GOOGLE HACKING: THE COMPLETE STEP BY STEP DETAILED TUTORIAL

INTRODUCTION

In this smart world if we are connected to the internet we can find many types of details using a google search engine. Google is used for everything to find out the details about any topics which we don't know or having any type of confusion in it and now using the same search engine we can find out some sensitive information called google dorking

Google hacking is also known as Dorking. Google hacking is a passive information gathering or footprinting technique that is used to extract information about vulnerabilities data exposure and security misconfiguration in websites which stored on a server

POPULAR POSTS:

GOT WARNING "UNUSUAL INSTAGRAM LOGIN ATTEMPT FROM…

INSTASHELL: FREE TOOL TO HACK INSTAGRAM ACCOUNTS

HOW TO HACK TWITTER ACCOUNTS WITH JUST 10 COMMANDS…

HOW TO HACK WIFI ROUTERS FROM YOUR SMARTPHONE WITH…

HOW TO HACK VIA SMARTPHONE LIKE MR. ROBOT USING TERMUX

NEW SCAM AND WHATSAPP VIRUS:

TUTORIALS

HOW
FTK IM
THE D
FORE
TOOL
INVES
COMP
CRIME
YOUR
COMP

7 EAS
CONF
SETTI
SECU
APACI
TOMC
SERVI
HACK

HOW
CONT
YOUR
WINDO
MACH
FROM
MALW
WITHO
ANTIV
USING
MALW
EFFEC

It involves using specialized search query operation to find out the right results based on what you are looking for, By some advanced operators like (inurl, filetype, intitle) using this advanced operators we can find out some information which is openly connected to the internet it may happen in a different way like mostly The first is when the server or other service is configured incorrectly, and administrative logs are available via the Internet. In the event of a password change or failure during authorization, account leakage through these logs is possible. The second scenario is when configuration files containing the same information become available. It is assumed that these files are for internal use only, but often confidential information is available in cleartext. Both of these scenarios allow you to gain control over the entire deal if an attacker manages to find the files of this kind

FIND OPEN FTP SERVERS WITH GOOGLE HACKING

- Now We use the dork to search for FTP servers available after 2018. These servers allow you to find out the files of internal use but unknowingly ended up in public access. **intitle:"index of" inurl:ftp after:2018**. This URL will list out only FTP servers

THE FREE COCA COLA FRIDGE

USING TERMGUARD FREE ANTIVIRUS IN TERMUX TO PROTECT…

TOP 10 UNDERGROUND TELEGRAM BOTS TO FIND PERSONAL…

CREATE YOUR OWN WORDLIST TO BRUTE FORCE A WEBSITE,…

ENCROCHAT, THE ENCRYPTED PHONE USED BY CARTELS AND…

VULNERABILITIES

2 IMPORTA VULNERABILITIES IN PHP ALLOW ADVISORY TO COMPLETELY TAKE OVER THE APPLICATION SERVER

HOW THIS SIMPLE GITHUB FLAW ALLOWED THREAT ACTORS TO DO REPOJACKING (TAKING OVER OTHERS

REME TOOL

HOW HACK ANDR SMAR WITH DROI

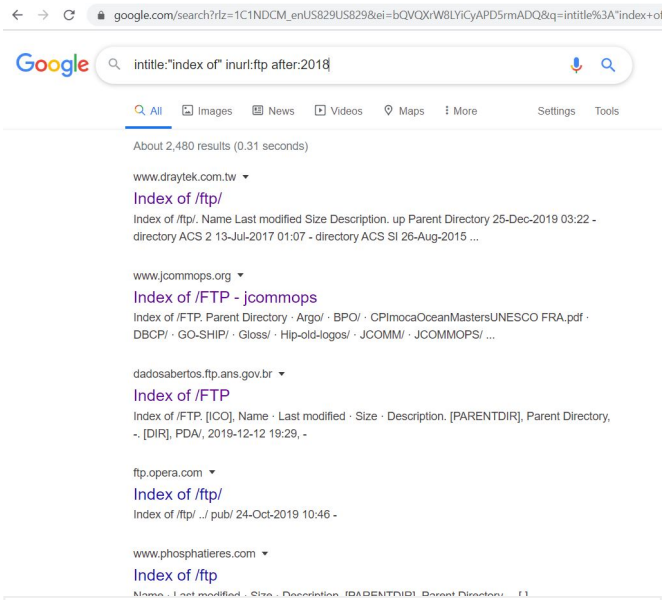
HOW CRAC THE PASS OF A FILE KALI

HOW FIND NAME PHON NUMB EMAIL ADDR AND PERS DATA ANY INSTA USER

HOW CYBE CRIMI HIDE PHISH WEBS ON TH INTER

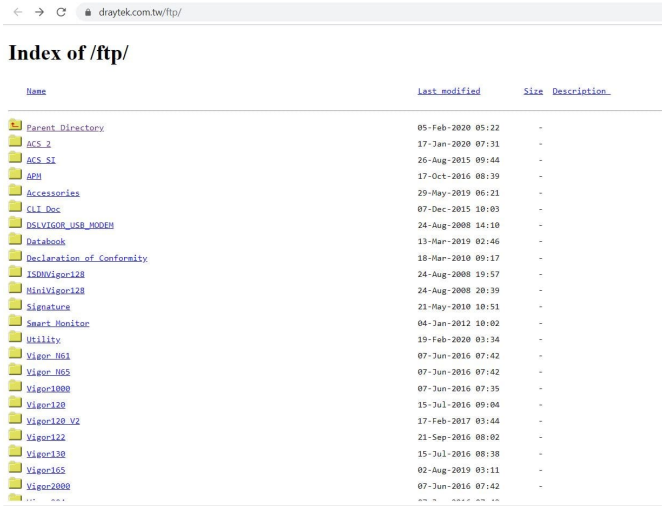
COMP MARY FRAM TUTO TOOL INCRE EMPL INFO SECU AWAR

HOW HACK



FTP Pages

- Now click on any link from that FTP pages, Let's see any data is available or not



FTP Files

- Yes, we see some data on this.
- Next, let's open this FTP Files. Let's check whether we can any confidential information

FTP Confidential Information

- Yes. we see some confidential information. If you click on any link in this we can download and see

REPOSITC
AND POISI
THEM WITH
MALWARE)

ORACLE
RELEASEI
PATCHES
370
VULNERAI
AND 200 OF
THEM ARE
REMOTELY
EXPLOITABLE.
PATCH NOW

COBALT
STRIKE
SOFTWAR
CONTAINS
CRITICAL
REMOTE (
EXECUTION
(RCE)
VULNERABILITY
THAT MIGHT
ALLOW
ANYONE TO
TAKE OVE
VICTIM
SYSTEMS

CVE-2022-
38465: VERY
CRITICAL
VULNERAI
WITH CVS
SCORE OF
AFFECT M
POPULAR PLC
DEVICE
SIEMENS
SIMATIC S
1200/1500

VIEW ALL

DATA BREACH

NEW
YORK
POST'S
WEBSITE

ANYO
USING
JUST
QR
CODE

HOW
LEAKI
NEW
ENGIN
CYBE
PROF
THAT
EASIE
DETE
VULNI
DEVIC

HOW
HACK
CREA
ANDR
SMAR
VIRUS
AHMY
AND S
ANYO

TOP 5
TECHI
USED
HACK
BLUE
DEVIC

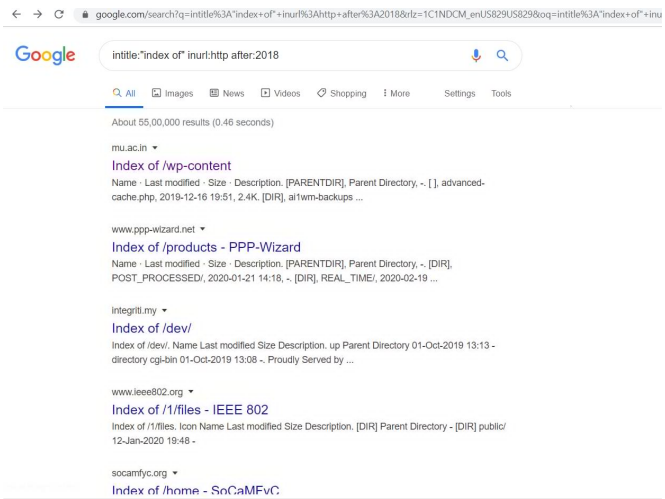
THE B
HACK
FOR
CYBE
PROF

7 EAS
STEPS
TO
INSTA
A
VIRTU
IMAGE
ON
ANDR
PHON
TO SU
DARK
AND

the content in this files

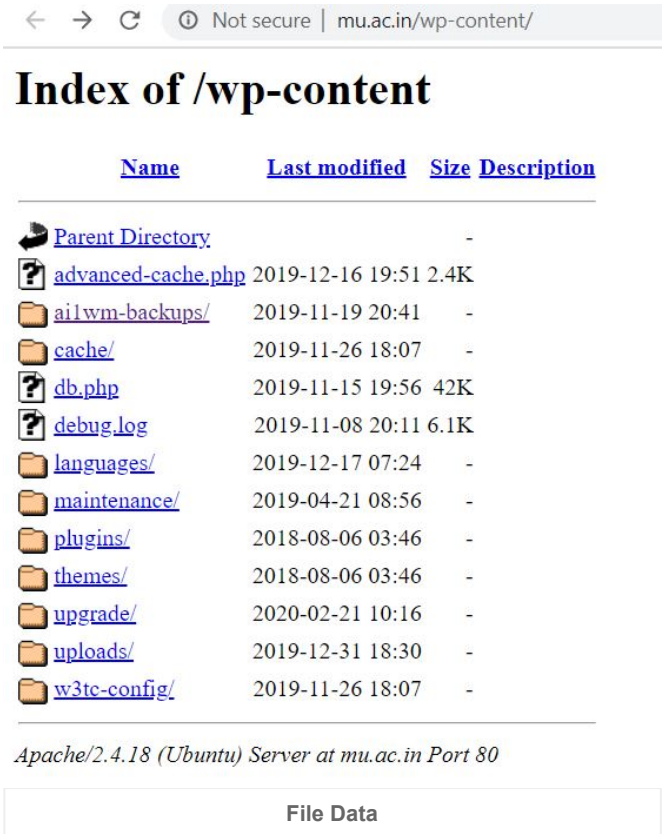
FIND UNSECURE WEBSITES WITH GOOGLE HACKING

- If we want to find out insecure HTTP pages, we have to modify the request above by changing “FTP” to “HTTP” **intitle:”index of” inurl:http after:2018.** This URL will list out only unsecured HTTP pages, In this results, we can find hundreds of HTTP pages and ready to compromise



Unsecure HTTP Page

- Now click on any link from that HTTP pages, Let’s see any data is available



File Data

AND TWITTER ACCOUNT HACKED

BINANCE HACKED AGAIN, THIS TIME $110 MILLION FUND STOLEN

AMERICAN AIRLINES, LARGEST AIRLINE THE WORLD HACKED VIA SOCIAL ENGINEEF

UBER INVESTIGATING MASSIVE DATA BREACH AFFECTING ALL ITS SYSTEMS. BLOCK YOUR CREDIT CARDS USED IN U APPS

U-HAUL HACKED. CUSTOMERS NAME AND DRIVER’S LICENSE OR STATE IDENTIFICATION NUMBER LEAKED

MONTENEGRO UNDER ALLEGED RUSSIAN CYBERATT

META’S PIXEL TOOL, USED TO

PROT YOUR IDENT

HOW FIND LOCA OF A PHON WITH JUST PHON NUMB FREE COST

VIEW ALL

VIRUS

THESI STRAI OF-SA MALW AND T HUNT STEAL OF CF FROM TERM

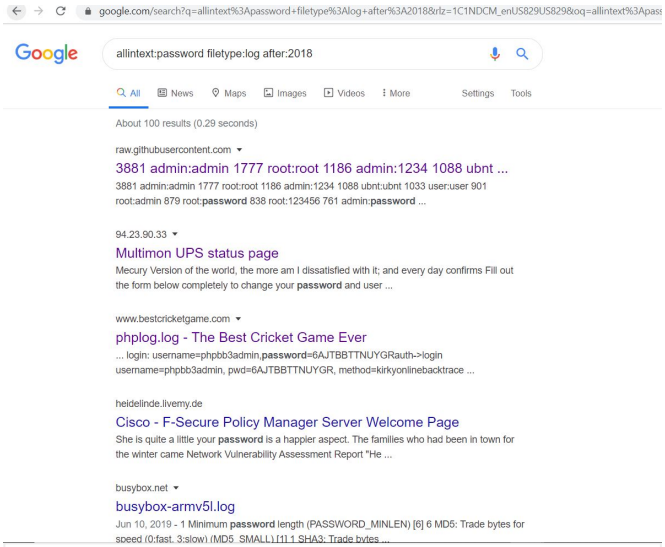
NEW ROOT MALW BLACK OF JU KB IN ALLO HACK COMP FORE EVEN HARD IS RE AND T JUST $5000

LORE RANS HACK ENTE NETW

- In the above picture, we see some file containing confidential data in it

SEARCH LOGS FOR PASSWORDS

- Passwords that are available in internet **allintext:password filetype:log after:2018**. when we use this URL we can see password list in plain text



Password Pages

- In the below picture we login details for links we directly download the data and we can search in that file

Plain Text Password

SEARCH FOR CONFIGURATION FILES WITH PASSWORDS

- Configuration files should never be accessible externally. When we use this URL we can find some password and database. **filetype:env "DB_PASSWORD" after:2018**.
- Now, Let's click on any link whether we get the password list

MONITOR THE PERFORMANCE OF FACEBOOK ADS, ENABLED THE COLLECTION OF SENSIT DATA FRO OVER MILI OF MEDIC PATIENTS

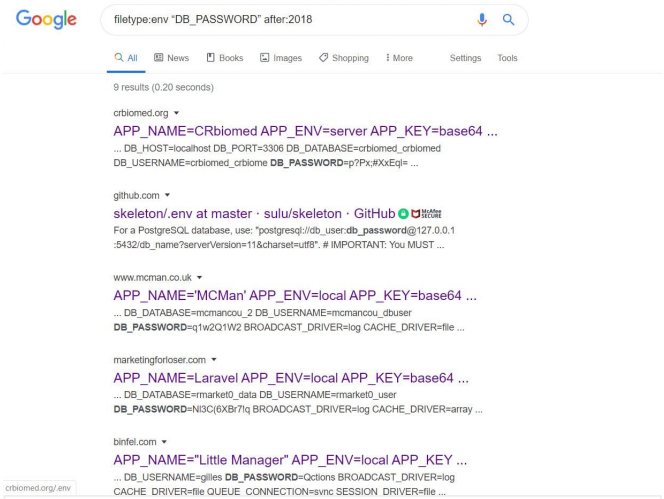
VIEW ALL

THRO VOIP I SYSTE SECU VOIP S

YOUR LINK ROUT IS AT I WITH NEW MOON BOTN

NEW RANS AGEN BOOT MACH SAFE TO EN THE F WITH GETTI DETE

VIEW ALL



Password Page

- Yes we found login details

Password List 1

- In some cases, we see invalid URL or Any error, in that case, click below arrow after the link we see the cached option click on it then we can see the data
- In the below picture we see another login credentials

```
# Django variables
DB_HOST=db
DB_PORT=5432
DB_USER=postgres
DB_NAME=postgres
DB_PASSWORD=8auidMBnPjMW6dTAfyZDkurOpFqI7p
DJANGO_DEBUG=False

# Postgresql env variables.
POSTGRES_PASSWORD=8auidMBnPjMW6dTAfyZDkurOpFqI7p
```

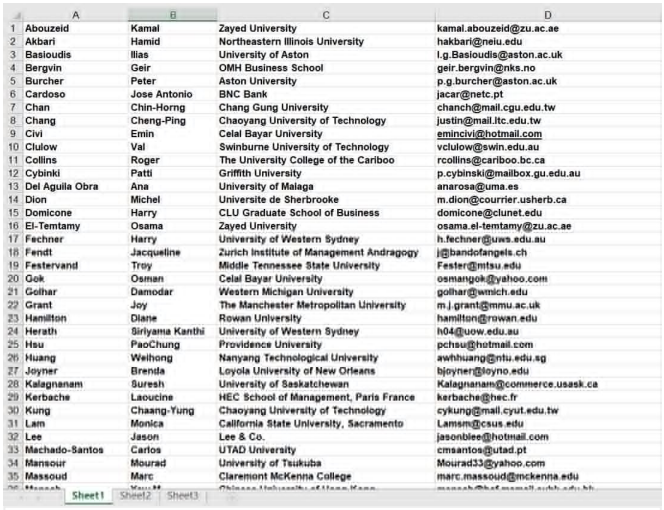
Password List 2

FINDING EMAILS FROM GOOGLE

- We will search for e-mail lists in spreadsheets (files with the .XLS extension). In the search query inside the URL, set the file name “email.xls” this will Be Collecting email lists is a great way to find information about various organizations. Use **filetype:xls inurl:”email.xls**

Email Page

- Now we see Email pages in the above picture, if we click on those links we can directly download the email list.



	A	B	C	D
1	Abouzeid	Kamal	Zayed University	kamal.abouzeid@zu.ac.ae
2	Akbari	Hamid	Northeastern Illinois University	hakbari@neiu.edu
3	Basioudis	Ilias	University of Aston	I.g.Basioudis@aston.ac.uk
4	Bergvin	Geir	OMH Business School	geir.bergvin@nks.no
5	Burcher	Peter	Aston University	p.g.burcher@aston.ac.uk
6	Cardoso	Jose Antonio	BNC Bank	jacar@netc.pt
7	Chan	Chin-Horng	Chang Gung University	chanch@mail.cgu.edu.tw
8	Chang	Cheng-Ping	Chaoyang University of Technology	justin@mail.ltc.edu.tw
9	Civi	Emin	Celal Bayar University	emincivi@hotmail.com
10	Clulow	Val	Swinburne University of Technology	vclulow@swin.edu.au
11	Collins	Roger	The University College of the Cariboo	rcollins@cariboo.bc.ca
12	Cybinki	Patti	Griffith University	p.cybinski@mailbox.gu.edu.au
13	Del Aguila Obra	Ana	University of Malaga	anarosa@uma.es
14	Dion	Michel	Universite de Sherbrooke	m.dion@courrier.usherb.ca
15	Domicone	Harry	CLU Graduate School of Business	domicone@clunet.edu
16	El-Temtamy	Osama	Zayed University	osama.el-temtamy@zu.ac.ae
17	Fechner	Harry	University of Western Sydney	h.fechner@uws.edu.au
18	Fendt	Jacqueline	Zurich Institute of Management Andragogy	j@bandofangels.ch
19	Festervand	Troy	Middle Tennessee State University	Fester@mtsu.edu
20	Gok	Osman	Celal Bayar University	osmangok@yahoo.com
21	Golhar	Damodar	Western Michigan University	golhar@wmich.edu
22	Grant	Joy	The Manchester Metropolitan University	m.j.grant@mmu.ac.uk
23	Hamilton	Diane	Rowan University	hamilton@rowan.edu
24	Herath	Siriyama Kanthi	University of Western Sydney	h04@uow.edu.au
25	Hsu	PaoChung	Providence University	pchsu@hotmail.com
26	Huang	Weihong	Nanyang Technological University	awhhuang@ntu.edu.sg
27	Joyner	Brenda	Loyola University of New Orleans	bjoyner@loyno.edu
28	Kalagnanam	Suresh	University of Saskatchewan	Kalagnanam@commerce.usask.ca
29	Kerbache	Laoucine	HEC School of Management, Paris France	kerbache@hec.fr
30	Kung	Chaang-Yung	Chaoyang University of Technology	cykung@mail.cyut.edu.tw
31	Lam	Monica	California State University, Sacramento	Lamsm@csus.edu
32	Lee	Jason	Lee & Co.	jasonblee@hotmail.com
33	Machado-Santos	Carlos	UTAD University	cmsantos@utad.pt
34	Mansour	Mourad	University of Tsukuba	Mourad33@yahoo.com
35	Massoud	Marc	Claremont McKenna College	marc.massoud@mckenna.edu

Sheet1 Sheet2 Sheet3

Email Sheet

- In the above picture, this is the data I have downloaded we see the data in the spreadsheet.

HACK CAMERAS USING GOOGLE

- We can access the camera via HTTP pages One of the most common queries contains the name “top.htm” to search the URL along with the current time and date. Using the below dork, you will get many pages. Use `inurl:top.htm inurl:currenttime` OR **inurl:/view/index.shtml”Camera”**.

Web Pages

- Now open another link **inurl:top.htm inurl:currenttime**, let,s see from this page

weather we see any live camera or not.

Web Page 2

- The above Picture we see live traffic cameras in the USA, Oregon, city of Salem, this camera is available without a password this advantage may use any unusual activity and this how dorks allow you to find authorization pages for cameras that use normal passwords.

Live Traffic Cameras in USA

- In the above picture, we see live traffic cameras in USA.

Live Traffic Camera in Russia

- In the above picture, we see a live traffic camera in Russia.

Live camera in Italy

- In the above picture, we see a live camera in Italy.

CONCLUSION

- Since Google has everything that is connected to the Internet and has a web interface, we can easily find incorrectly configured devices and services. However, it is better not to connect to these devices and there may be problems with application works.

ADVANCED OPERATORS

- This is the advanced operators that we can use to exploit insecure websites.

Advanced Operators

Jim Gill

Cyber Security Researcher. Information security specialist, currently working as risk infrastructure specialist & investigator.

He is a cyber-security researcher with over 18 years of experience. He has served with the Intelligence Agency as a Senior Intelligence Officer. He has also worked on the projects of Citrix and Google in deploying cyber security solutions. He has aided the government and many federal agencies in thwarting many cyber crimes. He has been writing for us in his free time since last 5 years.

ON: DECEMBER 4, 2020 / IN: TUTORIALS / TAGGED: GOOGLE HACKING