CEH Lab Report: Information Gathering & Reconnaissance

Target: Telenor.com

Executive Summary

This lab demonstrates passive and active reconnaissance techniques against Telenor.com, a telecommunications company. The objective was to gather publicly available information to identify the organization's infrastructure, CDN provider, nameservers, and subdomains without triggering security alerts.

Key Findings:

- CDN Provider: Azure Front Door
- Nameservers: ns1.nextra.no, ns2.nextra.no, nsp.dnsnode.net
- Subdomains Discovered: 810 (via passive methods)
- Primary IP: 20.100.134.111

Objectives

1. Identify the primary domain and IP address
2. Discover nameservers and DNS infrastructure
3. Enumerate subdomains using passive and active methods
4. Identify the CDN provider and architecture
5. Document findings for further penetration testing phases

Methodology

Phase 1: Passive Information Gathering

Passive reconnaissance involves collecting publicly available information without directly interacting with target systems.

Tools Used:

- WHOIS databases
- DNS records (public databases)
- Certificate Transparency logs
- Website footprinting tools

Techniques:

- Searched public DNS records
- Queried Certificate Transparency databases (crt.sh)
- Analyzed WHOIS registration information
- Reviewed DNS TXT records for SPF, DKIM configurations

Findings:

- Primary domain resolves to: 20.100.134.111
- Organization uses Azure Front Door CDN service (Microsoft infrastructure)
- 810 subdomains identified through passive enumeration

Phase 2: Active Information Gathering

Active reconnaissance directly queries the target's DNS servers and infrastructure.

Tools Used:

- `dig` (DNS Information Gatherer)
- `nslookup`
- DNS zone transfer attempts

Task 1: Primary Domain Lookup

```
dig telenor.com
```

Output Analysis:

```
telenor.com.            5       IN      A       20.100.134.111
Query time: 3 msec
SERVER: 192.168.198.2#53
```

Findings:

- Domain resolves to IP: 20.100.134.111 (Azure owned IP range)
- Response time: 3ms (indicates cached/fast response)
- Single A record (basic DNS configuration)

Task 2: Nameserver Enumeration

```
dig telenor.com NS +noall +answer
```

Output:

```
telenor.com.            5       IN      NS      ns1.nextra.no.
telenor.com.            5       IN      NS      ns2.nextra.no.
telenor.com.            5       IN      NS      nsp.dnsnode.net.
```

Nameserver Details:

Nameserver	IP Address	Provider
ns1.nextra.no	148.122.208.98	Nextra (Norwegian hosting)
ns2.nextra.no	148.122.161.2	Nextra (Norwegian hosting)
nsp.dnsnode.net	194.58.198.32	DNSNode

Analysis:

- DNS hosted externally (not on Azure infrastructure)
- Multiple providers indicate redundancy
- Nextra is primary DNS provider (Norway-based)
- DNSNode provides tertiary backup

Task 3: Zone Transfer Attempt

```
dig @ns1.nextra.no telenor.com AXFR
```

Result: Transfer Failed

Analysis:

- Zone transfer properly restricted (security best practice)
- Indicates mature DNS security configuration
- No DNS enumeration possible via AXFR method

Task 4: Additional DNS Records

```
dig telenor.com MX +noall +answer
dig telenor.com TXT +noall +answer
```

Mail Server Records (MX):

- Identifies email infrastructure
- Used for SMTP routing

Text Records (TXT):

- SPF (Sender Policy Framework): Defines authorized mail servers
- DKIM: Email authentication
- Verification records

Subdomain Enumeration Results

Passive Method Results: 810 Subdomains

Tools/Sources Used:

- Certificate Transparency logs (crt.sh database)
- WHOIS historical data
- Search engine indexes
- DNS record aggregators

Example Subdomains Discovered:

- api.telenor.com
- mail.telenor.com
- cdn.telenor.com
- web.telenor.com
- admin.telenor.com
- dev.telenor.com
- staging.telenor.com
- customer.telenor.com

Why Passive Enumeration is Effective:

- No direct queries to target systems (stealthy)
- Uses public certificate logs (SSL/TLS certificates must be logged)
- Reveals infrastructure planning and services
- 810 subdomains indicate large, complex infrastructure

Infrastructure Analysis

CDN Provider: Azure Front Door

Identification Method: wmtips tool analysis

What This Reveals:

- Telenor uses Microsoft Azure cloud services
- Traffic routed through Azure's global CDN network
- DDoS protection and WAF (Web Application Firewall) capabilities
- Content delivery optimization

Security Implications:

- Azure infrastructure is hardened and monitored
- Rate limiting and bot protection likely enabled
- SSL/TLS termination at edge locations

- Geographic redundancy across Azure regions

Security Assessment

Strengths Identified:

1. Zone transfers properly disabled
2. External DNS provider (reduces single point of failure)
3. Multiple nameserver redundancy
4. Azure CDN protection (advanced filtering)
5. HTTPS enforcement (implied by CDN usage)

Potential Weaknesses:

1. Large subdomain footprint (810 discovered) increases attack surface
2. Legacy subdomains may not be maintained
3. Passive enumeration revealed extensive infrastructure
4. External DNS providers increase dependency chain

Tools & Techniques Summary

Tool	Type	Purpose	Result
dig	Active DNS	Query DNS records directly	Found nameservers, IPs
nslookup	Active DNS	Interactive DNS queries	Confirmed DNS infrastructure
wmtips	Passive	CDN/Infrastructure fingerprinting	Identified Azure Front Door
crt.sh	Passive	Certificate Transparency logs	Found 810 subdomains
WHOIS	Passive	Domain registration info	Company details

Recommendations for Next Steps

1. **Vulnerability Scanning:** Scan discovered subdomains for open ports and services
2. **Web Application Testing:** Analyze web applications for vulnerabilities
3. **Email Security:** Test SPF/DKIM/DMARC configuration
4. **Further Enumeration:** Perform brute-force subdomain discovery on high-value targets
5. **Social Engineering:** Research employee information for phishing campaigns
6. **Exploit Research:** Identify known vulnerabilities in discovered services

Conclusion

The reconnaissance phase successfully identified Telenor's infrastructure, revealing a mature organization with:

- Centralized CDN protection (Azure Front Door)
- Distributed DNS infrastructure
- Extensive service footprint (810 subdomains)
- Proper security controls (zone transfer restrictions)

The combination of passive and active methods provided comprehensive visibility into the target's infrastructure without triggering security alerts, making this an effective foundation for subsequent penetration testing phases.

Timeline

Date	Task	Status
2025-10-28	Passive reconnaissance	Complete
2025-10-28	Active DNS enumeration	Complete
2025-10-28	Infrastructure analysis	Complete

Disclaimer

This lab report is for educational and authorized testing purposes only. Unauthorized access to computer systems is illegal. Always obtain proper authorization before conducting security assessments.

Lab Conducted By: [Taha Asim]
Date: October 28, 2025
Course: CEH Preparation