Rekonesans i recon-ng

Podstawy programowania dla fizyków

Krzysztof Kubień, Mikołaj Wielebnowski

WIMiF PK

03.02.2019

Plan

Pojęcie

Rekonesans to pierwszy krok do przygotowania audytu bezpieczeństwa jak i również przy rozpoczynaniu ataku hakerskiego.Umożliwia on lepsze poznanie celu, jego struktury oraz miejsc podatnych na atak.
Podczas rekonesansu można uzyskać:

- Nazwę domeny
- Bloki sieci
- Adresy IP hostów
- Architekturę sieci oraz system operacyjny
- Używane protokoły
- Mechanizmy autoryzacji

Informacje umożliwiające atak można pozyskać:

Pasywny bez ingerencji atakującego, zostawiania śladów po stronie celu.

Aktywny korzystając z narzędzi wymagających interakcji z systemem celu.

Metoda pasywna

Pasywne pozyskiwanie informacji wykorzystuje informacje dostępne już w internecie. Udostępnione przez cel lub pozyskane przez zewnętrną firmę i udostępnione w bazach.

Przykładowe informacje dostępne w bazach:

- Adresy serwerów w domenie.
- Lokalizacje serwerów.
- Dane osób związanych z celem.

Metoda aktywna

Do aktywnego pozyskiwania danych stosuje się narzędzia pozyskujące bezpośrednio dane wysyłając zapytania do serwerów celu.

Przykładowe proste narzędzia:

- **traceroute** badanie topologii sieci.
- **ping** znajdowanie adresow ip oraz portów hostów.

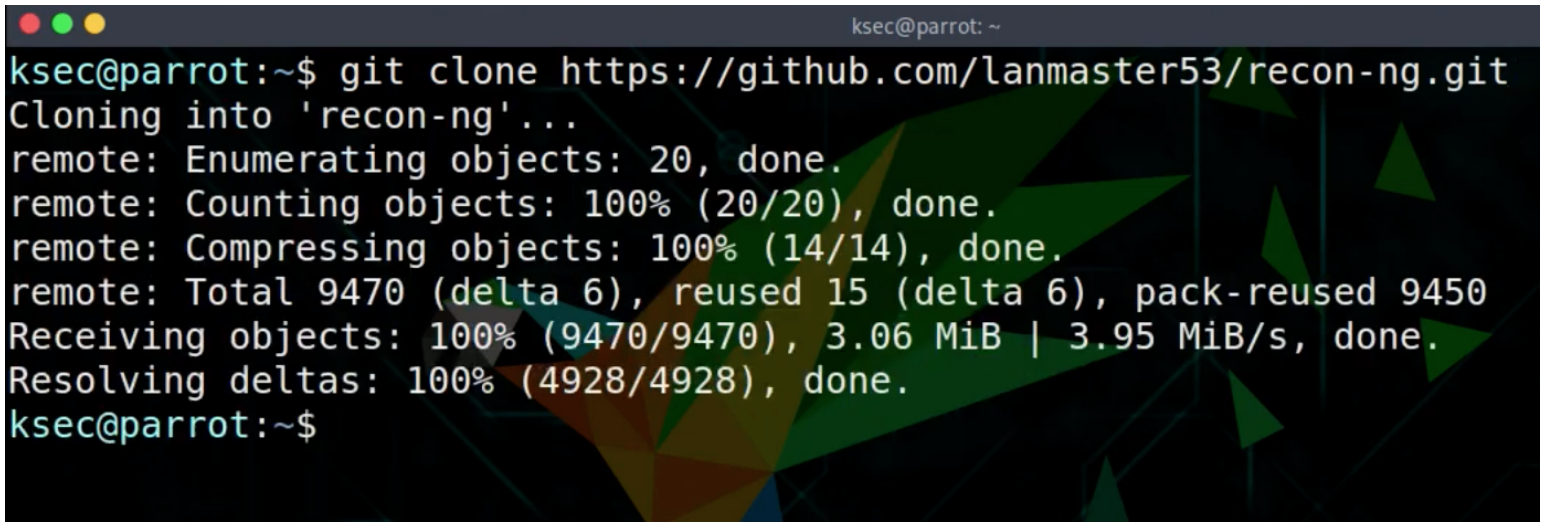
Zarys programu

Framework recon-ng to zbiór narzędzi służących analizy publicznie dostępnych danych. Dostępne jest dla systemów Linux oraz Mac OS. Składa się ono z modułów umożliwiające zbieranie pasywne i aktywne danych celu.

Rysunek: ekran powitalny recon-ng

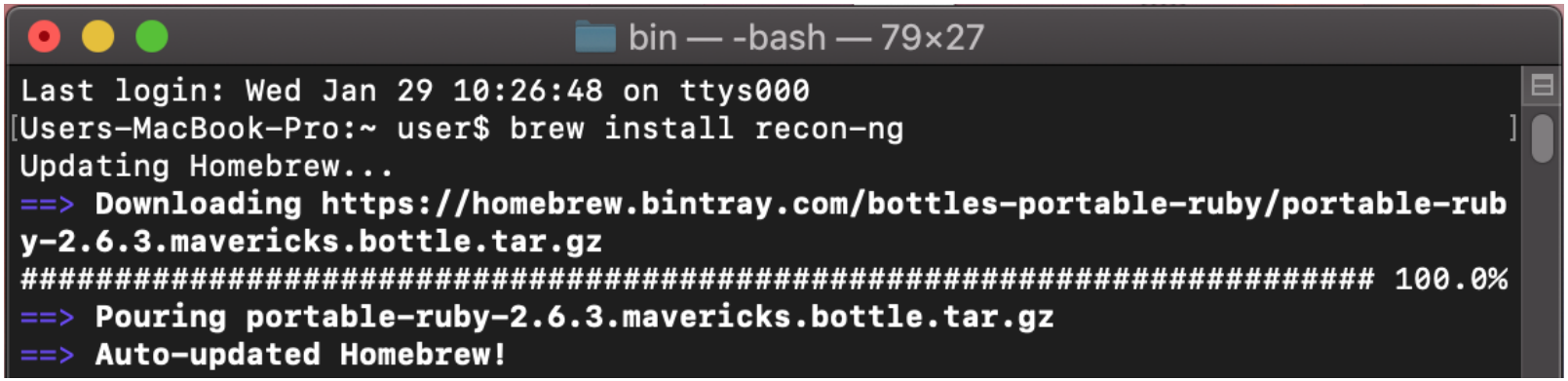
Instalacja

Program można uzyskać na Linuxie klonując oficialne repozytorium.
git clone https://github.com/lanmaster53/recon-ng



Rysunek: Instalacja na systemie Linux.

Na systemie Mac OS można program pozyskać przy pomocy platformy Brew.
brew install recon-ng



Rysunek: Instalacja na systemie Mac OS.

Działanie programu

```
Commands (type [help|?] <topic>):
---------------------------------
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
```

Wskazówka

Po uruchomieniu programu zawsze warto użyć komendy help.

Działanie programu

```
Commands (type [help|?] <topic>):
---------------------------------
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
```

Wskazówka

Po uruchomieniu programu zawsze warto użyć komendy help.

Framework bazuje na małych skryptach zwanych modułami, komenda umożliwiająca ich pozyskanie to marketplace.

```
[[recon-ng][default] > marketplace
 Interfaces with the module marketplace

 Usage: marketplace <info|install|refresh|remove|search> [...]

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

- **search** wyszukuje moduły dla danej frazy, bez żadnej frazy pokazuje wszystkie dostępne.
- **info** wyświetla krótki opis modułu.
- **install** instaluje moduł o podanej nazwie.
- **remove** usuwa moduł o danej nazwie.

Sposób rozpoznawania modułu:

```
+-------------------------------------------------------------------------------------------+
|                    Path                    | Version |     Status    |  Updated   | D | K |
+-------------------------------------------------------------------------------------------+
| recon/domains-credentials/scylla           | 1.1     | not installed | 2019-10-15 |   |   |
| recon/domains-domains/brute_suffix         | 1.0     | not installed | 2019-06-24 |   |   |
| recon/domains-hosts/binaryedge             | 1.0     | not installed | 2019-06-24 |   | * |
```

Druga część ścieżki określa, które dane otrzymamy na podstawie których. np.:
domains-credentials na podstawie danej domeny uzyskuje dane uwierzytelniające;
hosts-hosts na podstawie adresów hostów uzyskuje więcej adresów hostów.
Gwiazdka w ostatnich dwóch kolumnach informuje odpowiednio czy dany moduł potrzebuje innego do działania (dependencies), czy dany moduł potrzebuje klucza API do działania przy korzystaniu z serwisu (przykładowo `http://ipstacks.com/`).

Po wybraniu odpowiedniego modułu należy go zainstalować, załadować i uruchomić:

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

Wskazówka

W każdym momencie działa autouzupełnianie komendy przy pomocą klawisza Tab.

Po wybraniu odpowiedniego modułu należy go zainstalować, załadować i uruchomić:

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

Wskazówka

W każdym momencie działa autouzupełnianie komendy przy pomocą klawisza Tab.

Używanie programu

Jako przykład wykorzystamy domenę `pk.edu.pl` i postaramy się znaleźć jak najwięcej hostów, portów oraz ich lokalizajcę.

```
[[recon-ng][default] > workspaces create pk
[[recon-ng][pk] > db insert domains
[domain (TEXT): pk.edu.pl
[notes (TEXT):
 [*] 1 rows affected.
```

Rysunek: Tworzenie projektu pk i dodawanie domeny pk.edu.pl.

```
[[recon-ng][pk] > marketplace install recon/domains-hosts/google_site_web
 [*] Module installed: recon/domains-hosts/google_site_web
 [*] Reloading modules...
[[recon-ng][pk] > modules load recon/domains-hosts/google_site_web
[[recon-ng][pk][google_site_web] > run
-------
SUMMARY
-------
[*] 153 total (153 new) hosts found.
```

Rysunek: Znajdowanie hostów w bazie google web (bez API).

```
[recon-ng][pk] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][pk] > modules load recon/domains-hosts/hackertarget
-------
SUMMARY
-------
[*] 501 total (501 new) hosts found.
[recon-ng][pk][hackertarget] > back
```

Rysunek: Znajdowanie hostów w bazie hackertarget.

```
[recon-ng][pk] > marketplace install recon/hosts-hosts/resolve
[*] Module installed: recon/hosts-hosts/resolve
[*] Reloading modules...
[recon-ng][pk] > modules load recon/hosts-hosts/resolve
[recon-ng][pk][resolve] > run
```

Rysunek: Translacja adresów hostów na ip.

```
[recon-ng][pk] > keys add binaryedge_api [redacted]
[*] Key 'binaryedge_api' added.
[recon-ng][pk] > marketplace install recon/hosts-ports/binaryedge
[*] Module installed: recon/hosts-ports/binaryedge
[*] Reloading modules...
[recon-ng][pk] > modules load recon/hosts-ports/binaryedge
[recon-ng][pk][binaryedge] > run
-------
SUMMARY
-------
[*] 838 total (593 new) ports found.
```

Rysunek: Dodawanie klucza API dla binaryedge i znajdowanie portów.

```
[recon-ng][pk] > marketplace install ipstack
[*] Module installed: recon/hosts-hosts/ipstack
[*] Reloading modules...
[recon-ng][pk] > keys add ipstack_api [redacted]
[*] Key 'ipstack_api' added.
[recon-ng][pk] > modules load ipstack
[recon-ng][pk][ipstack] > run
```

Rysunek: Znajdowanie lokalizacji hostów.

```
[recon-ng][pk][ipstack] > dashboard

  +-------------------------------------------------------+
  |                   Activity Summary                    |
  +-------------------------------------------------------+
  |                    Module                       | Runs |
  +-------------------------------------------------------+
  | recon/domains-contacts/whois_pocs               | 2    |
  | recon/domains-hosts/certificate_transparency    | 2    |
  | recon/domains-hosts/google_site_web             | 1    |
  | recon/domains-hosts/hackertarget                | 1    |
  | recon/hosts-hosts/ipinfodb                      | 14   |
  | recon/hosts-hosts/ipstack                       | 3    |
  | recon/hosts-hosts/resolve                       | 1    |
  | recon/hosts-ports/binaryedge                    | 1    |
  +-------------------------------------------------------+


  +----------------------------+
  |      Results Summary       |
  +----------------------------+
  |     Category     | Quantity |
  +----------------------------+
  | Domains          | 1        |
  | Companies        | 0        |
  | Netblocks        | 0        |
  | Locations        | 0        |
  | Vulnerabilities  | 0        |
  | Ports            | 593      |
  | Hosts            | 654      |
  | Contacts         | 0        |
  | Credentials      | 0        |
  | Leaks            | 0        |
  | Pushpins         | 0        |
  | Profiles         | 0        |
  | Repositories     | 0        |
  +----------------------------+
```

Rysunek: Podsumowanie ilości użytych modułów i uzyskanych wyników.

```
[recon-ng][pk][ipstack] > show hosts

+-----------------------------------------------------------------------------------------------------------------------------------------------------------+
| rowid |                host                |    ip_address    |         region         | country |     latitude     |     longitude     | notes |      module      |
+-----------------------------------------------------------------------------------------------------------------------------------------------------------+
| 1     | bim.pk.edu.pl                      | 149.156.132.42   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 2     | fitnesskwadrat.pk.edu.pl           | 149.156.132.41   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 3     | www.kwadrat.pk.edu.pl              | 149.156.132.152  | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 4     | cantata.pk.edu.pl                  | 149.156.132.42   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 5     | ankiety.pk.edu.pl                  | 149.156.132.53   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 6     | www.a34.pk.edu.pl                  | 149.156.151.90   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 7     | osz-zywiec.pk.edu.pl               | 149.156.132.41   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 8     | imf.pk.edu.pl                      | 149.156.132.36   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 9     | m7.mech.pk.edu.pl                  | 149.156.158.212  | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 10    | audytbrd.pk.edu.pl                 | 149.156.132.41   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 11    | sjo.pk.edu.pl                      | 149.156.132.41   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 12    | www.nowinki.pk.edu.pl              | 149.156.157.82   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
| 13    | olf2.pk.edu.pl                     | 149.156.142.10   | Kraków, Lesser Poland | Poland  | 50.0707206726074 | 19.9309902191162  |       | google_site_web |
```

Rysunek: Wypisanie wszystkich uzyskanych danych dotyczących hostów.

```
[recon-ng][pk] > marketplace install reporting/csv
[*] Module installed: reporting/csv
[*] Reloading modules...
[recon-ng][pk] > modules load csv
[recon-ng][pk][csv] > run
```

Rysunek: Eksportowanie uzyskanych danych do pliku CSV.

```
"a-1.pk.edu.pl","149.156.132.44","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","google_site_web"
"a-1.pk.edu.pl","149.156.132.44","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","hackertarget"
"a1-galeria.pk.edu.pl","149.156.132.41","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","google_site_web"
"a1-galeria.pk.edu.pl","149.156.132.41","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","hackertarget"
"a2.arch.pk.edu.pl","149.156.132.44","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","google_site_web"
"a3-1.mech.pk.edu.pl","149.156.153.253","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","hackertarget"
"abaqus31.mech.pk.edu.pl","149.156.154.86","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","hackertarget"
"ac2.mech.pk.edu.pl","149.156.156.80","Kraków, Lesser Poland","Poland","50.0707206726074","19.9309902191162","","hackertarget"
```

Rysunek: Zawartość pliku.

```
| 292  | mt-its2019.pk.edu.pl | 77.79.233.102  | Mokotów, Mazovia    | Poland  | 52.1806297302246 | 21.0752105712891 |      | hackertarget |
| 354  | modularlab.pk.edu.pl | 86.111.241.89  | Sopot, Pomerania    | Poland  | 54.3638496398926 | 18.4333591461182 |      | hackertarget |
| 351  | s2b.pk.edu.pl        | 88.198.20.57   | Nürnberg, Bavaria   | Germany | 49.4519996643066 | 11.0768003463745 |      | hackertarget |
```

Rysunek: Ciekawe lokalizacje hostów.

Źródła

- http://edu.pjwstk.edu.pl/wyklady/bsi/scb/index.html
- https://hackertarget.com/recon-ng-tutorial/
- https://www.youtube.com/channel/UC7AEWW3pBeOwHsUnyJB_7Jg

Koniec

Dziękujemy za uwagę.