

Université Cheikh Anta Diop (UCAD)



Ecole Supérieure Polytechnique
Département Génie Informatique
Année Universitaire 2023-2024

Veille Technologique

Prenom et nom:

Assane Gueye (GLSIB)

Professeur :

Mr Doudou Fall

ATELIER 2: Reconnaissance

Partie 1: Systèmes autonomes, Autonomous Systems (AS)

Le numéro du système autonome de l'UCAD est : **37649**

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.19045.4170]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>nslookup www.ucad.sn
Serveur : liveboxfibre.home
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : www.ucad.sn
Address: 154.65.39.1

C:\Windows\system32>
```

Le sous-réseau, au format CIDR, lié au numéro du système autonome de l'UCAD est:

En tant que nombre	Comme nom	Gamme CIDR	Moniteur
37649	Inconnu	154.65.39.0/24	
37649	Inconnu	154.65.38.0/23	
37649	Inconnu	154.65.36.0/22	
37649	Inconnu	154.65.32.0/21	

La notation CIDR **154.65.39.0/24** indique que les 24 premiers bits de l'adresse IP (154.65.39) restent constants, tandis que les 8 derniers bits peuvent varier pour représenter différents ordinateurs dans le sous-réseau. La première adresse utilisable est 154.65.39.0 et la dernière est 154.65.39.255, permettant ainsi un total de 256 adresses possibles dans cette plage.

Partie 2 : Shodan

Après création de compte nous avons recherché les hôtes avec le nom de domaine **ucad.sn**. Le nombre trouvé est de **103**

SHODAN

hostname:ucad.sn

TOTAL RESULTS

103

TOP COUNTRIES

Senegal97

United S...5

Finland1

TOP PORTS

443

88

View Report

View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Accueil | FAD-FASTEF

2024-04-22T12:42:32.236075

196.1.97.250

fad-fastef.ucad.sn

ENSUT-LPA

Senegal, Dakar

SSL Certificate

Issued By: Common Name: R3 Organization: Let's Encrypt Issued To: Common

HTTP/1.1 200 OK

Date: Mon, 22 Apr 2024 09:43:12 GMT

Server: Apache/2.4.56 (Debian)

Set-Cookie: MoodleSession=hmcv01mjpnhfivdjsl

Expires: Mon, 20 Aug 1969 09:23:00 GMT

Cache-Control: no-store, no-cache, must-reval

Pragma: no-cache

Content-Language...

Par Contre le nombre d'hôte dans le sous réseau CIDR de l'UCAD est: **31**

SHODAN

net:154.65.39.0/24

TOTAL RESULTS

31

TOP PORTS

4439

807

33337

80803

532

More...

TOP PRODUCTS

Apache...14

OpenSSH7

nginx2

View Report

View on Map

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

154.65.39.8

SAGA AFRICA HOLDINGS LIMITED

Senegal, Dakar

HTTP/1.1 200 OK

Expires: 0

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

X-XSS-Protection: 1; mode=block

Pragma: no-cache

Referrer-Policy: strict-origin-when-cross-origin

Accept-Ranges: bytes

Content-Security-Policy: default-src 'self'; frame-src 's'

2024-04-22T12:02:51.278136

État HTTP 404 – Non trouvé

154.65.39.3

SAGA AFRICA HOLDINGS LIMITED

Senegal, Dakar

HTTP/1.1 404

Content-Type: text/html; charset=utf-8

Content-Language: fr

Content-Length: 433

Date: Mon, 22 Apr 2024 05:34:06 GMT

2024-04-22T05:34:06.725832

Parmis les hôtes trouves précédemment **14** utilisent **APACHE** ; **2** utilisent **NGINX** pour **microsoft IIS** c'est **0**.

SHODAN

net:154.65.39.0/24 product:"apache"

TOTAL RESULTS

14

TOP PORTS

4438

806

TOP VERSIONS

2.4.382

2.4.532

2.4.562

View Report

View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

Intouch

154.65.39.5

ucad.sn

SAGA AFRICA HOLDINGS LIMITED

Senegal, Dakar

SSL Certificate

Issued

By: Intouch

Common Name: Senegal, Dakar

Sectigo RSA Domain Validation Secure Server CA

HTTP/1.1 200 OK

Date: Sun, 21 Apr 2024 05:36:19 GMT

Server: Apache/2.4.56 (Debian)

Cache-control: no-cache, private

Set-Cookie: XSRF-TOKEN=eyJ3pd1I6IlpLRWntdGJyV3

2024-04-21T08:36:25.134056

Parmi les hôtes identifiés précédemment, quelles sont les versions des serveurs Microsoft IIS httpd et/ou Apache :

Les **versions d'Apache** sont 2.4.38, 2.4.53 et 2.4.56.

Parmi les hôtes identifiés précédemment, plusieurs possèdent des certificats SSL (pour HTTPS).

Quels sont les noms communs (c'est-à-dire les noms de domaine) pour lesquels ces certificats sont émis :

- Il y en a **9** au total, et ils ont tous un nom commun qui est **.ucad.sn**.

SHODAN net:154.65.39.0/24 ssl:true

TOTAL RESULTS
9

TOP PRODUCTS
Apache ... 8
nginx 1

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

Intouch 2024-04-21T08:35:25.134058

154.65.39.5
ucad.sn
SAGA AFRICA HOLDINGS LIMITED
Senegal, Dakar

SSL Certificate

HTTP/1.1 200 OK
Date: Sun, 21 Apr 2024 05:36:19 GMT
Server: Apache/2.4.56 (Debian)
Cache-Control: no-cache, private
Set-Cookie: XSRF-TOKEN=eyJpdii6IlpLRfNtdGJyV3:

Issued By: Common Name: Sectigo RSA Domain Validation Secure Server CA
Organization: Sectigo Limited

Pour la question précédente sur les certificats SSL, quelle était la requête de recherche Shodan que vous avez saisie?

La commande saisie est **net:154.65.39.0/24 ssl:true**

Partie 3: Whois

Le système WHOIS permet d'accéder aux informations du répertoire stockées par les bureaux d'enregistrement des noms de domaine.

L'adresse électronique associée au contact technique pour le nom de domaine ucad.sn : **disi@ucad.edu.sn**

```
[TECH_C]
ID Contact:          FB147
Type:                Personne Physique
Nom:                 Samba DIAW
Adresse:             Avenue Cheikh Anta DIOP
Code postal:         5005
Ville:               Dakar
Pays:                SN
Téléphone:           +22.1338235719
Courriel:            disi@ucad.edu.sn
Dernière modification: 2022-06-08T08:52:18Z
```

Les serveurs de noms faisant autorité pour le nom de domaine ucad.sn:

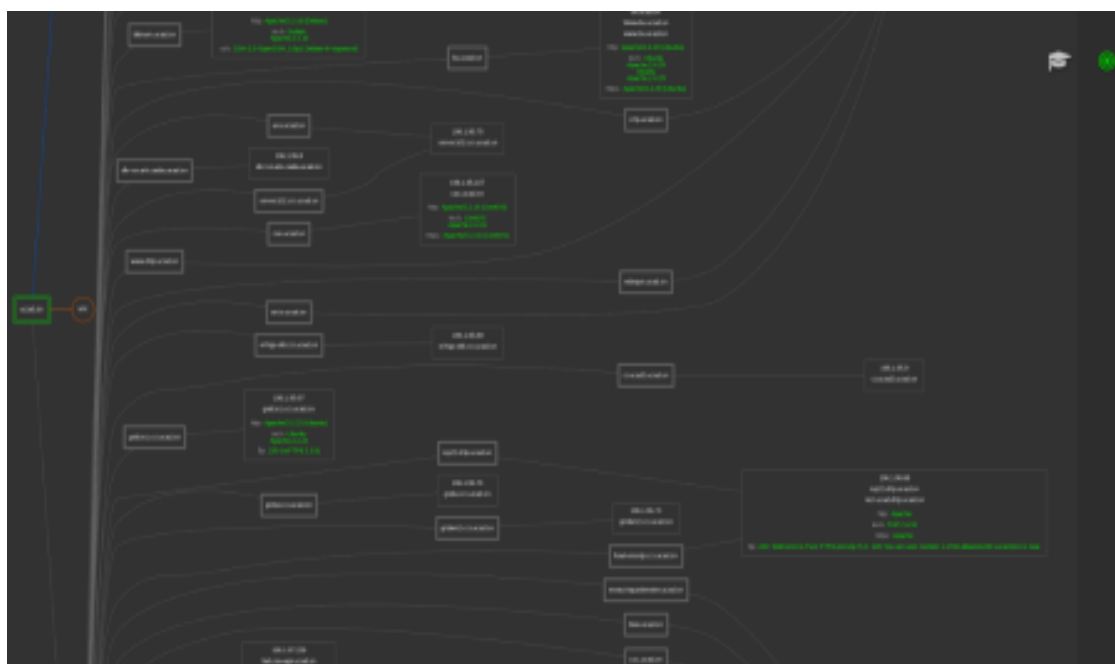
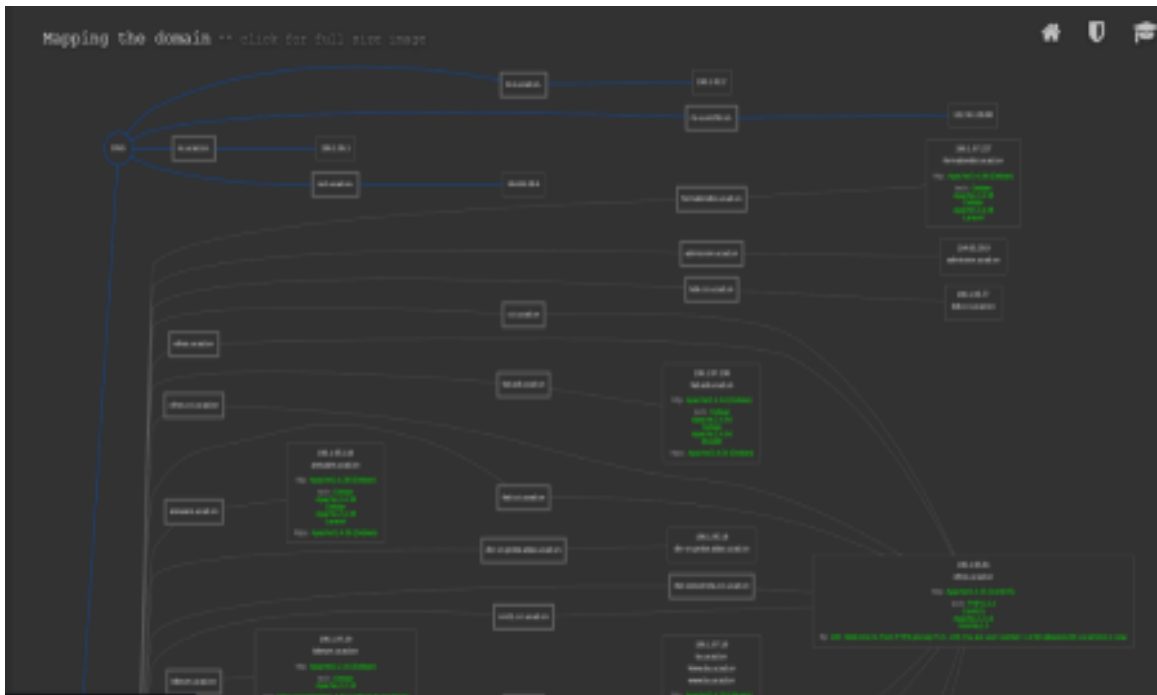
```
Serveur de noms: ns.ucad.sn
Serveur de noms: ns1.ucad.sn
Serveur de noms: ns2.ucad.sn
```

Partie 4: DNS

Fournissons une liste de 5 sous-domaines de ucad.sn qui sont particulièrement « intéressants » et dont vous ne connaissiez pas l'existence avant de lancer le scan.

```
ifan.ucad.sn
ifantest.ucad.sn
ifee.ucad.sn
imap.ucad.sn
inseps.ucad.sn
intranet.ucad.sn
```

Fournissons l'image « Domain Map » de DNS Dumpster qui résume les résultats de la recherche pour "ucad.sn".






Fournir deux noms de domaines et leurs adresses IP

```
└─$ fierce --domain www.ucad.sn
NS: ns1.ucad.sn. ns-a.unchk.sn. ns.ucad.sn. ns2.ucad.sn.
SOA: ns1.ucad.sn. (196.1.92.2)
```

Partie 5: Certificats SSL

Pour le nom d'hôte `www.ucad.sn`, quels sont les « noms alternatifs » ou « noms DNS » figurant dans le certificat SSL ? Il s'agit d'une liste d'autres noms d'hôtes qui sont également signés/sécurisés par le même certificat. Vous pouvez le vérifier dans votre navigateur web ou à l'aide de l'un des outils de recherche en ligne répertoriés.

Certificate #1: RSA 2048 bits (SHA256withRSA)	
 Server Key and Certificate #1	
Subject	*.ucad.sn Fingerprint SHA256: d3M8a7e4e14cd1a7e67b6d94dbeca3865f1ad8e76b756688fac2625d63d8c Pin SHA256: PQyP+oC5eYc38KaceP5uJTRR8o3kZntF8AvevdgY=
Common names	*.ucad.sn
Alternative names	*.ucad.sn ucad.sn
Serial Number	25ae8f9656f8e0513c779808334c00b6
Valid from	Wed, 07 Jun 2023 00:00:00 UTC
Valid until	Sun, 07 Jul 2024 23:59:59 UTC (expires in 2 months and 15 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Secigo RSA Domain Validation Secure Server CA Alt: http://ot.secigo.com/SecigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation Information	OCSP OCSP: http://ocsp.secigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Configuration	
 Protocols	
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No
 Cipher Suites	
# TLS 1.3 (server has no preference)	
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS 128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS 256
# TLS 1.2 (server has no preference)	
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS WEAK