

# Using Search Engines against a Target

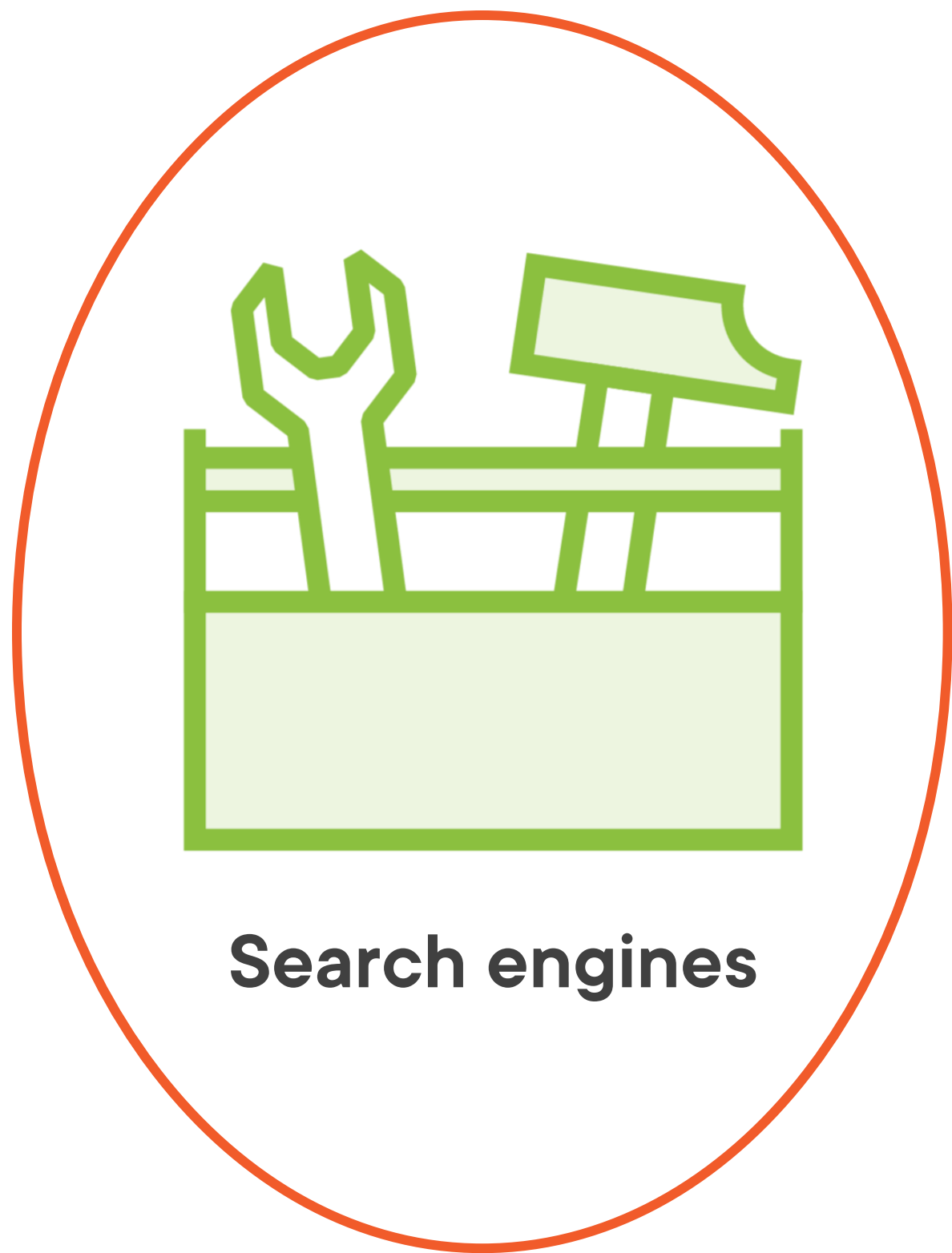
---



**Dale Meredith**

MCT | CEI | CEH | MCSA | MCSE  
Cyber Security Expert

[dalemeredith.com](http://dalemeredith.com) | Twitter: [@dalemeredith](https://twitter.com/dalemeredith) | LinkedIn: [dalemeredith](https://www.linkedin.com/in/dalemeredith)



**Search engines**

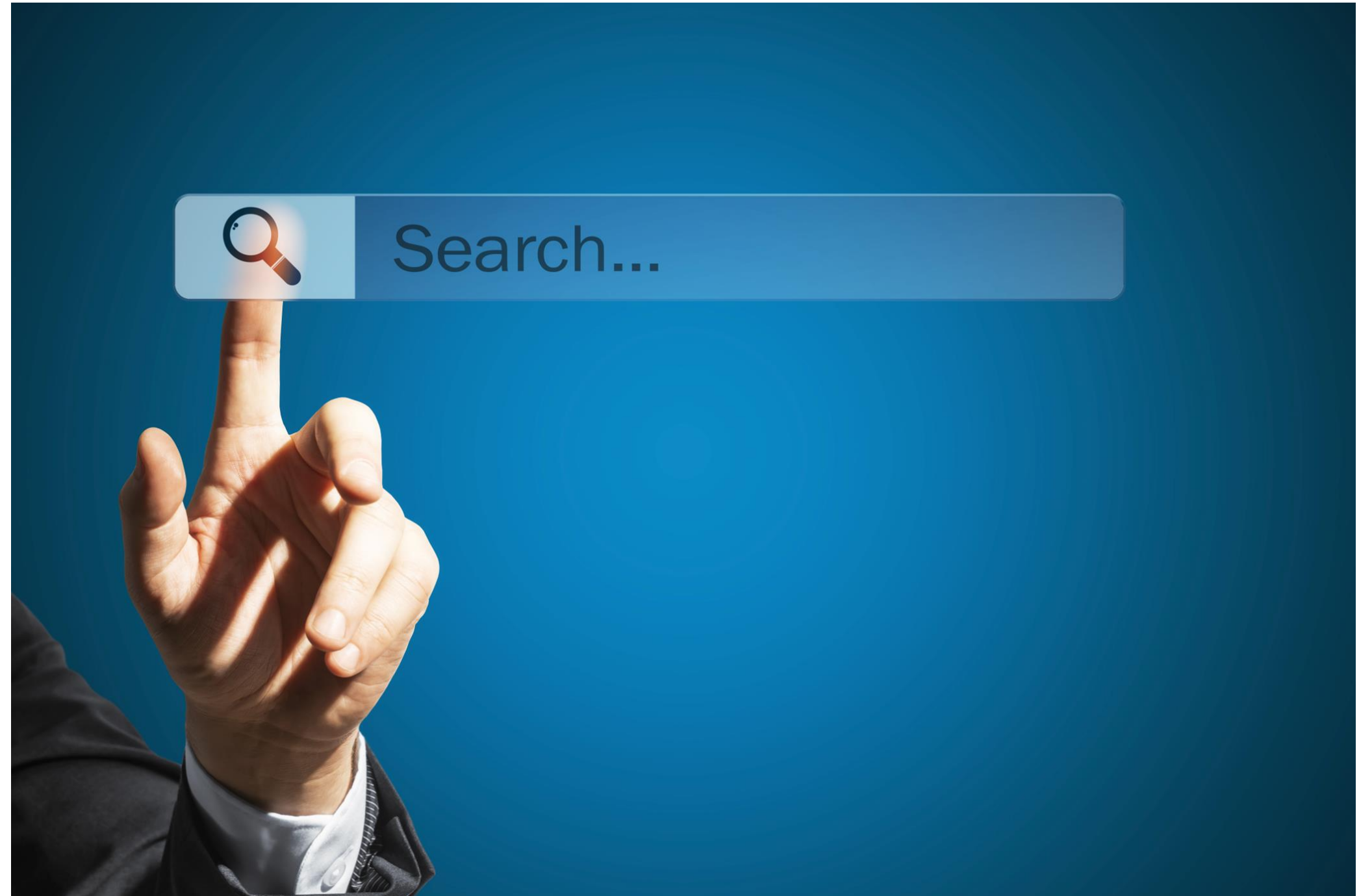


**Websites**



**Applications**

**Search engines**  
**Company website**  
**Company giveaways**  
**Employees**



# Demo



## Google Advance Search

# Demo



## Google hacking

# Demo



## Using the Basic Operators

# Advanced Google Operators

---

# Advanced Operators



Cache:

**Displays Google's cached version**

Link:

**Show a list of web pages that have links to your target**

Related:

**Similar web pages**

Info:

**View information Google has on the target**

Site:

**Limits results to just the domain listed**



# More Advanced Operators

allintitle:

Limits results to those websites with **ALL** the search words in the title

intitle:

Limits results to documents that contain the search word in the title

allinurl:

Limits results to only those webpages with **ALL** search words in the URL

inurl:

Limits results to documents that contain the search word in the URL



Demo



## **Advanced Google Hacking**

# What We Can Find with Google Hacking

---

# Understanding is Everything

## Devices and appliances

**Default settings**

**Accessible via browser**

**Application defaults**

**Internet printing**

**Internet cameras**

**Server defaults**

## Think outside the box

**Directories:** `intitle:index.of`.  
(Admin directories?)

**Find specific files**  
(Logs, password files,  
by file extension)

**Web servers**

**Directory traversal**

**Extension walking**



# Demo



## More Google Hacking

# Demo



## Using the Google Hacking Data Base (GHDB)





CYLANEE

OFFENSIVE  
security



# Demo



## Other Search Engines

- Image searching
- Video search engines
- FTP searching
- Finding VPN and VoIP



# Demo



## Discovering IoT Devices on Shodan

# Learning Check

---

# Learning Check



**Inurl:**



**Filetype:**



**Cache:**



**No space between operator and keyword**



**Napalm FTP Indexer**



Up Next:

Capturing Intel through Web Services

---