SECURITY ASSESSMENT

MONTHLY SCAN REPORT

Comprehensive cybersecurity analysis and vulnerability assessment for network infrastructure and digital assets.

26 MAY 2026

PREPARED FOR

EXAMPLE.COM

External Security Scan

REPORT TYPE	Monthly
CLASSIFICATION	Confidential
FORMAT	PDF
VERSION	2.1

SECURITY ASSESSMENT SUMMARY

EXECUTIVE OVERVIEW

Comprehensive analysis of your digital infrastructure security posture and vulnerability landscape

18	5	42	3
EXPOSED DOMAINS	IP ADDRESSES	LEAKED PASSWORDS	HIGH-RISK PORTS
Subdomains Discovered	With Open Ports	Credential Compromises	Critical Services Exposed

OVERALL RISK ASSESSMENT

6.5

HIGH RISK

Your organization faces significant cybersecurity risks requiring urgent attention and remediation.

PRIORITY SECURITY CONCERNS

- 42 compromised credentials found on dark web
- 3 high-risk ports exposed on public infrastructure
- 18 subdomains exposed, expanding attack surface
- 5 IP addresses require port configuration review
- Regular security monitoring and updates recommended

SCAN DATE	RISK SCORE	LAST DATA BREACH
26 MAY 2026	6.5/10	2024-03-12

PREPARED FOR
EXAMPLE.COM

SECURITY WARNING

LEAKED PASSWORDS

42

PREPARED FOR

EXAMPLE.COM

LEAKED PASSWORDS

42 Found

Critical Security Alert: The following credentials have been identified in data breaches and are publicly available. Immediate action is required to secure these accounts and prevent unauthorized access.

	SEARCHED VALUE	SOURCE	DETECTED	SOURCE_LOCATIONS	PASSWORD
1	alice@example.com	linkedin-2021	2024-01-01	US,FR	P@ssw0rd!
2	bob@example.com	collection#1	2024-02-04	FR,DE	letmein2024
3	carol@example.com	exploit.in-2020	2024-03-07	DE,UK	qwerty123
4	dan@example.com	anti-public-2017	2024-04-10	UK,MA	summer2023
5	eve@example.com	facebook-2019	2024-05-13	MA,ES	Welcome1
6	frank@example.com	stealer-logs-2024	2024-06-16	ES,IT	Admin@123
7	grace@example.com	dropbox-2012	2024-07-19	IT,NL	Pa$$w0rd
8	heidi@example.com	rambler-2014	2024-08-22	NL,BR	ch4ngeme
9	ivan@example.com	linkedin-2021	2024-09-25	BR,JP	monkey99
10	judy@example.com	collection#1	2024-10-28	JP	dragon!2
11	kara@example.com	exploit.in-2020	2024-11-03	US,FR	P@ssw0rd!10
12	leo@example.com	anti-public-2017	2024-12-06	FR,DE	letmein202411

	SEARCHED VALUE	SOURCE	DETECTED	SOURCE_LOCATIONS	PASSWORD
13	mallory@example.com	facebook-2019	2024-01-09	DE,UK	qwerty12312
14	niaj@example.com	stealer-logs-2024	2024-02-12	UK,MA	summer202313
15	olivia@example.com	dropbox-2012	2024-03-15	MA,ES	Welcome114
16	peggy@example.com	rambler-2014	2024-04-18	ES,IT	Admin@12315
17	quentin@example.com	linkedin-2021	2024-05-21	IT,NL	Pa$$w0rd16
18	ruth@example.com	collection#1	2024-06-24	NL,BR	ch4ngeme17
19	sybil@example.com	exploit.in-2020	2024-07-27	BR,JP	monkey9918
20	trent@example.com	anti-public-2017	2024-08-02	JP	dragon!219
21	uma@example.com	facebook-2019	2024-09-05	US,FR	P@ssw0rd!20
22	alice1@example.com	stealer-logs-2024	2024-10-08	FR,DE	letmein202421
23	bob1@example.com	dropbox-2012	2024-11-11	DE,UK	qwerty12322
24	carol1@example.com	rambler-2014	2024-12-14	UK,MA	summer202323
25	dan1@example.com	linkedin-2021	2024-01-17	MA,ES	Welcome124
26	eve1@example.com	collection#1	2024-02-20	ES,IT	Admin@12325
27	frank1@example.com	exploit.in-2020	2024-03-23	IT,NL	Pa$$w0rd26
28	grace1@example.com	anti-public-2017	2024-04-26	NL,BR	ch4ngeme27
29	heidi1@example.com	facebook-2019	2024-05-01	BR,JP	monkey9928

	SEARCHED VALUE	SOURCE	DETECTED	SOURCE_LOCATIONS	PASSWORD
30	ivan1@example.com	stealer-logs-2024	2024-06-04	JP	dragon!229
31	judy1@example.com	dropbox-2012	2024-07-07	US,FR	P@ssw0rd!30
32	kara1@example.com	rambler-2014	2024-08-10	FR,DE	letmein202431
33	leo1@example.com	linkedin-2021	2024-09-13	DE,UK	qwerty12332
34	mallory1@example.com	collection#1	2024-10-16	UK,MA	summer202333
35	niaj1@example.com	exploit.in-2020	2024-11-19	MA,ES	Welcome134
36	olivia1@example.com	anti-public-2017	2024-12-22	ES,IT	Admin@12335
37	peggy1@example.com	facebook-2019	2024-01-25	IT,NL	Pa$$w0rd36
38	quentin1@example.com	stealer-logs-2024	2024-02-28	NL,BR	ch4ngeme37
39	ruth1@example.com	dropbox-2012	2024-03-03	BR,JP	monkey9938
40	sybil1@example.com	rambler-2014	2024-04-06	JP	dragon!239
41	trent1@example.com	linkedin-2021	2024-05-09	US,FR	P@ssw0rd!40
42	uma1@example.com	collection#1	2024-06-12	FR,DE	letmein202441

MODERATE EXPOSURE

EXPOSED DOMAINS

18

PREPARED FOR

EXAMPLE.COM

DETECTED SUBDOMAINS

18 Found

Subdomain Discovery: The following subdomains have been identified through reconnaissance techniques. These represent your organization's attack surface and should be monitored for security vulnerabilities.

INDEX	DOMAIN NAME	SUBDOMAIN
1	example.com	https://api.example.com
2	example.com	https://mail.example.com
3	example.com	https://staging.example.com
4	example.com	https://dev.example.com
5	example.com	https://vpn.example.com
6	example.com	https://git.example.com
7	example.com	https://wiki.example.com
8	example.com	https://crm.example.com
9	example.com	https://shop.example.com
10	example.com	https://blog.example.com
11	example.com	https://admin.example.com
12	example.com	https://test.example.com

INDEX	DOMAIN NAME	SUBDOMAIN
13	example.com	https://qa.example.com
14	example.com	https://demo.example.com
15	example.com	https://old.example.com
16	example.com	https://new.example.com
17	example.com	https://support.example.com
18	example.com	https://portal.example.com

LOW VULNERABILITIES

SUBDOMAIN VULNERABILITIES

9

PREPARED FOR

EXAMPLE.COM

VULNERABILITY ASSESSMENT

9 Found

CRITICAL VULNERABILITIES

	URL	TITLE	COMPONENT	METADATAS
1	https://api.example.com	RCE via deserialization	Tomcat	CVE-2023-1234 / patch in 9.0.71
2	https://staging.example.com	Unauthenticated Admin Access	Jenkins	CVE-2024-23897 / arbitrary file read

HIGH VULNERABILITIES

	URL	TITLE	COMPONENT	METADATAS
1	https://mail.example.com	SQL Injection in login	Custom PHP	Param: username
2	https://api.example.com	Stored XSS in comments	Custom JS	Cookie session theft viable
3	https://www.example.com	Outdated WordPress core	WordPress 5.8	12 known CVEs / upgrade to 6.5

MEDIUM VULNERABILITIES

	URL	TITLE	COMPONENT	METADATAS
1	https://api.example.com	Missing security headers	Nginx	CSP, X-Frame-Options, HSTS absent
2	https://mail.example.com	Weak TLS ciphers enabled	Postfix	TLS 1.0/1.1 still negotiable

LOW VULNERABILITIES

	URL	TITLE	COMPONENT	METADATAS
1	https://www.example.com	Server version disclosure	Apache/2.4.41	Banner reveals version

INFORMATIONAL

	URL	TITLE	COMPONENT	METADATAS
1	https://api.example.com	robots.txt exposes admin path	Static	Disallow: /admin/ / informational only

LIMITED PORT EXPOSURE

IP ADDRESSES & PORTS

3

PREPARED FOR

EXAMPLE.COM

NETWORK INFRASTRUCTURE

3 IPs

Network Discovery: The following IP addresses and open ports have been identified. High-risk ports require immediate attention to prevent potential security breaches.

IP ADDRESS	OPEN PORTS
203.0.113.10	80 443 22
198.51.100.5	80 8080 3389
192.0.2.41	443 21 139

PORT RISK LEVELS

- Critical Risk Ports (SSH, FTP, SMB, RDP, etc.)
- Standard Web Ports (HTTP, HTTPS)
- Other / Unknown Ports

CloudKey

REPORT COMPLETE

SCAN COMPLETED

This concludes your comprehensive cybersecurity assessment. Thank you for choosing CloudKey for your security analysis needs.

FOR ADDITIONAL INFORMATION

CLOUDKEY

contact@cloudkey-teck.com

www.cloudkey-teck.com

INDUSTRY IT Solutions & Cybersecurity

LOCATION Casablanca, Morocco

PHONE +212 641 051 662

REPORT GENERATED 2026