Connected Pakistan Scanning and Enumeration Report

1. Purpose of This Report

This report details the findings from the comprehensive external and internal network scanning and enumeration activities conducted at Connected Pakistan. The primary objective was to identify accessible hosts, open ports, running services, and initial information about potential vulnerabilities, providing a foundational understanding of the company's digital footprint and attack surface.

2. Key Principles of Scanning and Enumeration

Scanning and enumeration are crucial initial phases in a security assessment, aiming to:

- **Discover Assets:** Identify active devices and services within the network and on the internet.
- **Map Network Topology:** Understand how systems are interconnected.
- **Identify Open Doors:** Find open ports and running services that could be entry points.
- **Gather Information:** Collect version numbers, configurations, and potential user/resource details.
- **Inform Further Testing:** Provide data for subsequent vulnerability analysis and penetration testing.

3. Scanning and Enumeration Findings

Based on the external and internal network scans, and web application enumeration, the following key findings were identified:

3.1. External Network Scan Findings (ehostpk.net / 5.9.177.100)

- **Target:** ehostpk.net (resolved to 5.9.177.100).
- **Open Ports & Services:**

- **Port 21/tcp (FTP):** open ftp Pure-FTPd
- **Finding:** An FTP server is exposed to the internet. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. While a subsequent test confirmed anonymous login was denied (a positive control), the presence of FTP still represents a potential attack surface if weak credentials or vulnerabilities are present.

- **Port 22/tcp (SSH):** open ssh OpenSSH 8.0 (protocol 2.0)
- **Finding:** SSH is exposed to the internet. This is a common administrative access point. OpenSSH 8.0 is a relatively recent version, but ensuring it's fully patched and configured with strong authentication (e.g., disabling password authentication, enforcing key-based authentication) is crucial.

- **Port 25/tcp (SMTP):** open tcpwrapped
- **Finding:** This port is open but reported as tcpwrapped, and Nmap couldn't establish an SMTP connection. This often indicates a firewall or rate-limiting in place, which is a positive security measure.

- **Port 26/tcp (SMTP):** open smtp Exim smtpd 4.98.2
- **Finding:** An alternative SMTP server is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. Exim 4.98.2 is a specific version that should be monitored for known vulnerabilities.

- **Port 53/tcp (DNS):** open domain ISC BIND 9.11.36 (RedHat Enterprise Linux 8)
- **Finding:** A DNS server is exposed. BIND 9.11.36 is a specific version that should be kept updated to prevent DNS-based attacks (e.g., cache poisoning, DDoS amplification).

- **Port 80/tcp (HTTP):** open http

- **Finding:** An HTTP server is exposed. It immediately redirects to https://ehostpk.net/ and returns a 404 Not Found for direct requests, indicating that the main website is enforced to use HTTPS. However, the fingerprint shows a cgi-sys/defaultwebpage.cgi redirect, which might indicate a default hosting configuration.

- **Port 110/tcp (POP3):** open pop3 Dovecot pop3d
- **Finding:** POP3 mail service is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. Supports STLS and AUTH PLAIN LOGIN, which should be secured with strong passwords and ideally MFA.

- **Port 143/tcp (IMAP):** open imap Dovecot imapd
- **Finding:** IMAP mail service is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. Supports STARTTLS and AUTH PLAIN LOGIN, requiring strong credentials.

- **Port 443/tcp (HTTPS):** open ssl/https
- **Finding:** An HTTPS web server is exposed. The SSL certificate bh02.ehostpk.net is valid from 2025-06-21 to 2025-09-19. It returns a 404 Not Found for direct requests, suggesting the primary website content is not hosted directly on this root path or requires specific paths.

- **Port 587/tcp (submission):** open tcpwrapped
- **Finding:** Similar to port 25, this port is open but tcpwrapped, and Nmap couldn't establish an SMTP connection, indicating a potential firewall or rate-limiting.

- **Port 993/tcp (IMAPS):** open imaps?
- **Finding:** Secure IMAP service is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26.

- **Port 995/tcp (POP3S):** open pop3s?
- **Finding:** Secure POP3 service is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26.

- **Port 2077/tcp (tsrmagt?):** open tsrmagt?
- **Finding:** The service operating on this port could not be definitively identified. Additional investigation is necessary to determine its purpose and potential security risks.

- **Port 2078/tcp (cPanel HTTP):** open ssl/http cPanel httpd (unauthorized)
- **Finding:** cPanel's HTTP administrative interface is exposed, requiring Basic authentication. It supports potentially risky WebDAV methods (LOCK, GET, MKCOL, PUT, MOVE, HEAD, POST, UNLOCK, COPY, DELETE, PROPPATCH, PROPFIND, OPTIONS). The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26.

- **Port 2082/tcp (infowave?):** open infowave?
- **Finding:** Unidentified service. Further investigation needed.

- **Port 2083/tcp (cPanel HTTPS):** open ssl/radsec?
- **Finding:** cPanel's HTTPS administrative interface is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. Fingerprint shows cPanel login page HTML. It sets several cookies and includes X-Frame-Options: SAMEORIGIN and X-Content-Type-Options: nosniff.

- **Port 2086/tcp (gnunet?):** open gnunet?
- **Finding:** Unidentified service. Further investigation needed.

- **Port 2087/tcp (WHM HTTPS):** open ssl/eli?
- **Finding:** Web Host Manager (WHM) HTTPS administrative interface is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-

    13 to 2026-05-26. Fingerprint shows WHM login page HTML. It also sets cookies and includes X-Frame-Options: SAMEORIGIN and X-Content-Type-Options: nosniff.

    - **Port 2091/tcp (tcpwrapped):** open tcpwrapped
    - **Finding:** Unidentified service, possibly firewalled or rate-limited.

    - **Port 2095/tcp (nbx-ser?):** open nbx-ser?
    - **Finding:** Unidentified service. Further investigation needed.

    - **Port 2096/tcp (Webmail HTTPS):** open ssl/nbx-dir?
    - **Finding:** Webmail HTTPS administrative interface is exposed. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. Fingerprint shows Webmail login page HTML. It also sets cookies and includes X-Frame-Options: SAMEORIGIN and X-Content-Type-Options: nosniff.

    - **Port 8887/tcp (ssl/unknown):** open ssl/unknown
    - **Finding:** Returns an "Unauthorized Access" page with a Google reCAPTCHA. The SSL certificate server.domaincontrol.pk is valid from 2025-05-13 to 2026-05-26. This is likely another administrative interface or service portal.

    - **Port 8888/tcp (sun-answerbook?):** open sun-answerbook?
    - **Finding:** Similar to 8887, returns an "Unauthorized Access" page with a Google reCAPTCHA.

    - **Port 8889/tcp (ddi-tcp-2?):** open ddi-tcp-2?
    - **Finding:** Returns a firewall blocking message ("The firewall on this server is blocking your connection."). This indicates an active security control.

- **Impact:** The extensive number of open ports and exposed services, particularly administrative panels like cPanel, WHM, and Webmail, along with other unidentified services, significantly broadens Connected Pakistan's external attack surface. Each exposed service represents a potential entry point for attackers if not properly secured, patched, and monitored. The presence of multiple mail services (25, 26, 465, 587) and various administrative ports (2077, 2078, 2082, 2083, 2086, 2087, 2091, 2095, 2096, 8887, 8888, 8889) indicates a complex and potentially over-exposed infrastructure. While some ports show signs of filtering or access control (25, 587, 8889), the sheer volume of open ports increases the likelihood of discovering a misconfiguration or vulnerability. The SSL certificates are relatively new, but their common name server.domaincontrol.pk suggests a shared hosting environment, which can sometimes introduce additional security considerations.

3.2. Internal Network Scan Findings - Production Segment (192.168.18.0/24)

Target: 192.168.18.0/24 subnet (254 devices).

Identified Hosts & Services:

- **192.168.18.1 (Huawei Technologies - Router/Gateway):**
  - **Open Ports**: 53/tcp (domain?), 80/tcp (ssl/http), 27998/tcp (ssl/unknown - potential Kerberos/SMBProgNeg), 37443/tcp (upnp - Portable SDK for UPnP devices 1.6.18), 37444/tcp (tcpwrapped).
  - **Filtered Ports:** 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet).
  - **MAC Address:** E0:4B:A6:CE:10:B7 (Huawei Technologies)
  - **Device Type:** General purpose, Linux 3.X.
  - **Impact:** This host appears to be a central network device, likely the main router or a gateway. The open HTTP port (80) suggests a web administration interface, which is a prime target for password guessing. The open UPnP service (37443) is a common vulnerability vector, as UPnP devices can often be misconfigured or exploited. The filtered administrative ports (SSH, Telnet, FTP) are a positive security measure.

- **192.168.18.13 (Intel Corporate - Workstation/Device):**

    - **Ports:** All 65535 scanned ports are in ignored/filtered states (no-response).
    - **MAC Address:** 8C:70:5A:F2:0D:60 (Intel Corporate)
    - **Impact:** This host is active but appears to be well-protected by a host-based firewall, as no open ports were identified. This indicates a good security posture for this endpoint.

- **192.168.18.16 (Hangzhou Hikvision Digital Technology - IP Camera/NVR):**
    - **Open Ports:** 80/tcp (http - HikVision NVR or camera http config), 554/tcp (rtsp - Apple AirTunes rtspd), 7681/tcp (unknown), 8000/tcp (ipcam - Hikvision IPCam control port), 30960/tcp (tcpwrapped), 49152/tcp (upnp - Portable SDK for UPnP devices 1.6.18).
    - **MAC Address:** C0:51:7E:42:B9:94 (Hangzhou Hikvision Digital Technology)
    - **Device Type:** General purpose, Linux 2.6.X|3.X, webcam.
    - **Impact:** This host is clearly an IP camera or Network Video Recorder (NVR). The numerous open ports, including HTTP, RTSP, and a dedicated IPCam control port, expose a significant attack surface. IP cameras and NVRs are frequently targeted due to default credentials, unpatched firmware, and known vulnerabilities, which could lead to unauthorized surveillance, network access, or inclusion in botnets.

- **192.168.18.25 (Unknown - Workstation/Device):**
    - **Ports:** All 65535 scanned ports are in ignored/closed states (reset).
    - **MAC Address:** C6:C9:02:5F:73:E3 (Unknown)
    - **Impact:** Similar to 192.168.18.13, this host is active but appears to be well-protected by a host-based firewall, as no open ports were identified. This indicates a good security posture for this endpoint.

3.3. Internal Network Scan Findings - Virtualized Segments (192.168.44.0/24 and 192.168.122.0/24)

Target: 192.168.44.0/24 and 192.168.122.0/24 subnets (likely virtualized environments).

Identified Hosts & Services:

- **192.168.44.1 (VMware - Filtered Host):**
    - **Ports:** All 65535 scanned ports are in ignored/filtered states (no-response).
    - **MAC Address:** 00:50:56:C0:00:08 (VMware)
    - **Impact:** A heavily filtered host, likely a virtual machine or gateway within a VMware environment. No services identified.

- **192.168.44.2 (VMware - DNS Server):**
    - **Open Ports:** 53/tcp (domain?).
    - **MAC Address:** 00:50:56:E8:99:9E (VMware)
    - **OS Guesses:** VMware Player virtual NAT device, various Windows/Linux/RouterOS.
    - **Impact:** A virtual machine running a DNS service. If this is a critical internal DNS server, its configuration and patch level would need further review.

- **192.168.44.135 (Linux - Web Server with Directory Listing):**
    - **Open Ports:** 5500/tcp (hotline? - identified as an HTTP server with "listing directory /" in its title).
    - **Impact:** This is a critical information disclosure vulnerability. An active web server on port 5500 is configured to allow directory listing, meaning an attacker can browse the file system contents of the web root. This can expose sensitive files, configuration data, or other valuable information.

- **192.168.44.254 (VMware - Filtered Host):**
    - **Ports:** All 65535 scanned ports are in ignored/filtered states (no-response).
    - **MAC Address:** 00:50:56:E9:AE:6E (VMware)
    - **Impact:** Another heavily filtered host, likely a virtual machine.

- **192.168.122.1 (KVM Virtual Gateway/VM):**
    - **Filtered Ports:** 22/tcp (ssh), 25/tcp (smtp), 465/tcp (smtps), 587/tcp (submission), 2525/tcp (ms-v-worlds).

    - **Network Distance:** 6 hops (indicating multiple hops within the virtual network or from the scanning origin).
    - **Impact:** This host appears to be a virtual gateway within a KVM NAT network. While active, all common administrative and mail-related ports were filtered, indicating a degree of protection. No services were openly accessible for direct password cracking within the scope of this test.

3.4. Other Internal Network Scan Findings (192.168.1.0/24)

Target: 192.168.1.0/24 subnet.

Identified Hosts & Services:

- **192.168.1.85 (Workstation/Device):**
    - **Ports:** All common ports (21, 22, 23, 25, 53, 80, 110, 135, 139, 143, 443, 445, 3389, 8080, 8443) are closed or filtered.
    - **Impact:** This host is active but appears to be well-protected by a host-based firewall, as no common services were identified as open. This indicates a good security posture for this endpoint.

3.5. Web Application Enumeration Findings (connectedpakistan.pk via Nikto)

- **Tool Used:** Nikto (for web server and application vulnerability scanning).
- **Key Findings:**
    - **Missing HTTP Security Headers:** Lack of X-Frame-Options, Strict-Transport-Security (HSTS), and X-Content-Type-Options.
    - **Uncommon Headers:** Presence of wpo-cache-status, x-redirect-by (WordPress), wpo-cache-message, and alt-svc (HTTP/3 advertising).
    - **robots.txt Entries:** Contains 4 entries that should be manually reviewed for sensitive paths.
    - **BREACH Attack Potential:** Content-Encoding header set to "deflate" may indicate vulnerability to the BREACH attack.
    - **Drupal Link Header:** Drupal Link header found, despite the site being a WordPress installation, which might indicate remnants or misconfigurations.

    - **sitemap.xml Listing:** Provides a comprehensive listing of site content, which can be useful for attackers.
    - **/img-sys/ Directory Listing:** Default image directory should not allow directory listing, as this can expose file structures.
    - **WordPress Specific Files:** wp-links-opml.php (reveals installed version) and license.txt (identifies site software).
    - **WordPress Installation Confirmed:** The site is identified as a WordPress installation.
- **Impact:** These findings indicate significant weaknesses in the web server's configuration and the web application itself. Missing security headers can lead to client-side attacks, while outdated components or exposed default files can provide direct avenues for exploitation. Information disclosure through robots.txt, sitemap.xml, and directory listing provides attackers with valuable reconnaissance data. The confirmed WordPress installation requires diligent patching of core, themes, and plugins, as it is a frequent target for attackers.

4. Recommendations for Enhanced Scanning and Enumeration Posture

To address the identified findings and enhance Connected Pakistan's overall security posture, the following recommendations are provided:

4.1. Minimize External Attack Surface

- **Review and Justify Exposed Services:** Conduct a thorough review of all externally accessible services. Disable any services that are not strictly necessary for business operations.
- **Restrict Administrative Access:** Implement strict firewall rules to restrict access to administrative interfaces (cPanel, WHM, Webmail, SSH, and other custom admin portals like 8887, 8888) to only trusted IP addresses (e.g., specific office IPs, VPN users). Consider placing these behind a VPN.
- **Harden Exposed Services:** Ensure all necessary exposed services (SSH, SMTP, DNS, HTTP/S, POP3/S, IMAP/S) are hardened according to security best practices, including:

  - Disabling unnecessary features.
  - Changing default configurations/credentials.
  - Implementing strong authentication (e.g., SSH key-based authentication, MFA for mail services and admin panels).
  - Ensuring all SSL/TLS certificates are valid, up-to-date, and used consistently.
  - Investigate unidentified services (2077, 2082, 2086, 2091, 2095) to determine their purpose and secure them appropriately.

4.2. Internal Network Segmentation and Hardening

- **Identify and Harden All Internal Devices:** Conduct a comprehensive inventory and configuration review of all internal network devices, servers, and IoT devices (like IP cameras/NVRs).
- **Change All Default Credentials:** Ensure all default usernames and passwords on internal devices are changed immediately upon deployment. This is especially critical for devices like IP cameras and routers.
- **Remove Default Pages/Services:** Replace default web server pages with appropriate content or redirects. Disable directory listing and any unnecessary services on internal hosts. The directory listing on 192.168.44.135:5500 must be disabled immediately.
- **Implement Network Segmentation:** Isolate critical systems, sensitive data, and IoT devices (like cameras) from general user networks to limit lateral movement and contain potential breaches. Devices like IP cameras should be on their own isolated VLAN.
- **Review UPnP Usage:** Assess the necessity of UPnP on internal devices. If not strictly required, disable it to remove a common vulnerability vector.

4.3. Web Application Security Configuration

- **Implement HTTP Security Headers:** Configure the web server for connectedpakistan.pk to send crucial HTTP security headers (X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Content-Security-Policy, Referrer-Policy).

- **Review and Restrict Information Disclosure:**
  - Ensure robots.txt does not expose sensitive directories or files.
  - Disable directory listing on all web servers, particularly for /img-sys/.
  - Review sitemap.xml for any unintended information disclosure.
  - Address WordPress Specific Hardening:
  - Regularly update WordPress core, themes, and all plugins.
  - Remove or rename wp-links-opml.php and license.txt if they are not essential or if their information disclosure poses a risk.
  - Implement WordPress security plugins and best practices (e.g., limiting login attempts, strong user roles, file integrity monitoring).

- **Mitigate BREACH Attack Risk:** Investigate and mitigate the potential BREACH attack vulnerability if the Content-Encoding: deflate header is used for sensitive content.

4.4. Continuous Monitoring and Patch Management

- **Centralized Logging:** Establish centralized logging for all network devices and servers to monitor for suspicious activities and attempted attacks.
- **Robust Patch Management:** Implement a systematic process for regularly patching and updating all operating systems, applications, frameworks, and network device firmware to address known vulnerabilities. This is particularly important for older Linux kernels and embedded devices like Hikvision NVRs, and all identified software versions (OpenSSH 8.0, Exim 4.98.2, BIND 9.11.36).

5. Management & IT Responsibilities

- Allocate resources for continuous security monitoring, vulnerability management, and patch management.
- Conduct regular security training for IT staff on secure configuration and network hardening.
- Establish clear procedures for deploying and maintaining secure network infrastructure and web applications.

- This report provides a foundational understanding of Connected Pakistan's current network and web application exposure, highlighting critical areas for immediate attention to reduce the attack surface and improve overall security.