2ND MAY 2019 BY CTRLALTDEL

How To Hack With Google Dorks

Google dorking or Google Hacking is a hacking technique that uses the advance search functionality in Googles search engine.

Now a hacker isn't going to just search your company name and have Google return all of your vulnerable web applications or exposed documents. What it will do is return hundreds of sites that match or are similar to each word that you have searched for. Some will be relevant and a lot of it won't be. You would be pretty desperate to ever go past page 6 and a hacker isn't going to waste time doing this. Instead, they are going to use Google Dorks to have Google return specific queries such as URLs that contain certain file extensions.

If you don't want to go through the hassle of remembering them, you could also use the advance search page:
https://www.google.com/advanced_search?

The other thing to note is that Google records all searches. If you are thinking about doing some reconnaissance under the radar, you would be better using DuckDuckGo.

If you want to use the examples below, you will just need to replace [Keyword] with your query. You can also add another layer by adding keywords in front of the query or other Dorks, such as:
“Why did they make Vista site:Microsoft.com”

The “” are needed.

If you wanted to search keywords within a URL, you could use:
inurl:[Keyword]
Example: **inurl:admin.php**

If you wanted to only search withing a given domain:
site:[Keyword]
Example: **site:Microsoft.com**

If you wanted to only search for certain files:
filetype:[Keyword]
Example: **filetype:log**

If you wanted to search the body of the website for specific text:
intext:[Keyword]
Example: **intext:username filetype:log**

If you wanted to search for links:
link:[Keyword]
Example: **link:microsoft.com**

If you wanted to find information Google has on a page:
info: [Keyword]

Example: **info:www.myspace.com**

These are very basic examples in which you can use to return specific information from Google. When you mix these with known vulnerabilities or common vendor variables you can get some pretty interesting results.

Finding indexed SSH private keys:
intitle:index.of id_rsa -id_rsa.pub

Fetching SSH usernames from logs:
filetype:log username putty

Open FTP servers:
intitle:"index of" inurl:ftp

Finding saved email addresses:
filetype:xls inurl:"email.xls"

If you wanted to search a specific company, remember you can add a common search or add another dork:
"[Keyword]" filetype:xls inurl:"email.xls"

IP Based Cameras:
inurl:top.htm inurl:currenttime

Juniper Web Device Manager Login:
intitle:"Log In – Juniper Web Device Manager"

Dell Server IDRAC Login Portals:
intitle:"iDRAC-login"

Finding company default passwords. You can either narrow it down by one file type or pipe several, like so:
"your default password is" filetype:doc | filetype:pdf | filetype:csv | filetype:pdf | filetype:docx

Cisco GroupPwds:
filetype:pcf "cisco" "GroupPwd"

As you can see, if you get creative, you can find some really interesting stuff. Vendors often follow common patterns, so try and have a think of keywords you could use to pull specific results back. If you can't think of any, try looking through the Google Hacking DB: https://www.exploit-db.com/google-hacking-database?

Remember, reconnaissance isn't illegal but acting on what you fine might.

Related

Check How Exposed You Are Online Part 2

How The Phishers Phish
In "Cyber Security"

Why Securing Your Email Account Is Important

In "Cyber Security"

In "Cyber Security"

DORKING, DORKS, GOOGLE, HACKING

2 Replies to “How To Hack With Google Dorks”

Pingback: Check How Exposed You Are Online Part 2 – Ctrl Alt Del

Pingback: Using Open Source Intelligence (OSINT) – Ctrl Alt Del

Leave a Reply

Enter your comment here...

PREVIOUS

← Checking If A Site Or Email Is Genuine

NEXT

Enabling MFA On Shared Service Accounts →

Search …