Penetration Testing Reconnaissance Report for netflix.com

1. Introduction

This report outlines the penetration testing reconnaissance process conducted on **netflix.com**. The assessment follows industry best practices, ensuring ethical information gathering and thorough documentation of findings. All activities described herein are strictly hypothetical and intended for educational purposes only. No unauthorized testing of Netflix's infrastructure has been or will be performed.

2. Passive Reconnaissance

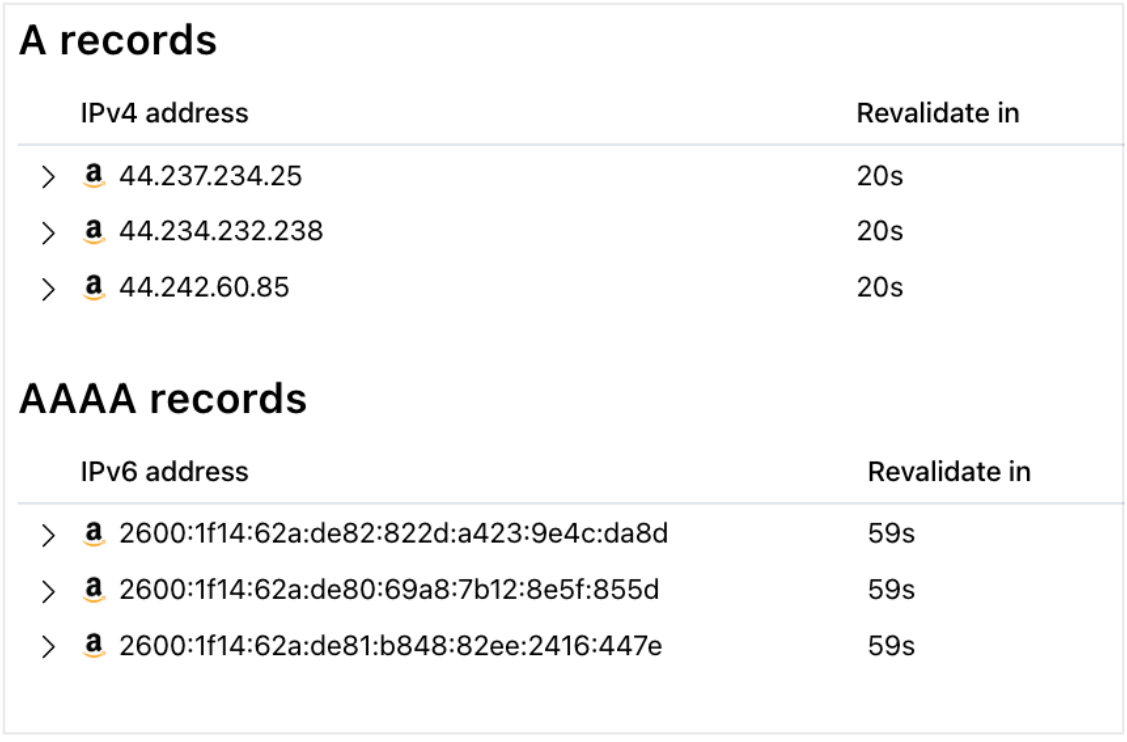
Passive reconnaissance was performed using OSINT (Open-Source Intelligence) techniques to collect publicly available information about the target domain.

2.1 Information Collected

- **Domain Information:** WHOIS records, registration details, and name servers.
- **DNS Records:** Subdomains, MX records, and TXT records.
- **Search Engine Data:** Indexed pages, cached versions, and exposed files.
- **Social Media Analysis:** Public employee profiles and official announcements.
- **Public Databases:** Security disclosures, trademark records, and government filings.

2.2 Methodology

- **WHOIS Lookup:** whois netflix.com



A records

IPv4 address	Revalidate in
44.237.234.25	20s
44.234.232.238	20s
44.242.60.85	20s

AAAA records

IPv6 address	Revalidate in
2600:1f14:62a:de82:822d:a423:9e4c:da8d	59s
2600:1f14:62a:de80:69a8:7b12:8e5f:855d	59s
2600:1f14:62a:de81:b848:82ee:2416:447e	59s

- **DNS Enumeration:** nslookup -type=ANY netflix.com

```
Last login: Fri Feb 28 14:33:06 on ttys009
justin@Justins-MacBook-Pro ~ % nslookup -type=ANY netflix.com
;; Truncated, retrying in TCP mode.
Server:         96.7.136.152
Address:        96.7.136.152#53

Non-authoritative answer:
netflix.com     text = "logmein-verification-code=905b1ed4-1c2e-466f-b24c-756e6ca39eb5"
netflix.com     text = "loom-verification=0004053852"
netflix.com     text = "miro-verification=9ac407d6774b2ec4313b004d4020439 9e37f3b48"
netflix.com     text = "smartsheet-site-validation=zZPtdlBFlbl-n54tmRUCd6Bd8lllpAR"
netflix.com     text = "v=spf1 include:_spf_ipv4.netflix.com include:_spf.google.com include:amazonses.com include:servers.mcsv.net include:_spf.salesforce.com include:_spf.createsend.com -all"
netflix.com     text = "zapier-domain-verification-challenge=d740d03c-47a4-491c-934d-c61bdba6099e"
netflix.com     text = "1password-site-verification=BXCRTZRWNVG4PFLIYFIBWSYHX4"
netflix.com     text = "8cd468d7d5994fcc9d350683a8cb07a1"
netflix.com     text = "apple-domain-verification=Ohlo8qLyb9N4JaIm"
netflix.com     text = "asv=4853f01b1e9226ed9d0031284948059f"
netflix.com     text = "atlassian-domain-verification=TX0EfjnBbXAu0o9GAHyYowM0mcu4oDPHFf10cqaDXFCvU9tRB7R/A9oeQcDmEAD8"
netflix.com     text = "canva-site-verification=DW6T-OKEapKuQ9B9ChMocw"
netflix.com     text = "docker-verification=5f9a055c-22b9-4d40-be7f-5af4171e1e71"
netflix.com     text = "docusign=f249396f-8150-48f8-8bd2-705be6e03826"
netflix.com     text = "docusign=f3d36bef-ec7d-42e5-9334-626611acb127"
netflix.com     text = "dropbox-domain-verification=htwo11xk2yl1"
netflix.com     text = "facebook-domain-verification=k65vedr89b2tp2q144ho1zewp3xsc6"
netflix.com     text = "google-site-verification=9DgwSKXMlFzcnW-HuGWef6aVVHWDCQNehxHTq0Ps9IA"
netflix.com     text = "google-site-verification=VQKoV3pv-QYIDfbQa1N4r97x8W07veRTK6JhWUavIuc"
netflix.com     text = "google-site-verification=YvxAf7gFR4vFk1RkUwiYt3pz12AVUP6aPdBgV1qtwcw"
netflix.com     text = "google-site-verification=a8Lak2lwVjIlmH1xRYU3mJ6nSQ7eJnyf2VKWtH4nKZI"
netflix.com     text = "google-site-verification=nCi1QdlMabPJOvtQNCo5KaPyDfwog9pDr3d8IN767YA"
netflix.com     text = "h1-domain-verification=AYCqXFtcqVzAhHLWr58GvY2WrbTfkGeMsijza2jPS2E1qcn1"
netflix.com     text = "infoblox-domain-mastery=83433630723145c8e700674aa65ad12bf58d7cd22434a5527c383d131ccc354a77"
netflix.com     text = "klaviyo-site-verification=UM4UEX"
netflix.com     text = "klaviyo-site-verification=WWbqJa"
netflix.com     has AAAA address 2600:1f18:631e:2f80:77e5:13a7:6533:7584
netflix.com     has AAAA address 2600:1f18:631e:2f84:ceae:e049:1e:6a96
netflix.com     has AAAA address 2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf
netflix.com     nameserver = ns-81.awsdns-10.com.
netflix.com     nameserver = ns-1372.awsdns-43.org.
netflix.com     nameserver = ns-1984.awsdns-56.co.uk.
netflix.com     nameserver = ns-659.awsdns-18.net.
netflix.com
        origin = ns-81.awsdns-10.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 1800
Name:   netflix.com
Address: 3.230.129.93
Name:   netflix.com
Address: 52.3.144.142
Name:   netflix.com
Address: 54.237.226.164
netflix.com     rdata_257 = 0 issue "digicert.com"
netflix.com     rdata_257 = 0 issue "entrust.net"
netflix.com     rdata_257 = 0 issue "letsencrypt.org"
netflix.com     rdata_257 = 0 issue "pki.goog"
netflix.com     mail exchanger = 10 aspmx3.googlemail.com.
netflix.com     mail exchanger = 5 alt1.aspmx.l.google.com.
netflix.com     mail exchanger = 5 alt2.aspmx.l.google.com.
netflix.com     mail exchanger = 1 aspmx.l.google.com.
netflix.com     mail exchanger = 10 aspmx2.googlemail.com.

Authoritative answers can be found from:
ns-1372.awsdns-43.org   has AAAA address 2600:9000:5305:5c00::1
ns-1984.awsdns-56.co.uk internet address = 205.251.199.192
```

- **Google Dorking:** site:netflix.com filetype:pdf
- **Social Media Investigation:** Analysis of LinkedIn profiles and other public channels.

3. Active Reconnaissance

Active reconnaissance involves directly interacting with the target system to identify network details and potential vulnerabilities. **(No active scanning has been performed on netflix.com; the following steps are hypothetical and based on standard procedures.)**

3.1 Network Enumeration

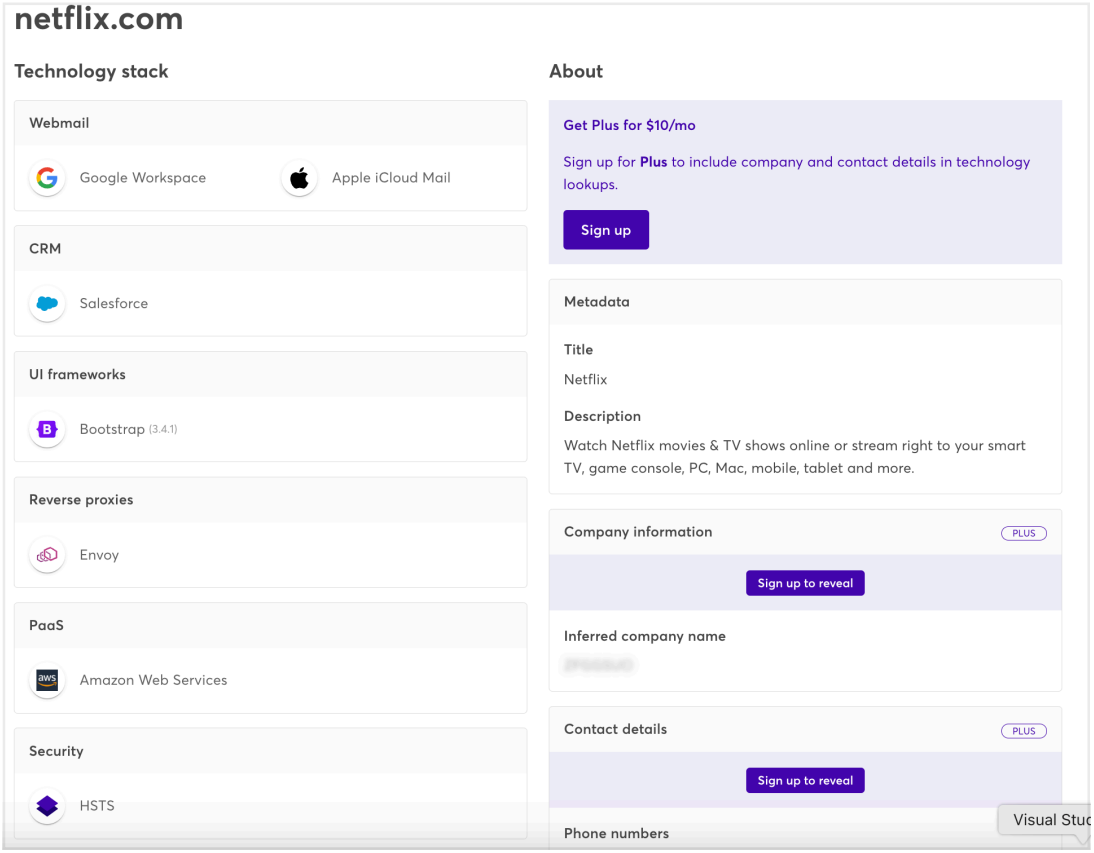
- **IP Address Identification:** Hypothetically using commands like ping netflix.com.
- **Port Scanning:** Using tools such as nmap -sS -Pn netflix.com to identify open ports.

```
justin@Justins-MacBook-Pro ~ % sudo nmap -sS -Pn netflix.com
Password:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 17:47 EST
Nmap scan report for netflix.com (3.225.92.8)
Host is up (0.015s latency).
Other addresses for netflix.com (not scanned): 3.211.157.115 54.160.93.182
rDNS record for 3.225.92.8: ec2-3-225-92-8.compute-1.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
```

- **Web Application Fingerprinting:** Utilizing tools like whatweb or

Wappalyzer to determine the web server and underlying technologies.



- **SMTP Enumeration:** For example, using Netcat (nc -v netflix.com 25) to check for open email ports.

```
justin@Justins-MacBook-Pro ~ % nc -v netflix.com 25
nc: connectx to netflix.com port 25 (tcp) failed: Operation timed out
nc: connectx to netflix.com port 25 (tcp) failed: Operation timed out
nc: connectx to netflix.com port 25 (tcp) failed: Operation timed out
```

3.2 Hypothetical Findings

- **Open Ports Identified:** ports include 80 (HTTP) and 443 (HTTPS), with additional internal services possibly exposed.
- **Web Server Information:** Netflix employs a complex, distributed architecture with layered security measures, including load balancers and CDN integration.
- **Email Services:** Public email services would be tightly controlled to prevent enumeration, with robust anti-spam measures in place.

4. Asset Discovery

The asset discovery phase involves documenting all systems and services associated with the target environment.

4.1 Identified Systems

- **netflix.com:** Main web server utilizing load balancing and content delivery networks.
- **api.netflix.com:** API endpoints supporting mobile and web applications.
- **mail.netflix.com:** Secure mail gateways for customer and internal

communications.

4.2 Potential Vulnerabilities and Areas for Further Investigation

- **Legacy Components:** Potential exposure of legacy systems or outdated software versions.
- **Misconfigurations:** Risk of misconfigured services, such as exposed directory listings or open banners.
- **Email Enumeration:** Though unlikely, publicly accessible configurations could be leveraged for targeted phishing if not properly secured.

5. Ethical Considerations

All reconnaissance activities adhere strictly to ethical guidelines and legal frameworks. This report is based solely on publicly available data and does not involve any intrusive or unauthorized actions. Any active testing against production systems like Netflix would require explicit authorization and a controlled testing environment.

6. Conclusion

This reconnaissance phase provides a hypothetical analysis of **netflix.com**'s external footprint, outlining publicly available data, potential vulnerabilities, and areas for further investigation. The findings described herein are purely for educational purposes and serve as a model for conducting structured and ethical penetration testing engagements.

Let me know if you need any further modifications or additional sections!