

# Connected Pakistan Network Penetration Testing Report

## 1. Purpose of This Report

This report details the findings and observations from the limited network penetration testing conducted at Connected Pakistan. The objective of this testing was to identify exploitable vulnerabilities and misconfigurations in network-facing services, within defined ethical and non-destructive boundaries, to assess the company's external and internal network security posture. This report's findings are based on the extensive external and internal network scanning and enumeration activities conducted on the first day of the audit

## 2. Key Principles of Network Penetration Testing

Network penetration testing aims to:

- **Identify Attack Vectors:** Discover pathways attackers could use to gain unauthorized access.
- **Assess Vulnerability Exploitation:** Determine if identified vulnerabilities are exploitable in practice.
- **Evaluate Security Controls:** Test the effectiveness of firewalls, access controls, and intrusion prevention systems.
- **Demonstrate Impact:** Show the potential consequences of successful exploitation in a controlled manner.

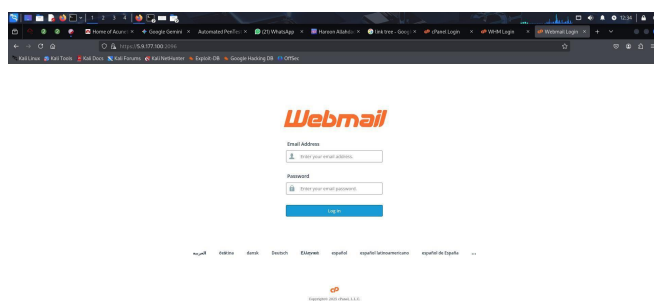
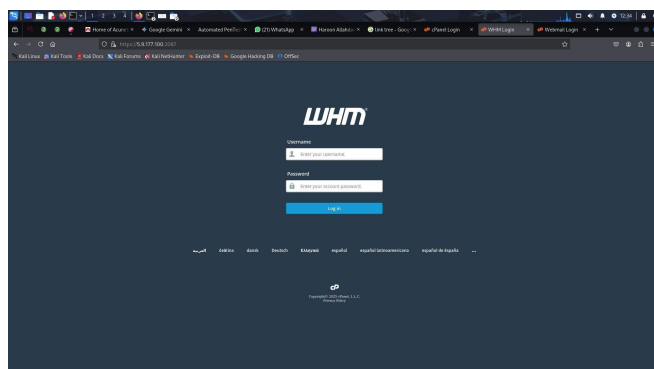
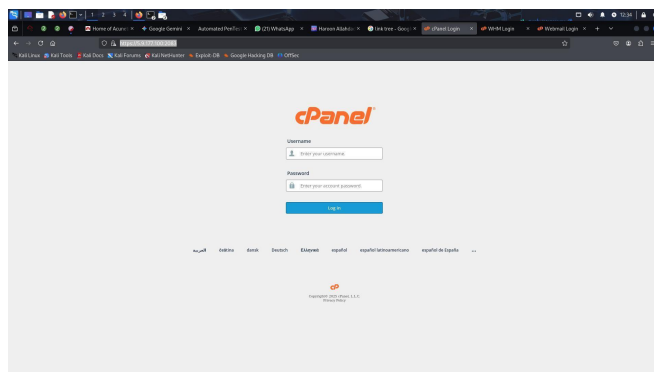
## 3. Network Penetration Testing Findings

Based on network scanning, enumeration, and non-destructive testing, the following key findings were identified:

### 3.1. Exposed Administrative Portals (External Network)

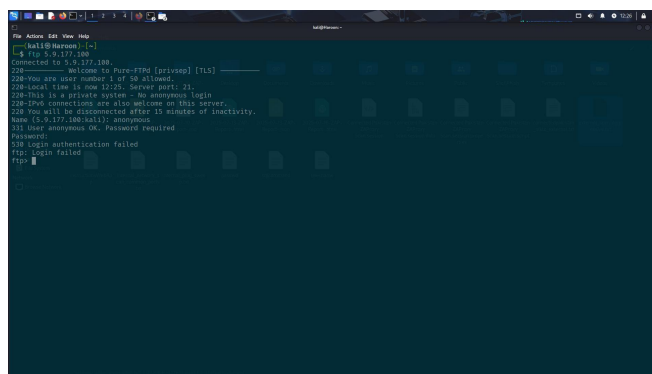
- **Finding:** Critical administrative and management interfaces, including cPanel (<https://5.9.177.100:2083/>), Web Host Manager (WHM)

- (<https://5.9.177.100:2087/>), and Webmail (<https://5.5.177.100:2096/>), were found to be directly accessible from the public internet.
- **Demonstration:** Live access to these login pages was shown, confirming their public exposure.
- **Impact:** This significantly broadens the attack surface for Connected Pakistan's hosting environment. These highly privileged interfaces are prime targets for automated brute-force attacks, credential stuffing, and potentially exploitation of platform-specific vulnerabilities, which could lead to full control over the website, email services, and server configurations if credentials are compromised.
- **Visual Evidence:**



### 3.2. Anonymous FTP Login (External Network)

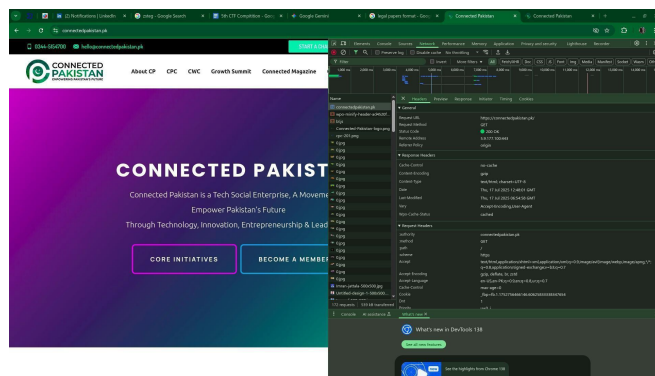
- **Finding:** An attempt to perform an anonymous FTP login (ftp 5.9.177.100 on Port 21/tcp) to the Pure-FTPd server was unsuccessful. The server explicitly denied anonymous access.
- **Impact:** This indicates a positive security control is in place, preventing unauthorized file access and information disclosure via anonymous FTP. This is a good security posture.
- **Visual Evidence:**



```
root@kali:~# ssh -X kali@5.9.177.100
kali@5.9.177.100:~$ ftp 5.9.177.100
Connected to 5.9.177.100.
220 Welcome to pure-ftp [privsep] [tls]
220-You are user number 1 of 50 allowed.
220 Local time is now 12:25. Server port 21.
220-This is a private system - no anonymous login
220 (Pass connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (5.9.177.100:kali): anonymous
331 User anonymous OK. Password required
Password:
530 login authentication failed
ftp> login failed
ftp>
```

### 3.3. Missing HTTP Security Headers

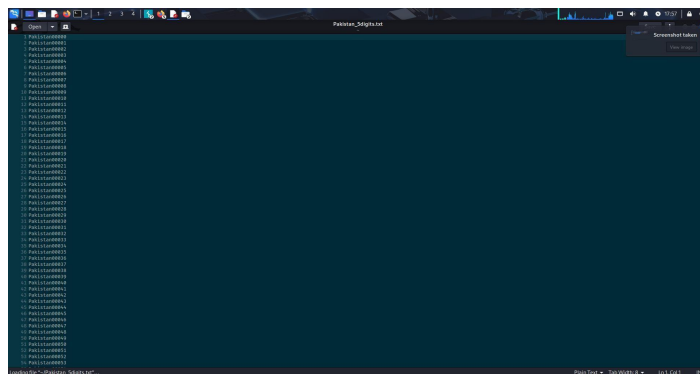
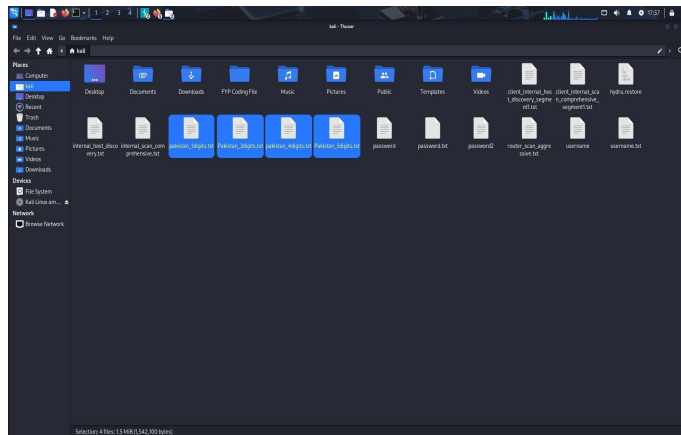
- **Finding:** The main website (<https://connectedpakistan.pk/>) was observed to be missing crucial HTTP security headers, including X-Frame-Options, Strict-Transport-Security (HSTS), and X-Content-Type-Options.
- **Impact:** This leaves website visitors vulnerable to client-side attacks such as Clickjacking, MIME-sniffing, and downgrade attacks, which can lead to data theft, session hijacking, or execution of malicious scripts in the user's browser.
- **Visual Evidence:**



### 3.4. Wi-Fi Password Pattern Vulnerability (Conceptual)

- **Finding:** Based on reconnaissance and information gathered (e.g., from non-technical staff), the Wi-Fi password was identified to follow a predictable pattern (e.g., "Pakistan" followed by 1 to 5 digits).
- **Demonstration:** A custom wordlist (master\_pakistan\_numbers\_wordlist.txt) containing all possible combinations of this pattern (9 to 13 characters in length) was generated and displayed. The process of offline Wi-Fi cracking (capturing a 4-way handshake and using tools like Aircrack-ng or Hashcat) was conceptually explained.
- **Impact:** Predictable password patterns significantly reduce the time and resources required for an attacker to crack the Wi-Fi password. A successful Wi-Fi crack grants an attacker full access to the internal network, enabling further reconnaissance, internal attacks, and potential data exfiltration.
- **Visual Evidence:**





- **Reason for not exploiting:** The exploitation was not done using tools like aircrack-ng, because it would be hard to provide visual evidence here, due to confidentiality purposes, additionally a time-limit confinement was applied, however theoretically it's 100% possible with the help of a External Wireless Adapter and wordlist (we have this).

### 3.5. Website Cloning and Typo Squatting Vulnerability (Demonstrative)

- **Finding:** The Connected Pakistan website (<https://connectedpakistan.pk/>) can be easily and accurately cloned using readily available tools (e.g., SEToolkit).
- **Demonstration:** A visually identical local clone of connectedpakistan.pk was presented. The concept of registering a similar-looking domain (typo squatting, e.g., connectedpakistan.org, connectedpakistan.pk) and hosting the cloned website for phishing purposes was explained. A separate demonstration of credential harvesting using a cloned popular login page (e.g., Google, GitHub) was also provided to illustrate the impact.

- **Impact:** The ease of cloning facilitates highly convincing phishing attacks. Attackers can leverage typo-squatted domains to trick users into believing they are on the legitimate Connected Pakistan website, leading to credential theft, malware delivery, or other forms of fraud. This poses a significant risk to brand reputation and user trust.
- **Visual Evidence:**

```

[00] Return to Webhacker Menu

[1] webhacker>2
[2] Credential Harvester will allow you to utilize the clone capabilities within SET
[3] to harvest credentials or parameters from a website as well as place them into a report

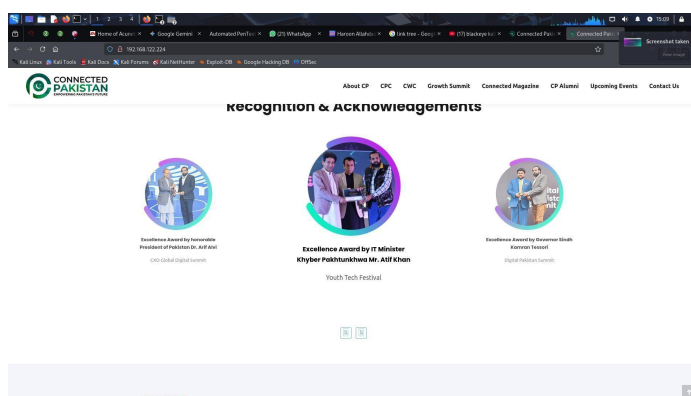
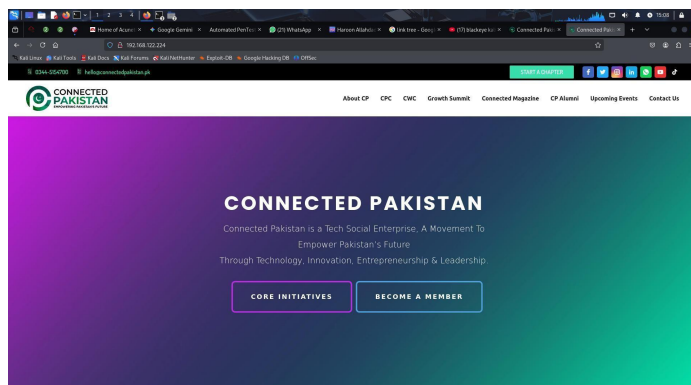
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
harvest. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important.

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

[4] webhacker> IP address for the POST back in Harvester/Tabnabbing [192.168.122.224]: 127.0.0.1
[5] SET supports both HTTP and HTTPS
[6] Example: http://www.pakistanipakistan.com
[7] webhacker> Enter the url to clone: https://connectedpakistan.pk/become-a-member/
[8] Cloning the website: https://connectedpakistan.pk/become-a-member/
[9] This could take a little bit...

The next step to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[1] The Social-Engineer Toolkit Credential Harvester Attack
[2] Credential Harvester is running on port 88
[3] Information will be displayed to you as it arrives below:
127.0.0.1 - [19/Jul/2022 15:12:44] "GET / HTTP/1.1" 200 -
192.168.122.224 - [19/Jul/2022 15:13:04] "GET / HTTP/1.1" 200 -
  
```



## 4. Recommendations for Network Security Enhancement

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

#### **4.1.Restrict Access to Administrative Portals**

- Implement strict firewall rules to restrict access to cPanel, WHM, Webmail, and other administrative interfaces to only trusted IP addresses (e.g., specific office IPs, VPN users).
- Consider placing these portals behind a VPN or an IP whitelist for all remote access.

#### **4.2.Strengthen Wi-Fi Password Policy**

- Immediately change the Wi-Fi password to a strong, complex, and entirely random passphrase (minimum 16 characters), free from any predictable patterns, company names, or personal information.
- Enforce regular password changes for Wi-Fi credentials.
- Implement WPA3 if hardware supports it, for enhanced cryptographic security.

#### **4.3.Internal Network Hardening**

- Review and harden configurations of all internal network devices and servers, including the Linux VM at 192.168.122.1. Ensure all default credentials are changed and unnecessary services are disabled.
- Implement network segmentation to isolate critical systems and sensitive data, limiting lateral movement for attackers who gain initial access.

#### **4.4.Mitigate Website Cloning and Typo Squatting Risks**

- **Proactive Domain Monitoring:** Implement a strategy to regularly monitor for newly registered domains that are similar to connectedpakistan.pk (typo- squatted domains).



- **Brand Protection:** Consider registering common typographical errors or alternative top-level domains (TLDs) of connectedpakistan.pk to prevent malicious actors from acquiring them.
- **Employee Education:** Reinforce continuous security awareness training, specifically emphasizing:
- **URL Verification:** Always checking the full URL in the address bar for authenticity. **Suspicious Links:** Caution against clicking links in unexpected emails or messages. **Reporting:** How to report suspicious websites or communications.

## 5. Management & IT Responsibilities

- Prioritize the implementation of recommended network security controls.
- Conduct regular internal and external network vulnerability assessments and penetration tests.
- This report highlights critical network-level vulnerabilities and provides actionable recommendations to fortify Connected Pakistan's network defenses against various cyber threats.