

# Recon: Technical information

Learning about your target from the outside

# What I'm covering and what comes later

- ▶ This is “passive” recon
  - ▶ We are not touching the target
  - ▶ Should be undetectable
- ▶ Active scanning will be covered later
  - ▶ Involves talking directly to target infrastructure
  - ▶ Can be detected with adequate logging



# OSINT

Open Source INTeligence

# Google Dorks

## ▶ Tonnes of search filters

▶ inurl

▶ filetype

▶ intitle

## ▶ Google Hacking DataBase (GHDB)

▶ <https://exploit-db.com/ghdb>



## Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Search

SEARCH

Date	Title	Category
2018-08-08	inurl:lighttpd.conf lighttpd site:github.com	Files Containing Juicy Info
2018-08-08	-site:smarty.net ext:tpl intext:"	Files Containing Juicy Info
2018-08-07	inurl:nginx.conf nginx site:github.com	Files Containing Juicy Info
2018-08-07	intext:"successfully" intitle:"index of" config   log   logged -stackoverflow	Files Containing Juicy Info
2018-08-07	ext:log intext:"connection" intitle:"index of" -stackoverflow	Files Containing Juicy Info
2018-08-07	employee "training" intitle:index.of ext:doc   pdf   xls   docx   xlsx	Files Containing Juicy Info

# The classic camera search(es)

## ▶ “Various Online Devices”

- ▶ <https://www.exploit-db.com/google-hacking-database/13/>
- ▶ Google end up indexing a bunch of publicly accessible camera systems aswell.

- ▶ <https://www.google.com/search?q=inurl:jpegpull.htm>
- ▶ <https://www.google.com/search?q=inurl:embed.html%20inurl:dvr>

## Interesting information

- ▶ Files that shouldn't be available
- ▶ Information that gives insight into the systems
- ▶ <https://www.google.com/search?q=inurl:%22/wp-content/uploads/db-backup%22>
- ▶ <https://www.exploit-db.com/ghdb/1098/>

# WHOIS : the dried up oilwell

- ▶ *Thanks GDPR*
- ▶ Managed by ICANN
- ▶ WHOIS stores information on domain owners
  - ▶ Usually an email address, phone number and postal address
  - ▶ Should be properly verified by the registra
    - ▶ Sometimes requires legal documents to be sent
- ▶ <https://whois.icann.org/en/lookup?name=x>
- ▶ Has been looking to be scrapped since 2014

Registry Domain ID: f09f1be851914e9ca79a69bfe290babcd-DONUTS  
Registrar WHOIS Server: whois.namecheap.com  
Registrar URL: <https://www.namecheap.com/>  
Updated Date: 2018-06-23T01:54:34Z  
Creation Date: 2016-09-21T15:52:06Z  
Registry Expiry Date: 2018-09-21T15:52:06Z  
Registrar: NameCheap, Inc.  
Registrar IANA ID: 1068  
Registrar Abuse Contact Email: [abuse@namecheap.com](mailto:abuse@namecheap.com)  
Registrar Abuse Contact Phone: +1.6613102107  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Registry Registrant ID: REDACTED FOR PRIVACY  
Registrant Name: REDACTED FOR PRIVACY  
Registrant Organization: WhoisGuard, Inc.  
Registrant Street: REDACTED FOR PRIVACY  
Registrant City: REDACTED FOR PRIVACY  
Registrant State/Province: Panama  
Registrant Postal Code: REDACTED FOR PRIVACY  
Registrant Country: PA  
Registrant Phone: REDACTED FOR PRIVACY  
Registrant Phone Ext: REDACTED FOR PRIVACY  
Registrant Fax: REDACTED FOR PRIVACY  
Registrant Fax Ext: REDACTED FOR PRIVACY  
Registrant Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
Registry Admin ID: REDACTED FOR PRIVACY  
Admin Name: REDACTED FOR PRIVACY  
Admin Organization: REDACTED FOR PRIVACY  
Admin Street: REDACTED FOR PRIVACY  
Admin City: REDACTED FOR PRIVACY



# Post GDPR

- ▶ <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>
- ▶ Essentially they're now looking at a system where only certain people can access certain information about a domain registrant.
  - ▶ There will probably be ways to sign up for some access.

# Certificate Transparency

- ▶ A log of every certificate issued for a domain
- ▶ <https://www.certificate-transparency.org/how-ct-works>
- ▶ Can help find out linked domains.
- ▶ There are website to search for this:
  - ▶ <https://www.google.com/transparencyreport/https/ct/>
  - ▶ <https://crt.sh>



Can I do all this really easily?

*Is there an app for that?*

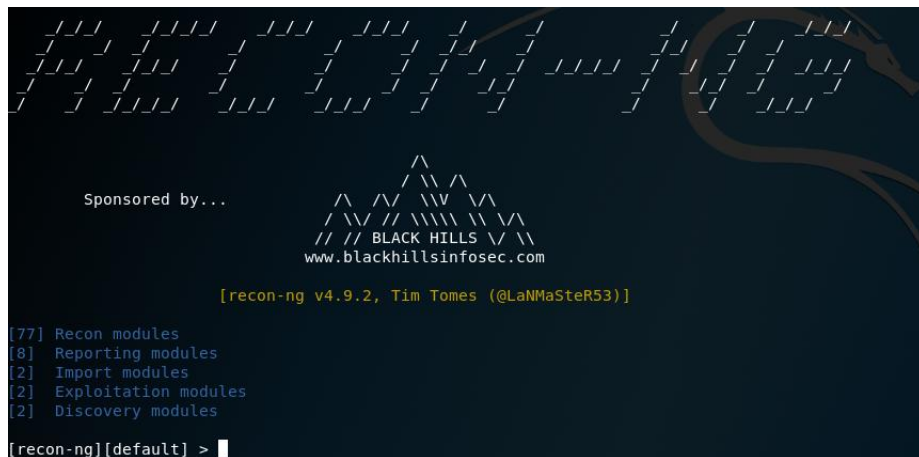


# Recon-ng

- ▶ Built in python and highly extensible
- ▶ The basic premise is to allow you use one piece of data to try and find more associated data from other sources.
- ▶ Stores all found information in an SQLite DB
  - ▶ Can also export to other formats

# Starting a recon-ng session

- ▶ recon-ng
- ▶ workspace add <name>
- ▶ show modules
- ▶ use <module>
- ▶ show info
- ▶ set <param name> <value>
- ▶ run



```
recon-ng

Sponsored by...

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

[recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]

[77] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

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

## Demo (and some useful modules)

- ▶ domains-hosts/hackertarget
- ▶ domains-hosts/certificate-transparency
- ▶ Try using the modules to find out things about things from a target domain

## Example chain (passive)

- ▶ Domain-hosts/hackertarget
- ▶ hosts-hosts/reverse-resolve
- ▶ Hosts-domains/migrate\_hosts
- ▶ Domains-hosts/certificate\_transparency
- ▶ Domains-contacts/whois\_pocs