

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
Кафедра кібербезпеки

**Звіт до лабораторної роботи № 5**  
на тему “ Дослідження основних інструментів Kali Linux  
для збору інформації про цільовий ресурс ”

**Виконав студент(ка)**

Борщ Дмитро

**Група**

КБ-01

**Перевірила**

Лаврик Т.В.

**Суми 2023**

## ЗВІТ

про виконану роботу

### Вивчення основних утиліт Kali Linux для збору інформації про цільову систему.

Розглянемо основні утиліти, які допоможуть для збору інформації про цільову систему.

**Введіть `hostname: bktbntu.com.ua`**

#### Утиліта `host`

2.1 У командному рядку терміналу введіть команду:  
`man host`.

З якою метою використовується утиліта **`host`**?

Для проведення пошуку по DNS

2.2 У командному рядку терміналу введіть команду:  
`host --help`.

З якою метою використовується опція `-a`?

З прапором `-a` буде виконано пошук по всім типам DNS записів + буде розширений формат виводу

2.3 У командному рядку терміналу введіть послідовно кожен з команд і порівняйте результати їх виконання:

`host < hostname>`.

Який результат отримали після команди **`host`**?

```
bktbntu.com.ua has address 185.68.16.103
bktbntu.com.ua has IPv6 address 2a00:7a60:0:1067::1
bktbntu.com.ua mail is handled by 15 mx15.ukraine.com.ua.
bktbntu.com.ua mail is handled by 20 mx20.ukraine.com.ua.
```

```
host -a < hostname>.
```

Який результат отримали після команди з опцією **host -a**?

```
Trying "bktbntu.com.ua"
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 54715
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;bktbntu.com.ua.                IN      ANY

;; ANSWER SECTION:
bktbntu.com.ua.                900     IN      A       185.68.16.103

Received 48 bytes from 8.8.8.8#53 in 60 ms
```

## Утиліта DMitry

2.4 У командному рядку терміналу введіть команду:

```
man dmitry .
```

З якою метою використовується утиліта **DMitry**?

DMitry — це програма командного рядка UNIX/(GNU)Linux, написана мовою C. DMitry може знаходити можливі субдомени, адреси електронної пошти, інформацію про аптайм, виконувати сканування портів tcp, шукати whois тощо.

Запишіть синтаксис команди:

```
dmitry [Options] host
```

2.5 У командному рядку терміналу введіть команду:

```
dmitry --help.
```

Яке призначення опції **-p**?

```
Сканування TCP портів
```

Яке призначення опції **-f**?

Показувати при виводі фільтровані(закриті фаєрволлом, але активні) порти

Яке призначення опції **-b**?

```
Виводи банери при скануванні TCP портів
```

2.6 Закрийте вікно терміналу.

2.7 Запустіть утиліту DMitry з меню Kali Linux. Для цього перейдіть у розділ Applications / Information Gathering / dmitry.

2.8 У командному рядку терміналу введіть команди:

```
dmitry -i -w -s -e < hostname>
```

або

```
dmitry -iwse < hostname>;
```

Який результат отримали?

```
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:185.68.16.103
HostName:bktbntu.com.ua

Gathered Inet-whois information for 185.68.16.103
-----

inetnum:          185.68.16.0 - 185.68.16.255
netname:          HUPROXY
descr:            Hosting Ukraine Proxies
country:          UA
admin-c:          HU2012-RIPE
tech-c:           HU2012-RIPE
status:           ASSIGNED PA
mnt-by:           HOSTINGUKRAINE-MNT
mnt-lower:        HOSTINGUKRAINE-MNT
mnt-routes:       HOSTINGUKRAINE-MNT
created:          2015-10-29T18:10:49Z
last-modified:    2015-10-29T18:10:49Z
source:           RIPE

role:             Hosting Ukraine Ltd. Netmaster
org:              ORG-HUL6-RIPE
address:          Hosting Ukraine LTD
address:          PO Box 65
phone:            +380443927433
address:          04112, Kiev, Ukraine
admin-c:          IR1628-RIPE
abuse-mailbox:    network@abuse.team
nic-hdl:          HU2012-RIPE
mnt-by:           HOSTINGUKRAINE-MNT
created:          2013-04-18T07:53:53Z
last-modified:    2018-08-13T08:44:09Z
source:           RIPE # Filtered

% Information related to '185.68.16.0/22AS2000000'

route:            185.68.16.0/22
descr:            DX-DC network
origin:           AS2000000
mnt-by:           HOSTINGUKRAINE-MNT
created:          2014-09-08T18:25:48Z
last-modified:    2014-09-08T18:25:48Z
```

```

source:          RIPE

% This query was served by the RIPE Database Query Service version
1.106 (SHETLAND)

Gathered Inic-whois information for bktbntu.com.ua
-----
domain:          bktbntu.com.ua
dom-public:      NO
mnt-by:          ua.ukraine
nserver:         ns118.inhostedns.com
nserver:         ns218.inhostedns.net
nserver:         ns318.inhostedns.org
status:          ok
created:         2014-12-30 14:07:04+02
modified:        2023-02-14 22:00:40+02
expires:         2023-12-30 14:07:04+02
source:          UAEPP

% Registrar:
%
% The following disclaimer was provided by the domain name registrar
% =====
% Предоставленная информация является неполной и может содержать
ошибки, связанные с особенностями механизмов кеширования информации,
% несинхронного обновления реестров и т.п., поэтому не является
достовѣрною, однако не несет ответственности за использование
*** stack smashing detected ***: terminated
Aborted

```

`dmitry -p < hostname> -f -b.`

Який результат отримали?

Повне сканування TCP портів

## Утиліта Recon-NG

2.9 У командному рядку терміналу введіть команду:

`man recon-ng .`

З якою метою використовується утиліта **Recon-NG**?

Recon-ng — це повнофункціональний розвідувальний фреймворк, розроблений з метою надання потужного середовища для швидкого та ретельного проведення веб-розвідки з відкритим кодом.

2.10 Для запуску утиліти з командного рядка терміналу введіть команду:  
**Recon-ng**.

2.11 У командному рядку терміналу введіть команди:  
**help**

Запишіть які команди доступні для **Recon-NG**.

back	Exits the current context
dashboard	Displays a summary of activity
db	Interfaces with the workspace's database
exit	Exits the framework
help	Displays this menu
index	Creates a module index (dev only)
keys	Manages third party resource credentials
marketplace	Interfaces with the module marketplace
modules	Interfaces with installed modules
options	Manages the current context options
pdb	Starts a Python Debugger session (dev only)
script	Records and executes command scripts
shell	Executes shell commands
show	Shows various framework items
snapshots	Manages workspace snapshots
spool	Spools output to a file
workspaces	Manages workspaces

### options list

Запишіть які опції доступні.

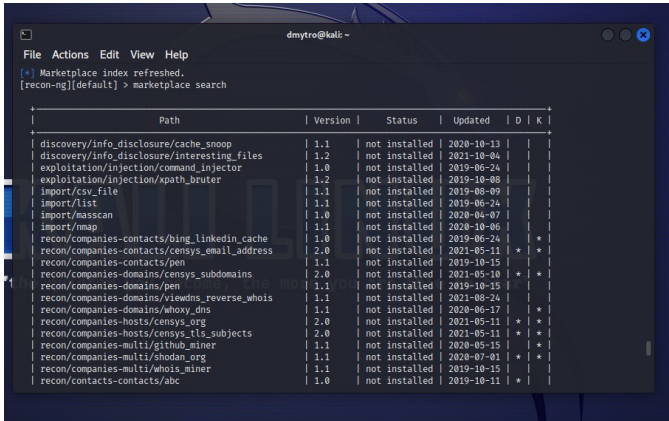
NAMESERVER	8.8.8.8	yes	default nameserver for the resolver mixin
PROXY		no	proxy server (address:port)
THREADS	10	yes	number of threads (where applicable)
TIMEOUT	10	yes	socket timeout (seconds)
USER-AGENT	Recon-ng/v5	yes	user-agent string
VERBOSITY	1	yes	verbosity level (0 = minimal, 1 = verbose, 2 = debug)

2.12 Для роботи з модулями утиліти їх список треба оновити.

У командному рядку терміналу введіть команди:

```
marketplace refresh
marketplace search
```

Збережіть скріншот зі списком доступних модулів. Чи встановлені ці модулі?



Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
discovery/info_disclosure/interesting_files	1.2	not installed	2021-10-04		
exploitation/injection/command_injector	1.0	not installed	2019-06-24		
exploitation/injection/xpath_bruter	1.2	not installed	2019-10-08		
import/csv_file	1.1	not installed	2019-08-09		
import/list	1.1	not installed	2019-06-24		
import/masscan	1.0	not installed	2020-04-07		
import/nmap	1.1	not installed	2020-10-06		
recon/companies-contacts/bing_linkedin_cache	1.0	not installed	2019-06-24		
recon/companies-contacts/censys_email_address	2.0	not installed	2021-05-11	*	*
recon/companies-contacts/pen	1.1	not installed	2019-10-15		
recon/companies-domains/censys_subdomains	2.0	not installed	2021-05-10	*	*
recon/companies-domains/pen	1.1	not installed	2019-10-15		
recon/companies-domains/viewdns_reverse_whois	1.1	not installed	2021-08-24		
recon/companies-domains/whoxy_dns	1.1	not installed	2020-06-17		
recon/companies-hosts/censys_org	2.0	not installed	2021-05-11	*	*
recon/companies-hosts/censys_tls_subjects	2.0	not installed	2021-05-11	*	*
recon/companies-multi/github_miner	1.1	not installed	2020-05-15		
recon/companies-multi/shodan_org	1.1	not installed	2020-07-01	*	*
recon/companies-multi/whois_miner	1.1	not installed	2019-10-15		
recon/contacts-contacts/abc	1.0	not installed	2019-10-11	*	

Усі ці модулі відмічені як “not installed”

2.13 Розглянемо модуль **recon / domains-hosts / hackertarget**.

Знайдіть інформацію про цей модуль. З якою метою його можна використовувати?

Він використовує API HackerTarget.com для пошуку хостів

2.14 Для встановлення модуля «**hackertarget**» введіть команду:

```
marketplace install
recon/domains-hosts/hackertarget
або
```

```
marketplace install hackertarget.
```

Введіть у командному рядку терміналу команди:

```
modules load recon/domains-hosts/hackertarget ;
```

Що змінилося в командному рядку?

Було:

```
[recon-ng][default] >
```

Стало:

```
[recon-ng][default][hackertarget] >
```

## info

Збережіть скріншот з результатом виконання команди.

```
[recon-ng][default][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. 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][hackertarget] > █
```

2.15 Встановіть SOURCE на потрібний ресурс такою командою:

`options set SOURCE < hostname> .`

Після заповнення усіх обов'язкових параметрів запустіть роботу модуля за допомогою команди

`run .`

Який результат використання модуля *domains-hosts* / *hackertarget* отримано?

```
-----
BKTBTU.COM.UA
-----
[*] Country: None
[*] Host: bktbntu.com.ua
[*] Ip_Address: 185.68.16.103
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: www.bktbntu.com.ua
[*] Ip_Address: 185.68.16.103
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----

-----
SUMMARY
-----
[*] 2 total (2 new) hosts found.
```



2.16 У командному рядку терміналу введіть команду:

`show hosts`

Яку інформацію отримано?

```
[recon-ng][default][hackertarget] > show hosts
+-----+-----+-----+-----+-----+-----+-----+-----+
| rowid | host           | ip_address | region | country | latitude | longitude | notes | module |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1     | bktbntu.com.ua | 185.68.16.103 |      |      |      |      |      | hackertarget |
| 2     | www.bktbntu.com.ua | 185.68.16.103 |      |      |      |      |      | hackertarget |
+-----+-----+-----+-----+-----+-----+-----+-----+

[*] 2 rows returned
[recon-ng][default][hackertarget] > 
```

Ми дізналися, що існує ще субдомен `www.*`

2.17 Для виходу із Recon-NG у командному рядку терміналу введіть команду:

`exit`

### Висновок:

**Яку інформацію вдалося зібрати про цільовий ресурс?**

Інформацію від DNS провайдера, на якому зареєстрований домен, про власника сайту, підмережу в якій він знаходиться, а ще те, що існує ще один субдомен, який скоріш за все просто реверсивний проксі на основний.