Configuration Testing Report - Employee Workstation (Haseeb Ali, Director Admin)

1. Purpose of This Report

This report details the findings from a limited configuration assessment performed on the workstation of Haseeb Ali, Director Admin at Connected Pakistan. The objective was to evaluate the security posture of a typical employee endpoint, focusing on key security configurations and controls. This assessment was conducted with explicit permission and aimed to identify common misconfigurations that could pose a security risk.

2. Key Areas of Assessment

The assessment focused on:

- Operating System Firewall Status and Rules
- Antivirus/Endpoint Detection and Response (EDR) Status
- Software Update Mechanisms
- User Account Security (Local Administrator Privileges, Password Policy Adherence)

3. Configuration Testing Findings - Haseeb Ali's Workstation

3.1. Windows Firewall Status

- **Finding:** All three Windows Firewall profiles (Domain, Private, Public) were found to be enabled (ON).
- **Impact:** This indicates a strong baseline security posture, as the firewall is actively filtering incoming and outgoing network traffic, limiting unauthorized access to the workstation. This is a positive control.

3.2. Windows Firewall Rules - Service Access

- **Finding:** Several firewall rules for potentially risky services, such as File and Printer Sharing (LLMNR, NB-Session, SMB) and Network Discovery (SSDP, UPnPHost, WSD), were explicitly disabled (Enabled: No) for inbound connections.
- **Impact:** This significantly reduces the attack surface on the endpoint, preventing common lateral movement techniques and unauthorized access to shared resources. This is a positive security control.

3.3. Windows Defender Status (Antivirus)

- **Finding:** An attempt to manually update Windows Defender signatures resulted in a "The system cannot find the path specified" error.
- **Impact:** This error suggests a potential issue with the Windows Defender installation or its update mechanism. If Defender is not updating correctly, the workstation may be vulnerable to the latest malware and threats, as its definitions would be outdated. This poses a moderate to high risk.

3.4. Application-Specific Firewall Rules

- **Finding:** Numerous "Allow" rules are enabled for common applications (e.g., Microsoft Store, Google Chrome, Microsoft Edge, WhatsApp, Dropbox, Microsoft Teams, Microsoft Office Outlook).
- **Impact:** While necessary for functionality, a large number of broad "Allow" rules could potentially be exploited by malicious applications or allow unnecessary outbound connections. A detailed review is needed to ensure these rules adhere to the principle of least privilege.

3.5. User Account Security (General Observation)

- **Finding:** (Based on the password policy interview) There is a general tendency among some staff to use predictable password patterns, including personal information like Date of Birth and CNIC combinations. While not directly tested on this specific workstation's local account, this organizational trend poses a risk if local administrator accounts or other sensitive accounts follow similar patterns.

- **Impact:** Predictable passwords make accounts highly susceptible to brute-force and dictionary attacks, potentially leading to local privilege escalation or unauthorized access if an attacker gains physical or network access to the workstation.

4. Recommendations for Workstation Security Enhancement

To address the identified findings and enhance the security posture of employee workstations at Connected Pakistan, the following recommendations are provided:

4.1. Resolve Windows Defender Update Issue

- Investigate and resolve the "The system cannot find the path specified" error for Windows Defender. Ensure that Windows Defender is fully functional, receiving regular signature updates, and actively protecting the workstation.
- Confirm that a robust Endpoint Detection and Response (EDR) solution (if applicable) is correctly installed, configured, and updating.

4.2. Maintain Strong Firewall Posture

- Commend the active state of all Windows Firewall profiles and the explicit disabling of risky services. Ensure these configurations are consistently applied and maintained across all employee workstations, ideally through Group Policy or a centralized management solution.
- Regularly review and refine application-specific "Allow" rules in the Windows Firewall to ensure they adhere to the principle of least privilege, only permitting essential inbound and outbound connections.

4.3. Enforce Strong Password Policy

- Strictly enforce the new password policy across all user accounts, including local workstation accounts.

- Conduct mandatory security awareness training for all employees, specifically highlighting the dangers of using personal information (DOB, CNIC) or predictable patterns in passwords.

4.4. Implement Centralized Patch Management

Ensure the workstation is part of a centralized patch management system that automatically applies operating system and application updates, including critical security patches.

5. Management & IT Responsibilities

- Prioritize the resolution of endpoint security software issues.
- Implement centralized management for workstation security configurations.
- Provide ongoing security awareness training to all employees.
- Conduct regular audits of workstation configurations to ensure compliance with security policies.
- This report provides specific findings and actionable recommendations to improve the security of employee workstations at Connected Pakistan, reducing the risk of endpoint-based attacks.