SYSTEMS DOCUMENTATION

*ZHENGZHENG LI*

# SYSTEM 1 Windows Server 2022 (Evaluation)

**IP Address:** 192.168.2.102

**Services Installed:** File and Storage Services (SMB), WinRM

**Tasks taken to secure the server and services installed:**

* Configured Windows Firewall to explicitly allow only SMB (TCP/445) and WinRM (TCP/5985); all other ports are blocked.
* Disabled SMBv1 and applied all security patches.
* Enforced password policies and enabled audit logging for login attempts.

# SYSTEM 2 Fedora 41 (Workstation Live)

**IP Address:** 192.168.2.105

**Services Installed:** systemd-resolved (DNS resolver), LLMNR

**Tasks taken to secure the server and services installed:**

* Disabled and removed unnecessary services (Avahi-daemon).
* Configured firewalld with a default deny policy for all incoming connections.
* Enabled SELinux in enforcing mode for stronger isolation.

# SYSTEM 3 Ubuntu 24.04.2 LTS (Server)

**IP Address:** **192.168.2.103**

**Services Installed:** OpenSSH (TCP/22)

**Tasks taken to secure the server and services installed:**

* Configured UFW firewall to allow only SSH (TCP/22) and explicitly block all other ports.
* Disabled root login via SSH and enforced key-based authentication.
* Enabled unattended-upgrades for automatic security patches

# SYSTEM 4 Windows 10 (Client VM)

**IP Address:** 192.168.2.108

**Services Installed:** Core Windows client services. No network-facing services are exposed.

**Tasks taken to secure the server and services installed:**

* Configured Windows Firewall to block all unsolicited inbound connections, as appropriate for a client device.
* Enabled Windows Defender Antivirus with real-time protection.
* Applied latest Windows Updates and enforced strong password policy.