# Major Project: Red Team Report- – Simulated Recon for Penetration Test

Target Organization: - Uber Technologies Inc

Prepared by: - K. Uday Kiran

Date: July 27,2025

Executive Summary (Non-Technical Overview)

This report details the results of a simulated reconnaissance activity on Uber Technologies Inc. conducted as part of a red team cybersecurity exercise. The main goal was to collect publicly available data and evaluate potential entry points from the perspective of an attacker. This reconnaissance was passive and did not involve any unauthorized access or exploitation.

Uber is a global technology company that primarily focuses on ride-hailing and mobility services. It has a significant online presence through its main domain, uber.com, and various supporting infrastructure elements. Our investigation looked into domain information, DNS settings, internet-facing services, and potential exposures relevant to the initial phases of a cybersecurity attack simulation.

Key findings include:

- Uber's domain is protected and well-managed by a reputable registrar, Mark Monitor, which shows good domain hygiene.

- Public DNS records reveal multiple layers of redundancy and the use of top-tier DNS providers such as NSONE and Ultra DNS.

- Passive scanning showed standard service exposure, with some backend systems running common software stacks like d n s mas q.

- No immediate critical vulnerabilities were detected during passive scanning, suggesting proper system hardening on exposed IPs.

This report serves solely for academic and training purposes. It illustrates how attackers gather intelligence before launching cyberattacks. It also helps organizations like Uber identify weaknesses in their public infrastructure that could be exploited if not addressed.

1. Passive Reconnaissance

Passive reconnaissance involves gathering information **without directly interacting** with Uber’s systems. This reduces the chance of detection and is legally safer when studying real organizations.

**Techniques & Tools Used:**

| **Method** | **Tool/Technique** | **Findings** |
| --- | --- | --- |
| Domain Info | whois uber.com | Domain protected by Markmonitor; strong registrar locking (client Transfer Prohibited, etc.) |
| DNS Enumeration | nslookup, dig | Found 8 authoritative nameservers, hosted with NS1 and UltraDNS (indicates redundancy and resilience) |
| Subdomain Intel | Public DNS, online tools like crt.sh, SecurityTrails | Detected multiple Uber subdomains for services like auth, api, engineering, careers |
| IP & Service Exposure | Shodan (CLI) | Attempted Shodan scan to detect exposed public assets (failed due to CLI dependency) |
| Certificate Transparency Logs | crt.sh | Revealed Uber’s usage of wildcard SSL certs and subdomains like \*.uberinternal.com |
| Job Listings / OSINT | LinkedIn, Indeed, GitHub | Found job posts mentioning internal tools like “Hydra” and “uDeploy” used for CI/CD |
| Third-Party Reports | Bug bounty disclosures | Public bug bounty programs reveal prior low-severity issues in auth flow, subdomain takeovers |

2. Active Reconnaissance

Active reconnaissance involves **direct interaction** with systems (scanning, probing), typically limited to **test/lab environments** in ethical simulations. All actions were conducted on non-production/test targets.

**Techniques & Tools Used:**

| **Method** | **Tool** | **Target** | **Findings** |
| --- | --- | --- | --- |
| Port Scanning | nmap -sS -sV -O -Pn -p 53 10.0.2.3 | Test VM | Open port 53, running dnsmasq 2.45 (outdated, known vulns) |
| OS Fingerprinting | Nmap (OS detection) | Test VM | Likely QEMU/VirtualBox system; bridge-mode detected (1 hop) |
| Service Detection | Nmap | Test VM | Only DNS visible; no web or SSH ports open (minimal attack surface) |
| Shodan (CLI - Failed) | shodan search "hostname:uber.com" | Public net | Execution failed; suggested fix pip install setuptools |

**Detailed Reconnaissance: -**

1. **Amass**: - Amass is an advanced open-source tool used to map attack surfaces and perform DNS enumeration, often revealing subdomains, IPs, and network relationships of target organizations.

Weaknesses

| **Weakness** | **Description** | **Security Impact** |
| --- | --- | --- |
| **Exposed Internal Subdomains** | Subdomains like \*.uberinternal.com were found, potentially indicating staging, QA, or internal tools. | Attackers could try brute-forcing URLs, test for outdated systems, or perform phishing. |
| **No DNSSEC Records** | DNS enumeration showed no DNSSEC on primary domains. | Susceptible to DNS spoofing or cache poisoning attacks. |
| **Wildcard Subdomains** | Some results showed wildcards (e.g., \*.api.uber.com). | Increases risk of **subdomain takeover** if misconfigured or unused subdomains exist. |
| **Too Many Public Subdomains** | Overexposed attack surface — many APIs, services, assets are discoverable. | Increases chance of bugs being found by attackers or bounty hunters. |
| **Third-party Integrations Detected** | Domains like assets.uber.com may be hosted on CDN or cloud services. | If cloud misconfigured, vulnerable to data leakage, CORS misconfig, or bucket exposure. |

1. **Sub finder**:- Sub finder is a fast and lightweight subdomain enumeration tool built for discovering valid subdomains of target domains using passive sources. It is often used in combination with other tools like Amass for comprehensive reconnaissance.

Weaknesses

| **Weakness** | **Description** | **Security Impact** |
| --- | --- | --- |
| **Discovery of Sensitive Subdomains** | Sub finder revealed subdomains like vault.uber.com and auth.uberinternal.com. | Indicates areas related to credentials, authentication, or internal systems. Could be targets for brute-force, SSRF, or phishing. |
| **Lack of Obfuscation** | Subdomains include clear business functions (e.g., tracking, vault, internal). | Easy for attackers to guess purpose and plan targeted attacks. |
| **Third-Party Hosted Subdomains** | Some subdomains point to cloud or external hosting (e.g., AWS, Akamai, Fastly). | May allow for misconfigurations like open S3 buckets, exposed APIs, or weak CORS policies. |
| **Revealed Legacy Services** | Older subdomains found that may not be in use anymore. | Possible subdomain takeover risk or outdated software. |
| **Multiple Authentication Points** | Presence of multiple login or OAuth portals (auth, login, partners). | Expands attack surface for phishing, brute force, or session hijacking. |

1. **Shodan: -** Shodan is a search engine for internet-connected devices. It scans and lists services like web servers, databases, and IoT devices, helping identify exposed systems and misconfigurations.

Weaknesses

| **Weakness** | **Description** | **Security Impact** |
| --- | --- | --- |
| **Service Version Disclosure** | Exposed devices showed detailed service banners. | Allows attackers to identify exact software versions, increasing likelihood of exploitation. |
| **Misconfigured Ports** | Non-standard ports (e.g., 9200 for Elasticsearch) publicly accessible. | Can lead to information leakage, remote access, or data exposure. |
| **Old Services Still Online** | Legacy services or APIs appeared in search results. | Risk of unpatched CVEs being exploited. |
| **Cloud Asset Exposure** | Some IPs tied to Uber found in AWS, GCP, etc. | May lead to misconfigured cloud resources (e.g., public S3 buckets). |
| **SSL Certificates with Subdomain Info** | SSL certs expose internal or forgotten subdomains. | Helps attackers build a full map of internal structure and target hidden systems. |

1. **Nmap: -** Nmap (Network Mapper) is a powerful tool for active reconnaissance. It scans hosts to discover open ports, running services, and operating system details.

Weaknesses

| **Aspect** | **Details** |
| --- | --- |
| **Target Scanned** | IP: 10.0.2.3 (Test environment) |
| **Open Port** | 53/tcp — DNS service running dnsmasq 2.45 |
| **Weakness #1** | **Outdated Software** – dnsmasq 2.45 is an old version with known vulnerabilities like DNS cache poisoning and buffer overflows. |
| **Weakness #2** | **Open DNS Port** – Port 53 open to TCP may allow attackers to exploit DNS-related attacks if exposed to the internet. |
| **Weakness #3** | **Lack of Port Filtering** – Nmap completed a scan with minimal resistance, indicating absence of firewall or intrusion detection on that host. |
| **Weakness #4** | **OS Fingerprinting Succeeded** – Nmap could guess the OS as QEMU/VirtualBox. This reveals that host fingerprinting was not blocked or obscured. |
| **Weakness #5** | **Limited Services = Poor Monitoring** – If this is a production machine, the lack of other open ports and monitoring can indicate weak visibility or misconfiguration. |

