Network Reconnaissance Report

Report ID: [NR-YYYY-MM-DD-XXX]
Classification: [Confidential/Internal/Public]
Distribution: [Authorized Personnel Only]
Date: [Report Generation Date]
Analyst: [Your Name/Team]
Version: [1.0]

Executive Summary

[Provide a high-level overview of the reconnaissance findings, key discoveries, and overall security posture assessment. This should be 2-3 paragraphs maximum, suitable for management consumption.]

Key Findings:

- [Critical finding 1]
- [Critical finding 2]
- [Critical finding 3]

Risk Level: [Critical/High/Medium/Low]

---

1. Scope and Objectives

1.1 Target Information

- **Organization Name:** [Target Organization]
- **Primary Domain(s):** [example.com, subdomain.example.com]
- **IP Range(s):** [XXX.XXX.XXX.XXX/XX]
- **ASN(s):** [AS Numbers if applicable]
- **Industry/Sector:** [Technology, Finance, Healthcare, etc.]

1.2 Reconnaissance Objectives

□ Domain enumeration and mapping
□ Subdomain discovery
□ IP range identification
□ Service enumeration
□ Technology stack identification
□ Email harvesting

□ Social media intelligence

□ DNS analysis

□ Certificate transparency analysis

□ Other: [Specify]

1.3 Time Frame

- **Start Date:** [YYYY-MM-DD]
- **End Date:** [YYYY-MM-DD]
- **Total Duration:** [X days/hours]

---

2. Methodology

2.1 OSINT Sources Used

□ Search engines (Google, Bing, DuckDuckGo)

□ DNS enumeration tools

□ Certificate transparency logs

□ Social media platforms

□ Professional networks (LinkedIn, etc.)

□ Public repositories (GitHub, GitLab)

□ Job posting sites

□ Company websites and documentation

□ Archive.org (Wayback Machine)

□ Shodan/Censys

□ Other: [Specify tools and sources]

2.2 Tools and Techniques

```
Primary Tools:
- [Tool Name] - [Purpose]
- [Tool Name] - [Purpose]
- [Tool Name] - [Purpose]

Passive Reconnaissance Tools:
- [Tool Name] - [Purpose]
- [Tool Name] - [Purpose]

Verification Tools:
- [Tool Name] - [Purpose]
```

2.3 Limitations and Constraints

- [Legal and ethical boundaries observed]
- [Technical limitations encountered]
- [Time or resource constraints]
- [Data availability limitations]

---

3. Network Infrastructure Analysis

3.1 Domain Analysis

Primary Domain: [example.com]

Attribute	Value	Source	Notes
Registrar	[Company Name]	WHOIS	[Additional context]
Registration Date	[YYYY-MM-DD]	WHOIS	[Age analysis]
Expiration Date	[YYYY-MM-DD]	WHOIS	[Renewal status]
Name Servers	[ns1.example.com]	DNS	[Provider analysis]
MX Records	[mail.example.com]	DNS	[Email infrastructure]

3.2 Subdomain Enumeration

Total Subdomains Discovered: [Number]

Subdomain	IP Address	Status	Services	Notes
www.example.com	XXX.XXX.XXX.XXX	Active	HTTP/HTTPS	[Description]
mail.example.com	XXX.XXX.XXX.XXX	Active	SMTP	[Description]
ftp.example.com	XXX.XXX.XXX.XXX	Inactive	-	[Description]
dev.example.com	XXX.XXX.XXX.XXX	Active	HTTP	[Development server]

Notable Subdomains:

- [Subdomain] - [Significance and findings]
- [Subdomain] - [Significance and findings]

3.3 IP Address Analysis

IP Ranges Identified:

IP Range	Owner/ISP	Location	Services	Notes
XXX.XXX.XXX.XXX/XX	[ISP Name]	[City, Country]	[Web, Mail, etc.]	[Cloud provider info]

Geolocation Analysis:

- Primary hosting location: [City, Country]
- CDN usage: [Yes/No - Provider name]
- Cloud services: [AWS, Azure, GCP, etc.]

---

4. Service Enumeration

4.1 Web Services

URL	Technology Stack	Server Info	Security Headers	Notes
https://example.com	[WordPress, Apache, etc.]	[Apache/2.4.41]	[Present/Missing]	[CMS version, etc.]

4.2 Email Infrastructure

- **Mail Servers:** [List of mail servers]
- **SPF Record:** [Present/Absent - Details]
- **DKIM:** [Configured/Not Configured]
- **DMARC:** [Policy details]
- **Email Security:** [Analysis of email security posture]

4.3 Other Services Discovered

Port	Service	Version	Status	Vulnerability Notes
22	SSH	OpenSSH 7.4	Open	[Version analysis]
80	HTTP	Apache 2.4.41	Open	[Redirect to HTTPS]
443	HTTPS	Apache 2.4.41	Open	[Certificate details]
25	SMTP	Postfix 3.1.1	Open	[Configuration notes]

---

5. Technology Stack Analysis

5.1 Web Technologies

- **Content Management System:** [WordPress 5.8.1, Drupal, etc.]
- **Web Server:** [Apache, Nginx, IIS]
- **Programming Language:** [PHP, Python, .NET, etc.]
- **Database:** [MySQL, PostgreSQL, etc. - if detectable]
- **JavaScript Frameworks:** [React, Angular, Vue.js, etc.]

- **CDN/Caching:** [Cloudflare, AWS CloudFront, etc.]

5.2 Third-Party Services

- **Analytics:** [Google Analytics, Adobe Analytics]
- **Advertising:** [Google Ads, Facebook Pixel]
- **Social Media Integration:** [Facebook, Twitter, LinkedIn]
- **Payment Processing:** [PayPal, Stripe, etc.]
- **Chat/Support:** [Zendesk, Intercom, etc.]

5.3 Security Technologies

- **SSL/TLS Certificate:** [Issuer, expiration, SANs]
- **WAF Detection:** [Cloudflare, AWS WAF, etc.]
- **DDoS Protection:** [Service provider]
- **Security Headers:** [HSTS, CSP, X-Frame-Options status]

---

6. Human Intelligence (HUMINT)

6.1 Employee Information

Total Employees Identified: [Number]

Name	Position	Email Pattern	LinkedIn	Notes
[Name]	[Job Title]	[firstname.lastname@domain]	[Profile URL]	[Relevant info]

6.2 Organizational Structure

- **Key Departments Identified:**
  - IT/Security: [X employees]
  - Development: [X employees]
  - Management: [X employees]

6.3 Contact Information

- **Email Patterns:** [firstname.lastname@domain.com]
- **Phone Number Format:** [+1-XXX-XXX-XXXX]
- **Physical Addresses:** [Headquarters and branch locations]

6.4 Social Media Presence

Platform	Handle	Followers	Activity Level	Security Relevance
LinkedIn	[@company]	[Number]	[High/Medium/Low]	[Employee disclosure risks]
Twitter	[@company]	[Number]	[High/Medium/Low]	[Technical discussions]
Facebook	[@company]	[Number]	[High/Medium/Low]	[Employee photos, locations]

---

7. Certificate Transparency Analysis

7.1 SSL Certificate History

Certificate	Issued Date	Expiry Date	Issuer	SANs	Notes
[Domain]	[Date]	[Date]	[Let's Encrypt]	[List]	[Subdomain revelations]

7.2 Notable Findings

- [Previously unknown subdomains discovered]
- [Internal naming conventions revealed]
- [Development/staging environments exposed]

---

8. Threat Intelligence

8.1 Historical Security Incidents

- [Date]: [Brief description of any known security incidents]
- [Date]: [Data breaches, if publicly disclosed]

8.2 Dark Web/Breach Database Presence

- **Credentials Found:** [Yes/No - Source]
- **Data Types:** [Email addresses, passwords, personal info]
- **Breach Dates:** [Timeline of discovered compromises]

8.3 Vulnerability Indicators

- [Outdated software versions identified]
- [Known CVEs affecting identified technologies]
- [Misconfigurations observed]

---

9. Attack Surface Analysis

9.1 External Attack Vectors

High Priority Targets:

1. [Asset] - [Reason for priority]
2. [Asset] - [Reason for priority]
3. [Asset] - [Reason for priority]

Potential Entry Points:

- Web applications: [Number identified]
- Email services: [Security posture]
- Remote access services: [VPN, RDP, etc.]
- Cloud services: [Exposed buckets, databases]

9.2 Social Engineering Vectors

- **Employee Targeting:** [High-value targets identified]
- **Phishing Opportunities:** [Domain similarities, employee emails]
- **Physical Security:** [Office locations, employee habits]

---

10. Risk Assessment

10.1 Critical Findings

Finding	Risk Level	CVSS Score	Recommendation
[Specific vulnerability]	Critical	[9.0]	[Immediate action required]
[Configuration issue]	High	[7.5]	[Priority remediation]

10.2 Risk Matrix

Category	Risk Level	Likelihood	Impact	Mitigation Priority
Web Application Security	[High]	[Likely]	[High]	[1]
Email Security	[Medium]	[Possible]	[Medium]	[2]
Social Engineering	[High]	[Likely]	[High]	[1]

---

11. Recommendations

11.1 Immediate Actions (0-30 days)

1. **[Priority 1]:** [Specific recommendation with rationale]
2. **[Priority 2]:** [Specific recommendation with rationale]
3. **[Priority 3]:** [Specific recommendation with rationale]

11.2 Short-term Actions (1-6 months)

1. [Recommendation]
2. [Recommendation]
3. [Recommendation]

11.3 Long-term Strategic Initiatives (6+ months)

1. [Recommendation]
2. [Recommendation]
3. [Recommendation]

---

12. Appendices

Appendix A: Raw Data

[Include raw tool outputs, screenshots, or detailed technical data]

Appendix B: Tool Commands Used

```bash
# Domain enumeration
command1 -options target.com

# Subdomain discovery
command2 -wordlist wordlist.txt target.com

# Certificate transparency
command3 target.com
```

Appendix C: IOCs (Indicators of Compromise)

- IP Addresses: [List]
- Domains: [List]
- Email Addresses: [List]

- File Hashes: [If applicable]

Appendix D: References

1. [Source 1] - [URL] - [Access Date]
2. [Source 2] - [URL] - [Access Date]
3. [Tool Documentation] - [URL] - [Version]

Document Control

Version	Date	Author	Changes
1.0	[Date]	[Name]	Initial report
1.1	[Date]	[Name]	[Description of changes]

Document Classification: [Classification Level]
Distribution List: [Authorized recipients]
Retention Period: [As per organizational policy]
Next Review Date: [Date]

This report contains sensitive information and should be handled according to organizational data classification policies. Distribution should be limited to authorized personnel with a legitimate need to know.