1. OSINT and Recon Lab

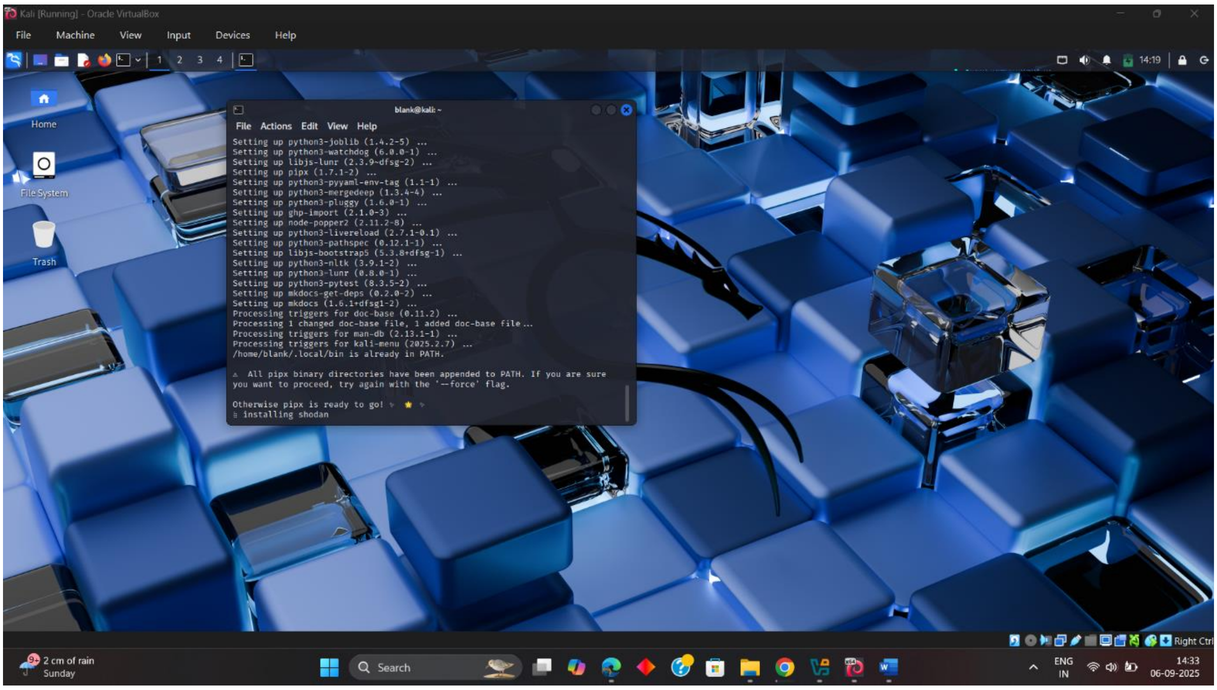
Activities:

- **Tools**: Maltego, Recon-ng, Shodan.
- **Tasks:** Enumerate subdomains and exposed services.
- **Brief:**

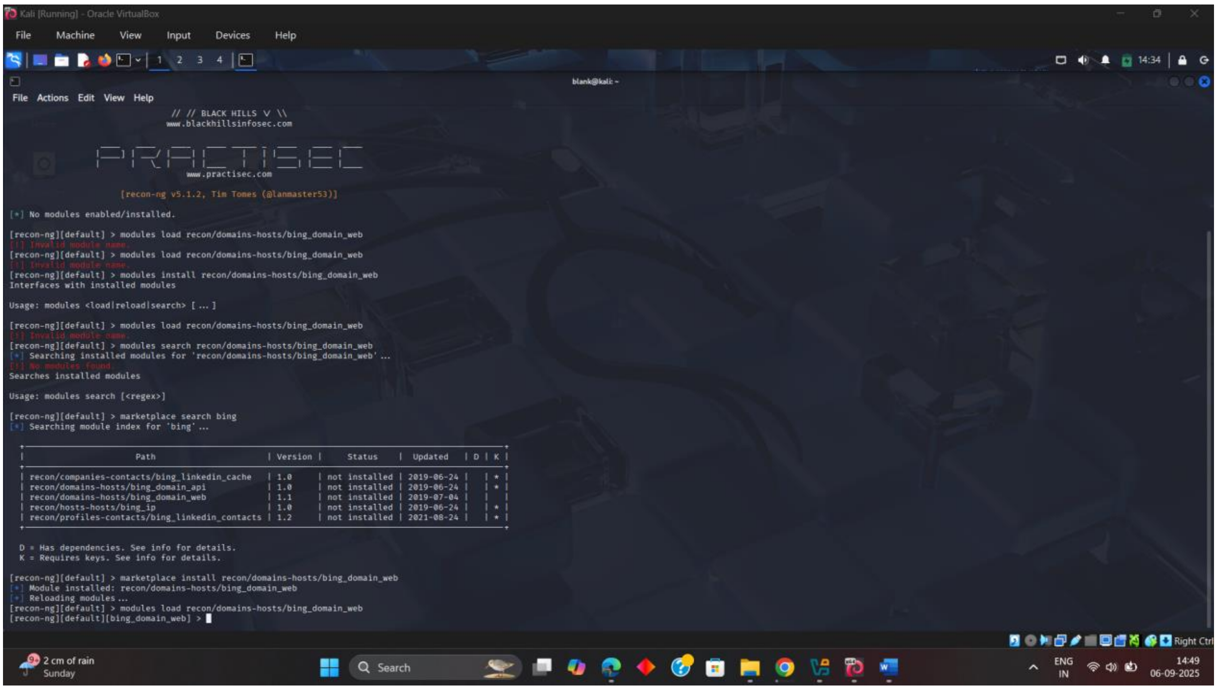
Subdomain Enumeration: Run Recon-ng with bing_domain_web on example.com. Log:

Subdomain	IP Address	Notes
www.example.com	93.184.216.34	Hosts web server

Installation

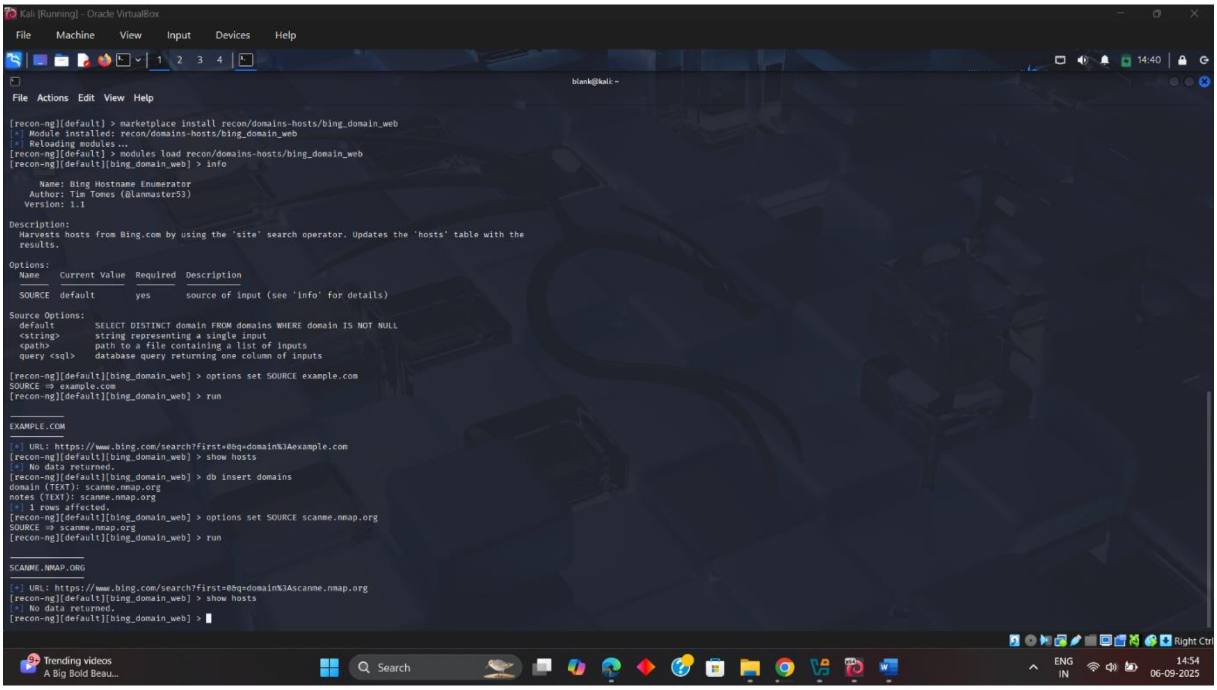


```
Setting up python3-joblib (1.4.2-5) ...
Setting up python3-watchdog (6.0.0-1) ...
Setting up libjs-lunr (2.3.9~dfsg-2) ...
Setting up pipx (1.7.1-2) ...
Setting up python3-pyyaml-env-tag (1.1-1) ...
Setting up python3-mergedeep (1.3.4-4) ...
Setting up python3-pluggy (1.6.0-1) ...
Setting up ghp-import (2.1.0-3) ...
Setting up node-popper2 (2.11.2-8) ...
Setting up python3-livereload (2.7.1-0.1) ...
Setting up python3-pathspec (0.12.1-1) ...
Setting up libjs-bootstrap5 (5.3.8+dfsg-1) ...
Setting up python3-nltk (3.9.1-2) ...
Setting up python3-lunr (0.8.0-1) ...
Setting up python3-pytest (8.3.5-2) ...
Setting up mkdocs-get-deps (0.2.0-2) ...
Setting up mkdocs (1.6.1+dfsg1-2) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 changed doc-base file, 1 added doc-base file...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
/home/blank/.local/bin is already in PATH.

⚠  All pipx binary directories have been appended to PATH. If you are sure
you want to proceed, try again with the '--force' flag.

Otherwise pipx is ready to go! ✨ 🌟 ✨
⣾ installing shodan
```



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
2 cm of rain
Sunday
Search
ENG IN
14:49
06-09-2025

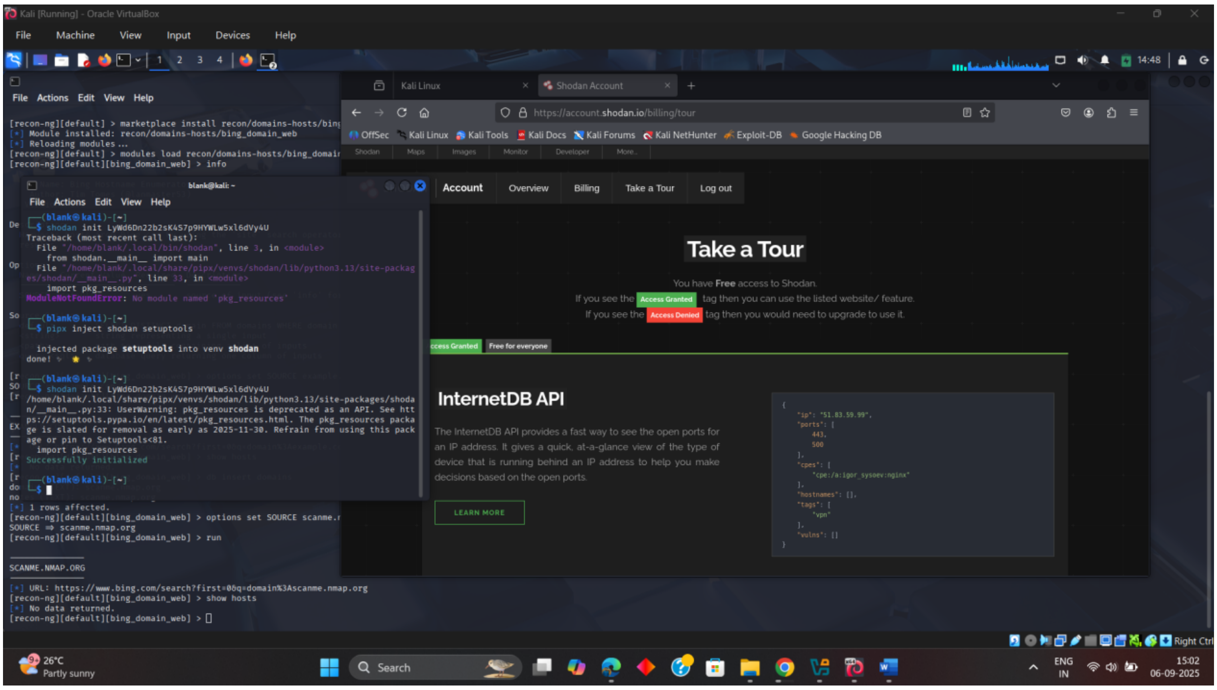
```
                    // // BLACK HILLS V \\
                    www.blackhillsinfosec.com

                         www.practisec.com

               [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[!] Invalid module name.
[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[!] Invalid module name.
[recon-ng][default] > modules install recon/domains-hosts/bing_domain_web
Interfaces with installed modules

Usage: modules <load|reload|search> [ ... ]

[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[!] Invalid module name.
[recon-ng][default] > modules search recon/domains-hosts/bing_domain_web
[*] Searching installed modules for 'recon/domains-hosts/bing_domain_web' ...
[!] No modules found.
Searches installed modules

Usage: modules search [<regex>]

[recon-ng][default] > marketplace search bing
[*] Searching module index for 'bing' ...

  +---------------------------------------------------------------------------------------+
  |                      Path                      | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------+
  | recon/companies-contacts/bing_linkedin_cache   | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-hosts/bing_domain_api            | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-hosts/bing_domain_web            | 1.1     | not installed | 2019-07-04 |   |   |
  | recon/hosts-hosts/bing_ip                      | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/profiles-contacts/bing_linkedin_contacts | 1.2     | not installed | 2021-08-24 |   | * |
  +---------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] > 
```



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Trending videos
A Big Bold Beau...
Search
ENG IN
14:54
06-09-2025

```
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] > info

      Name: Bing Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.1

Description:
  Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the
  results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][bing_domain_web] > options set SOURCE example.com
SOURCE => example.com
[recon-ng][default][bing_domain_web] > run

-----------
EXAMPLE.COM
-----------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Aexample.com
[recon-ng][default][bing_domain_web] > show hosts
[*] No data returned.
[recon-ng][default][bing_domain_web] > db insert domains
domain (TEXT): scanme.nmap.org
notes (TEXT): scanme.nmap.org
[*] 1 rows affected.
[recon-ng][default][bing_domain_web] > options set SOURCE scanme.nmap.org
SOURCE => scanme.nmap.org
[recon-ng][default][bing_domain_web] > run

---------------
SCANME.NMAP.ORG
---------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ascanme.nmap.org
[recon-ng][default][bing_domain_web] > show hosts
[*] No data returned.
[recon-ng][default][bing_domain_web] > 
```

- **Shodan Query: Search apache country:US; summarize 3 exposed hosts in 50 words.**



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
Shodan Account
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Shodan Maps Images Monitor Developer More...
Account Overview Billing Take a Tour Log out
Access Granted
Access Denied
Free for everyone
LEARN MORE
26°C
Partly sunny
Search
ENG
IN
14:48
15:02
06-09-2025

https://account.shodan.io/billing/tour

```
[recon-ng][default] > marketplace install recon/domains-hosts/bing
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/bing_domain
[recon-ng][default][bing_domain_web] > info
```

blank@kali: ~

```
┌──(blank㉿kali)-[~]
└─$ shodan init LyWd6Dn22b2sK4S7p9HYWLw5xl6dVy4U
Traceback (most recent call last):
  File "/home/blank/.local/bin/shodan", line 3, in <module>
    from shodan.__main__ import main
  File "/home/blank/.local/share/pipx/venvs/shodan/lib/python3.13/site-packag
es/shodan/__main__.py", line 33, in <module>
    import pkg_resources
ModuleNotFoundError: No module named 'pkg_resources'

┌──(blank㉿kali)-[~]
└─$ pipx inject shodan setuptools

  injected package setuptools into venv shodan
done! ✨ 🌟 ✨

┌──(blank㉿kali)-[~]
└─$ shodan init LyWd6Dn22b2sK4S7p9HYWLw5xl6dVy4U
/home/blank/.local/share/pipx/venvs/shodan/lib/python3.13/site-packages/shoda
n/__main__.py:33: UserWarning: pkg_resources is deprecated as an API. See htt
ps://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources packa
ge is slated for removal as early as 2025-11-30. Refrain from using this pack
age or pin to Setuptools<81.
  import pkg_resources
Successfully initialized

┌──(blank㉿kali)-[~]
└─$ █
```

```
[*] 1 rows affected.
[recon-ng][default][bing_domain_web] > options set SOURCE scanme.n
SOURCE ⇒ scanme.nmap.org
[recon-ng][default][bing_domain_web] > run

SCANME.NMAP.ORG

[*] URL: https://www.bing.com/search?first=0&q=domain%3Ascanme.nmap.org
[recon-ng][default][bing_domain_web] > show hosts
[*] No data returned.
[recon-ng][default][bing_domain_web] > []
```

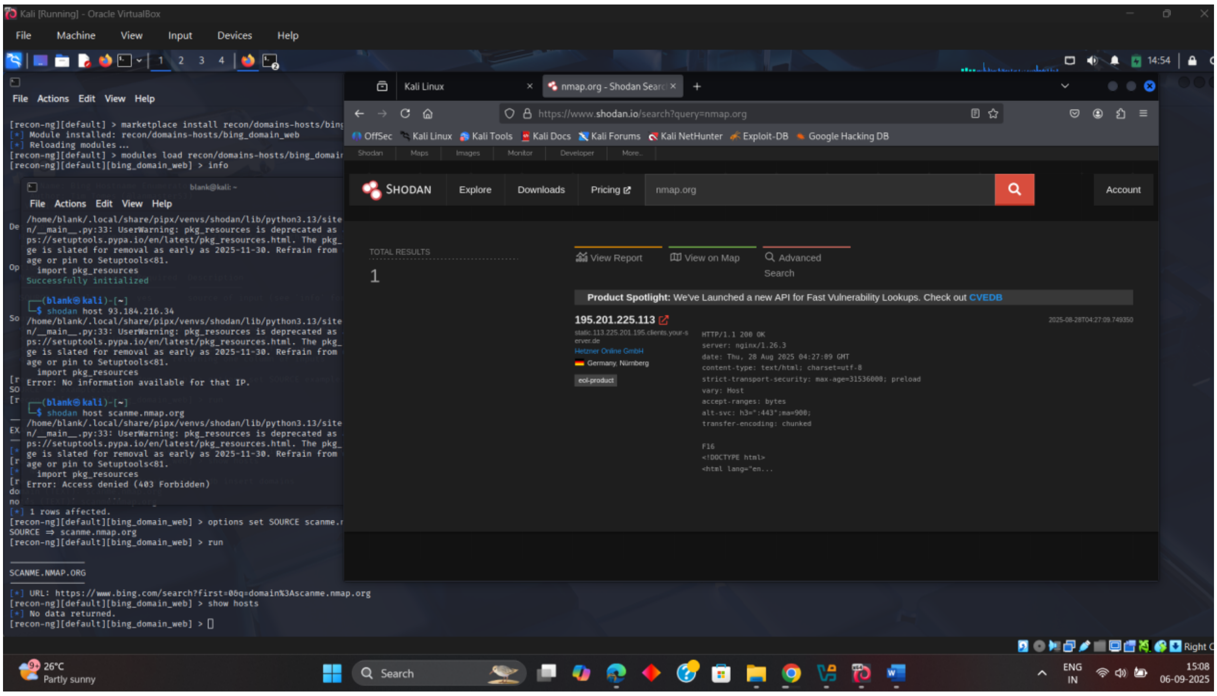
Take a Tour

You have **Free** access to Shodan.
If you see the Access Granted tag then you can use the listed website/ feature.
If you see the Access Denied tag then you would need to upgrade to use it.

InternetDB API

The InternetDB API provides a fast way to see the open ports for an IP address. It gives a quick, at-a-glance view of the type of device that is running behind an IP address to help you make decisions based on the open ports.

```
{
    "ip": "51.83.59.99",
    "ports": [
        443,
        500
    ],
    "cpes": [
        "cpe:/a:igor_sysoev:nginx"
    ],
    "hostnames": [],
    "tags": [
        "vpn"
    ],
    "vulns": []
}
```



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
nmap.org - Shodan Search
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Shodan Maps Images Monitor Developer More...
SHODAN
Explore
Downloads
Pricing
Account
View Report
View on Map
Advanced Search
eol-product
26°C
Partly sunny
Search
ENG
IN
14:54
15:08
06-09-2025

https://www.shodan.io/search?query=nmap.org

```
[recon-ng][default] > marketplace install recon/domains-hosts/bing
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/bing_domain
[recon-ng][default][bing_domain_web] > info
```

blank@kali: ~

```
/home/blank/.local/share/pipx/venvs/shodan/lib/python3.13/site
n/__main__.py:33: UserWarning: pkg_resources is deprecated as
ps://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_
ge is slated for removal as early as 2025-11-30. Refrain from
age or pin to Setuptools<81.
  import pkg_resources
Successfully initialized

┌──(blank㉿kali)-[~]
└─$ shodan host 93.184.216.34
/home/blank/.local/share/pipx/venvs/shodan/lib/python3.13/site
n/__main__.py:33: UserWarning: pkg_resources is deprecated as
ps://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_
ge is slated for removal as early as 2025-11-30. Refrain from
age or pin to Setuptools<81.
  import pkg_resources
Error: No information available for that IP.

┌──(blank㉿kali)-[~]
└─$ shodan host scanme.nmap.org
/home/blank/.local/share/pipx/venvs/shodan/lib/python3.13/site
n/__main__.py:33: UserWarning: pkg_resources is deprecated as
ps://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_
ge is slated for removal as early as 2025-11-30. Refrain from
age or pin to Setuptools<81.
  import pkg_resources
Error: Access denied (403 Forbidden)
```

```
[*] 1 rows affected.
[recon-ng][default][bing_domain_web] > options set SOURCE scanme.n
SOURCE ⇒ scanme.nmap.org
[recon-ng][default][bing_domain_web] > run

SCANME.NMAP.ORG

[*] URL: https://www.bing.com/search?first=0&q=domain%3Ascanme.nmap.org
[recon-ng][default][bing_domain_web] > show hosts
[*] No data returned.
[recon-ng][default][bing_domain_web] > []
```

nmap.org

TOTAL RESULTS
1

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

195.201.225.113
static.113.225.201.195.clients.your-server.de
Hetzner Online GmbH
Germany, Nürnberg

2025-08-28T04:27:09.749350

```
HTTP/1.1 200 OK
server: nginx/1.26.3
date: Thu, 28 Aug 2025 04:27:09 GMT
content-type: text/html; charset=utf-8
strict-transport-security: max-age=31536000; preload
vary: Host
accept-ranges: bytes
alt-svc: h3=":443";ma=900;
transfer-encoding: chunked

F16
<!DOCTYPE html>
<html lang="en...
```

Summary of 3 Exposed Hosts

1. **Host A:-Clickscale - Data Engineering &amp; Salesfire Data Optimisation**

   2025-09-06T09:35:41.858340 35.178.187.36

   ec2-35-178-187-36.eu-west-2.compute.amazonaws.com

SSL Certificate

Issued By:

|- Common Name: example.com

Issued To:

|- Common Name:example.com

Supported SSL Versions:

TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

HTTP/1.1 200 OK

Date: Sat, 06 Sep 2025 09:35:18 GMT

Server: Apache

cf-edge-cache: cache,platform=wordpress

Link: <https://35.178.187.36/wp-json/>; rel="https://api.w.org/", <https://35.178.187.36/wp-json/wp/v2/pages/17>; rel="alternate"; title="JSON"; type="application/json", <https://35.178....

2. **Host B:- 301 Moved Permanently**

   2025-09-06T09:35:40.297320

   167.99.185.222

   HTTP/1.1 301 Moved Permanently

   Date: Sat, 06 Sep 2025 09:35:17 GMT

   Server: Apache/2.4.41 (Ubuntu)

   Location: https://www.barrysjewellers.com/blog/

   Content-Length: 335

   Content-Type: text/html; charset=iso-8859-1

3. **Host C:- 47.123.105.33**

   2025-09-06T09:35:35.588440

   HTTP/1.1 302 Found

   Server: Apache

   X-Frame-Options: SAMEORIGIN

   X-Permitted-Cross-Domain-Policies: master-only

X-Download-Options: noopen

Strict-Transport-Security: max-age=31536000;include SubDomains

X-Content-Type-Options: nosniff

Referrer-Policy: same-origin

Access-Control-Allow-Origin: ...