PENETRATION TEST

SECURITY ASSESSMENT REPORT

Client	SafeNetKids
Assessment Date	01 May 2026
Report Generated	01 May 2026
Conducted By	A38 IT Ltd
Classification	CONFIDENTIAL
Overall Risk Rating	**HIGH**

0	2	1	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Contents

Executive Summary

Executive Summary

Penetration Testing Assessment - SafeNetKids

Assessment Date: May 1, 2026 **Risk Rating:** MEDIUM

SafeNetKids demonstrates a fundamentally sound security foundation with no critical vulnerabilities identified during our comprehensive penetration testing assessment. However, our evaluation uncovered five security findings that require management attention, including two high-severity issues that could potentially expose the organization to significant business risks if left unaddressed. The overall security posture reflects an organization that has implemented basic security controls but would benefit from enhanced monitoring and remediation of identified weaknesses.

The two high-severity findings present the most immediate concern for SafeNetKids' operations and reputation. These vulnerabilities could potentially allow unauthorized access to sensitive customer data or enable attackers to disrupt service availability, directly impacting your ability to serve families who depend on your platform for child safety online. Given SafeNetKids' mission-critical role in protecting children's digital experiences, any security incident could result in significant reputational damage, regulatory scrutiny, loss of customer trust, and potential legal liability. The medium-severity finding, while less urgent, represents an additional attack vector that could be exploited in conjunction with other vulnerabilities.

We strongly recommend immediate prioritization of the two high-severity vulnerabilities within the next 30 days, as these represent the most direct threats to business continuity and customer data protection. Your IT team should implement the specific remediation steps outlined in our technical findings section and conduct verification testing to ensure proper resolution. Additionally, we recommend establishing a regular vulnerability management program and scheduling quarterly security assessments to maintain the trust your customers place in SafeNetKids' commitment to protecting their families' digital safety.

Assessment Scope

Item	Detail
IP Ranges	217.154.53.177/32
Domains	safenetkids.co.uk
Modules Run	nmap, ssl, osint, credentials, openvas, dns
Total Hosts Scanned	2
Authorised By	Jason Roberts

Findings Summary

#	Finding	Severity	CVSS	Host	Status
1	Vulnerability Detected: vulners on 217.154.53.177:22	HIGH	7.5	217.154.53.177	OPEN
2	Vulnerability Detected: vulners on 217.154.53.177:22	HIGH	7.5	217.154.53.177	OPEN
3	Weak DMARC Policy for safenetkids.co.uk	MEDIUM	4.3	safenetkids.co.uk	OPEN
4	DNS Enumeration: 9 Subdomains Discovered	INFO	None		OPEN
5	Certificate Transparency: 3 Subdomains Exposed for safenetkids	INFO	None	safenetkids.co.uk	OPEN

Detailed Findings

#1 — Vulnerability Detected: vulners on 217.154.53.177:22	HIGH
Target	217.154.53.177:22
URL	N/A
Module	OPENVAS
CVSS Score	7.5
CVEs	CVE-2025-26465, CVE-2026-35387, CVE-2026-35388, CVE-2025-26466, CVE-2025-61984, CVE-2025-61985, CVE-2026-35
CWEs	None
Status	OPEN

Description

Nmap script vulners detected a vulnerability on ssh service. cpe:/a:openbsd:openssh:9.6p1: PACKETSTORM:179290 10.0 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT* 1EEC8894-D2F7-547C-827C-915BE866875C 10.0 https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C *EXPLOIT* 09B905C6-CD97-54E6-AD97-B0DD1AC4771B 10.0 https://vulners.com/githubexploit/09B905C6-CD97-54E6-AD97-B0DD1AC4771B *EXPLOIT* 33D623F7-98E0-5F75-80FA-81AA666D1340 9.8 https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EX

Risk Analysis

The SSH service on 217.154.53.177 is running OpenSSH version 9.6p1 which contains multiple critical vulnerabilities with CVSS scores of 10.0 and 9.8, including the RegreSSHion vulnerability (CVE-2024-6387). Public exploits are available for these vulnerabilities, allowing attackers to potentially gain remote code execution and full system compromise.

Evidence

```
cpe:/a:openbsd:openssh:9.6p1: PACKETSTORM:179290 10.0
https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT* 1EEC8894-D2F7-547C-827C-915BE866875C
10.0 https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C *EXPLOIT*
09B905C6-CD97-54E6-AD97-B0DD1AC4771B 10.0
https://vulners.com/githubexploit/09B905C6-CD97-54E6-AD97-B0DD1AC4771B *EXPLOIT*
33D623F7-98E0-5F75-80FA-81AA666D1340 9.8
https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EX
```

Remediation

1. Immediately update OpenSSH to the latest patched version (9.8p1 or later)

2. If immediate patching is not possible, implement network-level access controls to restrict SSH access to trusted IP addresses only

3. Enable SSH key-based authentication and disable password authentication

4. Configure SSH to use non-standard ports and implement rate limiting

5. Monitor SSH logs for suspicious connection attempts

6. Consider implementing a bastion host or VPN for SSH access

#2 — Vulnerability Detected: vulners on 217.154.53.177:22 HIGH

Target	217.154.53.177:22
URL	N/A
Module	OPENVAS
CVSS Score	7.5
CVEs	CVE-2025-26465, CVE-2026-35387, CVE-2026-35388, CVE-2025-26466, CVE-2025-61984, CVE-2025-61985, CVE-2026-35
CWEs	None
Status	OPEN

Description

Nmap script vulners detected a vulnerability on ssh service. cpe:/a:openbsd:openssh:9.6p1: PACKETSTORM:179290 10.0 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT* 1EEC8894-D2F7-547C-827C-915BE866875C 10.0 https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C *EXPLOIT* 09B905C6-CD97-54E6-AD97-B0DD1AC4771B 10.0 https://vulners.com/githubexploit/09B905C6-CD97-54E6-AD97-B0DD1AC4771B *EXPLOIT* 33D623F7-98E0-5F75-80FA-81AA666D1340 9.8 https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EX

Risk Analysis

Multiple critical vulnerabilities detected in OpenSSH 9.6p1 running on port 22, with several exploits publicly available scoring up to 10.0 CVSS. This represents an extremely high risk as SSH is typically used for administrative access, and successful exploitation could lead to complete system compromise and lateral movement throughout the network.

Evidence

```
cpe:/a:openbsd:openssh:9.6p1: PACKETSTORM:179290 10.0
https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT* 1EEC8894-D2F7-547C-827C-915BE866875C
10.0 https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C *EXPLOIT*
09B905C6-CD97-54E6-AD97-B0DD1AC4771B 10.0
https://vulners.com/githubexploit/09B905C6-CD97-54E6-AD97-B0DD1AC4771B *EXPLOIT*
33D623F7-98E0-5F75-80FA-81AA666D1340 9.8
https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EX
```

Remediation

1. Immediately update OpenSSH to the latest stable version (9.8p1 or newer) that addresses all listed CVEs. 2. If immediate patching is not possible, implement network segmentation to restrict SSH access to trusted networks only. 3. Enable SSH key-based authentication and disable password authentication. 4. Configure fail2ban or similar intrusion prevention system to block brute force attempts. 5. Monitor SSH logs for suspicious connection attempts and unauthorized access. 6. Consider changing the default SSH port and implementing port knocking if additional security is required.

#3 — Weak DMARC Policy for safenetkids.co.uk MEDIUM

Target	safenetkids.co.uk:None
URL	N/A
Module	DNS
CVSS Score	4.3
CVEs	None
CWEs	CWE-290
Status	OPEN

Description

DMARC policy is set to p=none which only monitors but does not reject or quarantine spoofed emails.

Risk Analysis

The domain safenetkids.co.uk has a weak DMARC policy set to 'none', which means spoofed emails claiming to be from this domain will be delivered normally rather than being blocked or quarantined. This creates a significant phishing risk as attackers can easily impersonate the organization in email communications, potentially damaging brand reputation and enabling social engineering attacks against customers, partners, or employees.

Evidence

```
"v=DMARC1; p=none; rua=mailto:admin@safenetkids.co.uk"
```

Remediation

1. Gradually implement a stricter DMARC policy by first changing p=none to p=quarantine to quarantine suspicious emails while monitoring results through the aggregate reports sent to admin@safenetkids.co.uk. 2. Ensure SPF and DKIM records are properly configured and aligned before implementing stricter DMARC policies. 3. Monitor DMARC aggregate reports for 2-4 weeks to identify any legitimate email sources that may be affected. 4. Once confident in the configuration, upgrade to p=reject to block spoofed emails entirely. 5. Consider adding pct=100 to apply the policy to 100% of emails and fo=1 for forensic reporting of policy failures.

#4 — DNS Enumeration: 9 Subdomains Discovered	INFO
Target	None:None
URL	N/A
Module	DNS
CVSS Score	None
CVEs	None
CWEs	None
Status	OPEN

Description

DNS reconnaissance discovered 9 subdomains across 1 domains. Each subdomain should be reviewed for unexpected exposure.

Risk Analysis

DNS enumeration revealed 9 subdomains for safenetkids.co.uk, exposing the organization's network infrastructure and services to potential attackers. This information disclosure allows threat actors to map attack surfaces and identify potentially vulnerable services like FTP, SSH, and email servers that may not be intended for public access.

Evidence

```
["www.safenetkids.co.uk", "mail.safenetkids.co.uk", "ftp.safenetkids.co.uk",
"webmail.safenetkids.co.uk", "smtp.safenetkids.co.uk", "app.safenetkids.co.uk",
"ftp.safenetkids.co.uk", "ssh.safenetkids.co.uk", "sftp.safenetkids.co.uk"]
```

Remediation

1. Review each discovered subdomain to verify it should be publicly accessible and remove or restrict access to any unnecessary services. 2. Implement DNS security measures such as limiting zone transfers and using split-horizon DNS to hide internal infrastructure. 3. Ensure all exposed services are properly hardened with strong authentication, updated software, and appropriate access controls. 4. Consider using a web application firewall or similar protection for publicly accessible services. 5. Regularly audit DNS records and remove obsolete or unused subdomains.

#5 — Certificate Transparency: 3 Subdomains Exposed for safenetkids.co.uk — INFO

Target	safenetkids.co.uk:None
URL	N/A
Module	OSINT
CVSS Score	None
CVEs	None
CWEs	None
Status	OPEN

Description

Certificate transparency logs reveal 3 subdomains. Attackers use this to discover attack surface without active scanning.

Risk Analysis

Certificate transparency logs have revealed 3 subdomains for safenetkids.co.uk, which attackers can use to map your infrastructure without directly scanning your systems. This provides potential attackers with additional targets to investigate for vulnerabilities, expanding the attack surface they're aware of.

Evidence

```
app.safenetkids.co.uk safenetkids.co.uk www.safenetkids.co.uk
```

Remediation

1. Review all exposed subdomains to ensure they are necessary and properly secured. 2. Implement proper access controls and authentication on all discovered subdomains. 3. Consider using wildcard certificates to reduce the number of specific subdomains exposed in CT logs. 4. Monitor certificate transparency logs regularly to track your organization's exposure. 5. Ensure any development or staging subdomains are not publicly accessible or use internal certificates.

Compliance Mapping

The following table maps identified findings to common compliance frameworks. This is provided as guidance only and does not constitute a formal compliance assessment.

Finding	Severity	Cyber Essentials	ISO 27001	PCI-DSS	NIST
Vulnerability Detected: vulners on 217.154.53...	HIGH	Software Security Updates, Secure Configuration	A.12.6.1, A.14.2.3	6.2, 2.2	—
Vulnerability Detected: vulners on 217.154.53...	HIGH	Secure Configuration, Boundary firewalls	A.13.1.1, A.14.2.3	6.1, 6.2	—
Weak DMARC Policy for safenetkids.co.uk	MEDIUM	BC4	A.13.2.1, A.13.2.3	—	—
DNS Enumeration: 9 Subdomains Discovered	INFO	Boundary firewalls and internet gateways	A.13.1.1, A.13.1.3	1.3.8, 11.2.1	—
Certificate Transparency: 3 Subdomains Expose...	INFO	Network Security	A.13.1.1, A.14.2.1	2.2.1	—

Remediation Roadmap

The following remediation actions are recommended, prioritised by risk level. Critical and High findings should be addressed within 24-48 hours where possible.

■ SHORT TERM (1-2 weeks)

• **Vulnerability Detected: vulners on 217.154.53.177:22** — 1. Immediately update OpenSSH to the latest patched version (9.8p1 or later)

• **Vulnerability Detected: vulners on 217.154.53.177:22** — 1. Immediately update OpenSSH to the latest stable version (9.8p1 or newer) that addresses all listed CVEs. 2. If immediate patching is not possible, implement network segmentation to restrict SSH access to trusted networks only. 3. Enable SSH key-based authentication and disable password authentication. 4. Configure fail2ban or similar intrusion prevention system to block brute force attempts. 5. Monitor SSH logs for suspicious connection attempts and unauthorized access. 6. Consider changing the default SSH port and implementing port knocking if additional security is required.

■ MEDIUM TERM (1 month)

• **Weak DMARC Policy for safenetkids.co.uk** — 1. Gradually implement a stricter DMARC policy by first changing p=none to p=quarantine to quarantine suspicious emails while monitoring results through the aggregate reports sent to admin@safenetkids.co.uk. 2. Ensure SPF and DKIM records are properly configured and aligned before implementing stricter DMARC policies. 3. Monitor DMARC aggregate reports for 2-4 weeks to identify any legitimate email sources that may be affected. 4. Once confident in the configuration, upgrade to p=reject to block spoofed emails entirely. 5. Consider adding pct=100 to apply the policy to 100% of emails and fo=1 for forensic reporting of policy failures.