



## 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

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2025.2-vmware-amd64
Shell No.1
File Actions Edit View Help

[recon-ng v5.1.2, Tin Tones (@lammaster33)]

[91] Recon modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules
[2] Disabled modules

[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] > info

Name: Bing Hostname Enumerator
Author: Tin Tones (@lammaster33)
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] >
```



```
File Actions Edit View Help
[4] Import modules
[2] Exploitation modules
[2] Discovery modules
[2] Disabled modules

[recon-ng][default] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][default][bing_domain_web] > info

Name: Bing Hostname Enumerator
Author: Tio Times (@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 bluedart.com
SOURCE => bluedart.com
[recon-ng][default][bing_domain_web] > info

Name: Bing Hostname Enumerator
Author: Tio Times (@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 | bluedart.com  | 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] >
```

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2025.2-vmware-amd64
Shell No. 1
File Actions Edit View Help

[*] 6 rows returned
[recon-ng][default][bing_domain_web] > input

Module Inputs
example.com

[recon-ng][default][bing_domain_web] > run

EXAMPLE.COM
[*] URL: https://www.bing.com/search?first=0&q=domain34example.com
[recon-ng][default][bing_domain_web] > show hosts

rowid | host | ip_address | region | country | latitude | longitude | notes | module
-----|-----|-----|-----|-----|-----|-----|-----|-----
1 | www.example.com-vs.edgesuite.net | 23.63.188.243 | | | | | | brute_hosts
2 | www.example.com | 23.63.188.243 | | | | | | brute_hosts
3 | a1422.dscr.akamai.net | 23.63.188.218 | | | | | | brute_hosts
4 | www.example.com | 23.63.188.243 | | | | | | brute_hosts
5 | www.example.com | 23.63.188.243 | | | | | | brute_hosts
6 | www.example.com-vs.edgesuite.net | 23.63.188.218 | | | | | | resolve
7 | www.example.com | 23.63.188.218 | | | | | | resolve
8 | a1422.dscr.akamai.net | 23.63.188.243 | | | | | | resolve

[*] 8 rows returned
[recon-ng][default][bing_domain_web] > input

Module Inputs
example.com

[recon-ng][default][bing_domain_web] > run

EXAMPLE.COM
[*] URL: https://www.bing.com/search?first=0&q=domain34example.com
[recon-ng][default][bing_domain_web] >
```



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

## Summary of 3 Exposed Hosts

1. **Host A** – [HURRICANE ELECTRIC](#) using outdate Apache version with no ssl.  
Server: **Apache/2.0.54** (Unix) mod\_perl/1.99\_09 Perl/v5.8.0 mod\_ssl/2.0.54  
OpenSSL/0.9.7l DAV/2 FrontPage/5.0.2.2635 PHP/4.4.0 mod\_gzip/2.0.26.1a  
  
Last-Modified: Wed, 01 Jul 1998 08:51:04 GMT.
2. **Host B** – [jeff2600](#) – using outdated Apache version with cPanel ssl which is no longer valid on browser and causes browser warning DATA can be steal using MITM attack.
3. **Host C** – [Index of /](#). Shows open file directory.