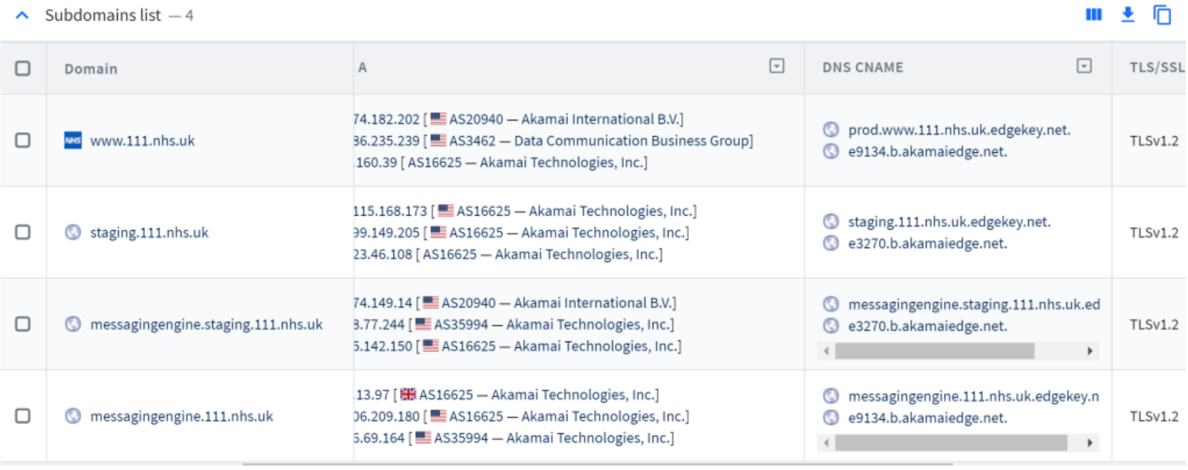
Spyse – A Cyber Security Search Engine

pentestlab.blog/category/general-lab-notes

June 15, 2020

Spyse is a search engine which can be used to identify internet assets and perform external reconnaissance easily. Results are delivered fast. Pentestlab has recently performed a review of the product and the results are presented in this article.

Subdomains of a particular domain can be easily discovered to aid in the process of asset discovery. Penetration testers and red teamers should be able to use it during Open Source Intelligence Assessments or while examining the external attack surface of their client. A records, DNS CNAME and version of TLS/SSL are also returned into the results. Since TLS and SSL are affected by a number of vulnerabilities it could be used as an initial step prior to any other tool.

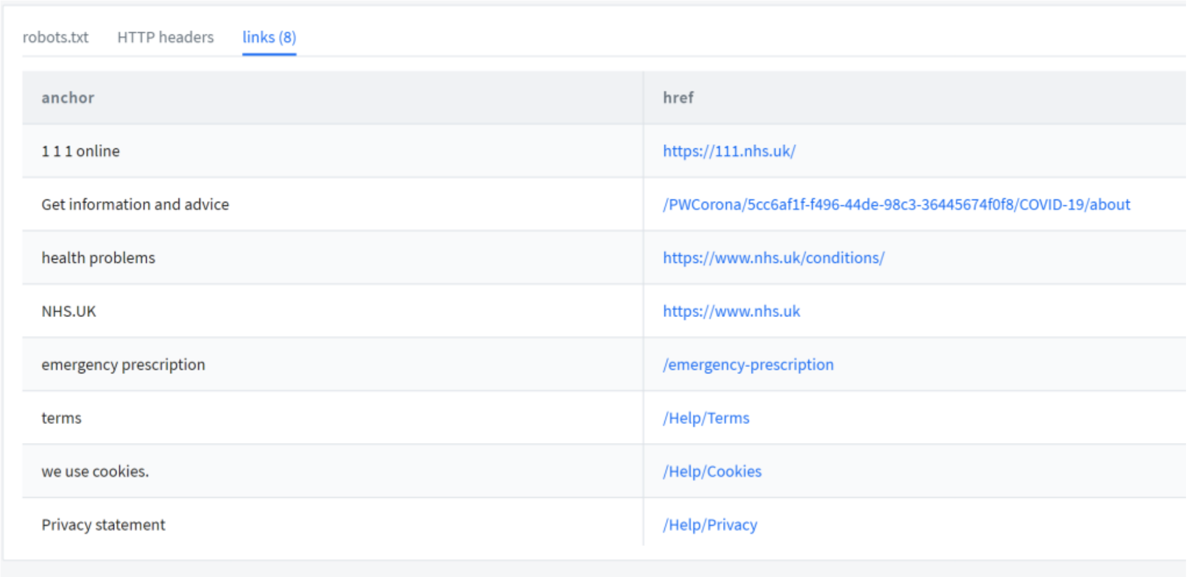


Subdomains list — 4

□	Domain	A	DNS CNAME	TLS/SSL
□	www.111.nhs.uk	74.182.202 [AS20940 — Akamai International B.V.] 36.235.239 [AS3462 — Data Communication Business Group] .160.39 [AS16625 — Akamai Technologies, Inc.]	prod.www.111.nhs.uk.edgekey.net. e9134.b.akamaiedge.net.	TLSv1.2
□	staging.111.nhs.uk	115.168.173 [AS16625 — Akamai Technologies, Inc.] 99.149.205 [AS16625 — Akamai Technologies, Inc.] 23.46.108 [AS16625 — Akamai Technologies, Inc.]	staging.111.nhs.uk.edgekey.net. e3270.b.akamaiedge.net.	TLSv1.2
□	messagingengine.staging.111.nhs.uk	74.149.14 [AS20940 — Akamai International B.V.] 3.77.244 [AS35994 — Akamai Technologies, Inc.] 5.142.150 [AS16625 — Akamai Technologies, Inc.]	messagingengine.staging.111.nhs.uk.ed e3270.b.akamaiedge.net.	TLSv1.2
□	messagingengine.111.nhs.uk	.13.97 [AS16625 — Akamai Technologies, Inc.] 06.209.180 [AS16625 — Akamai Technologies, Inc.] 5.69.164 [AS35994 — Akamai Technologies, Inc.]	messagingengine.111.nhs.uk.edgekey.n e9134.b.akamaiedge.net.	TLSv1.2

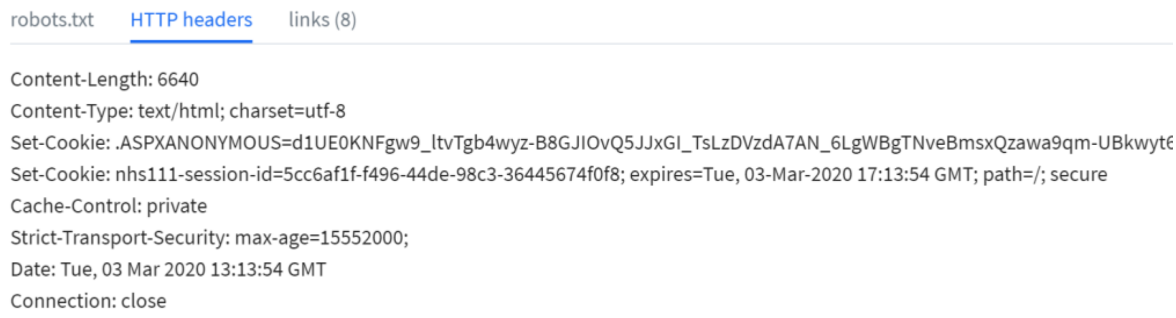
Subdomains List

Spyse also performs web spidering on the target domain therefore information such as the links, robots.txt files and HTTP headers can also retrieved. This can aid towards fingerprinting of the existing technologies in use by the website in scope, identification of sensitive URL’s and mapping the application.



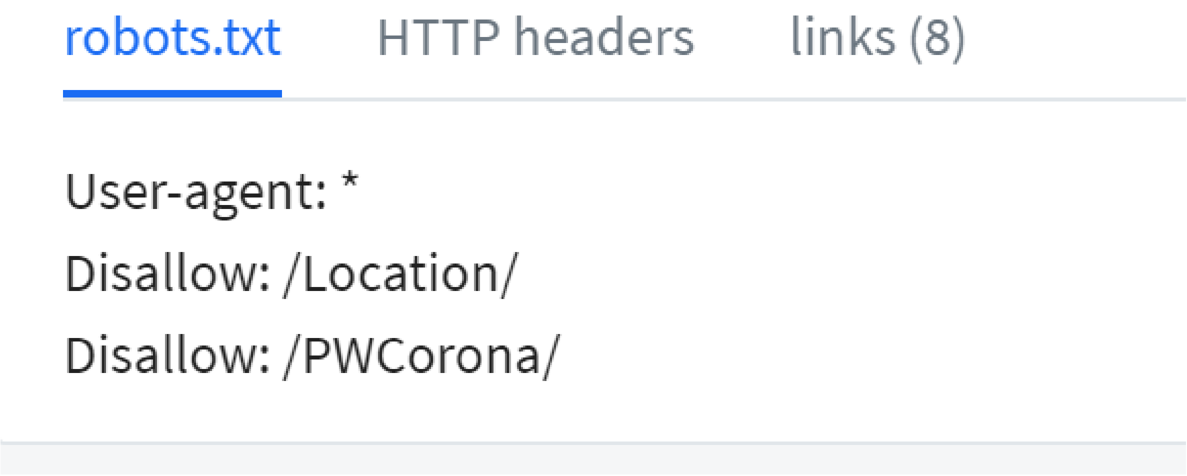
anchor	href
1 1 1 online	https://111.nhs.uk/
Get information and advice	/PWCorona/5cc6af1f-f496-44de-98c3-36445674f0f8/COVID-19/about
health problems	https://www.nhs.uk/conditions/
NHS.UK	https://www.nhs.uk
emergency prescription	/emergency-prescription
terms	/Help/Terms
we use cookies.	/Help/Cookies
Privacy statement	/Help/Privacy

Application Mapping



```
Content-Length: 6640
Content-Type: text/html; charset=utf-8
Set-Cookie: .ASPXANONYMOUS=d1UE0KNFgw9_ltvTgb4wyz-B8GJIOvQ5JJxGI_TsLzDVzdA7AN_6LgWBgTNveBmsxQzawa9qm-UBkwyt6
Set-Cookie: nhs111-session-id=5cc6af1f-f496-44de-98c3-36445674f0f8; expires=Tue, 03-Mar-2020 17:13:54 GMT; path=/; secure
Cache-Control: private
Strict-Transport-Security: max-age=15552000;
Date: Tue, 03 Mar 2020 13:13:54 GMT
Connection: close
```

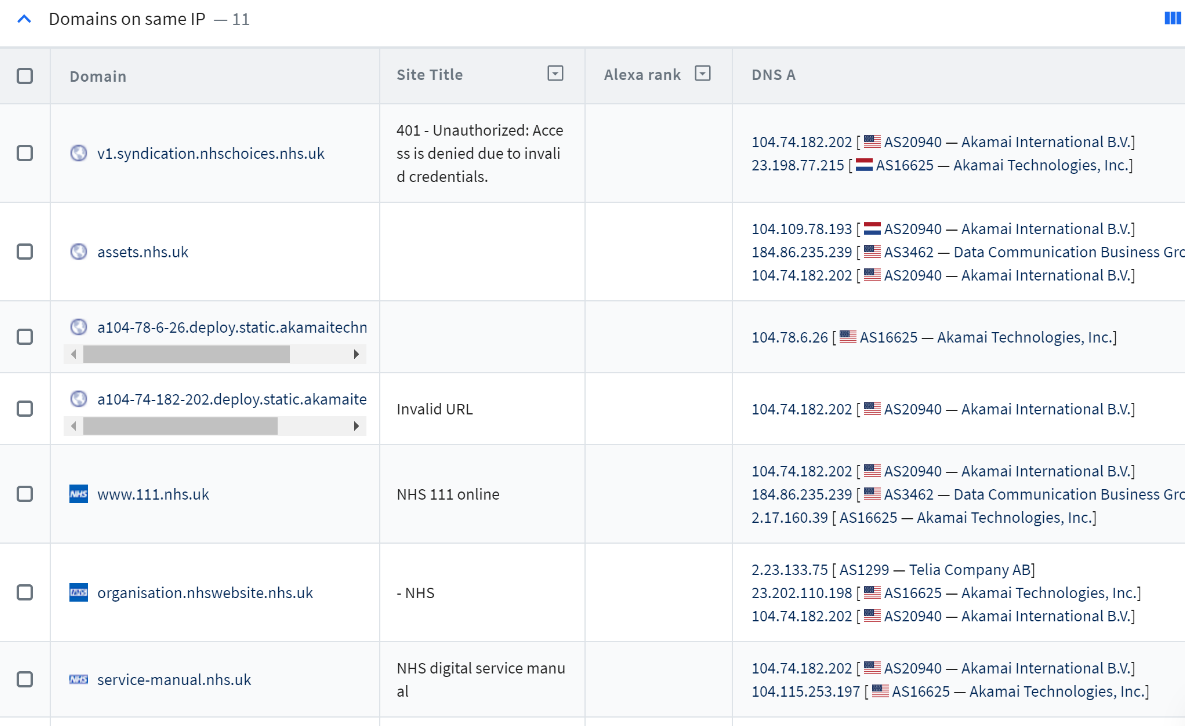
HTTP Headers



```
User-agent: *
Disallow: /Location/
Disallow: /PWCorona/
```

Robots.txt

Spyse has also the ability to discover other domains that exist on the same IP address. This is a common finding in penetration test reports since multiple domains on the same host increase the attack surface.



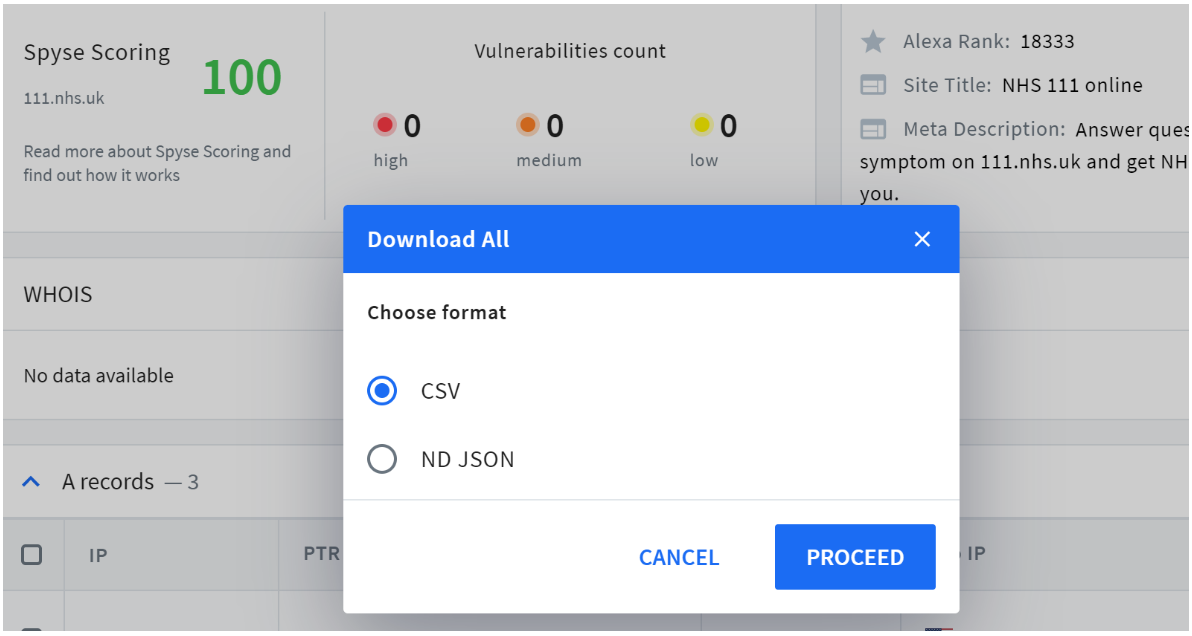
Domains on same IP — 11

□	Domain	Site Title	Alexa rank	DNS A
□	v1.syndication.nhschoices.nhs.uk	401 - Unauthorized: Access is denied due to invalid credentials.		104.74.182.202 [AS20940 — Akamai International B.V.] 23.198.77.215 [AS16625 — Akamai Technologies, Inc.]
□	assets.nhs.uk			104.109.78.193 [AS20940 — Akamai International B.V.] 184.86.235.239 [AS3462 — Data Communication Business Grc 104.74.182.202 [AS20940 — Akamai International B.V.]
□	a104-78-6-26.deploy.static.akamaitechn			104.78.6.26 [AS16625 — Akamai Technologies, Inc.]
□	a104-74-182-202.deploy.static.akamaite	Invalid URL		104.74.182.202 [AS20940 — Akamai International B.V.]
□	www.111.nhs.uk	NHS 111 online		104.74.182.202 [AS20940 — Akamai International B.V.] 184.86.235.239 [AS3462 — Data Communication Business Grc 2.17.160.39 [AS16625 — Akamai Technologies, Inc.]
□	organisation.nhswebsite.nhs.uk	- NHS		2.23.133.75 [AS1299 — Telia Company AB] 23.202.110.198 [AS16625 — Akamai Technologies, Inc.] 104.74.182.202 [AS20940 — Akamai International B.V.]
□	service-manual.nhs.uk	NHS digital service manual		104.74.182.202 [AS20940 — Akamai International B.V.] 104.115.253.197 [AS16625 — Akamai Technologies, Inc.]

Domains on same IP

All the output can be downloaded in two formats:

1. CSV (Comma-Separated Values)
2. ND JSON (Newline Delimited JSON)



Spyse Scoring 100
111.nhs.uk
Read more about Spyse Scoring and find out how it works

Vulnerabilities count
0 high
0 medium
0 low

Alexa Rank: 18333
Site Title: NHS 111 online
Meta Description: Answer ques
symptom on 111.nhs.uk and get NH
you.

WHOIS
No data available

A records — 3

□	IP	PTR	IP

Download All ×

Choose format

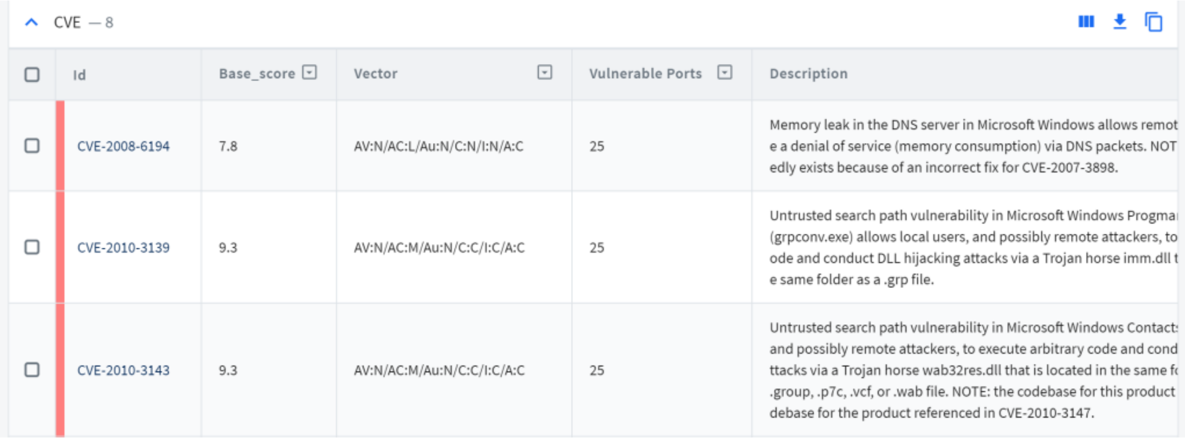
● CSV

○ ND JSON

Data Formatting

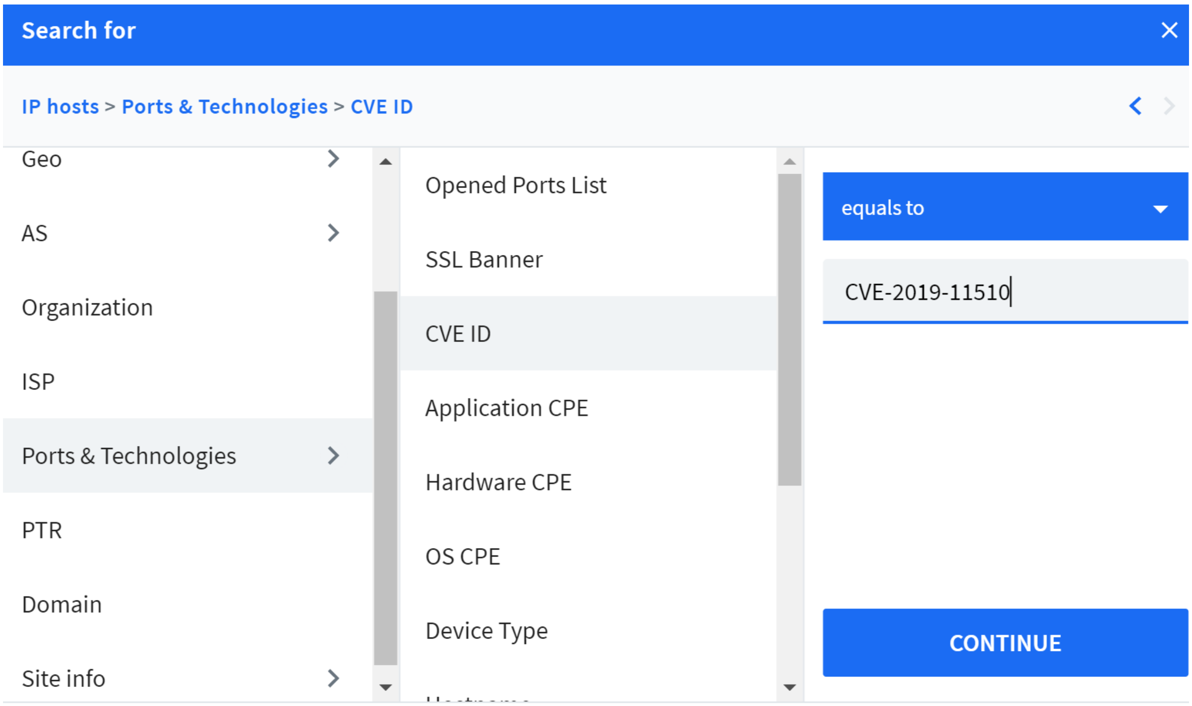
Vulnerabilities

Spyse can also perform vulnerability discovery by identifying open ports and matching the port discovery with a CVE (Common Vulnerabilities & Exposures) number. The search functionality also allows users of the service to search by CVE number:



☐	Id	Base_score	Vector	Vulnerable Ports	Description
☐	CVE-2008-6194	7.8	AV:N/AC:L/Au:N/C:N/I:N/A:C	25	Memory leak in the DNS server in Microsoft Windows allows remot e a denial of service (memory consumption) via DNS packets. NOT edly exists because of an incorrect fix for CVE-2007-3898.
☐	CVE-2010-3139	9.3	AV:N/AC:M/Au:N/C:C/I:C/A:C	25	Untrusted search path vulnerability in Microsoft Windows Progma (grpconv.exe) allows local users, and possibly remote attackers, to ode and conduct DLL hijacking attacks via a Trojan horse imm.dll t e same folder as a .grp file.
☐	CVE-2010-3143	9.3	AV:N/AC:M/Au:N/C:C/I:C/A:C	25	Untrusted search path vulnerability in Microsoft Windows Contact and possibly remote attackers, to execute arbitrary code and cond ttacks via a Trojan horse wab32res.dll that is located in the same f .group, .p7c, .vcf, or .wab file. NOTE: the codebase for this product debase for the product referenced in CVE-2010-3147.

CVE Number

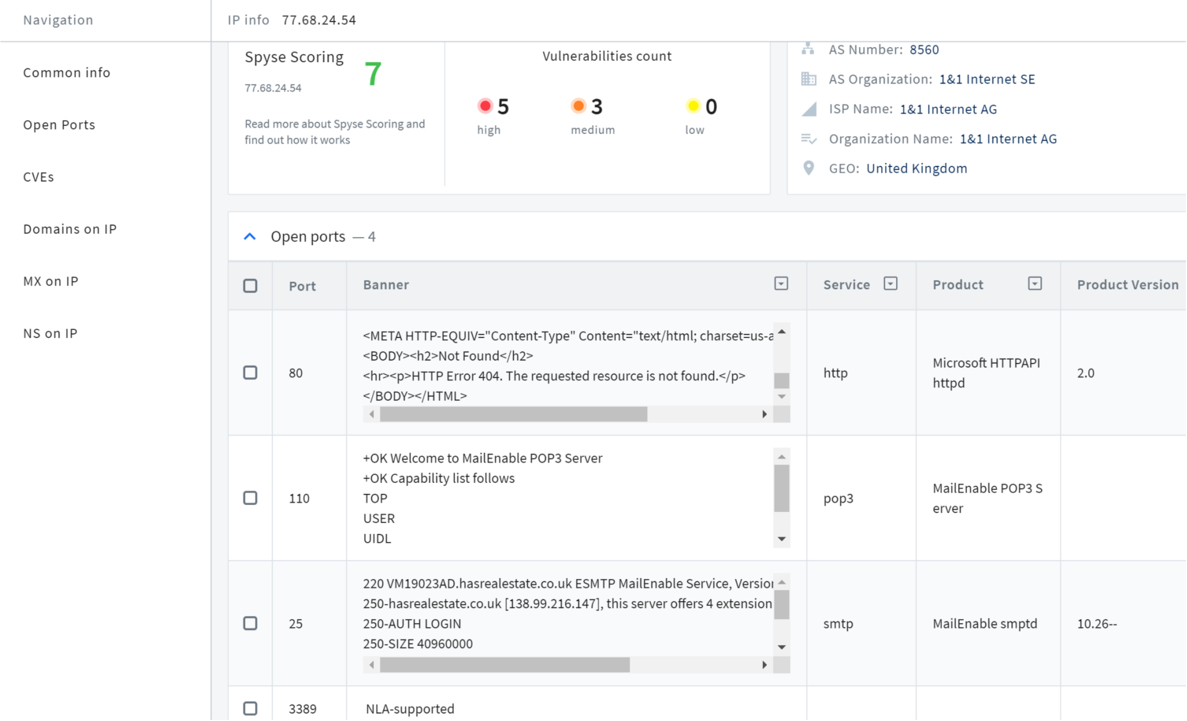


equals to

CVE-2019-11510

Search CVE Numbers

During the port discovery banners and versions are also retrieved which could help to retrieve further information for reporting purposes and for correlations of versions with any existing vulnerabilities.



Navigation

Common info

Open Ports

CVEs

Domains on IP

MX on IP

NS on IP

IP info 77.68.24.54

Spyse Scoring 7

77.68.24.54

Read more about Spyse Scoring and find out how it works

Vulnerabilities count

● 5 high

● 3 medium

● 0 low

AS Number: 8560

AS Organization: 1&1 Internet SE

ISP Name: 1&1 Internet AG

Organization Name: 1&1 Internet AG

GEO: United Kingdom

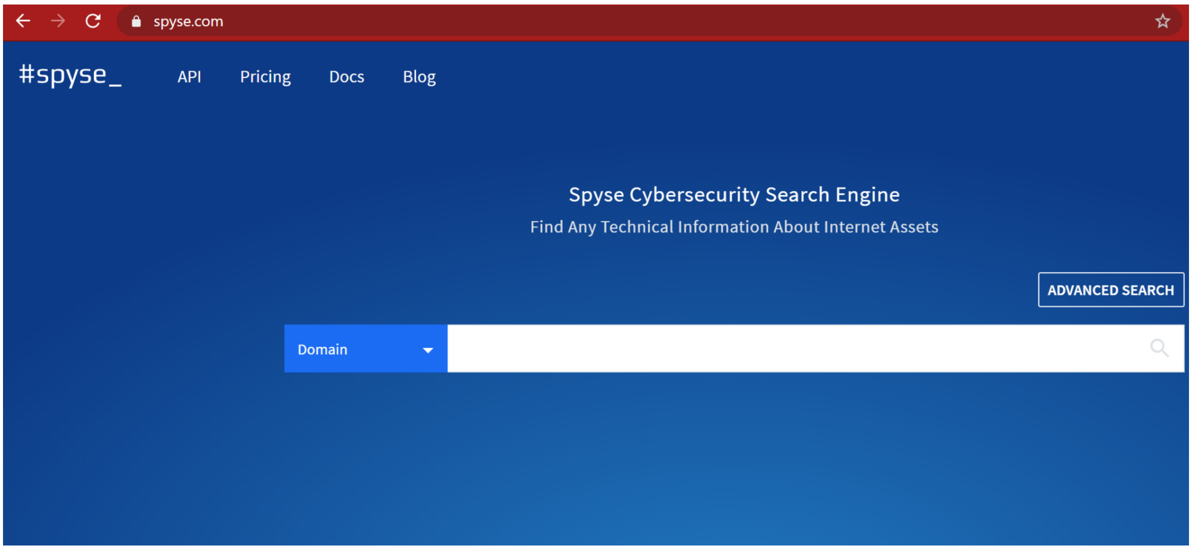
Open ports — 4

□	Port	Banner	Service	Product	Product Version
□	80	<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-a <BODY><h2>Not Found</h2> <hr><p>HTTP Error 404. The requested resource is not found.</p> </BODY></HTML>	http	Microsoft HTTPAPI httpd	2.0
□	110	+OK Welcome to MailEnable POP3 Server +OK Capability list follows TOP USER UIDL	pop3	MailEnable POP3 S erver	
□	25	220 VM19023AD.hasrealestate.co.uk ESMTP MailEnable Service, Versio 250-hasrealestate.co.uk [138.99.216.147], this server offers 4 extension 250-AUTH LOGIN 250-SIZE 40960000	smtp	MailEnable smptd	10.26--
□	3389	NLA-supported			

Open Ports

Conclusion

Passive reconnaissance it is the first step on every red team engagement or external security assessment. Spyse has the ability to return data back to the user very fast and with efficiency by performing a semi-automatic information gathering. Internal cyber security teams and penetration testers could benefit from the service especially if they have to perform recon in companies that have big external presence with multiple assets as Spyse can accelerate this kind of activities. Still not convinced? Give it a try!


spyse.com
#spyse_
API
Pricing
Docs
Blog
Spyse Cybersecurity Search Engine
Find Any Technical Information About Internet Assets
ADVANCED SEARCH
Domain

Spyse Cybersecurity Search Engine