Cloud Mapping Report:

University of California, Irvine

Created by Edwin Miyatake
University of California, Irvine

Objective

This report documents the methodology, tools, findings, and security analysis of publicly exposed cloud application assets associated with the University of California, Irvine (UCI). The goal is to map UCI's cloud presence and identify potential risks.

Passive Reconnaissance

The reconnaissance began with identifying publicly available information about UCI's domains. Whois.com was used to gather basic network information. Given that UCI is a public university, it provides organizational details that facilitate information gathering. The primary goal of this phase was to identify UCI's cloud resources, including associated domains and IP addresses. To enumerate subdomains, I initially attempted to use pen-tools.com for scanning. However, the output format was not accessible through terminal commands. To resolve this, I used a Python package called sublist3r to generate a text file containing all discovered subdomains.

```
py sublist3r.py -d uci.edu -o uci_subdomains.txt
```

To resolve the IP addresses associated with UCI's subdomains, I utilized the dig command. The script used was:

```
cat uci_subdomains.txt | while read domain; do dig +short $domain; done > subdomain_ips.txt
```

This process produced a list of IP addresses corresponding to UCI's subdomains.

To determine which cloud service providers UCI utilizes, I compared the discovered IP addresses against known IP address ranges of major cloud providers such as AWS, Azure, and Google Cloud. The process included downloading JSON files containing IP ranges for each provider, formatting the JSON files by removing unnecessary characters to ensure proper structure for comparison, and using the comm function to identify matches between UCI's subdomain IP addresses and the cloud provider IP ranges. The results indicated that UCI uses a combination of AWS, Azure, and Google Cloud services. Code used:

- Amazon Web Services

    -
      ```
      curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq '.prefixes[] | .ip_prefix'
      ```
- Azure Cloud Computing Services

    -
      ```
      curl -O https://download.microsoft.com/download/1/4/4/1442A4FB-6FE6-45DB-973C-9E17F50E03AC/ServiceTags_Public_20250217.json
      ```

    -
      ```
      jq '.values[] | .properties.addressPrefixes[]' ServiceTags_Public_20250217.json
      ```
- Google Cloud Services

    - *curl -s https://www.gstatic.com/ipranges/cloud.json | jq '.prefixes[] | .ipv4Prefix' > google_ips.txt*
- Script used to compare each list of IP ranges to UCI subdomain IPs
    - *comm -12 aws_ips_sorted.txt subdomain_ips_sorted.txt > matching_ips.txt*

Active Reconnaissance

For active information retrieval, an nmap scan was conducted to identify open ports on UCI's cloud assets. The scan targeted the most commonly used ports, including SSH (22), HTTP (80), and HTTPS (443). Initially, an attempt was made to scan all ports, but due to hardware limitations, specifically high CPU usage and excessive fan noise, the process was terminated after approximately twenty minutes. Instead, I performed a targeted scan of the three aforementioned ports.

```
nmap -p 22,80,443 -iL subdomain_ips.txt -T4 -oN uci_ports_scan.txt
```

The scan generated extensive results, with over 10,000 lines of text for just three ports. To document the findings, I uploaded a screenshot confirming the scan completion and a sample page from the scan results to illustrate the findings without overwhelming detail.

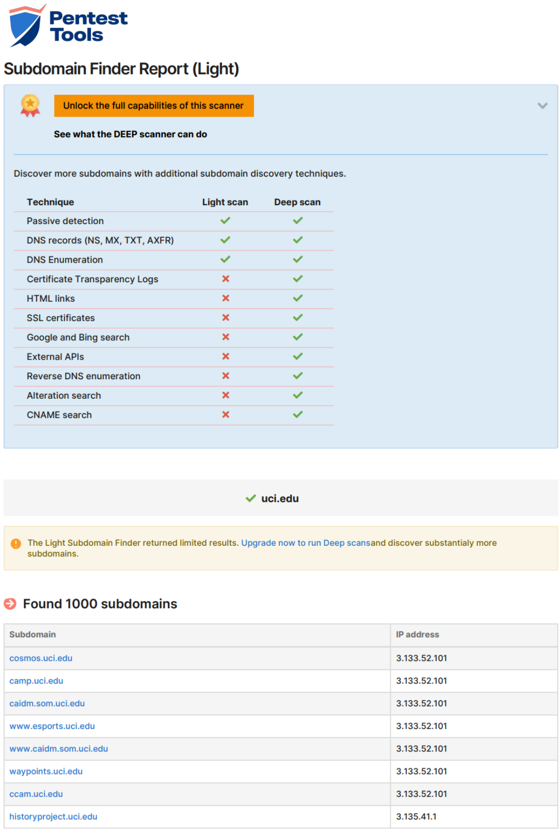
Conclusion

Through this cloud reconnaissance process, I successfully identified UCI's cloud service usage, including subdomains, IP addresses, and active ports. The university employs a hybrid cloud approach, leveraging AWS, Azure, and Google Cloud. While passive reconnaissance provided valuable insights, active scanning revealed additional security details. Further analysis could include deeper penetration testing, but such activities would require appropriate authorization.

End of Report

Screenshots

Light Scan of UCI (Pen-Tools) - will attach full report to canvas submission*



Subdomain Finder Report (Light)

See what the DEEP scanner can do

Discover more subdomains with additional subdomain discovery techniques.

Technique	Light scan	Deep scan
Passive detection	✓	✓
DNS records (NS, MX, TXT, AXFR)	✓	✓
DNS Enumeration	✓	✓
Certificate Transparency Logs	✗	✓
HTML links	✗	✓
SSL certificates	✗	✓
Google and Bing search	✗	✓
External APIs	✗	✓
Reverse DNS enumeration	✗	✓
Alteration search	✗	✓
CNAME search	✗	✓

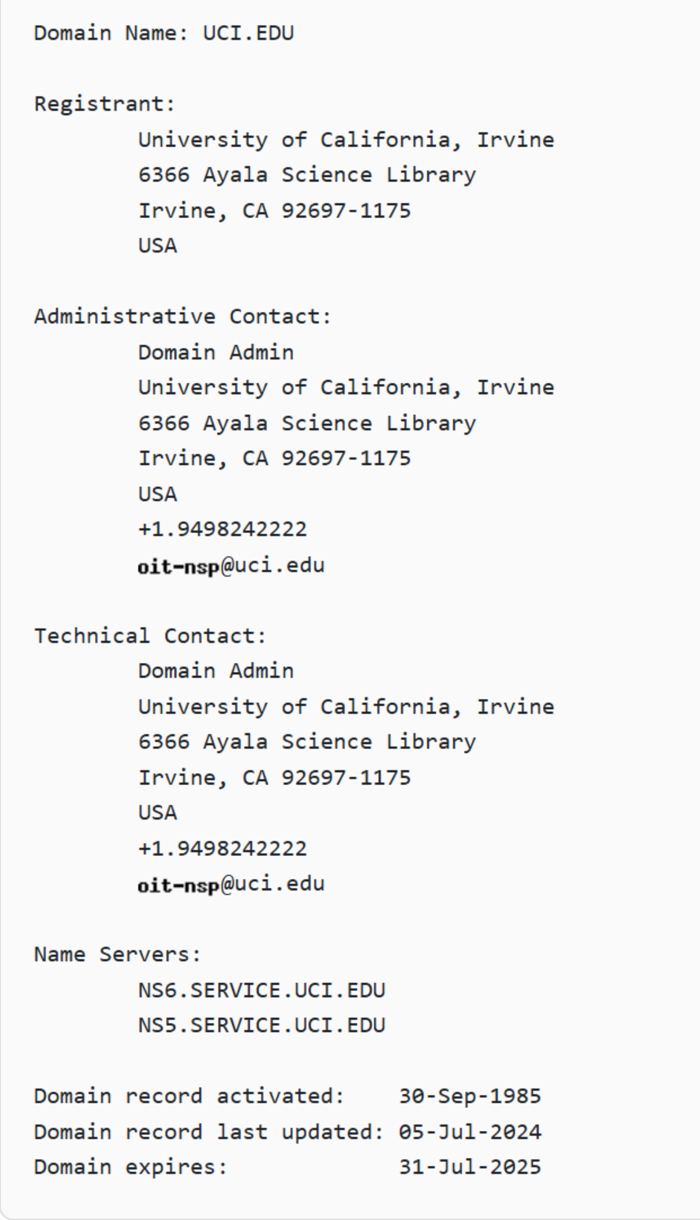
✓ uci.edu

The Light Subdomain Finder returned limited results. Upgrade now to run Deep scansand discover substantially more subdomains.

Found 1000 subdomains

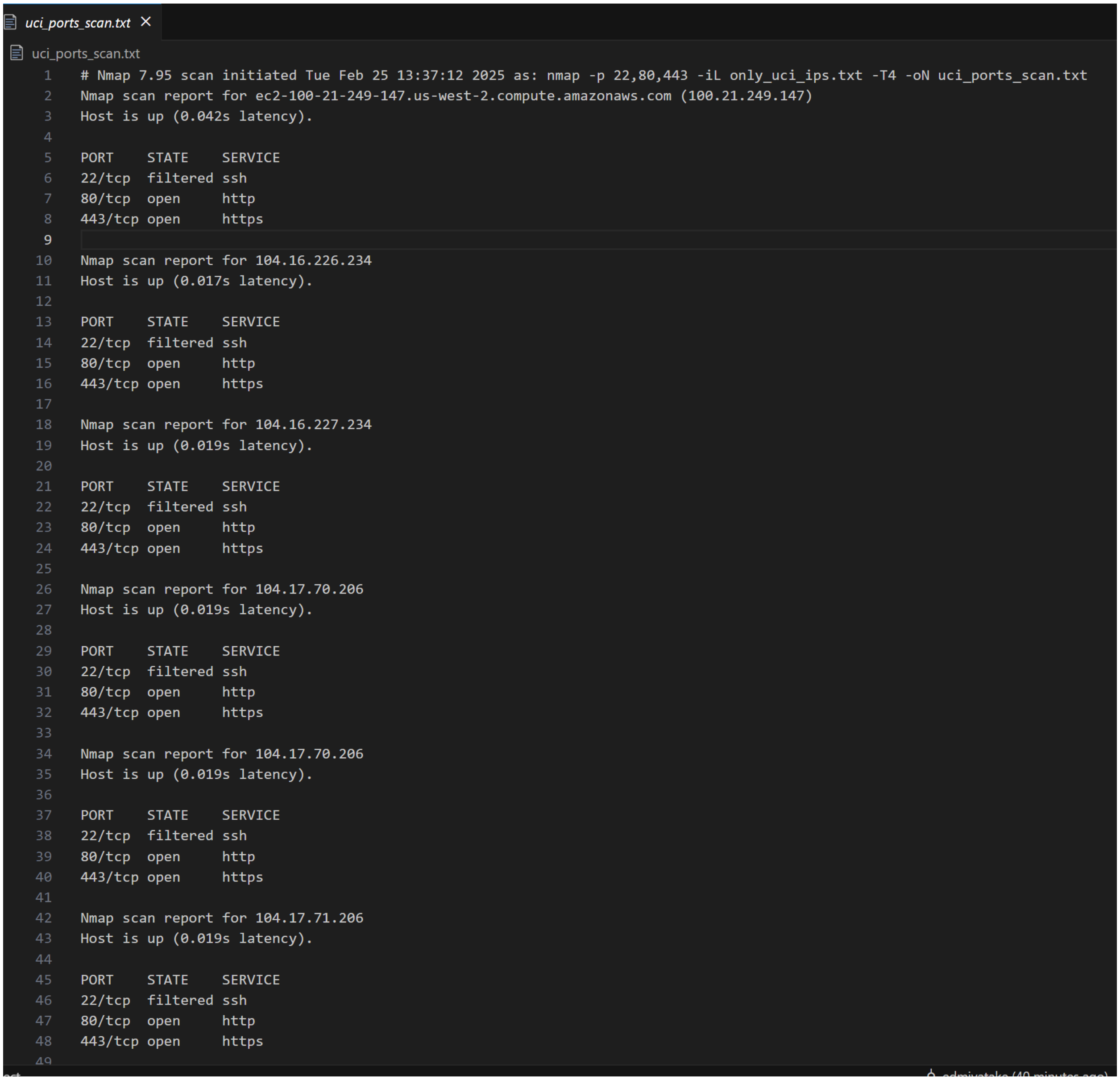
Subdomain	IP address
cosmos.uci.edu	3.133.52.101
camp.uci.edu	3.133.52.101
caidm.som.uci.edu	3.133.52.101
www.esports.uci.edu	3.133.52.101
www.caidm.som.uci.edu	3.133.52.101
waypoints.uci.edu	3.133.52.101
ccam.uci.edu	3.133.52.101
historyproject.uci.edu	3.135.41.1

Whois Lookup (uci.edu)

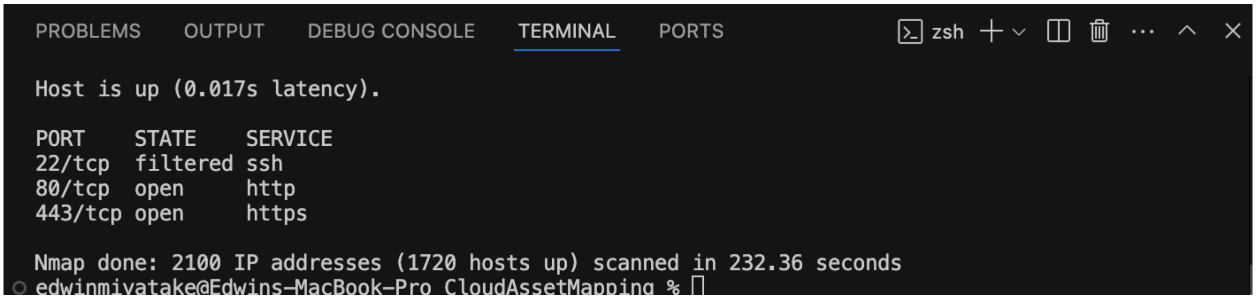


```
Domain Name: UCI.EDU

Registrant:
        University of California, Irvine
        6366 Ayala Science Library
        Irvine, CA 92697-1175
        USA

Administrative Contact:
        Domain Admin
        University of California, Irvine
        6366 Ayala Science Library
        Irvine, CA 92697-1175
        USA
        +1.9498242222
        oit-nsp@uci.edu

Technical Contact:
        Domain Admin
        University of California, Irvine
        6366 Ayala Science Library
        Irvine, CA 92697-1175
        USA
        +1.9498242222
        oit-nsp@uci.edu

Name Servers:
        NS6.SERVICE.UCI.EDU
        NS5.SERVICE.UCI.EDU

Domain record activated:    30-Sep-1985
Domain record last updated: 05-Jul-2024
Domain expires:             31-Jul-2025
```

Nmap scan of UCI



```
# Nmap 7.95 scan initiated Tue Feb 25 13:37:12 2025 as: nmap -p 22,80,443 -iL only_uci_ips.txt -T4 -oN uci_ports_scan.txt
Nmap scan report for ec2-100-21-249-147.us-west-2.compute.amazonaws.com (100.21.249.147)
Host is up (0.042s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap scan report for 104.16.226.234
Host is up (0.017s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap scan report for 104.16.227.234
Host is up (0.019s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap scan report for 104.17.70.206
Host is up (0.019s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap scan report for 104.17.70.206
Host is up (0.019s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap scan report for 104.17.71.206
Host is up (0.019s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https
```



```
Host is up (0.017s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap done: 2100 IP addresses (1720 hosts up) scanned in 232.36 seconds
edwinmiyatake@Edwins-MacBook-Pro CloudAssetMapping %
```