**Network Administration Final Lab Report**

**Student:** Hussein Reslan  
**ID:** 1122037  
**Course:** SECU316 System and Network Administration  
**Instructor:** Hisham Yassine  
**Date:** 15-May-2025

**Table of Contents**

1. Introduction & Objectives
2. Software & Tools Used
3. Network Topology
4. Step-by-Step Configuration
   * 4.1 GNS3 & VM Setup
   * 4.2 Windows Server Configuration
     + 4.2.1 Active Directory Domain Services
     + 4.2.2 DHCP Server & Failover
     + 4.2.3 DHCP Reservations
     + 4.2.4 Group Policy Implementation
     + 4.2.5 SNMP Monitoring
     + 4.2.6 Automated Backups
   * 4.3 Ubuntu Server Configuration
     + 4.3.1 Apache Web Server & HTTPS
     + 4.3.2 SSH Hardening
     + 4.3.3 UFW Firewall & Geo-blocking
     + 4.3.4 SNMP Monitoring
     + 4.3.5 Automated Backups
   * 4.4 VLAN & Inter-VLAN Routing(Canceled)
   * 4.5 Network Security & Testing
   * 4.6 Monitoring & Troubleshooting
5. Conclusion

**1. Introduction & Objectives**

This project demonstrates the end-to-end deployment and hardening of a simulated enterprise network using GNS3. The lab covered configuring Active Directory, DHCP failover, advanced firewalling, secure Apache web and SSH services, automated backups, SNMP monitoring, and in-depth troubleshooting. The objective was to reinforce hands-on skills in both Windows Server and Ubuntu Linux administration and to develop a secure, resilient infrastructure.

**2. Software & Tools Used**

* GNS3 (latest version)
* Windows Server 2022
* Widows 10 Client
* Ubuntu Server 22.04 LTS
* Wireshark
* Putty/SSH Client

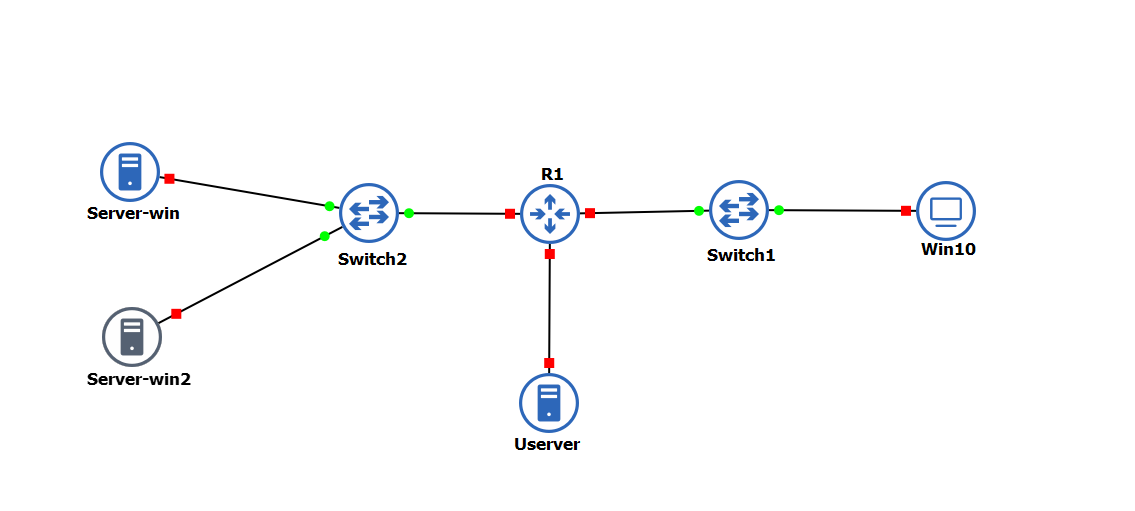
**3. Network Topology**

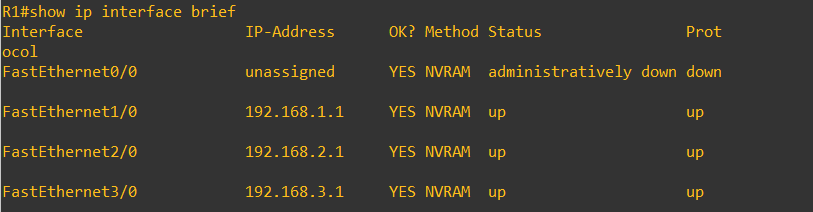
**Devices:**

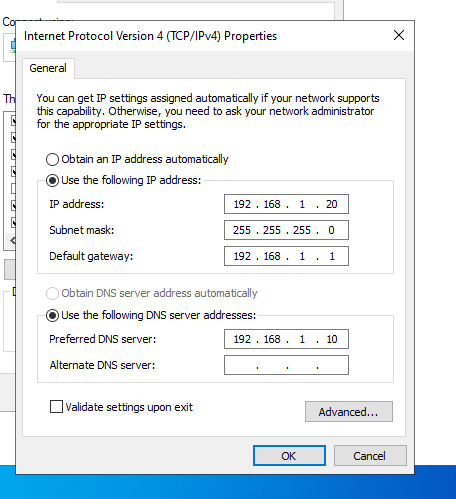
* Cisco Router
* Layer 2 Switch
* Windows Server (192.168.1.10)
* Windows Server-2 (192.168.1.20)
* Ubuntu Server (192.168.3.10)
* 1 x PCs (DHCP clients, 192.168.2.x)

**IP Addressing Scheme:**

| **Device** | **IP Address** | **Gateway** |
| --- | --- | --- |
| Router | 192.168.1.1-192.168.2.1-  192.168.3.1 | - |
| Windows Server | 192.168.1.10 | 192.168.1.1 |
| Ubuntu Server | 192.168.3.10 | 192.168.3.1 |
| Windows Server-2 | 192.168.1.20 | 192.168.1.1 |
| PC1 | DHCP | 192.168.2.55 |
|  |  |  |

****





A computer screen with text and numbers

AI-generated content may be incorrect.

Ubuntu Ip Config:   
sudo nano /etc/netplan/01-netcfg.yaml

**4. Step-by-Step Configuration**

**4.1 GNS3 & VM Setup**

* Installed GNS3 and imported both Windows Server and Ubuntu VMs.
* Allocated 2GB+ RAM for Windows, 1GB+ for Ubuntu.
* Built topology with router, switch, servers, and PCs.
* Connected all devices as per addressing plan.

**A screenshot of a computer

AI-generated content may be incorrect.**

A screenshot of a computer

AI-generated content may be incorrect.

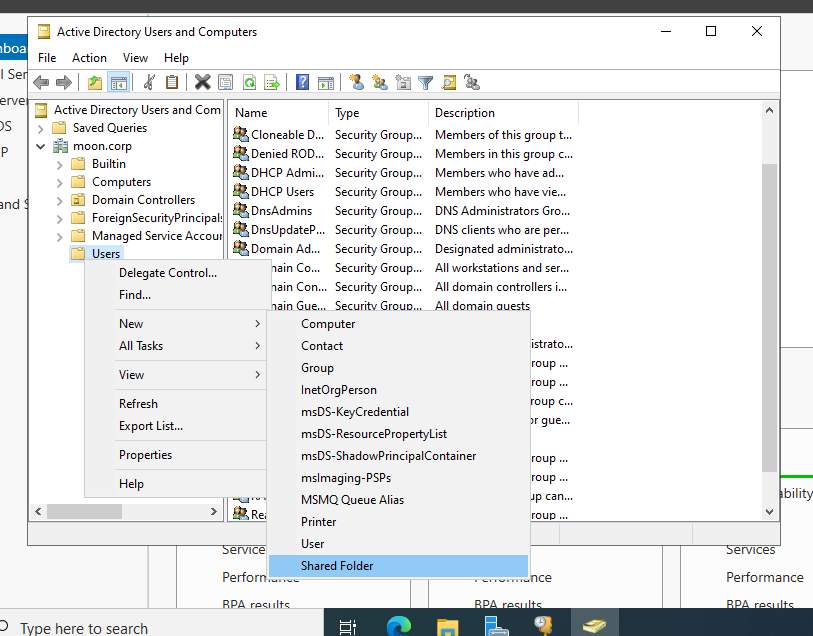
A screenshot of a computer

AI-generated content may be incorrect.

**4.2 Windows Server Configuration**

**4.2.1 Active Directory Domain Services (AD DS)**

* Installed the AD DS role from Server Manager.
* Promoted the Windows Server to Domain Controller (moon.corp).
* Created users admin and user: Jhon Smith.
* Created and organized OUs for future GPO targeting.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Key Steps:**

* Server Manager > Add roles and features > AD DS
* dcpromo to promote server as domain controller
* Created users via Active Directory Users and Computers

**4.2.2 DHCP Server & Failover**

* Installed DHCP role and authorized the server.
* Created DHCP scope: 192.168.2.50-100, gateway: 192.168.2.1, DNS: 192.168.1.10
* Set up a second Windows Server (192.168.1.20) for DHCP failover.
* Configured failover with load balancing (50/50), set MCLT and switchover intervals.
* Tested failover by stopping the main server’s DHCP service and verifying client renewal.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

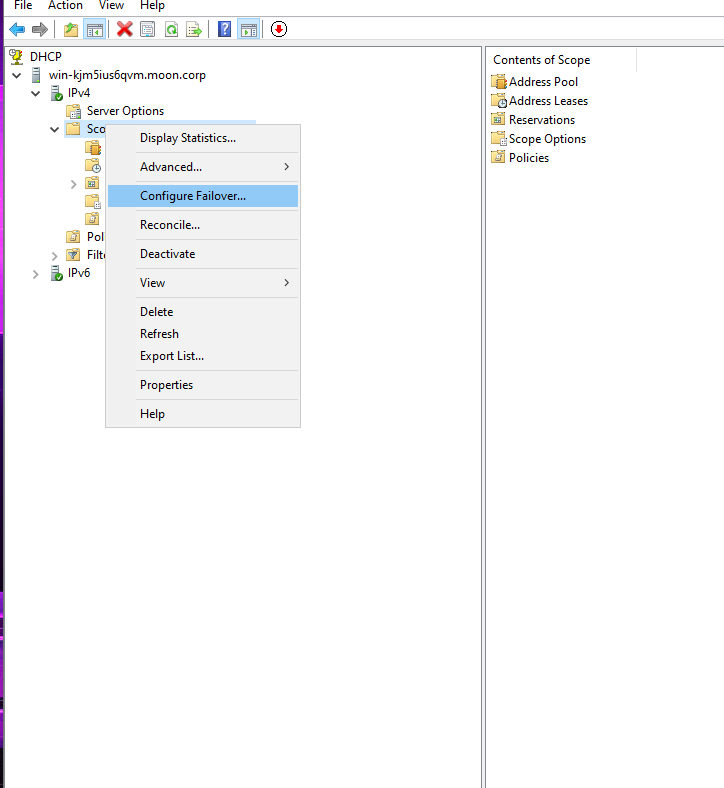
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

**Commands/Actions:**

* Add roles and features > DHCP Server
* Authorize DHCP
* Configure Failover via DHCP console
* Client: ipconfig /release + ipconfig /renew (should get IP from backup server)

**4.2.3 DHCP Reservations**

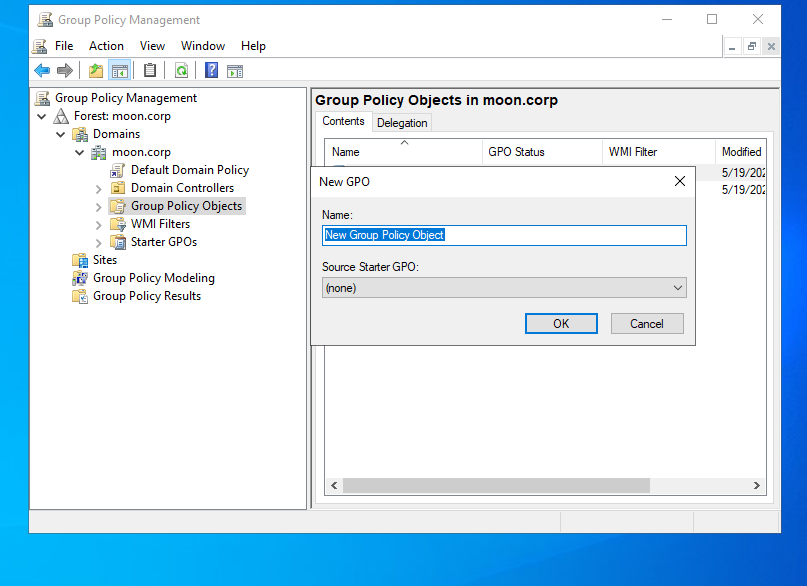
* Added reservations for critical clients using MAC address in the DHCP MMC.
* Verified by rebooting reserved client and checking assigned IP.

A computer screen shot of a computer screen

AI-generated content may be incorrect.

**4.2.4 Group Policy Implementation**

* Created and linked a GPO for workstation security: min password length 12, lockout after 5 attempts, 30 min lockout, and USB storage block.
* Linked the GPO to the correct OU.
* Used Group Policy Management Console (GPMC) for configuration.
* On a client, tested password policy enforcement and USB block.



A computer screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Commands/Actions:**

* gpmc.msc to open GPMC
* Edit GPO settings: Password Policy, Account Lockout, Device Installation Restrictions

**4.2.5 SNMP Monitoring**

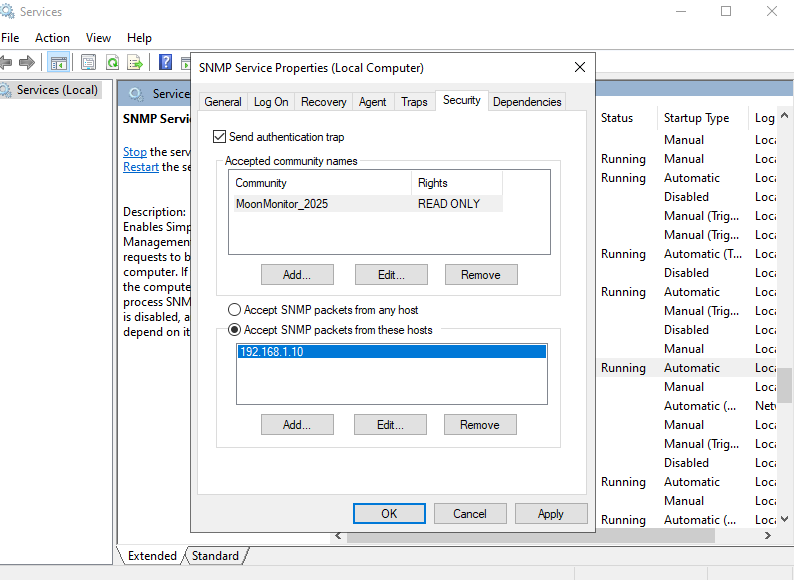
* Installed SNMP Service via Server Manager.
* Set complex community string and allowed management stations.
* Used an SNMP walk tool from management PC to confirm communication.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



**4.2.6 Automated Backups**

* Installed Windows Server Backup feature.
* Used Windows Server Backup (wbadmin.msc) to schedule daily backups to network share (\\192.168.1.20\Backups).
* Selected System State and all critical volumes.
* Verified backup completion and presence on share.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Commands/Actions:**

* wbadmin.msc to open GUI
* Or PowerShell: wbadmin get schedule, wbadmin start backup -backupTarget:...

**4.3 Ubuntu Server Configuration**

**4.3.1 Apache Web Server & HTTPS**

* Updated package lists: sudo apt update && sudo apt upgrade
* Installed Apache: sudo apt install apache2
* Enabled HTTPS:
  + sudo apt install openssl
  + sudo a2enmod ssl && sudo systemctl restart apache2
  + Created self-signed cert, updated /etc/apache2/sites-available/default-ssl.conf, enabled site.
* Hardened with security headers and ModSecurity: sudo apt install libapache2-mod-security2

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer screen

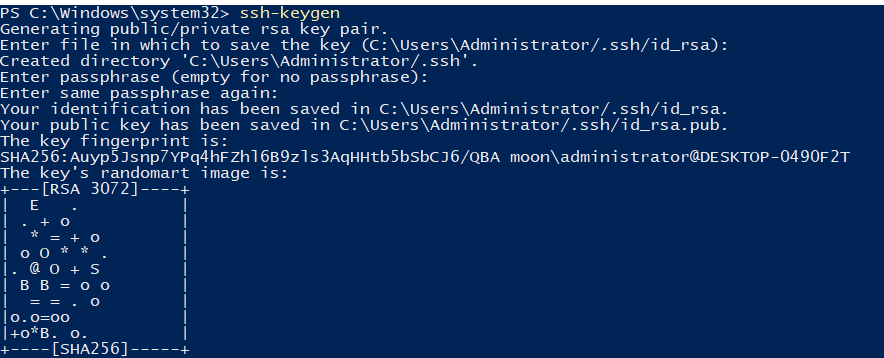
AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

**4.3.2 SSH Hardening**

* Edited /etc/ssh/sshd\_config: enabled PubkeyAuthentication yes, set PasswordAuthentication no.
* Added user’s public key to ~/.ssh/authorized\_keys:
  + mkdir -p ~/.ssh && chmod 700 ~/.ssh
  + nano ~/.ssh/authorized\_keys (paste pubkey)
  + chmod 600 ~/.ssh/authorized\_keys
* Restarted SSH: sudo systemctl restart ssh
* Verified key-only login and password denial.



A computer screen shot of a blue screen

AI-generated content may be incorrect.

A computer screen with a black screen

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.

A computer screen with blue text

AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**4.3.3 UFW Firewall & Geo-blocking**

* Enabled UFW: sudo ufw enable
* Allowed only required ports (SSH, HTTP, HTTPS):
  + sudo ufw allow 22/tcp
  + sudo ufw allow 80/tcp
  + sudo ufw allow 443/tcp
* Set default deny: sudo ufw default deny incoming
* Enabled rate limiting for SSH: sudo ufw limit 22/tcp
* (Optional) Installed geoip module and configured country blocking.
* Showed blocked rules: sudo ufw status verbose (DENY entries)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



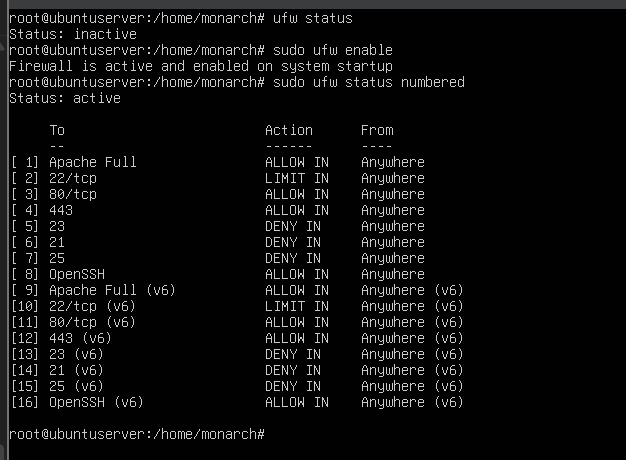


A black screen with white text

AI-generated content may be incorrect.

A black screen with white text

AI-generated content may be incorrect.

Allowed and Denied Ports on ufw:  


Adding Geo Ip rules using iptables:  
A computer screen with white text and blue text

AI-generated content may be incorrect.

A screen shot of a computer screen

AI-generated content may be incorrect.

**4.3.4 SNMP Monitoring**

* Installed SNMP daemon: sudo apt install snmpd
* Edited /etc/snmp/snmpd.conf for community string and access.
* Restarted SNMP: sudo systemctl restart snmpd
* Used snmpwalk to test: snmpwalk -v2c -c <community> localhost

A computer screen with white text

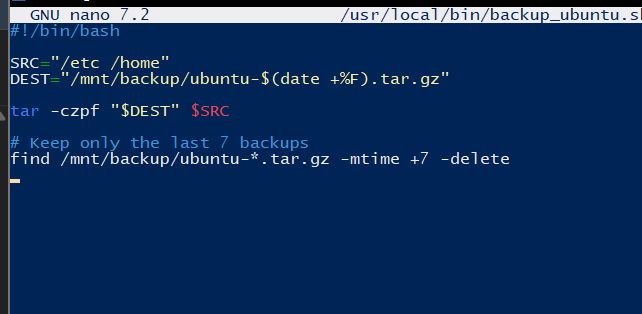
AI-generated content may be incorrect.

A computer screen shot of a black screen

AI-generated content may be incorrect.

**4.3.5 Automated Backups**

* Installed CIFS utils: sudo apt install cifs-utils
* Created mount point and mounted Windows share:
  + sudo mkdir -p /mnt/backup
  + sudo mount -t cifs -o username=Administrator,password=... //192.168.1.20/Backups/Ubuntu /mnt/backup
* Wrote backup script /usr/local/bin/backup\_ubuntu.sh:
  + tar -czpf /mnt/backup/ubuntu-$(date +%F).tar.gz /etc /home
  + find /mnt/backup/ubuntu-\*.tar.gz -mtime +7 -delete
* Scheduled with cron: sudo crontab -e:
  + 0 2 \* \* \* /usr/local/bin/backup\_ubuntu.sh
* Tested manual and scheduled runs, confirmed backup file on Windows share.



A screenshot of a computer

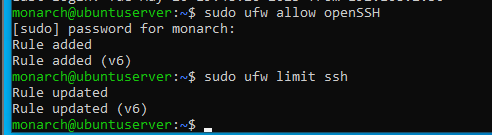
AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

**4.5 Network Security & Testing**

* Used Windows Defender Firewall to block unnecessary ports.
* Used UFW on Ubuntu to enforce policy.
* Used Wireshark to capture DHCP, HTTP, SSH traffic:
  + ipconfig /release / ipconfig /renew for DHCP
  + Opened web server and SSH session for capture
* Verified blocked connections failed as expected.



A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

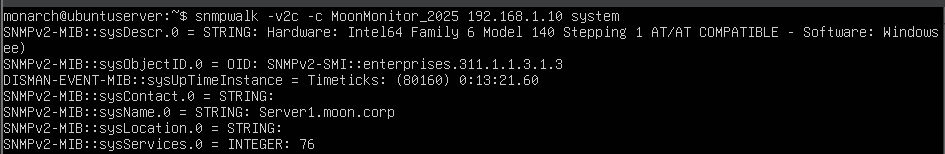
AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

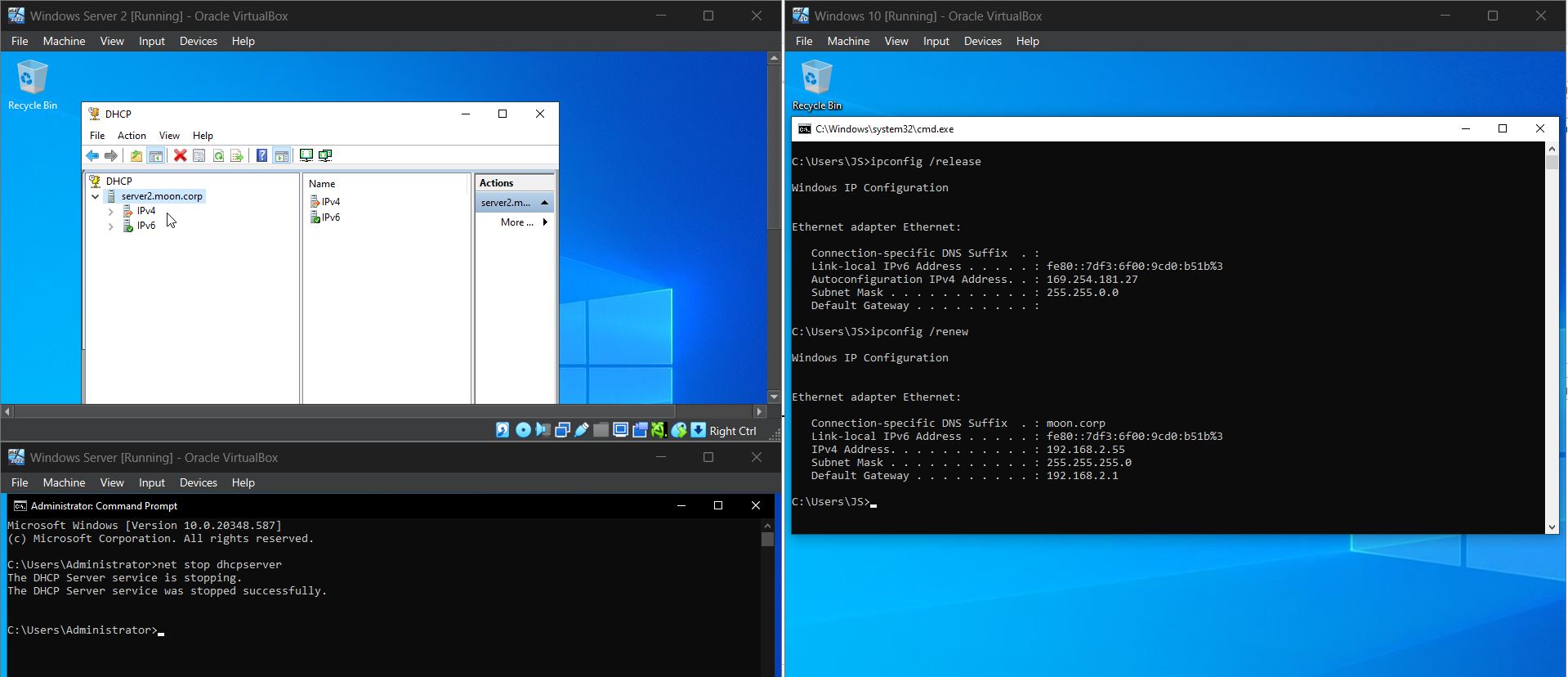
**4.6 Monitoring & Troubleshooting**

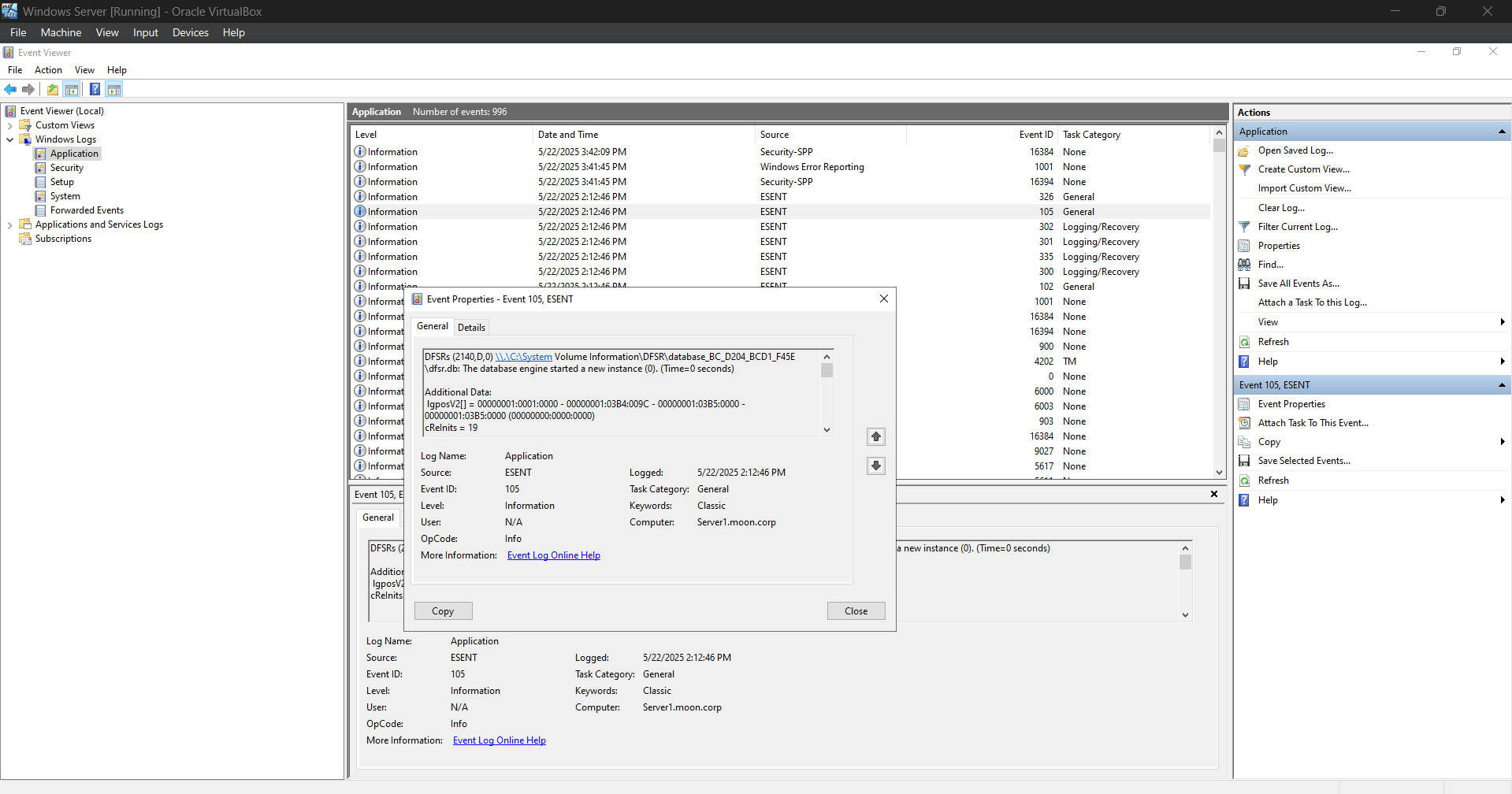
* Demonstrated SNMP polling from management station.
* Tested failover by shutting down main DHCP server and forcing client renewals.
* Used Windows Event Viewer and Linux logs for troubleshooting.

****

A screenshot of a computer

AI-generated content may be incorrect.





**5. Conclusion**

This project provided practical, in-depth experience in designing, configuring, securing, and monitoring a full-featured enterprise network using both Windows and Linux systems. All required services were deployed, tested, and validated, with detailed troubleshooting for advanced features like DHCP failover and automated cross-platform backups. The result is a secure, robust network following industry best practices.