# SEM 2 2022/2023

## MTN 3024

## Network Security

***LAB REPORT NO: 1***

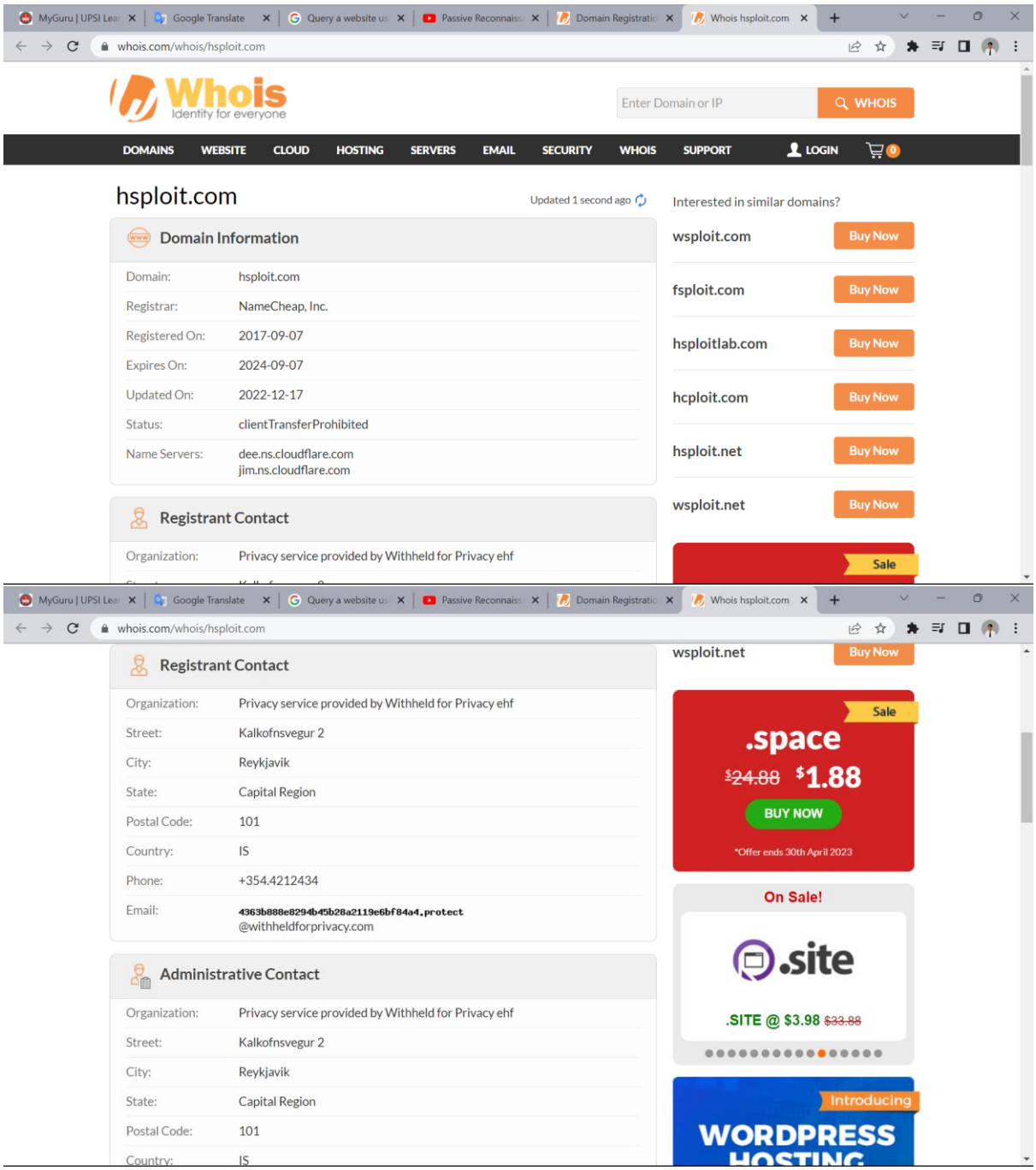
***Name: MOHD IZZUL IKHWAN BIN MOHD YUSOF***

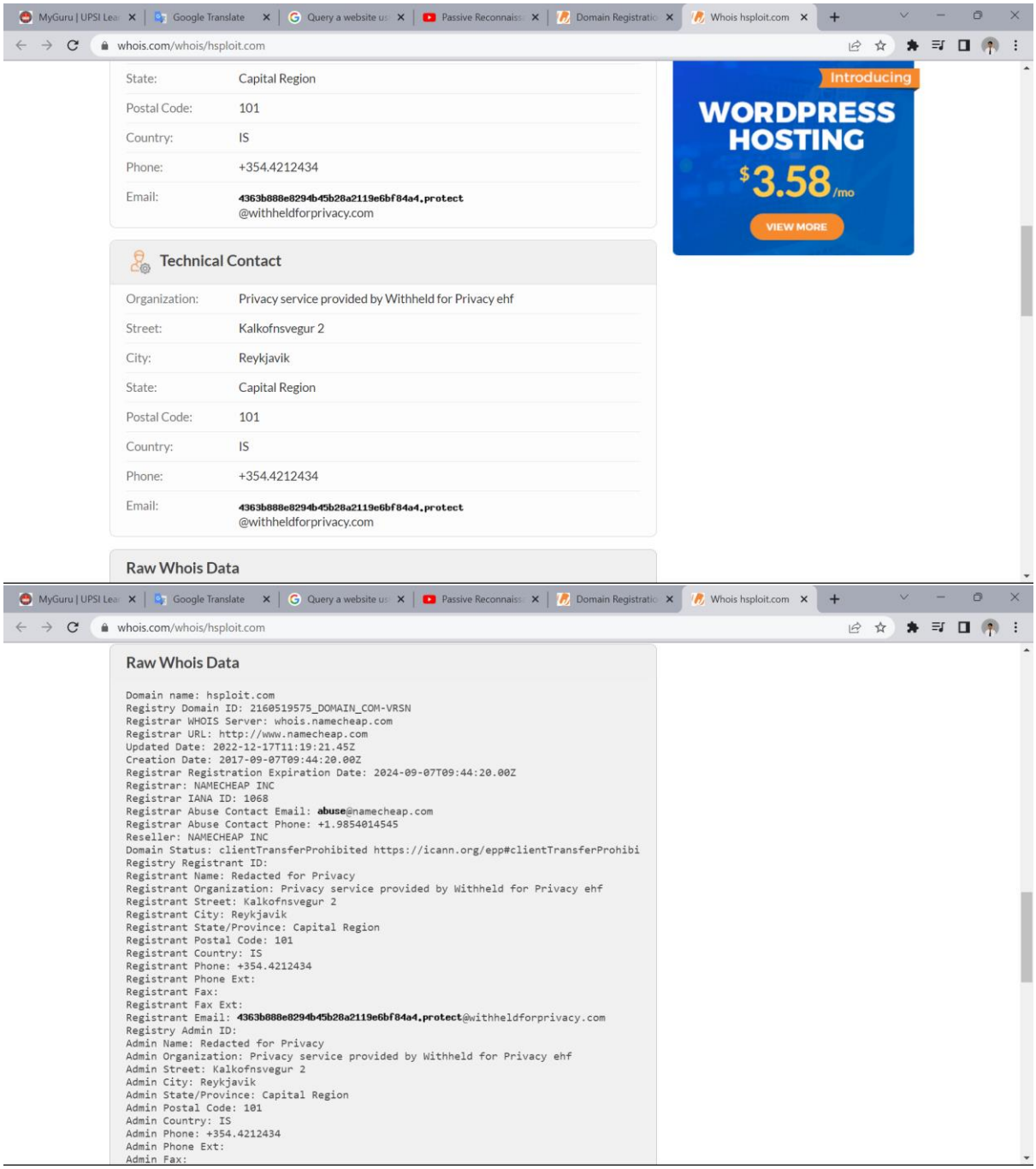
***Matric Number: D20201095609***

***Lecture Group: A***

***Lecturer: Dr. Okta Nurika***

# ACTIVITY 1


MyGuru | UPSI Lea
Google Translate
Query a website us
Passive Reconnaiss
Domain Registratio
Whois hsploit.com
whois.com/whois/hsploit.com
Whois
Identity for everyone
Enter Domain or IP
WHOIS
DOMAINS
WEBSITE
CLOUD
HOSTING
SERVERS
EMAIL
SECURITY
WHOIS
SUPPORT
LOGIN
hsploit.com
Updated 1 second ago
Domain Information
Domain: hsploit.com
Registrar: NameCheap, Inc.
Registered On: 2017-09-07
Expires On: 2024-09-07
Updated On: 2022-12-17
Status: clientTransferProhibited
Name Servers: dee.ns.cloudflare.com
jim.ns.cloudflare.com
Registrant Contact
Organization: Privacy service provided by Withheld for Privacy ehf
Interested in similar domains?
wsploit.com Buy Now
fsploit.com Buy Now
hsploitlab.com Buy Now
hcploit.com Buy Now
hsploit.net Buy Now
wsploit.net Buy Now
Sale
Registrant Contact
Organization: Privacy service provided by Withheld for Privacy ehf
Street: Kalkofnsvegur 2
City: Reykjavik
State: Capital Region
Postal Code: 101
Country: IS
Phone: +354.4212434
Email: 4363b888e8294b45b28a2119e6bf84a4.protect
@withheldforprivacy.com
Administrative Contact
Organization: Privacy service provided by Withheld for Privacy ehf
Street: Kalkofnsvegur 2
City: Reykjavik
State: Capital Region
Postal Code: 101
Country: IS
wsploit.net Buy Now
Sale
.space
$24.88 $1.88
BUY NOW
*Offer ends 30th April 2023
On Sale!
.site
.SITE @ $3.98 $33.88
Introducing
WORDPRESS



| | |
|---|---|
| State: | Capital Region |
| Postal Code: | 101 |
| Country: | IS |
| Phone: | +354.4212434 |
| Email: | 4363b888e8294b45b28a2119e6bf84a4.protect@withheldforprivacy.com |

Introducing
WORDPRESS HOSTING
$3.58/mo
VIEW MORE

## Technical Contact

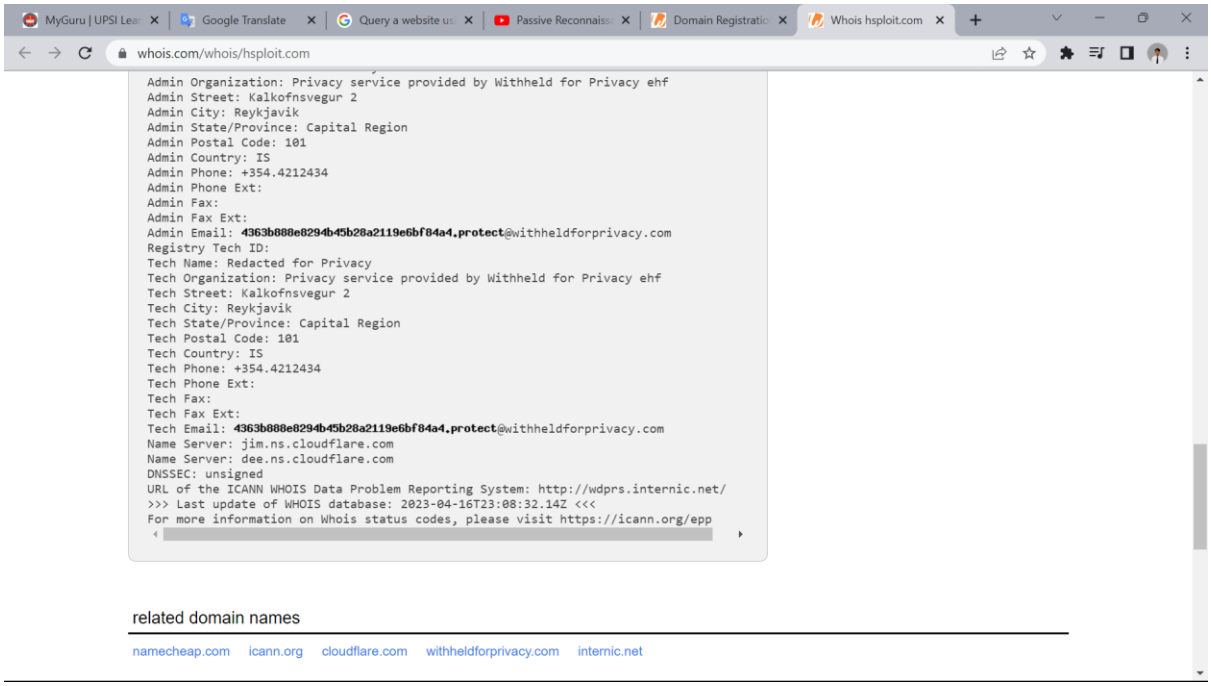
| | |
|---|---|
| Organization: | Privacy service provided by Withheld for Privacy ehf |
| Street: | Kalkofnsvegur 2 |
| City: | Reykjavik |
| State: | Capital Region |
| Postal Code: | 101 |
| Country: | IS |
| Phone: | +354.4212434 |
| Email: | 4363b888e8294b45b28a2119e6bf84a4.protect@withheldforprivacy.com |

## Raw Whois Data



## Raw Whois Data

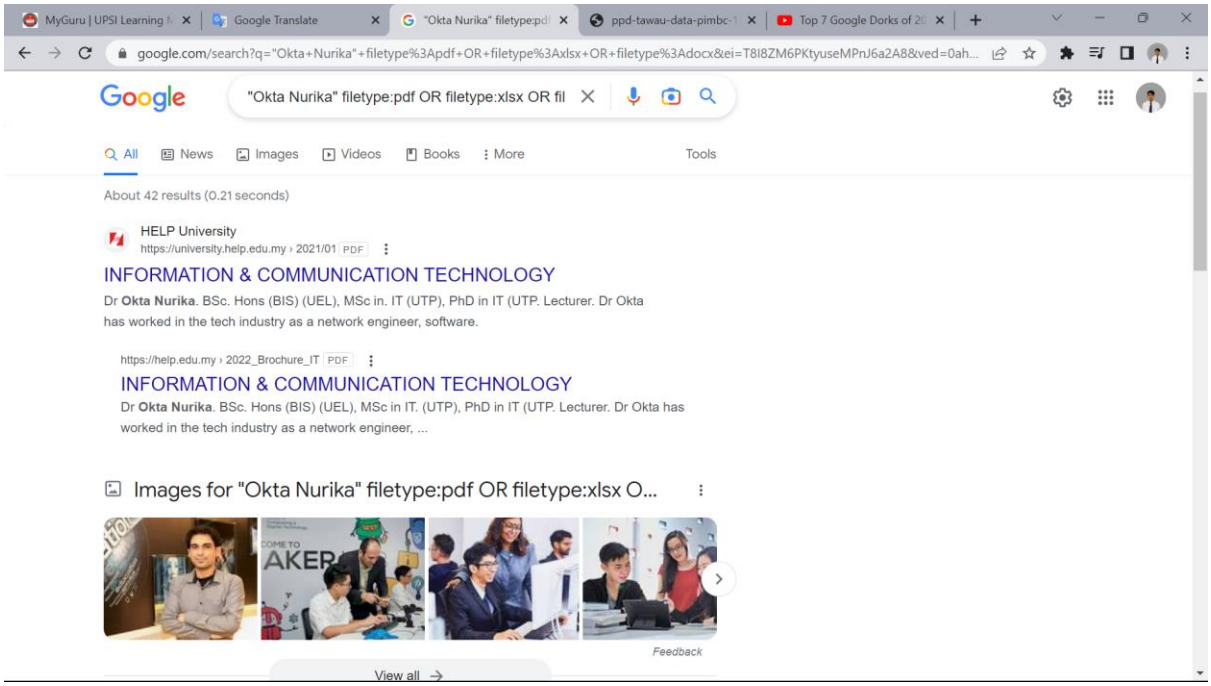
```
Domain name: hsploit.com
Registry Domain ID: 2160519575_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2022-12-17T11:19:21.45Z
Creation Date: 2017-09-07T09:44:20.00Z
Registrar Registration Expiration Date: 2024-09-07T09:44:20.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibi
Registry Registrant ID:
Registrant Name: Redacted for Privacy
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 4363b888e8294b45b28a2119e6bf84a4.protect@withheldforprivacy.com
Registry Admin ID:
Admin Name: Redacted for Privacy
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
```

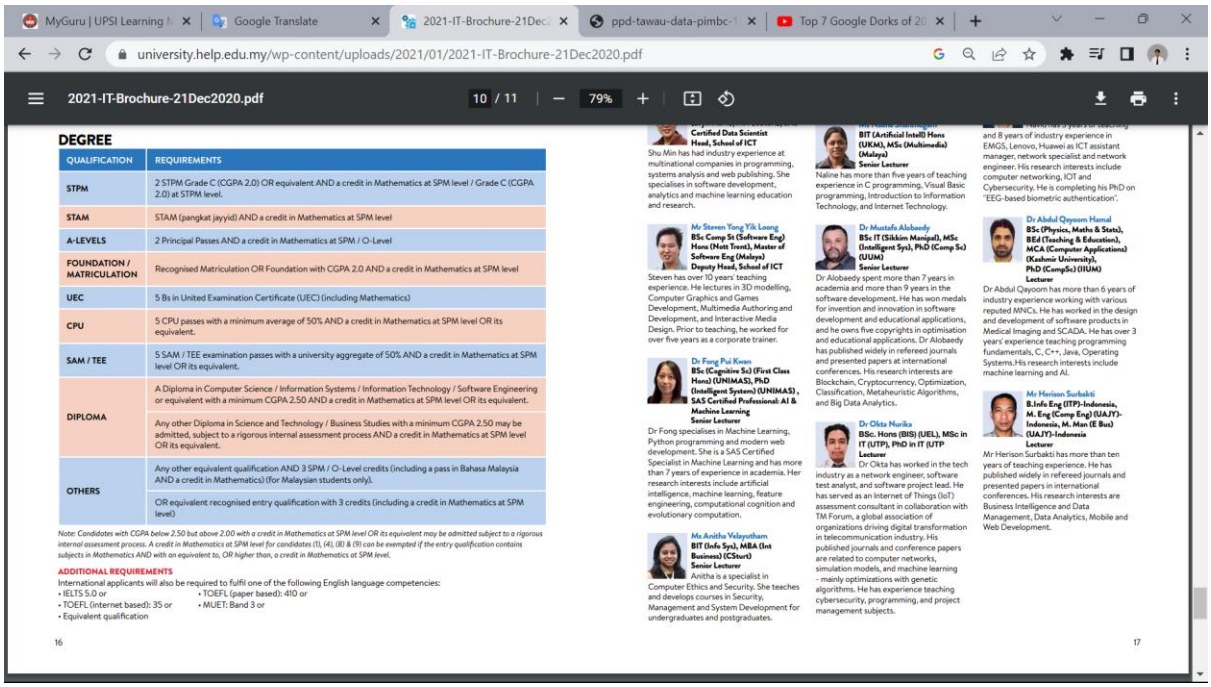

MyGuru | UPSI Lea
Google Translate
Query a website us
Passive Reconnaiss
Domain Registratio
Whois hsploit.com
whois.com/whois/hsploit.com
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 4363b888e8294b45b28a2119e6bf84a4.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Redacted for Privacy
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 4363b888e8294b45b28a2119e6bf84a4.protect@withheldforprivacy.com
Name Server: jim.ns.cloudflare.com
Name Server: dee.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-04-16T23:08:32.14Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
related domain names
namecheap.com
icann.org
cloudflare.com
withheldforprivacy.com
internic.net

# ACTIVITY 2

1. "Okta Nurika" filetype:pdf OR filetype:xlsx OR filetype:docx

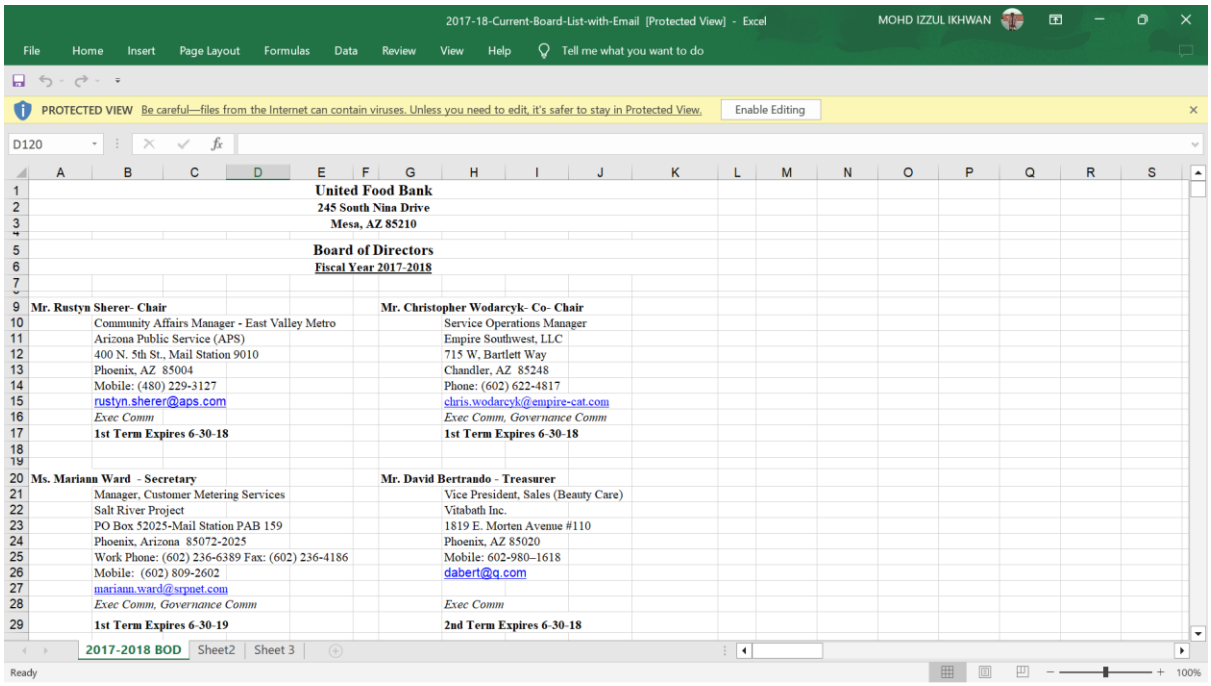
Web hosted docs that's can find your contact info, tools/application in your current or past employer's environment, LinkedIn account and sometimes your home address on the internet.



2. filetype:xls inurl:"email.xls" (in General)
3. site:.edu filetype:xls inurl:"email.xls" (in Education)

Email list that can gathered random email list from the internet in some environment e.g.



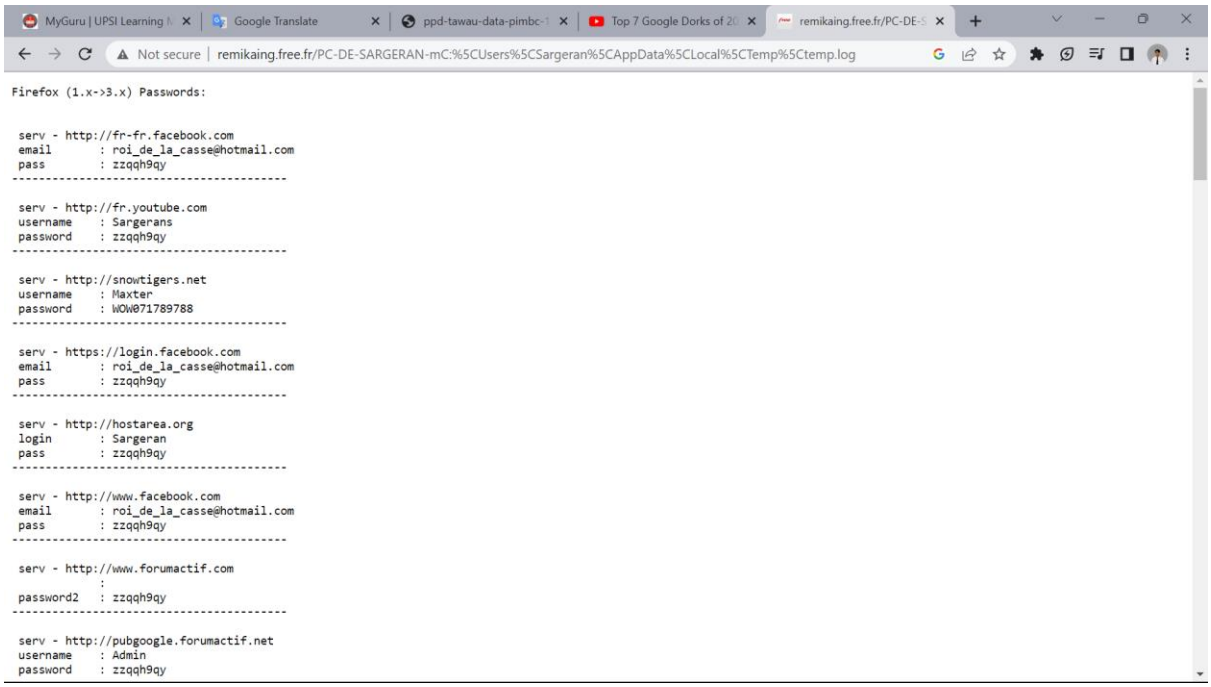
**United Food Bank**
**245 South Nina Drive**
**Mesa, AZ 85210**

**Board of Directors**
**Fiscal Year 2017-2018**

| | |
|---|---|
| **Mr. Rustyn Sherer- Chair** | **Mr. Christopher Wodarcyk- Co- Chair** |
| Community Affairs Manager - East Valley Metro | Service Operations Manager |
| Arizona Public Service (APS) | Empire Southwest, LLC |
| 400 N. 5th St., Mail Station 9010 | 715 W, Bartlett Way |
| Phoenix, AZ 85004 | Chandler, AZ 85248 |
| Mobile: (480) 229-3127 | Phone: (602) 622-4817 |
| rustyn.sherer@aps.com | chris.wodarcyk@empire-cat.com |
| *Exec Comm* | *Exec Comm, Governance Comm* |
| **1st Term Expires 6-30-18** | **1st Term Expires 6-30-18** |
| **Ms. Mariann Ward - Secretary** | **Mr. David Bertrando - Treasurer** |
| Manager, Customer Metering Services | Vice President, Sales (Beauty Care) |
| Salt River Project | Vitabath Inc. |
| PO Box 52025-Mail Station PAB 159 | 1819 E. Morten Avenue #110 |
| Phoenix, Arizona 85072-2025 | Phoenix, AZ 85020 |
| Work Phone: (602) 236-6389 Fax: (602) 236-4186 | Mobile: 602-980–1618 |
| Mobile: (602) 809-2602 | dabert@q.com |
| mariann.ward@srpnet.com | |
| *Exec Comm, Governance Comm* | *Exec Comm* |
| **1st Term Expires 6-30-19** | **2nd Term Expires 6-30-18** |

4. allintext:username filetype:log

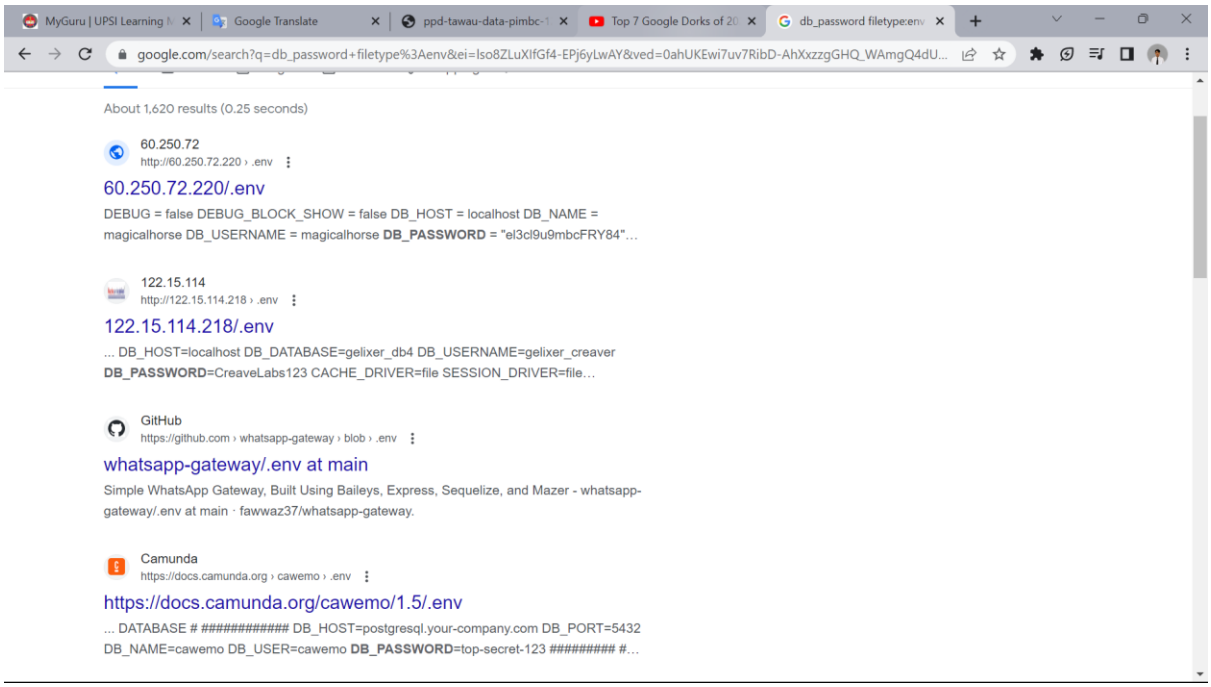
This Google hacking statement can access to some log files when the databases don't have enough security to secure the user username and password.



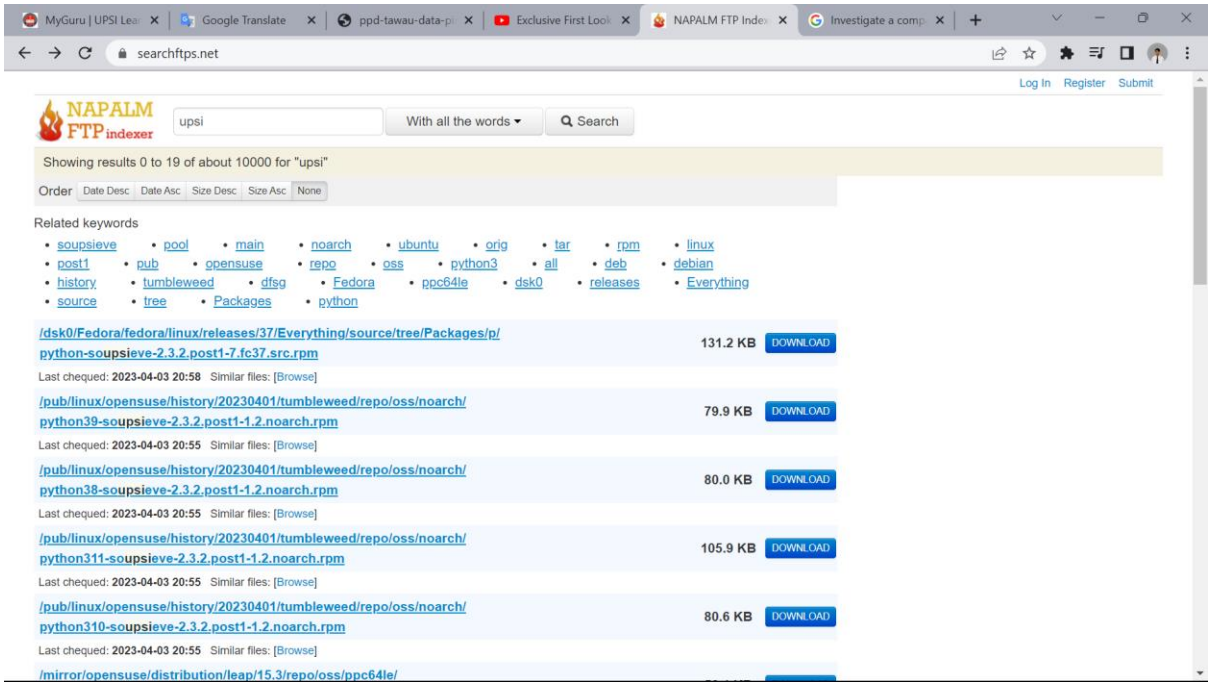
```
Firefox (1.x->3.x) Passwords:

 serv - http://fr-fr.facebook.com
 email       : roi_de_la_casse@hotmail.com
 pass        : zzqqh9qy
----------------------------------------

 serv - http://fr.youtube.com
 username    : Sargerans
 password    : zzqqh9qy
----------------------------------------

 serv - http://snowtigers.net
 username    : Maxter
 password    : WOW071789788
----------------------------------------

 serv - https://login.facebook.com
 email       : roi_de_la_casse@hotmail.com
 pass        : zzqqh9qy
----------------------------------------

 serv - http://hostarea.org
 login       : Sargeran
 pass        : zzqqh9qy
----------------------------------------

 serv - http://www.facebook.com
 email       : roi_de_la_casse@hotmail.com
 pass        : zzqqh9qy
----------------------------------------

 serv - http://www.forumactif.com
              :
 password2   : zzqqh9qy
----------------------------------------

 serv - http://pubgoogle.forumactif.net
 username    : Admin
 password    : zzqqh9qy
```

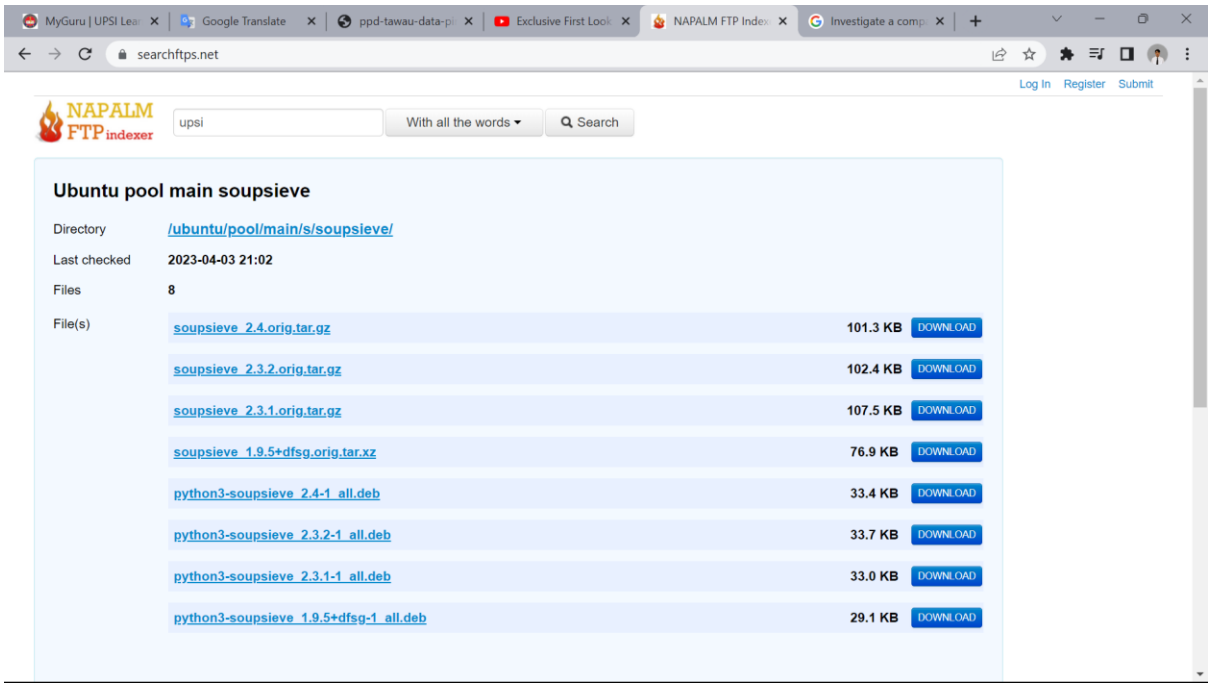
5. db_password filetype:env

This statement can show the list of unencrypted database information like database name, database host and the most important thing is database password.

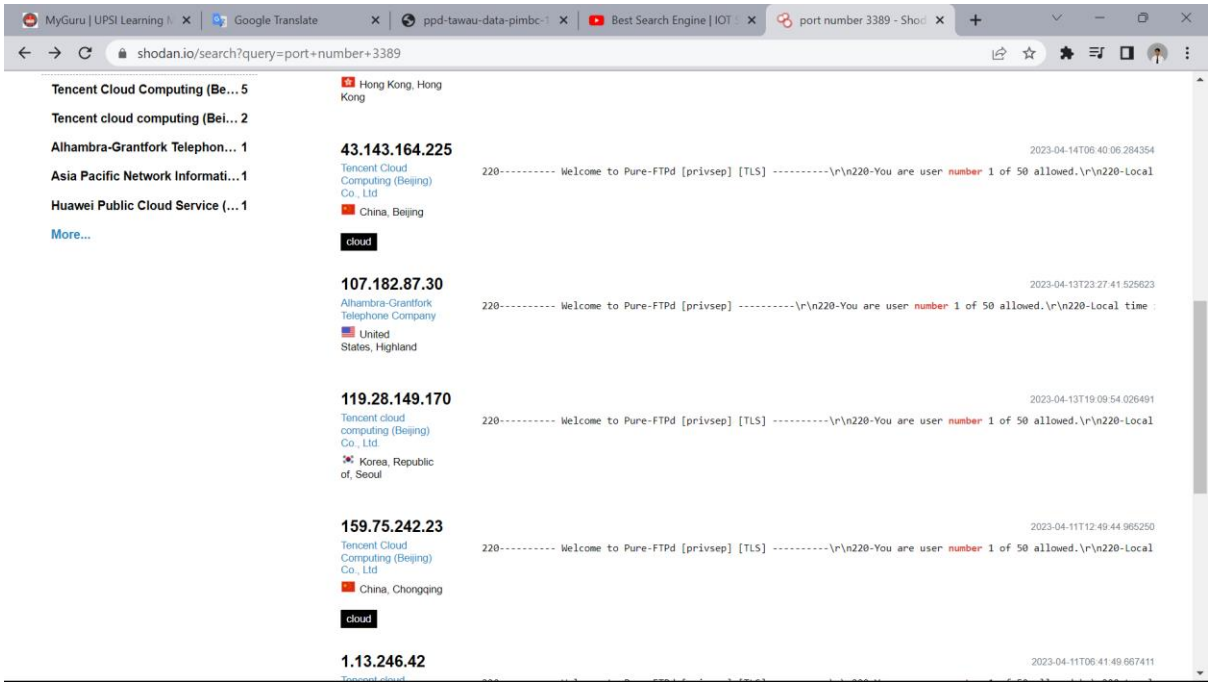


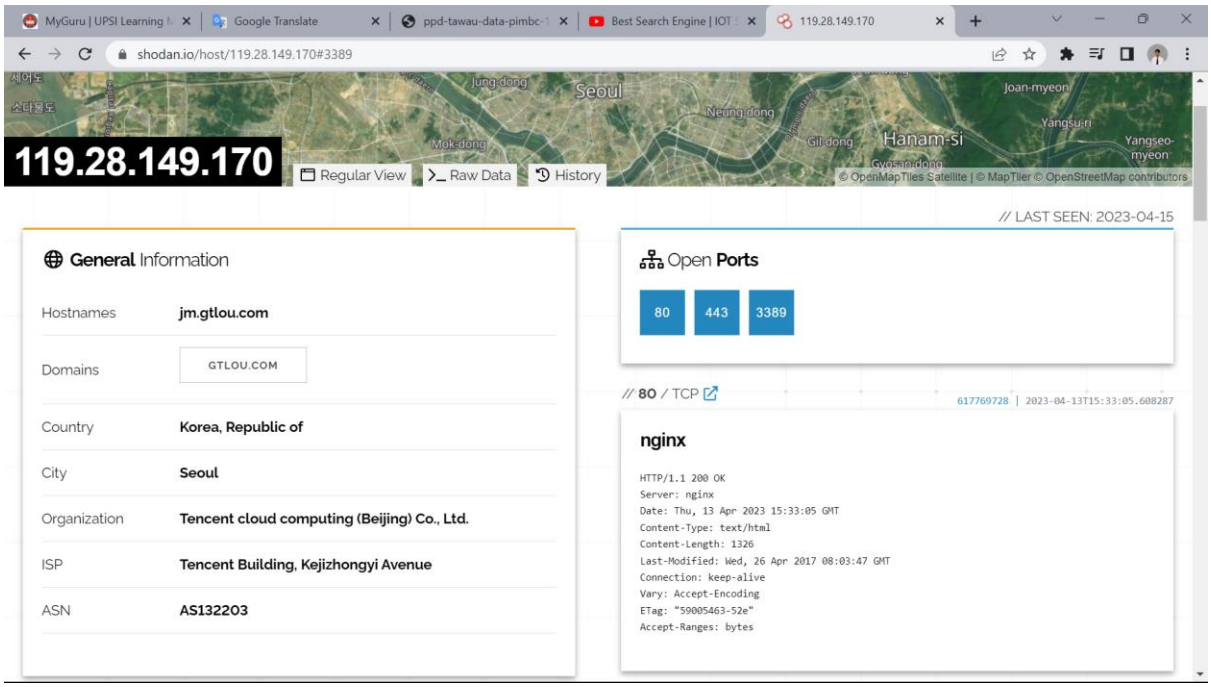
# ACTIVITY 3

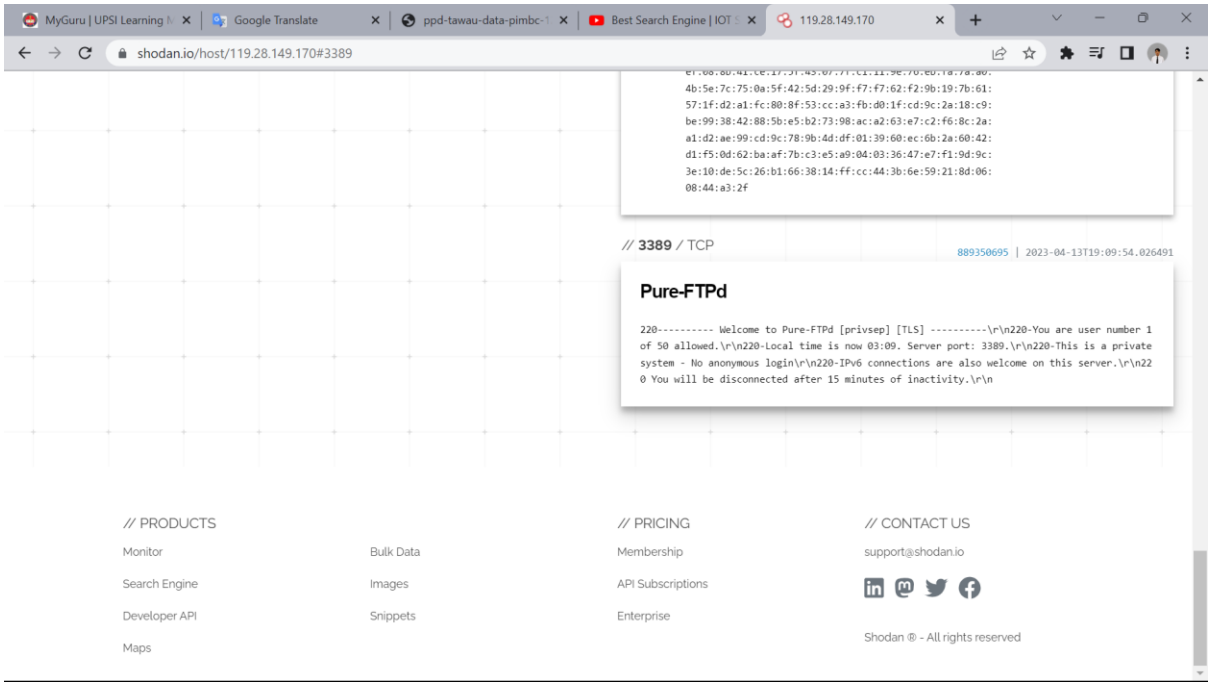

searchftps.net
Log In Register Submit
NAPALM FTP indexer
upsi
With all the words
Search
Showing results 0 to 19 of about 10000 for "upsi"
Order Date Desc Date Asc Size Desc Size Asc None
Related keywords
soupsieve pool main noarch ubuntu orig tar rpm linux
post1 pub opensuse repo oss python3 all deb debian
history tumbleweed dfsg Fedora ppc64le dsk0 releases Everything
source tree Packages python
/dsk0/Fedora/fedora/linux/releases/37/Everything/source/tree/Packages/p/python-soupsieve-2.3.2.post1-7.fc37.src.rpm 131.2 KB DOWNLOAD
Last chequed: 2023-04-03 20:58 Similar files: [Browse]
/pub/linux/opensuse/history/20230401/tumbleweed/repo/oss/noarch/python39-soupsieve-2.3.2.post1-1.2.noarch.rpm 79.9 KB DOWNLOAD
Last chequed: 2023-04-03 20:55 Similar files: [Browse]
/pub/linux/opensuse/history/20230401/tumbleweed/repo/oss/noarch/python38-soupsieve-2.3.2.post1-1.2.noarch.rpm 80.0 KB DOWNLOAD
Last chequed: 2023-04-03 20:55 Similar files: [Browse]
/pub/linux/opensuse/history/20230401/tumbleweed/repo/oss/noarch/python311-soupsieve-2.3.2.post1-1.2.noarch.rpm 105.9 KB DOWNLOAD
Last chequed: 2023-04-03 20:55 Similar files: [Browse]
/pub/linux/opensuse/history/20230401/tumbleweed/repo/oss/noarch/python310-soupsieve-2.3.2.post1-1.2.noarch.rpm 80.6 KB DOWNLOAD
Last chequed: 2023-04-03 20:55 Similar files: [Browse]
/mirror/opensuse/distribution/leap/15.3/repo/oss/ppc64le/


searchftps.net
Log In Register Submit
NAPALM FTP indexer
upsi
With all the words
Search
Ubuntu pool main soupsieve
Directory /ubuntu/pool/main/s/soupsieve/
Last checked 2023-04-03 21:02
Files 8
File(s)
soupsieve_2.4.orig.tar.gz 101.3 KB DOWNLOAD
soupsieve_2.3.2.orig.tar.gz 102.4 KB DOWNLOAD
soupsieve_2.3.1.orig.tar.gz 107.5 KB DOWNLOAD
soupsieve_1.9.5+dfsg.orig.tar.xz 76.9 KB DOWNLOAD
python3-soupsieve_2.4-1_all.deb 33.4 KB DOWNLOAD
python3-soupsieve_2.3.2-1_all.deb 33.7 KB DOWNLOAD
python3-soupsieve_2.3.1-1_all.deb 33.0 KB DOWNLOAD
python3-soupsieve_1.9.5+dfsg-1_all.deb 29.1 KB DOWNLOAD

# ACTIVITY 4


MyGuru | UPSI Learning
Google Translate
ppd-tawau-data-pimbc-1
Best Search Engine | IOT
port number 3389 - Shod
shodan.io/search?query=port+number+3389
Tencent Cloud Computing (Be... 5
Tencent cloud computing (Bei... 2
Alhambra-Grantfork Telephon... 1
Asia Pacific Network Informati... 1
Huawei Public Cloud Service (... 1
More...
Hong Kong, Hong Kong
43.143.164.225
Tencent Cloud Computing (Beijing) Co., Ltd
China, Beijing
cloud
2023-04-14T06:40:06.284354
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n220-You are user number 1 of 50 allowed.\r\n220-Local
107.182.87.30
Alhambra-Grantfork Telephone Company
United States, Highland
2023-04-13T23:27:41.525623
220---------- Welcome to Pure-FTPd [privsep] ----------\r\n220-You are user number 1 of 50 allowed.\r\n220-Local time
119.28.149.170
Tencent cloud computing (Beijing) Co., Ltd.
Korea, Republic of, Seoul
2023-04-13T19:09:54.026491
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n220-You are user number 1 of 50 allowed.\r\n220-Local
159.75.242.23
Tencent Cloud Computing (Beijing) Co., Ltd
China, Chongqing
cloud
2023-04-11T12:49:44.965250
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n220-You are user number 1 of 50 allowed.\r\n220-Local
1.13.246.42
2023-04-11T06:41:49.667411

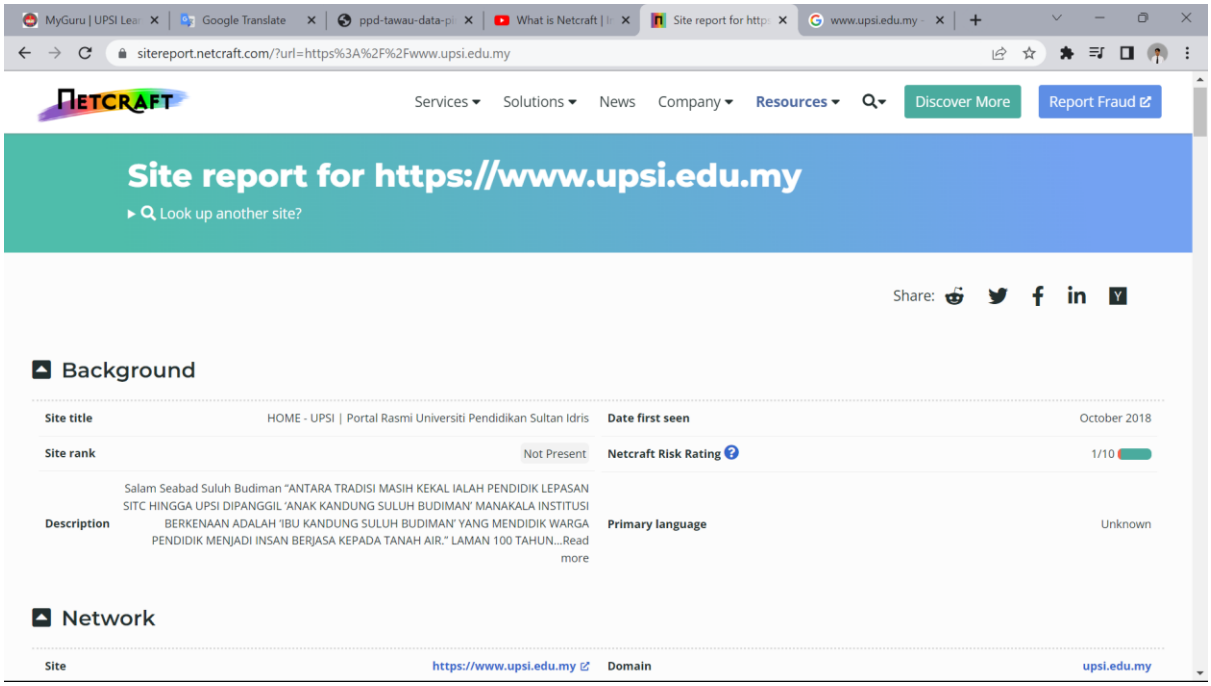

MyGuru | UPSI Learning
Google Translate
ppd-tawau-data-pimbc-1
Best Search Engine | IOT
119.28.149.170
shodan.io/host/119.28.149.170#3389
119.28.149.170
Regular View
Raw Data
History
Jung-dong
Seoul
Neung-dong
Mok-dong
Gil-dong
Hanam-si
Gyosan-dong
Joan-myeon
Yangsu-ri
Yangseo-myeon
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// LAST SEEN: 2023-04-15
General Information
Hostnames jm.gtlou.com
Domains GTLOU.COM
Country Korea, Republic of
City Seoul
Organization Tencent cloud computing (Beijing) Co., Ltd.
ISP Tencent Building, Kejizhongyi Avenue
ASN AS132203
Open Ports
80
443
3389
// 80 / TCP
617769728 | 2023-04-13T15:33:05.608287
nginx
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 13 Apr 2023 15:33:05 GMT
Content-Type: text/html
Content-Length: 1326
Last-Modified: Wed, 26 Apr 2017 08:03:47 GMT
Connection: keep-alive
Vary: Accept-Encoding
ETag: "59005463-52e"
Accept-Ranges: bytes

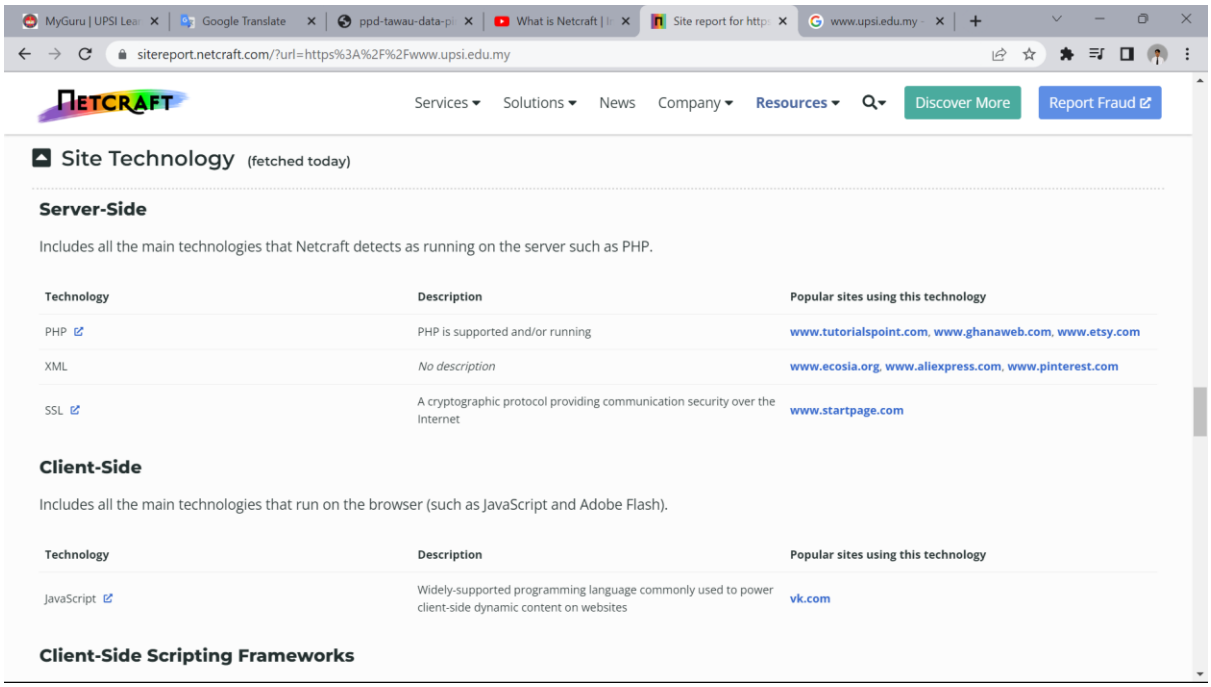

MyGuru | UPSI Learning
Google Translate
ppd-tawau-data-pimbc-1
Best Search Engine | IOT
119.28.149.170
shodan.io/host/119.28.149.170#3389
4b:5e:7c:75:0a:5f:42:5d:29:9f:f7:f7:62:f2:9b:19:7b:61:
57:1f:d2:a1:fc:80:8f:53:cc:a3:fb:d0:1f:cd:9c:2a:18:c9:
be:99:38:42:88:5b:e5:b2:73:98:ac:a2:63:e7:c2:f6:8c:2a:
a1:d2:ae:99:cd:9c:78:9b:4d:df:01:39:60:ec:6b:2a:60:42:
d1:f5:0d:62:ba:af:7b:c3:e5:a9:04:03:36:47:e7:f1:9d:9c:
3e:10:de:5c:26:b1:66:38:14:ff:cc:44:3b:6e:59:21:8d:06:
08:44:a3:2f
// 3389 / TCP
889350695 | 2023-04-13T19:09:54.026491
Pure-FTPd
220--------- Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n220-You are user number 1 of 50 allowed.\r\n220-Local time is now 03:09. Server port: 3389.\r\n220-This is a private system - No anonymous login\r\n220-IPv6 connections are also welcome on this server.\r\n220 You will be disconnected after 15 minutes of inactivity.\r\n
// PRODUCTS
Monitor
Search Engine
Developer API
Maps
Bulk Data
Images
Snippets
// PRICING
Membership
API Subscriptions
Enterprise
// CONTACT US
support@shodan.io
Shodan ® - All rights reserved

# ACTIVITY 5

Technology list (http://www.upsi.edu.my)

1. Server-side
    - PHP, XML, SSL
2. Client-side
    - JavaScript
3. Client-side Scripting Framework
    - jQuery
4. Blog
    - WordPress Self-Hosted
5. PHP Application
    - WordPress
6. RSS Feed
    - RSS
7. Character Encoding
    - UTF8
8. Web Browsing Targeting
    - Strict Transport Security
    - X-Content-Type-Options
    - X-XSS-Protection Disabled
    - X-Frame-Option Same Origin
9. Doctype
    - HTML5
    - HTML
10. CSS Usage
    - External
    - CSS Media Query
    - Embedded

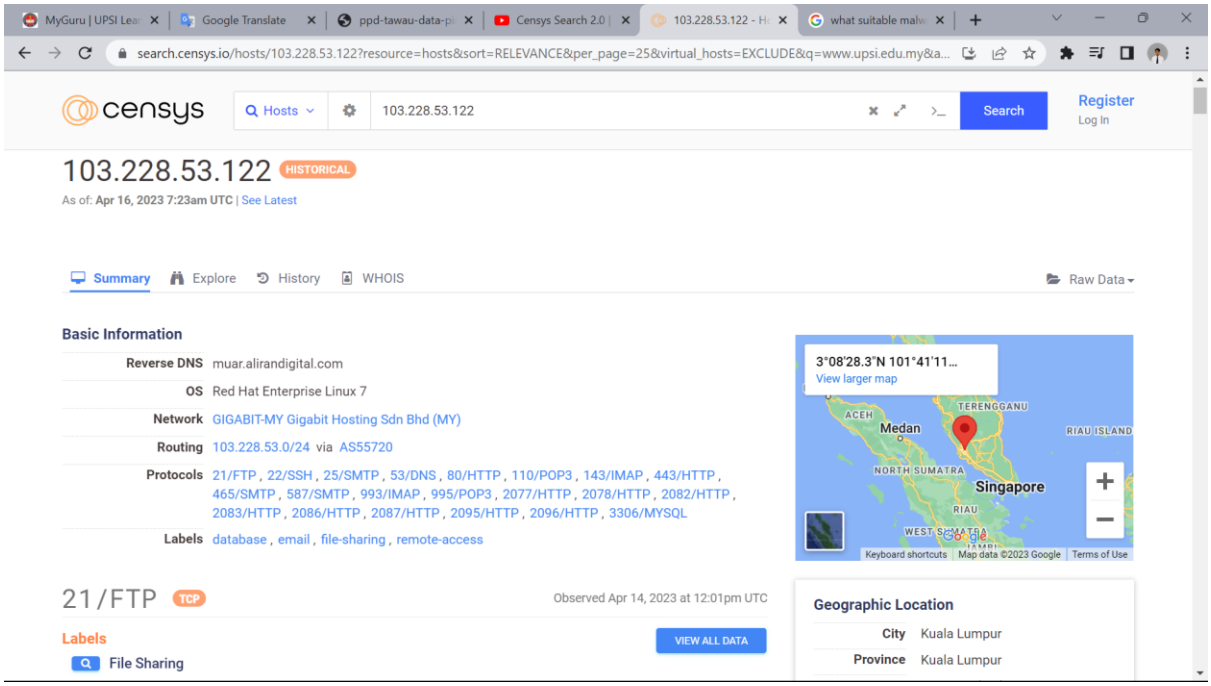

sitereport.netcraft.com/?url=https%3A%2F%2Fwww.upsi.edu.my
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Site report for https://www.upsi.edu.my
Look up another site?
Share:
Background
Site title
HOME - UPSI | Portal Rasmi Universiti Pendidikan Sultan Idris
Date first seen
October 2018
Site rank
Not Present
Netcraft Risk Rating
1/10
Description
Salam Seabad Suluh Budiman "ANTARA TRADISI MASIH KEKAL IALAH PENDIDIK LEPASAN SITC HINGGA UPSI DIPANGGIL 'ANAK KANDUNG SULUH BUDIMAN' MANAKALA INSTITUSI BERKENAAN ADALAH 'IBU KANDUNG SULUH BUDIMAN' YANG MENDIDIK WARGA PENDIDIK MENJADI INSAN BERJASA KEPADA TANAH AIR." LAMAN 100 TAHUN...Read more
Primary language
Unknown
Network
Site
https://www.upsi.edu.my
Domain
upsi.edu.my

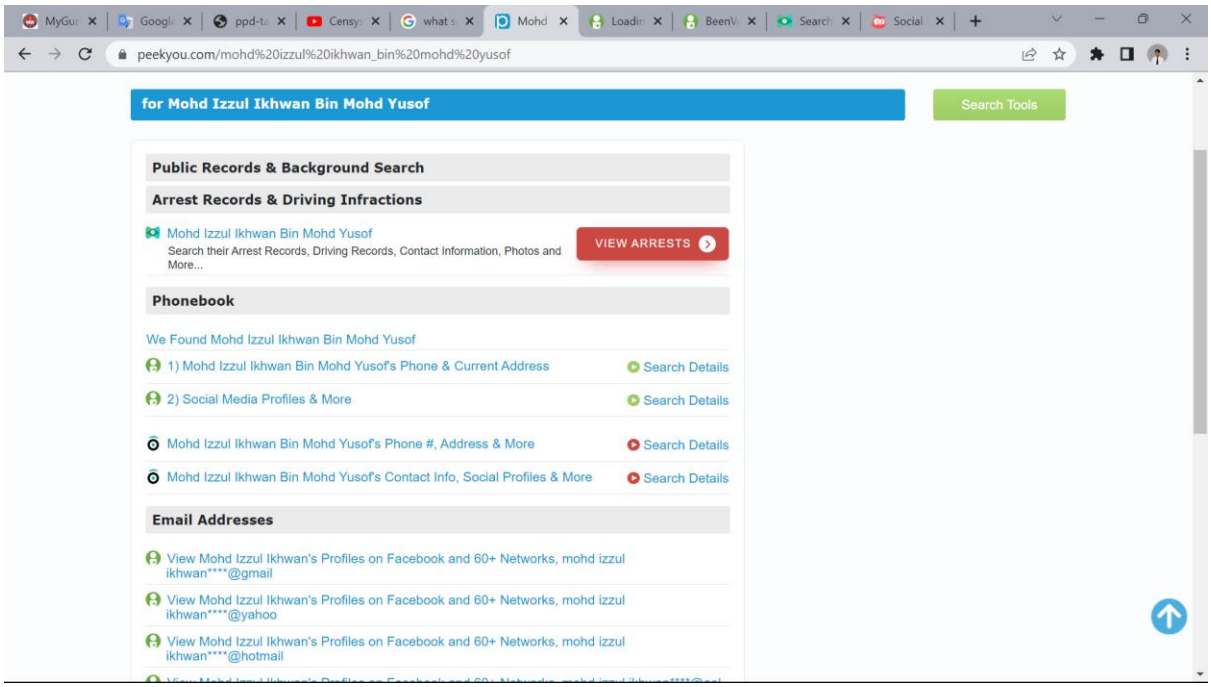

sitereport.netcraft.com/?url=https%3A%2F%2Fwww.upsi.edu.my
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Site Technology (fetched today)
Server-Side
Includes all the main technologies that Netcraft detects as running on the server such as PHP.
Technology
Description
Popular sites using this technology
PHP
PHP is supported and/or running
www.tutorialspoint.com, www.ghanaweb.com, www.etsy.com
XML
No description
www.ecosia.org, www.aliexpress.com, www.pinterest.com
SSL
A cryptographic protocol providing communication security over the Internet
www.startpage.com
Client-Side
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).
Technology
Description
Popular sites using this technology
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
vk.com
Client-Side Scripting Frameworks

## ACTIVITY 6

Operating System (OS): Red Hat Enterprise Linux 7

Suitable malware to exploitable: Ransomware, Trojans and Worms




## ACTIVITY 7