Submitted By:

Jawad Ali

Submitted To:

Mehar Muhammad Shaban Raza

TABLE OF CONTENT

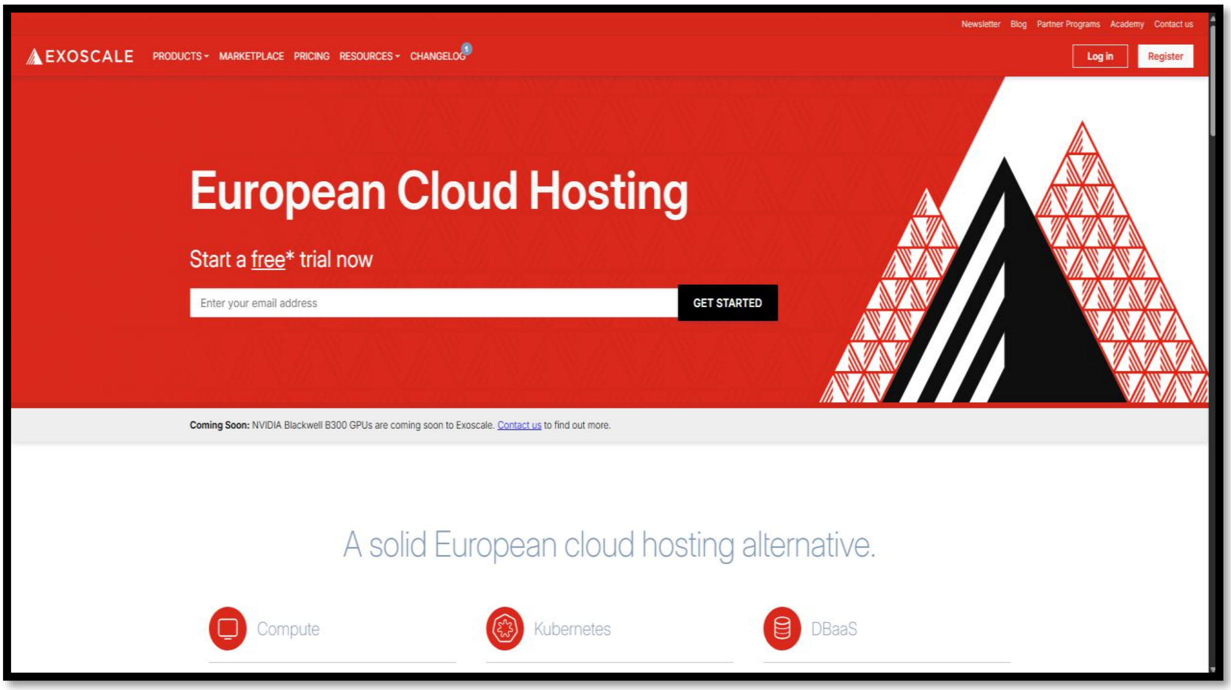
OSINT & Footprinting Investigation Report

Introduction:

OSINT and Footprinting are two of the most advance methodologies for collecting data about a target. **OSINT** (Open Source Intelligence) refers to the process of collecting and analyzing information from publicly available sources such as websites, social media, search engines, and public records. **Footprinting** is the initial phase of ethical hacking where a security professional or an attacker collects as much information as possible about a target. This includes details like domain names, IP addresses, operating systems, subdomains, technologies used, and network architecture.

Domain Under Investigation:

The domain under investigation is **Exoscale** which is a European cloud service provider. Exoscale was found in 2011, located in **Lausanne**, **Switzerland**. It is a subsidiary of **A1 Digital**, which itself is a part of **A1 Telekom Austria Group**. It has data centres in **Switzerland** (Geneva and Zurich), **Austria** (Vienna), **Germany** (Frankfurt and Munich), **Bulgaria** (Sofia), and **Croatia** (Zagreb). Reports indicate that Exoscale has around 86 employees across Europe.



European Cloud Hosting

Start a free* trial now

Enter your email address

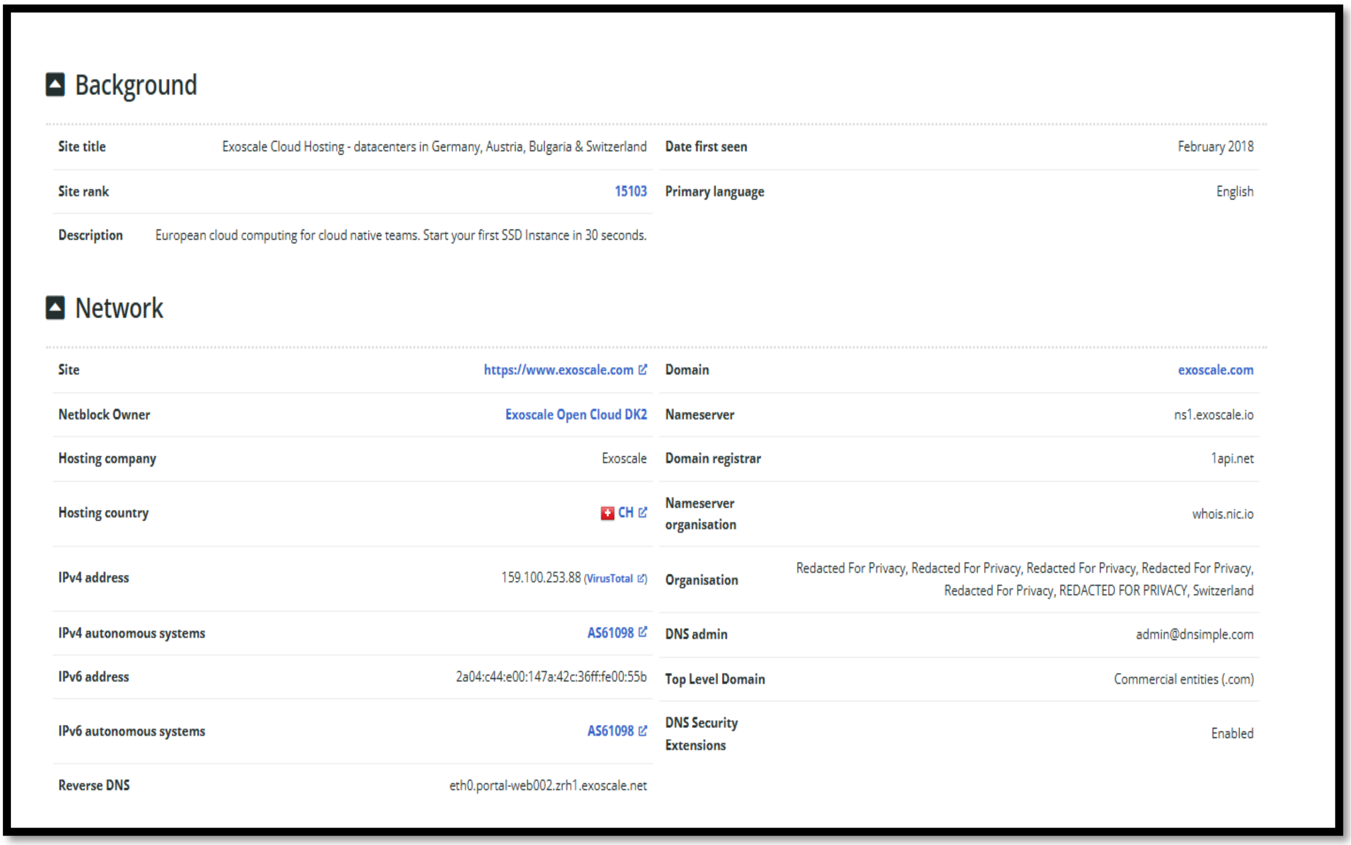
Coming Soon: NVIDIA Blackwell B300 GPUs are coming soon to Exoscale. Contact us to find out more.

A solid European cloud hosting alternative.

Domain and Subdomain Finding:

Domains and Subdomains are part of critical infrastructure for any organization. These can provide us useful information such as organizational history, services and products, and contact information. Here, we will use **Netcraft** to extract information about our target. Netcraft is used to collect data on hosting providers, IP addresses, DNS records, SSL certificates, and technologies in use.

Findings:



Background

Site title	Exoscale Cloud Hosting - datacenters in Germany, Austria, Bulgaria & Switzerland	Date first seen	February 2018
Site rank	15103	Primary language	English
Description	European cloud computing for cloud native teams. Start your first SSD Instance in 30 seconds.		

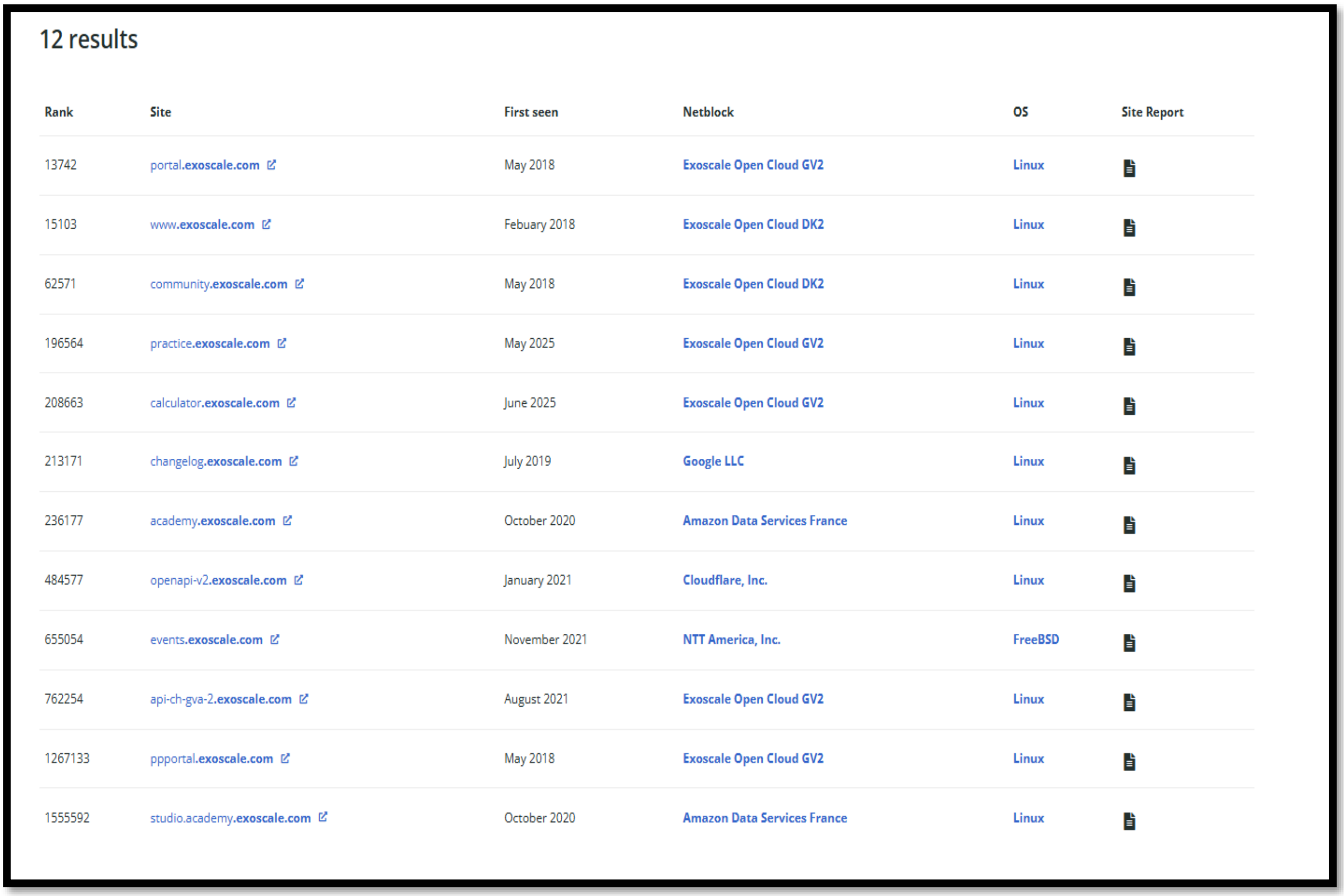
Network

Site	https://www.exoscale.com	Domain	exoscale.com
Netblock Owner	Exoscale Open Cloud DK2	Nameserver	ns1.exoscale.io
Hosting company	Exoscale	Domain registrar	1api.net
Hosting country	CH	Nameserver organisation	whois.nic.io
IPv4 address	159.100.253.88 (VirusTotal)	Organisation	Redacted For Privacy, Redacted For Privacy, Redacted For Privacy, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, Switzerland
IPv4 autonomous systems	AS61098	DNS admin	admin@dnsimple.com
IPv6 address	2a04:c44:e00:147a:42c:36ff:fe00:55b	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS61098	DNS Security Extensions	Enabled
Reverse DNS	eth0.portal-web002.zrh1.exoscale.net		

Here is what we found through Netcraft:

- **Domain:**
  The **domain** is exoscale.com.
- **Netblock Owner:**
  The netblock owner is **Exoscale Open Cloud DK2**. This refers to a subnet of IP addresses assigned to Exoscale.
- **Hosting Company and Country:**
  The hosting company is Exoscale, and the hosting country is Switzerland.
- **IPv4 Address:**
  The IPv4 address is 159.100.253.100.
- **Reverse DNS:**
  The reverse DNS is eth0.portal-web002.zrh1.exoscale.net. Here, **zrh1** strongly suggests that the server is in Zurich.

- **IPv4 Autonomous System (ASN):**
  The ASN for Exoscale is **AS61098** which is Exoscale's ASN. This confirms that Exoscale owns and operates its own IP ranges.
- **DNSSEC Enabled:**
  This tells us that domain is protected against certain DNS spoofing attacks.



12 results

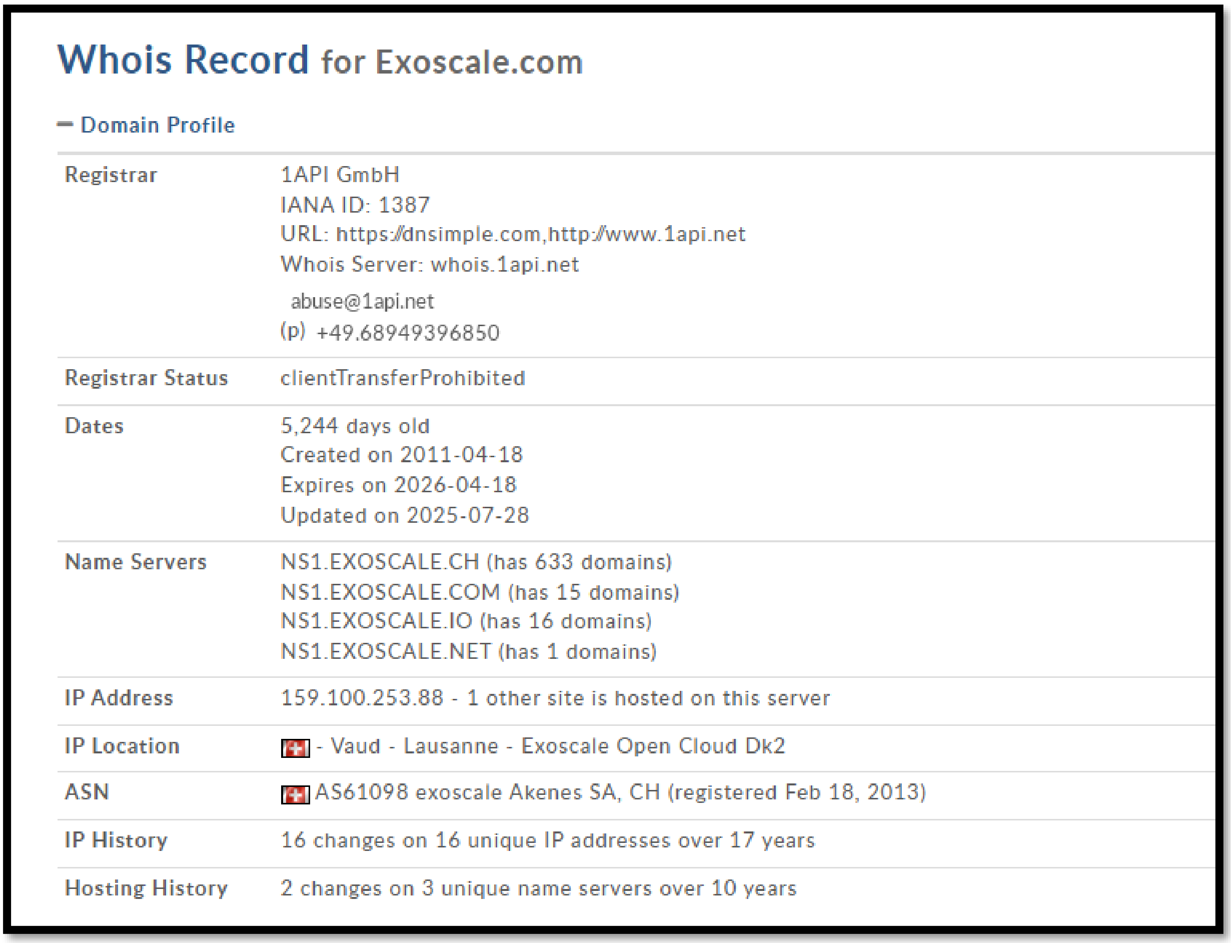
Rank	Site	First seen	Netblock	OS	Site Report
13742	portal.exoscale.com	May 2018	Exoscale Open Cloud GV2	Linux	📄
15103	www.exoscale.com	Febuary 2018	Exoscale Open Cloud DK2	Linux	📄
62571	community.exoscale.com	May 2018	Exoscale Open Cloud DK2	Linux	📄
196564	practice.exoscale.com	May 2025	Exoscale Open Cloud GV2	Linux	📄
208663	calculator.exoscale.com	June 2025	Exoscale Open Cloud GV2	Linux	📄
213171	changelog.exoscale.com	July 2019	Google LLC	Linux	📄
236177	academy.exoscale.com	October 2020	Amazon Data Services France	Linux	📄
484577	openapi-v2.exoscale.com	January 2021	Cloudflare, Inc.	Linux	📄
655054	events.exoscale.com	November 2021	NTT America, Inc.	FreeBSD	📄
762254	api-ch-gva-2.exoscale.com	August 2021	Exoscale Open Cloud GV2	Linux	📄
1267133	ppportal.exoscale.com	May 2018	Exoscale Open Cloud GV2	Linux	📄
1555592	studio.academy.exoscale.com	October 2020	Amazon Data Services France	Linux	📄

We found 12 subdomains associated with Exoscale. But the interesting result is that 11 of the subdomains are running on **Linux** Operating system while only one runs on **FreeBSD**. This could mean that:

- A specific service or software is running on FreeBSD. FreeBSD is often used for networking (firewalls, routers). It can also be used configured and used as a mail server, web server, firewall, FTP server, and DNS server.
- It is an old server that is still in production.
- It might be less maintained.
- It might prove to be a weak spot, and attackers might take advantage of this.

Domain History:

Next, we will investigate the domain history using **Whois** domain tools. Domain history is important because it tells us about ownership changes if there are any, it also shows past IP addresses, hosting providers, and DNS records.



Whois Record for Exoscale.com

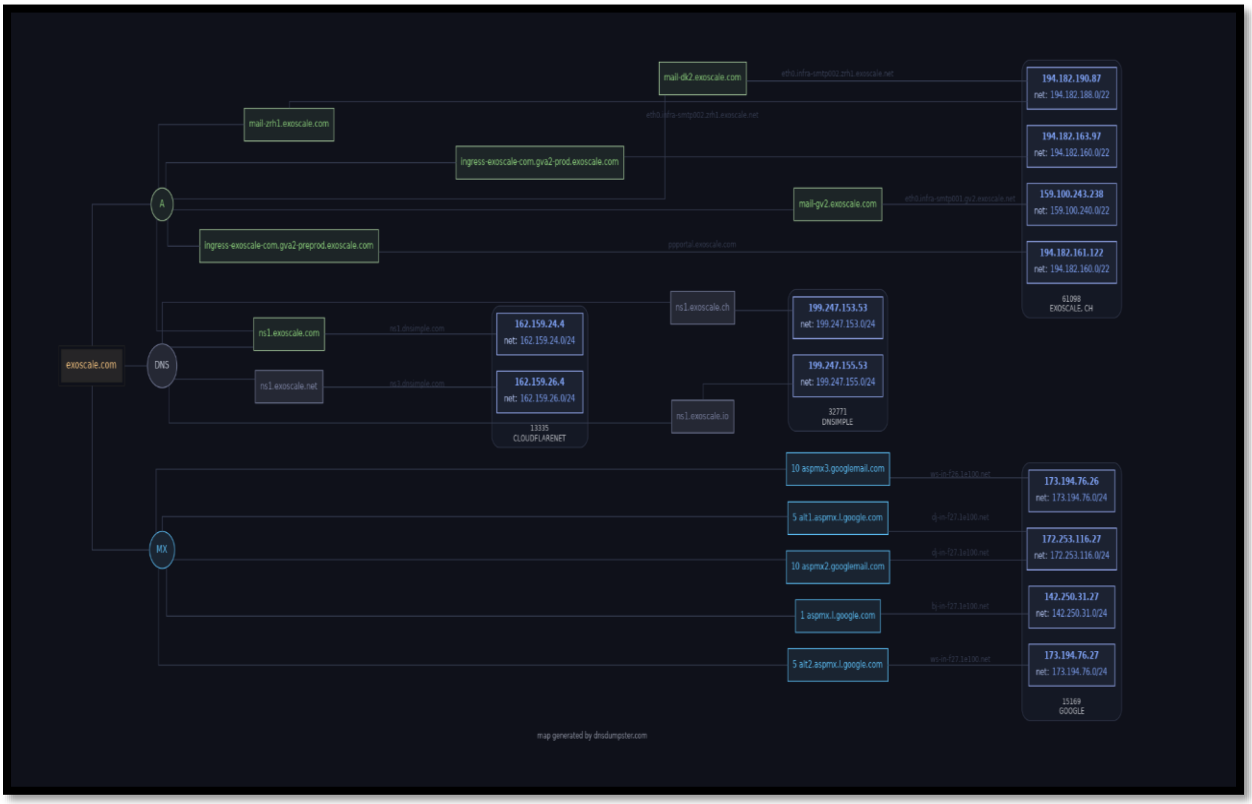
− Domain Profile

Registrar	1API GmbH IANA ID: 1387 URL: https://dnsimple.com,http://www.1api.net Whois Server: whois.1api.net abuse@1api.net (p) +49.68949396850
Registrar Status	clientTransferProhibited
Dates	5,244 days old Created on 2011-04-18 Expires on 2026-04-18 Updated on 2025-07-28
Name Servers	NS1.EXOSCALE.CH (has 633 domains) NS1.EXOSCALE.COM (has 15 domains) NS1.EXOSCALE.IO (has 16 domains) NS1.EXOSCALE.NET (has 1 domains)
IP Address	159.100.253.88 - 1 other site is hosted on this server
IP Location	- Vaud - Lausanne - Exoscale Open Cloud Dk2
ASN	AS61098 exoscale Akenes SA, CH (registered Feb 18, 2013)
IP History	16 changes on 16 unique IP addresses over 17 years
Hosting History	2 changes on 3 unique name servers over 10 years

The important information that we got from **Whois** is that the registrar is **1API GmbH,** which is a German company based in Homburg, Saarland, Germany. It only handles the domain registration for Exoscale. The second important information is Exoscale has been registered since **2011** and is valid until **2026**. A long registration history indicates a legitimate and established organization.

DNS Mapping:

DNS mapping is the process of identifying and visualizing how a domain name is connected to different DNS records. It helps us to see how a company's web, email, and other services are distributed. Here, we will use **dnsdumpster** to to do this task.



The above image shows the DNS infrastructure of Exoscale.

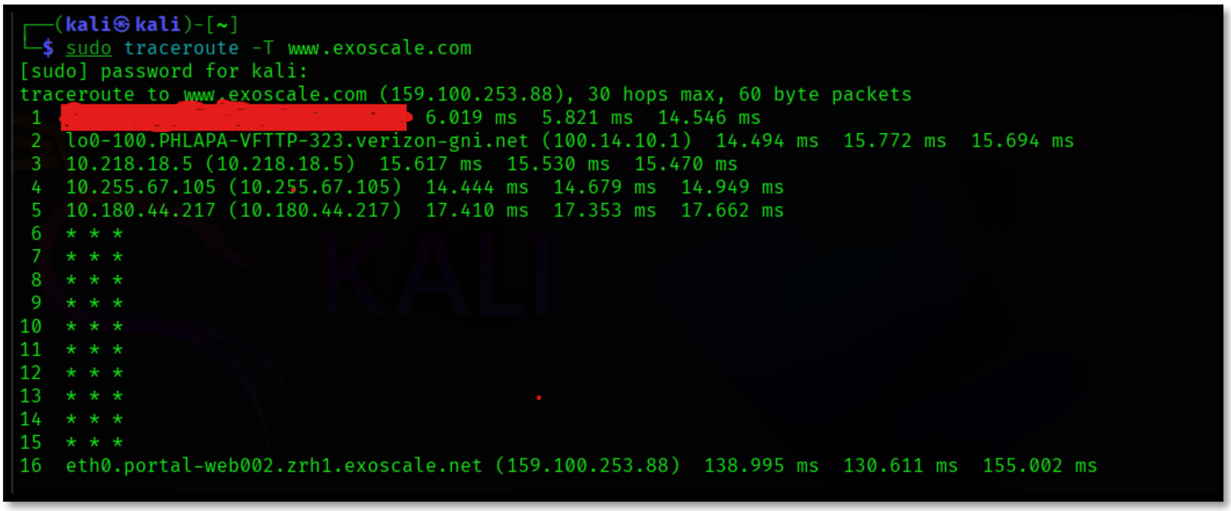
Findings:

Here is what we found through dnsdumpster:

- **Domain:**
  The center is **exoscale.com**, which is the main domain under investigation.
- **DNS Records:**
  We came to know that **mail-zh1.exoscale.com** goes to IPs in ranges 194.182.x.x or 159.100.x.x. This also shows us where the entry points are located.
- **MX Records:**
  Exoscale uses the email servers of Google.
- **NS Records:**
  Exoscale uses its own name servers (**ns1.exoscale.com**) but also external services like **DNSimple** and **Cloudflare**.

Network Footprinting:

Network footprinting is the process of gathering information about a target organization's network infrastructure. We use it to identify the attack surface of the target before performing penetration testing. We can also find outdated servers, misconfigured DNS, or exposed mail systems through network footprinting. Here, we will use **traceroute** to find out the path and hosts lying between us and Exoscale.

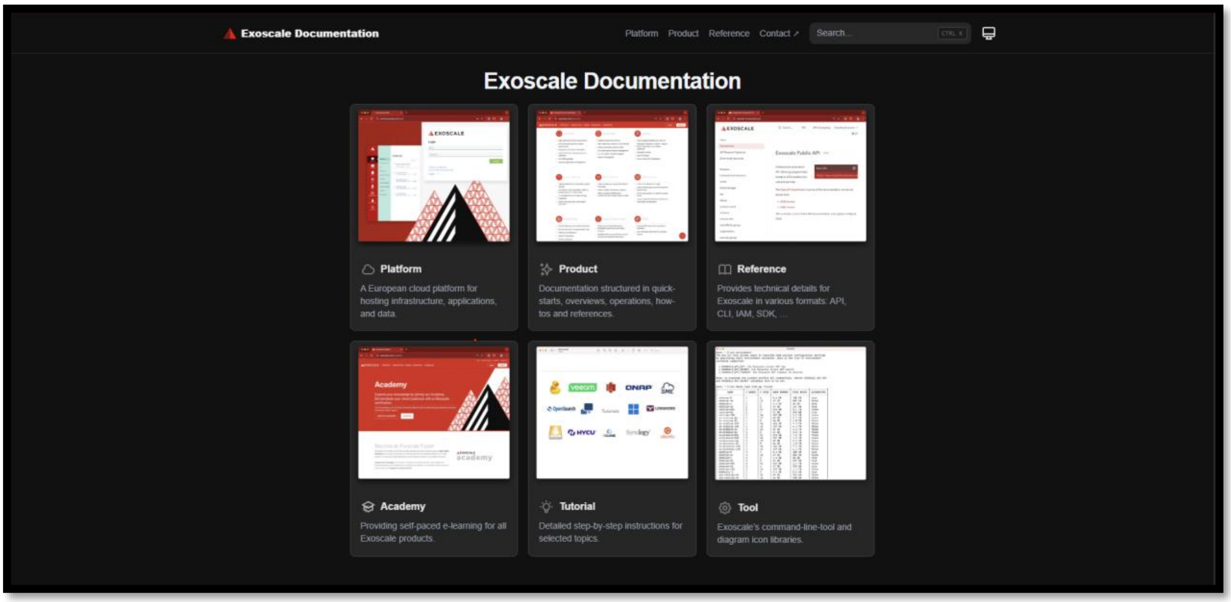


```
┌──(kali㉿kali)-[~]
└─$ sudo traceroute -T www.exoscale.com
[sudo] password for kali:
traceroute to www.exoscale.com (159.100.253.88), 30 hops max, 60 byte packets
 1  [redacted]  6.019 ms  5.821 ms  14.546 ms
 2  lo0-100.PHLAPA-VFTTP-323.verizon-gni.net (100.14.10.1)  14.494 ms  15.772 ms  15.694 ms
 3  10.218.18.5 (10.218.18.5)  15.617 ms  15.530 ms  15.470 ms
 4  10.255.67.105 (10.255.67.105)  14.444 ms  14.679 ms  14.949 ms
 5  10.180.44.217 (10.180.44.217)  17.410 ms  17.353 ms  17.662 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  eth0.portal-web002.zrh1.exoscale.net (159.100.253.88)  138.995 ms  130.611 ms  155.002 ms
```

Here, we can see the path from our device to our destination. The interesting part is the missing hops between 6 and 15. This does not indicate packet loss, it indicates that routers between Verizon ISP and Exoscale's Zurich data center are configured not to reply to traceroute probes. We also get to know the **IP address** of Exoscale that is **159.100.253.88**.

Ambiguity:

Here, we discovered that 159.100.253.88 does not lead to the main page of Exoscale. It leads to another page that appears to be unsafe. Now this could mean that Exoscale company points the root domain somewhere else.



Exoscale Documentation

Platform
A European cloud platform for hosting infrastructure, applications, and data.

Product
Documentation structured in quick-starts, overviews, operations, how-tos and references.

Reference
Provides technical details for Exoscale in various formats: API, CLI, IAM, SDK, ...

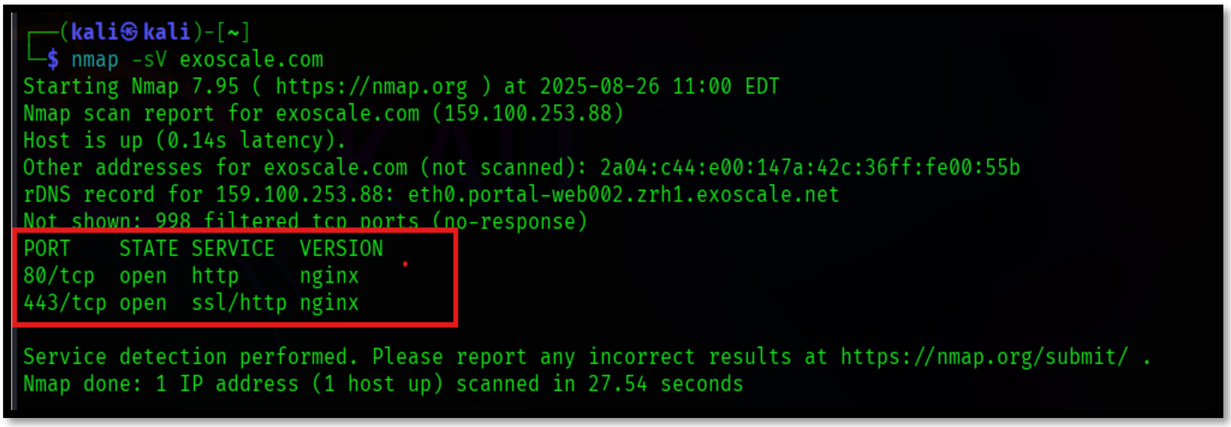
Academy
Providing self-paced e-learning for all Exoscale products.

Tutorial
Detailed step-by-step instructions for selected topics.

Tool
Exoscale's command-line-tool and diagram icon libraries.

Port and Service Discovery:

Port and Service discovery is the process of identifying open ports and services running on the target IP addresses. Here, we will use **Nmap** for this purpose. Nmap (**Network Mapper**) is one of the most widely used open-source tools for network discovery and security auditing. It allows security professionals and system administrators to identify live hosts, open ports, running services, operating systems, and potential vulnerabilities within a network.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV exoscale.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 11:00 EDT
Nmap scan report for exoscale.com (159.100.253.88)
Host is up (0.14s latency).
Other addresses for exoscale.com (not scanned): 2a04:c44:e00:147a:42c:36ff:fe00:55b
rDNS record for 159.100.253.88: eth0.portal-web002.zrh1.exoscale.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.54 seconds
```

Here, we found out that out of 1000 common ports only **Port 80** and **Port 443** are open. That is to be expected when we see that Exoscale is a cloud service provider. Also, both ports run on **nginx**, which is likely acting as a reverse proxy or a load balancer to the backend systems.

- **Port 80/TCP:**
  The webserver listens here, but it is just a redirector to HTTPS.
- **Port 443/TCP:**
  This is the real service endpoint which serves exoscale.com.

Furthermore, this tells us that Exoscale only exposes **HTTP/HTTPS** to the public, no mail, SSH, or other services.

Conclusion:

In this investigation, we conducted an OSINT and footprinting analysis of the domain **exoscale.com**. Through DNS record analysis, WHOIS lookups, domain history, and enumeration techniques, we were able to gather detailed insights about the company's online infrastructure.

The findings revealed that Exoscale uses a combination of its own infrastructure along with third-party services such as **Google Workspace (email hosting)**, **Cloudflare (DNS/DDoS protection)**, and **DNSimple (DNS management)**. Subdomain mapping identified production and pre-production environments, highlighting areas that could represent a potential attack surface if not properly secured.

Enumeration and **traceroute** further confirmed IP ranges, hosting ASNs, and the routing paths taken to reach the domain. The **WHOIS** domain history analysis provided visibility into registrar information and ownership changes, adding useful context for infrastructure monitoring and attribution.