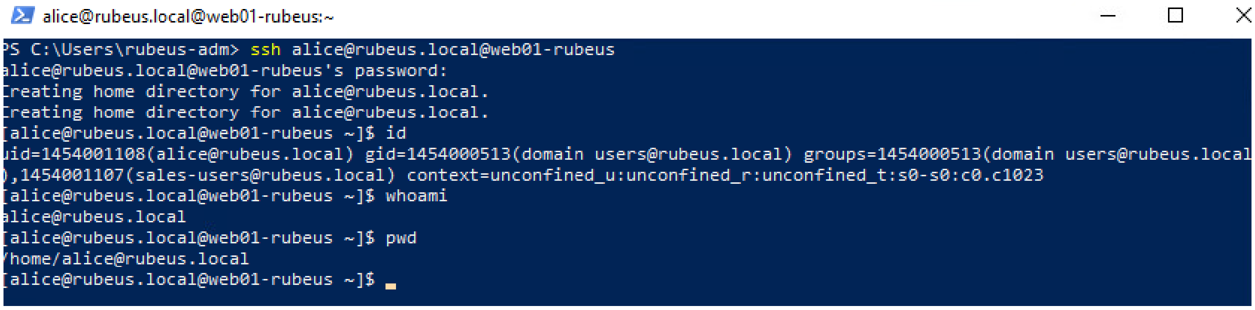


Select root@web01-rubeus:~

```
[root@web01-rubeus ~]# realm join --user=rubeus-adm@rubeus.local rubeus.local
Password for rubeus-adm@rubeus.local:
[root@web01-rubeus ~]# realm list
rubeus.local
  type: kerberos
  realm-name: RUBEUS.LOCAL
  domain-name: rubeus.local
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@rubeus.local
  login-policy: allow-realm-logins
[root@web01-rubeus ~]#
```

Logout and login again as an AD Domain Named user.

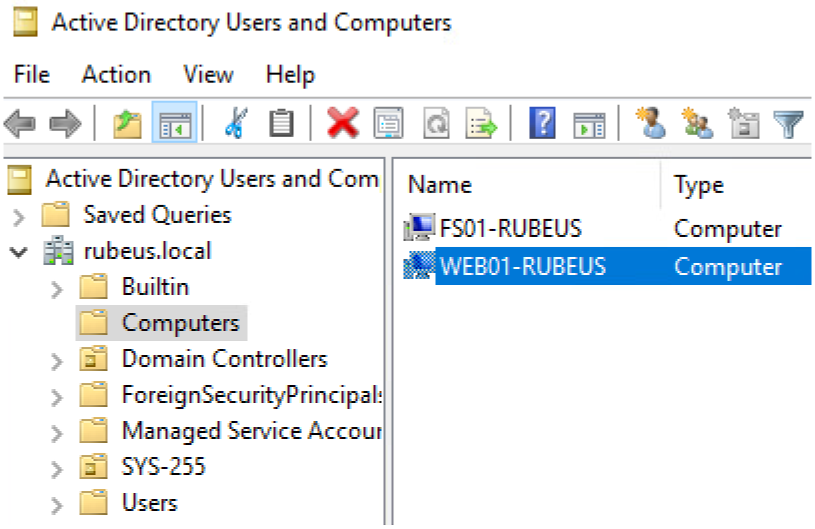
`Deliverable 6. Provide a screenshot showing a domain login via PuTTY or SSH to web01.  Issue the id, whoami and pwd commands.`



alice@rubeus.local@web01-rubeus:~

```
PS C:\Users\rubeus-adm> ssh alice@rubeus.local@web01-rubeus
alice@rubeus.local@web01-rubeus's password:
Creating home directory for alice@rubeus.local.
Creating home directory for alice@rubeus.local.
[alice@rubeus.local@web01-rubeus ~]$ id
uid=1454001108(alice@rubeus.local) gid=1454000513(domain users@rubeus.local) groups=1454000513(domain users@rubeus.local
),1454001107(sales-users@rubeus.local) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[alice@rubeus.local@web01-rubeus ~]$ whoami
alice@rubeus.local
[alice@rubeus.local@web01-rubeus ~]$ pwd
/home/alice@rubeus.local
[alice@rubeus.local@web01-rubeus ~]$
```

Deliverable 7. The realm join operation should add web01 to Active Directory Users and Computers on the Domain Controller. Provide a screenshot similar to the one below:



- Active Directory Users and Com
  - Saved Queries
  - rubeus.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal
    - Managed Service Accour
    - SYS-255
    - Users

Name	Type
FS01-RUBEUS	Computer
WEB01-RUBEUS	Computer

Deliverable 8. Provide a URL to a tech log entry on the Linux Domain Join.

Deliverable 9. Provide a URL to a tech log entry on Apache installation and firewall-cmd configuration.