Red Team Reconnaissance Report

Executive Summary

This report provides a high-level summary of reconnaissance findings.

Methodology

Data was collected using automated reconnaissance modules and mapped to MITRE ATT&CK; techniques.

Risk Assessment

High: Exposed credentials or misconfigurations were identified.

Medium: Publicly accessible information may increase attack surface.

Low: General OSINT artifacts discovered.

MITRE ATT&CK; Summary

Total Techniques: 20

Initial-access: 1

Reconnaissance: 11

Collection: 5

Resource-development: 1

Discovery: 1

Command-and-control: 1

MITRE ATT&CK; Mapping

Artifact	Tactic	Technique ID	Technique Name
clickjacking	initial-access	T1190	Exploit Public-Facing Application
dkim	reconnaissance	T1598.002	Unknown
dns	reconnaissance	T1590.001	DNS/Domain Discovery
doc_urls	collection	T1074.001	Document Collection
docx_urls	collection	T1074.002	Cloud Staging (docx)
domain	reconnaissance	T1590	Gather Victim Network Information
emailsecurity	reconnaissance	T1598	Email Security
gau_urls	reconnaissance	T1595	Active Scanning
google_dorks	reconnaissance	T1592	Unknown
ip	reconnaissance	T1590.005	IP Address Discovery
json_urls	collection	T1213.003	APIs / Data Repositories
link	reconnaissance	T1593	Unknown

pdf_urls	resource-development	T1608.001	PDF/Docs Resources
shodan_nmap	reconnaissance	T1595.001	Nmap/Shodan scanning
subdomains	reconnaissance	T1590.002	Subdomain Discovery
timestamp	discovery	T1082	System Information Discovery
txt_urls	collection	T1005	Data from Local System (txt)
url	command-and-control	T1071	Application Layer Protocol
whois	reconnaissance	T1596.001	WHOIS/Registration Data
xml_urls	collection	T1119	Automated Collection

Next Steps

Further validation and manual penetration testing are recommended.

Conclusion

This reconnaissance provides visibility into the target's exposure landscape.