Soft tools to conquer the target

Ignacio Brihuega Rodríguez (N4xh4ck5)

1. Whoami
2. Develop your own tools
3. N4xD0rk
4. Wh01p

1. Whoami
2. Develop your own tools
3. N4xD0rk
4. Wh01p

Whoami

- Senior Security Consultant – Tiger Team SIA
- Máster de Seguridad Informática en Universidad de la Rioja (UNIR)
- Grado en Ingeniería en Tecnologías de la Telecomunicación, especialidad en ingeniería telemática.
- Coautor en el blog “Follow the White Rabbit” – fwhibbit.es
- Info de contacto:
  - **Linkedin**: https://es.linkedin.com/in/ignacio-brihuega-rodr%25C3%25ADguez-b89564a6
  - **Twitter**: twitter.com/@nachoo_91

Disclamer

- La información que se va a mostrar es de carácter público.
- Se ofuscará la mayor parte de las ocasiones para no mostrar el origen de la información.
- Las técnicas demostradas son para fines académicos, no me hago responsable de su uso para otro fin.
- Hack&Learn&Share

HACK
&BEERS

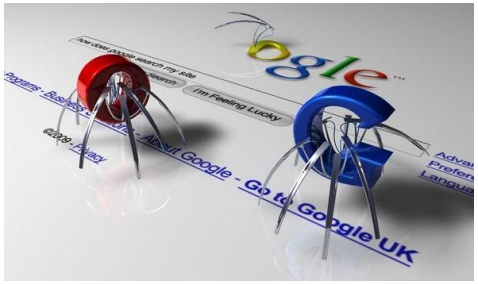
1. Whoami
2. Develop your own tools
3. N4xD0rk
4. Wh01p

Develop your own tools!

Si no existe la herramienta, desarrollará! -> El límite es tu imaginación

N4xd0rk

Wh01p



Develop your own tools!

HoneyCON
By HoneySec

Objetivos

- Listar toda la superficie web de un target aprovechando indexación resultados
- Listar dominios web no indexados a través
- Visualizar todo el mapa de red web del target

HACK &BEERS

1. Whoami
2. Develop your own tools
3. N4xD0rk
4. Wh01p

N4xD0rk

HoneyCON
By HoneySec

- Listar dominios y subdominios a través de Google y Bing.
- Python 2.7
- Versión 2.1:
  - Screenshot dominios.
  - Integración Dorkgo0
  - Integración Th4sD0m
  - Desarrollo modular.
- Tool que explota la indexación de resultados de buscadores.

HACK
&BEERS

N4xD0rk

- Descargable github.com/n4xh4ck5
- Visualización estado dominios.
- Footprinting -> Los buscadores hacen el trabajo sucio!

```
n4xdork-2.1# python n4xd0rk.py -h
usage: n4xd0rk.py [-h] -t TARGET -n NUMBER [-e EXPORT] [-l LANGUAGE]
                  [-c CAPTURE]

This script searchs the subdomains about a domain using the results indexed of Bing search.

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        The domain or IP which wants to search.
  -n NUMBER, --number NUMBER
                        Indicate the number of the search which you want to do.
  -e EXPORT, --export EXPORT
                        Export the results to a json file (Y/N)
                         Format available:
                                1.json
                                2.xlsx
  -l LANGUAGE, --language LANGUAGE
                        Indicate the language of the search
                                (es)-Spanish(default)
  -c CAPTURE, --capture CAPTURE
                        Indicate if you want to take a screenshot of each web (y/n)
```

Demo time!!!

1. Whoami
2. Develop your own tools
3. N4xD0rk
4. Wh01p

Wh01p

- Listar servicios web no indexados.
- Python 2.7
- Versión 1.1:
  - Screenshot dominios.
  - Validación API Shodan
  - Integración Th4sD0m.
- Tool que identifica servicios online no indexados.

Wh01p

HoneyCON
By HoneySec

- Listar servicios web no indexados.
- Identificar nombres de dominio.
- Listar dominios contenidas en la dirección IP

```
wh01p# python wh01p.py -h
usage: wh01p.py [-h] [-t TARGET] [-i INPUT]

Tool to obtain information about IP or domain: Geolocation, network, whois and open ports

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        The IP which it wants to search
  -i INPUT, --input INPUT
                        File which contains the domains or IP to obtain a piece of information in format txt or json
```

Demo time!!!

HACK &BEERS

TRABAJO FUTURO

- Integración Nmap en Wh0Ip.
- Integrar DuckduckGo y Exalead en N4xD0rk
- ~~¿Pagar API de Google?~~

HACK &BEERS

Ruegos Y Preguntas

¿?

Muchas gracias