**Penetration Testing on Web Server**

Website – <https://certifiedhacker.com>

**I. Executive Summary**

This report provides a concise overview of the security assessment conducted on certifiedhacker.com. Analysis of reconnaissance and vulnerability scan data reveals a critical security posture, primarily stemming from extensive information disclosure, widespread use of outdated software, and direct exposure of critical services. New findings from a Nessus scan highlight specific vulnerabilities, including DNS amplification and cache snooping, weak SSL/TLS configurations (SWEET32, TLS 1.0/1.1), missing HSTS, and an exposed SNMP agent with a default community string. These issues collectively present a high risk of compromise. Immediate and comprehensive remediation is crucial to enhance the domain's security posture and protect against potential cyber threats.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical | High | Medium | Low |

**II. Introduction**

**Purpose of the Report**

This document details the findings of a security assessment on certifiedhacker.com, fulfilling the "Footprinting and Reconnaissance" phase of a penetration testing project. Its aim is to systematically identify publicly accessible information, enumerate network services, detect potential vulnerabilities, and uncover misconfigurations within the external-facing infrastructure and web presence. The insights derived from this analysis are intended to guide security hardening efforts for the company's website and to identify potential vectors for social engineering against employees.

**Methodology**

The assessment employed a multi-faceted reconnaissance approach, integrating both passive and active techniques to gather comprehensive data:

* **Open Source Intelligence (OSINT):** Passive information gathering from public sources, including WHOIS databases and online platforms.
* **Network Scanning (Nmap & Nessus):** Active scanning to identify open ports, services, versions, and detailed vulnerability assessments. 1
* **Web Content Enumeration (Dirb):** Discovery of hidden directories and files, and identification of directory listing vulnerabilities.
* **Relationship Mapping (Maltego):** Visualization of domain-related entities and data leakage points.

**Scope**

The assessment was limited to the external-facing infrastructure and web presence of certifiedhacker.com. No internal network access, privileged operations, or intrusive penetration testing activities were performed beyond the information gathering techniques described.

**III. Tools Used**

|  |  |  |
| --- | --- | --- |
| Tool | Rationale | Application |
| Nmap (Network Mapper) | Essential for network discovery, identifying live hosts, open ports, services, and operating systems. | Used for comprehensive port scanning of 162.241.216.11 to identify 18 open TCP ports, service versions (e.g., OpenSSH 7.4, MySQL 5.7.23-23), and initial SSL/TLS details. |
| Tenable Nessus | A leading vulnerability scanner providing detailed insights into system weaknesses, misconfigurations, and compliance issues. | Performed a "Basic Network Scan" on 162.241.216.11 to identify critical, high, medium, and low-risk vulnerabilities, including DNS amplification, SNMP default community, weak SSL ciphers, and missing HSTS. 1 |
| Dirb (Directory Brute-Forcer) | Effective for discovering hidden or non-indexed web content, sensitive files, and administrative interfaces. | Scanned https://certifiedhacker.com/ to find accessible directories (e.g., /controlpanel, /webmail) and sensitive files (e.g., id\_rsa, .bash\_history), and identified numerous listable directories. |
| Maltego | Aggregates and visualises data from various sources to map relationships and identify information leakage. | Used to confirm WHOIS details, identify associated DNS names, and link discovered documents (e.g., NIST PDFs) to exposed directories. |
| OSINT (Open Source Intelligence) | Broad category for collecting foundational public information without direct interaction. | Applied for WHOIS lookups (domain registration, privacy service use), and checking for domain presence on various online platforms. |

**IV. Detailed Footprinting and Reconnaissance Findings**

|  |
| --- |
|  |
| **About the Company** |
|  |
| |  |  | | --- | --- | | Aspect | Details | | **Primary Focus** | Cybersecurity education and ethical hacking training, offering certifications (e.g., Certified Ethical Hacker v13 with AI capabilities), hands-on labs, and a cloud-based cyber range. | | **Secondary/Related Content** | Mentions "Oakridge International School" for broader education (primary to postgraduate in various fields), suggesting diverse offerings or content overlap. | |
|  |
| **IP Address of Website** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **Primary IP Address** | 162.241.216.11 | |
|  |
| **Location of Server** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **Country** | United States (US) | | **State/Region** | Utah | | **City** | Provo | | **Coordinates** | Latitude 40.2338 / Longitude -111.6586 | | **Hostname** | box5331.bluehost.com | |
|  |
| **Operating System of Server** |
|  |
| |  |  | | --- | --- | | Attribute | Details | | **Identified OS** | Linux Kernel 2.6 (Confidence 65%), Ubuntu 16.04 Linux Kernel 4.4 (Confidence 56%). Specifically, ISC BIND 9.11.4-P2 is identified on RedHat Enterprise Linux 7. | | **Inconsistency** | Presence of Windows/IIS artifacts (global.asa, main.mdb, web.config) suggests an incomplete migration or misconfigured hybrid environment. | |
|  |
| **Web Server Technology and Version** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **Technology** | Apache httpd | | **Version** | Not explicitly detailed beyond "Apache httpd" in Nmap, but Nessus indicates "unknown" version from banner. Likely consistent with Red Hat Enterprise Linux 7 packages. | |
|  |
| **Built-in Technology** |
|  |
| |  |  | | --- | --- | | Category | Technologies/Services Identified | | **Web Server** | Apache httpd | | **FTP Server** | Pure-FTPd | | **SSH Server** | OpenSSH 7.4 | | **DNS Server** | ISC BIND 9.11.4-P2 | | **Mail Servers** | Exim smtpd 4.98.1 (SMTP), Dovecot pop3d (POP3), Dovecot imapd (IMAP) | | **Databases** | MySQL 5.7.23-23, PostgreSQL DB | | **Web App Artefacts** | PHP (inferred from php.ini), Classic ASP (global.asa), ASP.NET (web.config), Microsoft Access (main.mdb). | | **SNMP Agent** | SNMPv2c (with default 'public' community string). | |
|  |
| **Website Publishing date** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **Creation Date** | 2002-07-30 T00:32:00Z | |
|  |
| **Previous Technology Used by Website** |
|  |
| |  |  | | --- | --- | | Attribute | Details | | **Indication** | Discovery of Windows-specific files (global.asa, main.mdb, web.config) on a Linux server strongly suggests prior hosting on a Microsoft Windows Server with IIS. | |
|  |
| **ISP-IP Range of Server** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **ISP** | Unified Layer | | **ASN** | 46606 | | **IP Range** | 162.241.216.0 to 162.241.216.255 | |
|  |
| **Other Domain Names** |
|  |
| |  |  | | --- | --- | | Attribute | Details | | **Shared Hosting** | Bluehost nameservers (ns1.bluehost.com, ns2.bluehost.com) and hostname (box5331.bluehost.com). Specific domain names are not provided. | |
|  |
| **Ports Open on Webserver** |
|  |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Port | Protocol | State | Service Name | Version | Key Observation | | 21 | tcp | open | ftp | Pure-FTPd | SSL/TLS enabled, TLS randomness warning. | | 22 | tcp | open | ssh | OpenSSH 7.4 (protocol 2.0) | Outdated software, 1024-bit DSA key. 1 | | 25 | tcp | open | smtp | Exim smtpd 4.98.1 | Connection issues, cleartext login permitted. | | 26 | tcp | open | smtp | Exim smtpd 4.98.1 | Connection issues. | | 53 | tcp | open | domain | ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7) | Outdated software, vulnerable to amplification DDoS and cache snooping. | | 80 | tcp | open | http | Apache httpd | Redirects to HTTPS, supports HTTP/2 cleartext. | | 110 | tcp | open | pop3 | Dovecot pop3d | SSL/TLS enabled, TLS randomness warning, supports PLAIN login, TLS 1.0/1.1 enabled. | | 143 | tcp | open | imap | Dovecot imapd | SSL/TLS enabled, TLS randomness warning, supports PLAIN login, TLS 1.0/1.1 enabled. | | 443 | tcp | open | ssl/http | Apache httpd | SSL/TLS enabled, TLS randomness warning, "404 Not Found" title, HSTS missing, TLS 1.2/1.3 supported. | | 465 | tcp | open | tcpwrapped | - | SSL/TLS enabled, TLS randomness warning, supports PLAIN login, TLS 1.0 enabled. | | 587 | tcp | open | tcpwrapped | - | Connection issues, cleartext login permitted. | | 993 | tcp | open | ssl/imap | Dovecot imapd | SSL/TLS enabled, TLS randomness warning, supports PLAIN login, TLS 1.0/1.1 enabled. | | 995 | tcp | open | ssl/pop3 | Dovecot pop3d | SSL/TLS enabled, TLS randomness warning, supports PLAIN login, TLS 1.0/1.1 enabled. | | 2000 | tcp | open | tcpwrapped | - | Unknown service. | | 2077 | tcp | open | - | - | Open port. | | 2078 | tcp | open | www | - | SSL/TLS enabled, TLS randomness warning, HSTS missing, TLS 1.0/1.1 enabled, HTTP methods allowed. | | 2082 | tcp | open | - | - | Open port. | | 2083 | tcp | open | www | - | SSL/TLS enabled, TLS randomness warning, HSTS missing, TLS 1.0/1.1 enabled. | | 2086 | tcp | open | - | - | Open port. | | 2087 | tcp | open | www | - | SSL/TLS enabled, TLS randomness warning, HSTS missing, TLS 1.0/1.1 enabled, port became unresponsive during scan. | | 2095 | tcp | open | - | - | Open port. | | 2096 | tcp | open | www | - | SSL/TLS enabled, TLS randomness warning, HSTS missing, TLS 1.0/1.1 enabled. | | 2222 | tcp | open | ssh | OpenSSH 7.4 (protocol 2.0) | Outdated software, duplicate of port 22. | | 3306 | tcp | open | mysql | MySQL 5.7.23-23 | **CRITICAL:** Directly exposed, outdated, TLS randomness warning, uses mysql\_native\_password. | | 5060 | tcp | open | tcpwrapped | - | Unknown service. | | 5432 | tcp | open | postgresql | PostgreSQL DB | **CRITICAL:** Directly exposed, unsupported frontend protocol. | | 161 | udp | open | snmp | - | **HIGH:** SNMP agent with default 'public' community name. | |
|  |
| **Registrar Information of Domain** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **Registrar** | Network Solutions, LLC | | **Registrant Organization** | PERFECT PRIVACY, LLC | | **Creation Date** | 2002-07-30 T 00:32:00Z | | **Expiry Date** | 2026-07-30 T 00:32:00Z | | **Domain Status** | Client Transfer Prohibited | | **Name Servers** | ns1.bluehost.com, ns2.bluehost.com | | **DNSSEC** | unsigned | |
|  |
| **Email ID‘s** |
|  |
| |  |  | | --- | --- | | Email Address | Type | | kq9t994x73e@networksolutionsprivateregistration.com | Registrant/Admin/Tech Contact (via privacy service) | | dnsadmin@box5331.bluehost.com | Hosting Provider Admin | | domain.operations@web.com | Registrar Abuse Contact | |
|  |
| **Social Networking Profiles** |
|  |
| |  |  | | --- | --- | | Platform | URL (for domain entity) | | Bug Crowd | https://bugcrowd.com/certifiedhacker.com | | Cults3D | https://cults3d.com/en/users/certifiedhacker.com/creations | | EyeEm | https://www.eyeem.com/u/certifiedhacker.com | | GNOME VCS | https://gitlab.gnome.org/certifiedhacker.com | | Giphy | https://giphy.com/certifiedhacker.com | | kaskus | https://www.kaskus.co.id/@certifiedhacker.com | | LibraryThing | https://www.librarything.com/profile/certifiedhacker.com | | Mydramalist | https://www.mydramalist.com/profile/certifiedhacker.com | | Nation States Nation | https://nationstates.net/nation=certifiedhacker.com | | Nation States Region | https://nationstates.net/region=certifiedhacker.com | | Velomania | https://forum.velomania.ru/member.php?username=certifiedhacker.com | |
|  |
| **LinkedIn Search for Profiles with Company Name** |
|  |
| |  |  | | --- | --- | | Attribute | Details | | **Findings** | No specific LinkedIn ID found | |
|  |
| **Address of Company** |
|  |
| |  |  | | --- | --- | | Attribute | Value | | **Registered Address** | 5335 Gate Parkway, Jacksonville, FL, 32256, US (via privacy service) | | **Website Mention**  **Address** | Systematic Software Limited 2512, Old Road - Alian Street, Alioha - Arizuwa  ZIP: 01234-567 | |
|  |
| **Director/CEO of Company** |
|  |
| |  |  | | --- | --- | | Attribute | Details | | **President** | Ted Nellig | | **CEO** | Staton Rogers | |
|  |
| **Check Firewall and Load Balancer** |
|  |
| |  |  | | --- | --- | | Component | Status/Details | | **Firewall** | Present, indicated by "982 closed TCP ports (reset)" responses from Nmap. | | **Load Balancer** | No direct evidence found; domain resolves to a single IP. | |

**V. Security Observations and Potential Vulnerabilities**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk Factor | Category | Observation Vulnerability | CVSS v3.0 Base Score | CVSS v2.0 Base Score | Impact |
| Medium | **Outdated Software** | OpenSSH 7.4, ISC BIND 9.11.4-P2, MySQL 5.7.23-23, Exim 4.98.1, Dovecot versions are significantly old. | N/A (for general outdatedness) | N/A (for general outdatedness) | High probability of known, exploitable CVEs leading to remote code execution, privilege escalation, or data breaches. |
| Medium | **DNS Vulnerabilities** | **DNS Server Spoofed Request Amplification DDoS (ID: 35450):** Remote DNS server answers to any request, allowing amplification attacks. | 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | 5.0 (AV:N/AC:L/  Au:N/C:N/I:N/A:P) | Can be leveraged to launch DDoS attacks against third-party hosts, potentially leading to IP blacklisting for certifiedhacker.com. |
| **DNS Server Cache Snooping Remote Information Disclosure (ID: 12217):** Responds to non-recursive queries for third-party domains. | 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) | 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Allows attackers to determine recently resolved domains and visited hosts, aiding reconnaissance for targeted attacks. |
| High | **Information Disclosure** | Numerous directories (/blog/, /docs/, /mailman/, /pipermail/, etc.) are publicly listable. | N/A | N/A | Allows attackers to map site structure, discover sensitive files (e.g., internal documents, mailing list archives), and aid targeted attacks. |
| Critical | **Sensitive File Exposure** | SSH private keys (id\_rsa) and shell history files (.bash\_history, .sh\_history) found in web-accessible directories (even with 406 response). | N/A | N/A | Critical risk of unauthenticated SSH access and exposure of sensitive commands/credentials if files are exfiltrated. |
| High | **Architectural Inconsistency** | Presence of both Linux-native services (Apache, MySQL) and Windows/IIS artifacts (global.asa, main.mdb, web.config). | N/A | N/A | Creates ambiguity, broader attack surface, and suggests poor file management or incomplete migration. |
| High | **Exposed Admin Interfaces** | /controlpanel, /cpanel, /webmail are directly accessible from the internet. | N/A | N/A | High risk of brute-force attacks and credential stuffing, leading to extensive control over the domain. |
| Critical | **Exposed Database Services** | MySQL (3306) and PostgreSQL (5432) are directly exposed to the internet. | N/A | N/A | Critical vulnerability for data compromise, unauthorized access, and potential full system compromise via database exploits. |
| Medium | **SSL/TLS Weaknesses** | **SSL Medium Strength Cipher Suites Supported (SWEET32) (ID: 42873):** Services support medium strength ciphers (e.g., 3DES). | 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) | 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | Easier to circumvent encryption, especially on the same physical network, compromising confidentiality. |
| **TLS Version 1.0 Protocol Detection (ID: 104743):** Services accept TLS 1.0, which has cryptographic design flaws. | 6.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N) | 6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N) | Vulnerable to downgrade attacks; non-compliant with modern security standards (e.g., PCI DSS). |
| **TLS Version 1.1 Deprecated Protocol (ID: 157288):** Services accept TLS 1.1, lacking modern cipher suite support. | 6.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N) | 6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N) | Vulnerable to downgrade attacks; non-compliant with modern security standards. |
| **SSL Certificate Signed Using Weak Hashing Algorithm (SHA-1) (ID: 95631):** Certificates signed with SHA-1 expiring after Jan 2017. | N/A | N/A | Vulnerable to collision attacks, allowing attackers to masquerade as the service. |
| High |  | **TLS randomness does not represent time:** Observed on multiple SSL-enabled services. | N/A | N/A | Indicates potential issue with server clock synchronization or cryptographic random number generator, undermining TLS security. |
| Low | **SMTP Vulnerabilities** | **SMTP Service Cleartext Login Permitted (ID: 54582):** Mail server allows cleartext logins over unencrypted channels. | N/A | 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) | Risk of username/password exposure via traffic sniffing if less secure authentication is used. |
| Medium | **Web Server Configuration** | **HSTS Missing From HTTPS Server (ID: 142960 & 84502):** Web server not enforcing HTTP Strict Transport Security. | 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N) | 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N) | Allows downgrade attacks, SSL-stripping, and weakens cookie-hijacking protections. |
| High | **SNMP Vulnerability** | **SNMP Agent Default Community Name (public) (ID: 41028):** Default 'public' community name is guessable. | N/A | 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Allows attackers to gain more knowledge about the host or potentially change its configuration. |
| Medium | **DNS Misconfigurations** | Nameservers allow recursive queries; SOA EXPIRE value is excessively high (41+ days); DNSSEC is unsigned. | N/A | N/A | Risk of DNS amplification attacks, slow propagation of DNS changes, and susceptibility to DNS spoofing/cache poisoning. |

**VI. Suggestions (Recommendations)**

|  |  |  |
| --- | --- | --- |
| Priority | Recommendation | Details |
| **Critical** | **Restrict Access to Admin & DB Interfaces** | Implement strict IP-based firewall rules for /controlpanel, /cpanel, /webmail, MySQL (3306), and PostgreSQL (5432). These services should *never* be directly exposed to the public internet. |
| **Critical** | **Remove/Secure Sensitive Files** | Immediately remove id\_rsa and shell history files (.bash\_history, .sh\_history) from web-accessible directories. Investigate and securely remove Windows artifacts (.mdb, .config, .asa) if remnants. |
| **High** | **Update All Software** | Prioritize updating OpenSSH, ISC BIND, Exim, Dovecot, and MySQL to their latest stable and patched versions. Establish a robust patch management program. |
| **High** | **Disable Directory Listing** | Immediately configure web server (Apache) to disable directory indexing for all public directories (Options -Indexes). |
| **High** | **Harden SSL/TLS Configuration** | Disable weak cipher suites (e.g., 3DES, identified by SWEET32). Disable deprecated TLS 1.0 and TLS 1.1 protocols. Investigate and resolve "TLS randomness does not represent time" warning. Replace certificates signed with SHA-1. |
| **High** | **Address DNS Vulnerabilities** | Restrict access to the DNS server from the public network or reconfigure it to reject spoofed amplification queries. Contact DNS software vendor for cache snooping fix. |
| **High** | **Secure SNMP Agent** | Disable the SNMP service if not used. If necessary, change the default 'public' community string and filter incoming UDP packets to port 161. |
| **Medium** | **Enforce Strong Authentication** | Mandate strong, unique passwords and enable Multi-Factor Authentication (MFA) for all administrative and database accounts. |
| **Medium** | **Implement HSTS** | Configure the web server to send the HTTP Strict Transport Security (HSTS) header to enforce HTTPS-only communication. |
| **Medium** | **Improve DNS Configuration** | Engage Bluehost to disable recursive queries on nameservers. Reduce SOA EXPIRE value to a more reasonable timeframe (e.g., 1-3 hours). Consider enabling DNSSEC. |
| **Low** | **Secure SMTP Cleartext Login** | Configure SMTP service to support less secure authentication mechanisms (LOGIN, PLAIN) only over an encrypted channel. |
| **Low** | **Review Web Root Content** | Conduct a thorough audit to ensure only necessary files are present in public web directories. |
| **Low** | **Address Architectural Inconsistencies** | Investigate and clean up Windows artifacts. Verify consistent Linux-based stack. |

**VII. Works cited**