SYS-255 || Final Project

💡Congratulations on making it to the last stretch of the course! Up to this point, we have covered a wide range of topics and hands-on labs to learn local area networking and system administration of Linux and Windows workstation and server systems.

List of topics we have covered that you now have practice with. Some have appeared more than once (and will continue to reappear throughout Champlain and beyond)

- Open Source Firewall
- DNS
- Active Directory Domain Services
- Navigating Linux
- Windows and Linux DHCP
- VMware Workstation & VMware vSphere
- Windows Server Core
- Windows File Services
- Linux Apache
- Bash & Powershell Scripting
- Automation & Troubleshooting

The goal of this final project is to give you a chance to select a topic you wish to dive more in depth on involving networking & system administration.

This project will involve a fair amount of self-research, trial & error, and documentation.

It's also a great talking point for future interactions with professionals. "Hey I did this project on X while at Champlain and can figure out and troubleshoot things myself based on the knowledge I have".

*You will create a demo video including **every** team member. This demonstration will be used to assess whether your project actually worked and will be used in grading.

Deliverables

1: First, select a topic and submit the topic to the Final Project Proposal Assignment.

Rules

- Select a topic from the *Topics* list below or propose a new one.
- Topics are first come, first serve. The time of submission in the assignment is used as the selection time.

- Teams can be made of up to 3 people if the proposed topic is excessively difficult.
- New topics that are proposed can be rejected if they are deemed too easy.

2. The project itself:

Description

What is the goal of your project in a few sentences?

Overview

Describe what systems and configurations are involved with your project. What VMs you used, how they talk to each other at a high level, and any applicable test methodology. Logical topologies are normally a plus.

References

You will be using outside resources than the labs since most of the topics expand on what we have done thus far. Please cite your references here.

Build Documentation

The body of the project. How are things set up? How did you get from point A to point B (the project description). This includes descriptions of what was done and specifics including but not limited to commands entered, files used, system networking settings, etc.

Completion Test

Show via video, your project working. It’s important here to display system names or uniquely identifiable info from VMware Workstation or vSphere so the instructor knows what system is what.

- Record this!

Discussion

Descriptions of difficulties you faced, how you troubleshooted them, and what the outcome was.

Topics

- Your own idea
    - Generally speaking, your own idea should take approximately 12 hours to complete. 4x4x4. 4 hours of research, 4 hours of implementation, and 4 hours of documentation.

- Sub-domains
    - Create a new Domain with a subdomain in Microsoft Active Directory with a file share on the master domain. Find a way of creating a file share that is only shared with specific groups on the subdomain using a one-way trust scenario.

- Advanced Group Policy
    - Create a more advanced group policy setup to include a customized start menu, automatically installing an application, setting up a file share via a logon script, and application allow listing to only allow essential Windows programs and things in the C:\Tools\ folder to run. Include logs.

- DNS - Linux
    - Create a BIND DNS server on Linux that provides what your Windows DNS server currently does. Include logs and Wireshark.

- Image Deployment
    - Deploy and configure Windows Deployment Services (WDS) or Linux PXE boot solution to build a system over the network. Include logs and Wireshark.

- Alternative Virtualization - Linux
    - Recreate the Assessment 1 environment on KVM, Proxmox or other hypervisors.

- Alternative Virtualization - Windows
    - Recreate the Assessment 1 environment on the Hyper-V hypervisor.

- Certificate Authority
    - Create your own Windows-based CA and use the certificate with a local web server. Include logs and Wireshark.

- Cloud Hosting
    - Create a CentOS machine on Azure or AWS and host a web service that is accessible from home. (free trials/options are available).

- SSH x509
    - Secure Linux SSH remote access with x509 certificates and domain user logins from a Windows Domain Controller. Include logs and Wireshark.

- Advanced SSH Security
    - Secure SSH on Linux with a hardened configuration, two factor authentication, and intrusion prevention (Fail2ban or similar). Include logs and Wireshark.

- Port Knocking
    - Secure SSH on Linux with prespecified closed ports, which open based upon a correct sequence. Include logs and Wireshark.

- Wordpress Web Server
    - Install and configure a Windows IIS web server using HTTPS to host Wordpress (with a legitimate amount of content). Include logs and Wireshark.

- DIY Firewall
    - Create a dual-homed DIY firewall to replace pfsense. Include logs and Wireshark.

- Samba Server
    - Replace AD01 with a Linux Samba server and a file share to test. Include logs and Wireshark.

- Windows Domain Controller High Availability

  - Setup a domain with multiple domain controllers and configure high availability via replication and failover with a dry-run test.

- Remote Desktop Services (RDS Server)
  - Enable remote desktop services (RDS) on a Windows server and publish Putty and Chrome as published applications to a Windows 10 workstation. Include logs and Wireshark.

- Alternative Linux Web Server
  - Replace Apache with NGiNX on Blog01 and run an open source CMS (content management system) - Ghost or Wordpress. Include logs and Wireshark.

- System Monitoring - Linux
  - Create a method of notifying you of when root logs in, the system drive falls outside of a % available range, the CPU becomes overworked for X amount of time, and when the network interface is receiving more than X amount of packets per second. Note: you can simulate these things happening with various tools/scripts/etc. Additional note: SMTP is involved for email notifications. Include logs and Wireshark.

- System Monitoring - Windows
  - Create a method of notifying you of when a domain administrator logs in, the system drive falls outside of a % available range, the CPU becomes overworked for X amount of time, and when the network interface is highly utilized. Note: you can simulate these things happening with various tools/scripts/etc. Include logs and Wireshark. Additional note: SMTP is involved for email notifications.

- System Logging - Linux
  - Create a Linux Syslog server to forward important logs from two other VMs to the syslog server. Include Wireshark.

- System Logging - Windows
  - Create a Windows Syslog server to forward important logs from two other VMs to the syslog server. Include Wireshark.

- Security - Windows

    - Create an IR script to secure a Windows server from a fresh installation. (User accounts, permissions, firewalling, services, attack surface limiting, logging, etc). Include logs and Wireshark.

- Security - Linux
    - Create an IR script to secure a Linux server from a fresh installation. (User accounts, permissions, firewalling, services, attack surface limiting, logging, etc). Include logs and Wireshark.

- Apache or NGINX Web Application
    - Create a basic web application on Linux using PHP/MYSQL/Apache (LAMP Stack). PHP templates can be used on this - It’s not a programming class, however Sysadmin-Programming-Scripting have gray areas that intertwine with each other.

- Open Source Backups - Rsync + SSH
    - Configure an open source backup solution to backup one Linux server to another using Rsync and SSH. Include logs and Wireshark.

- Hugo or other static web frameworks
    - Using hugo, import and recreate your tech journal. Include logs and Wireshark.