**Splunk Lab Environment**  
**1. VMware Configuration**

* VMware was installed on a server and configured with a **bridged network connection** to the internal network

**2. Host and Virtual Machines**

* A Windows Server 2021 VM was deployed to host Splunk Enterprise.
* A Windows 10 VM (with bridged connection) and 11 physical Windows 11 workstations were used as data sources.

**3. Splunk Enterprise Setup (Server)**

* Splunk Enterprise installed on Windows Server 2021.
* Ports 8000 and 9997 were opened for inbound connections in Windows Firewall.
  + Port 8000 → Splunk Web Interface access
  + Port 9997 → Receiving forwarded logs from clients

**Server**A screenshot of a computer

AI-generated content may be incorrect.**A screenshot of a computer

AI-generated content may be incorrect.**  
  
**4. Splunk Universal Forwarders (Clients)**

* Installed on both the Windows 10 VM and the Windows 11 workstations.
* Outbound (egress) firewall rules allowed traffic to ports 8000 and 9997.
  + Port 8000 → Access the Splunk web interface
  + Port 9997 → Forward logs to the Splunk instance

**Clients**  
**A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.**  
  
**5. Log Forwarding Configuration**

* Configuration files (inputs.conf and outputs.conf) on each forwarder were edited to send Security and System logs.
* Both log types were indexed under wineventlog.

A screenshot of a computer program

AI-generated content may be incorrect. A screenshot of a computer program

AI-generated content may be incorrect.