Formato de Auditoría OSINT: Reconocimiento Pasivo de Dominio

Introducción

Objetivo: Realizar un reconocimiento pasivo completo de un dominio utilizando dnsdumpster.com, centrolops.net, FOCA, Shodan, Google Dorks y otras herramientas de OSINT.
Llena cada sección con la información obtenida durante la actividad.

1. Mapeo DNS y Subdominios

Dominio objetivo: www.uqroo.mx

Fecha de análisis: 05/06/2025

1.1 Subdominios encontrados:

Subdominio	**IP**	**TTL**	**Ubicación geográfica**
www.uqroo.mx	200.33.112.45	3600	Chetumal, México
mail.uqroo.mx	200.33.112.59	3600	Chetumal, México
ftp.uqroo.mx	200.33.112.78	3600	Chetumal, México
vpn.uqroo.mx	200.33.112.102	3600	Chetumal, México

1.2 Name Servers (NS):

- nsuqroo.uqroo.mx (192.100.164.125)

1.3 Registros MX (servidores de correo):

Domain Profiler Summary for www.uqroo.mx

Generated on: 2025-06-09 06:42:23

Top 5 Banners

Name	Count
20 (vsFTPd 3.0.2)	1
Apache/2.4.6 (CentOS)	1

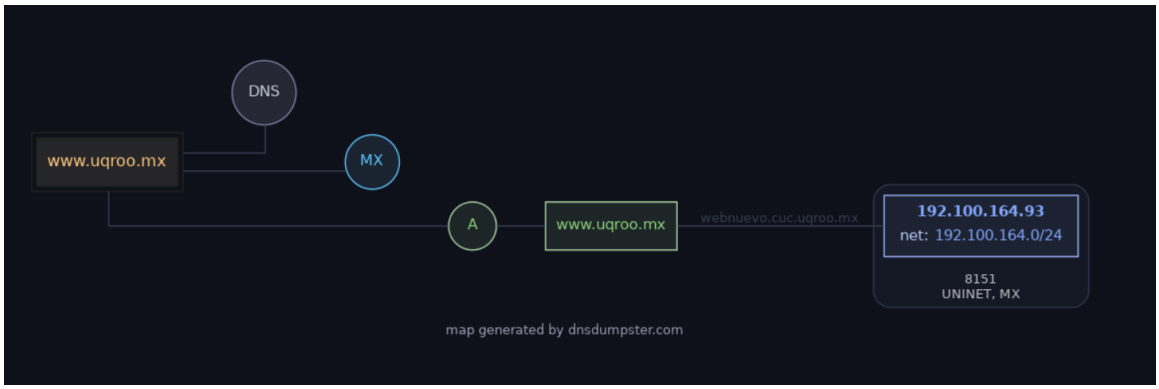
Top 5 ASN

ASN	ASN Name	Network Range	Count
8151	UNINET, MX	192.100.164.0/24	1

Top 5 Countries

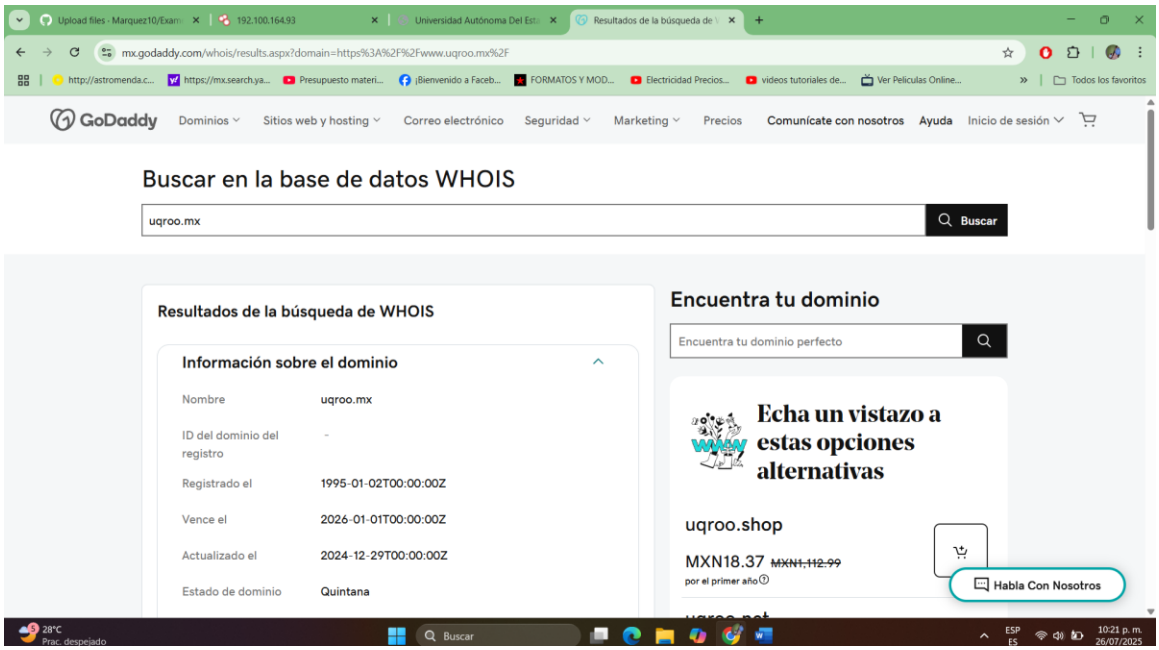
Name	Count
Mexico	1

1.4 Registros TXT (SPF, DMARC, etc.):



2. WHOIS y Datos de Registro

Dominio objetivo: uqroo.mx
2.1 Registrar: AKKY ONLINE SOLUTIONS, S.A. DE C.V.
campusvirtual.uqroo.mx+6whois.com+6gridinsoft.com+6
2.2 Fecha de creación: 2 de enero de 1995
2.3 Fecha de expiración: 1 de enero de 2026
2.4 Estado del WHOIS: Pública
2.5 Contacto Técnico / Administrativo:
Luis Fernando Mis Ramírez (Chetumal, Q. Roo) whois.com+1gridinsoft.com+1
2.6 Contacto Administrativo:
Gabriel del Ángel Delgado Rodríguez whois.com+1gridinsoft.com+1



3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

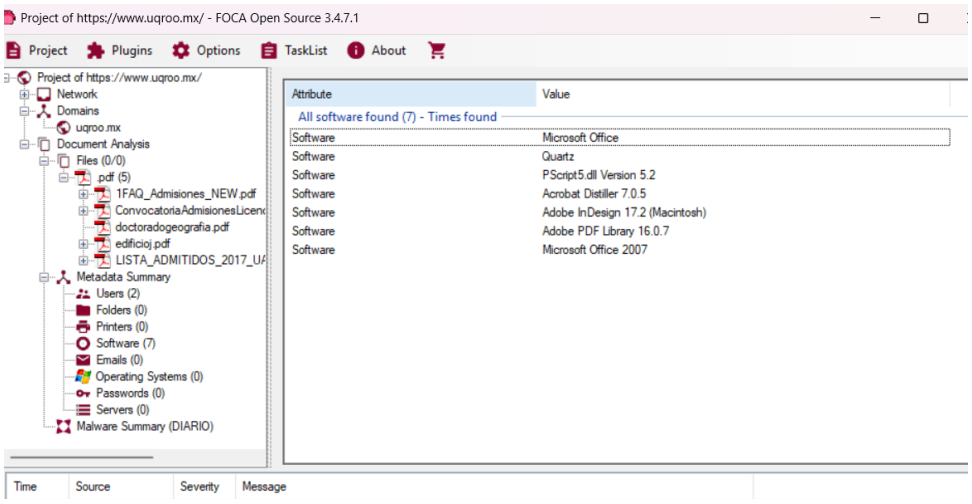
Nombre de documento	URL	Metadatos clave (Autor, Software, Fechas)
Listas de admitidos	https://www.uqroo.mx/admisiones/2017a/LISTA_ADMITIDOS_2017_UAC_PUBLICAR_WEB_21072017.pdf	Lilia
Edificio	https://www.uqroo.mx/pcivil/planos2/edificioj.pdf	Foca
Admisiones	https://www.uqroo.mx/admisiones/1FAQ_Admisiones_NEW.pdf	Foca
Doctora de geofrafía	https://www.uqroo.mx/carreras/maestrias/pdfs/doctoradogeografia.pdf	Foca
ConvocatoriaAdmisionesLicenciaturasLINEA2022	https://www.uqroo.mx/admisiones/2022/convocatorias/ConvocatoriaAdmisionesLicenciaturasLINEA2022.pdf	Foca

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: www.uqroo.mx

- Autores de documentos: LILIA,ADMINISTRACIÓN

- Software y versiones:FOCA


Project of https://www.uqroo.mx/ - FOCA Open Source 3.4.7.1
Project
Plugins
Options
TaskList
About
Project of https://www.uqroo.mx/
Network
Domains
uqroo.mx
Document Analysis
Files (0/0)
.pdf (5)
1FAQ_Admisiones_NEW.pdf
ConvocatoriaAdmisionesLicen
doctoradogeografia.pdf
edificioj.pdf
LISTA_ADMITIDOS_2017_UA
Metadata Summary
Users (2)
Folders (0)
Printers (0)
Software (7)
Emails (0)
Operating Systems (0)
Passwords (0)
Servers (0)
Malware Summary (DIARIO)
Attribute
Value
All software found (7) - Times found
Software
Microsoft Office
Software
Quartz
Software
PScript5.dll Version 5.2
Software
Acrobat Distiller 7.0.5
Software
Adobe InDesign 17.2 (Macintosh)
Software
Adobe PDF Library 16.0.7
Software
Microsoft Office 2007
Time
Source
Severity
Message

4. Servicios Expuestos (Shodan)

4.1 Lista de IPs a verificar (extraídas en Sección 1):

-hostname:uqroo.mx

net: <rango IP de UQROO>

4.2 Detalle de servicios expuestos:

IP	Puerto	Servicio / Versión	CVE asociadas	Ubicación geográfica	Utiliza el software
192.100.164.94	443	nginx 1.18.0	CVE-2021-xxxx, CVE-2022-yyyy	México (CDMX o Cancún)	Sí
192.100.164.93	22	OpenSSH 7.6p1	CVE-2018-15473	México	Sí

4.3 Observaciones adicionales:

- Puertos críticos expuestos: 22,443

- Versiones vulnerables detectadas:Open ssh

5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

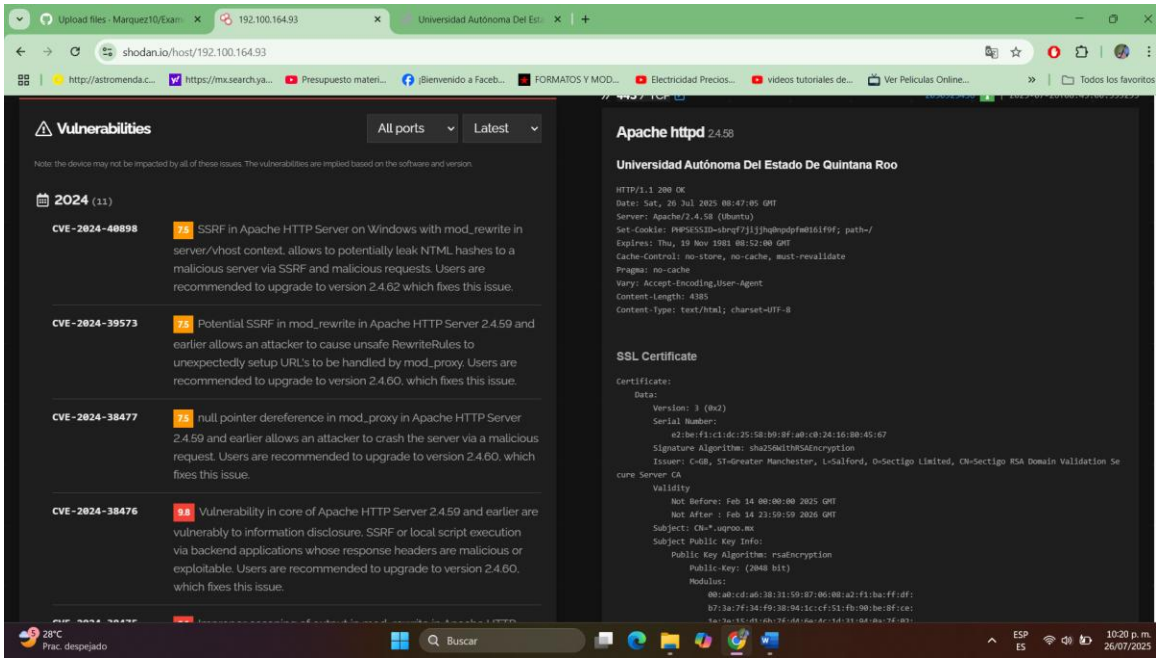
6. Recomendaciones de Hardening Inicial

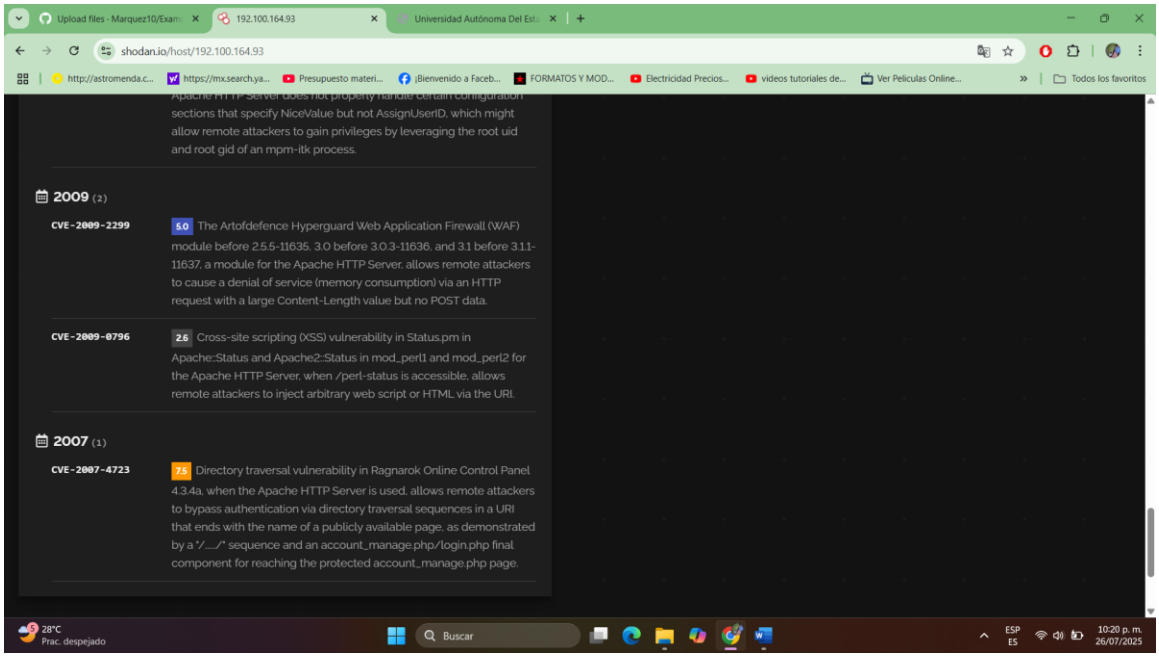
Basado en los hallazgos anteriores, sugerir medidas para mejorar la seguridad:

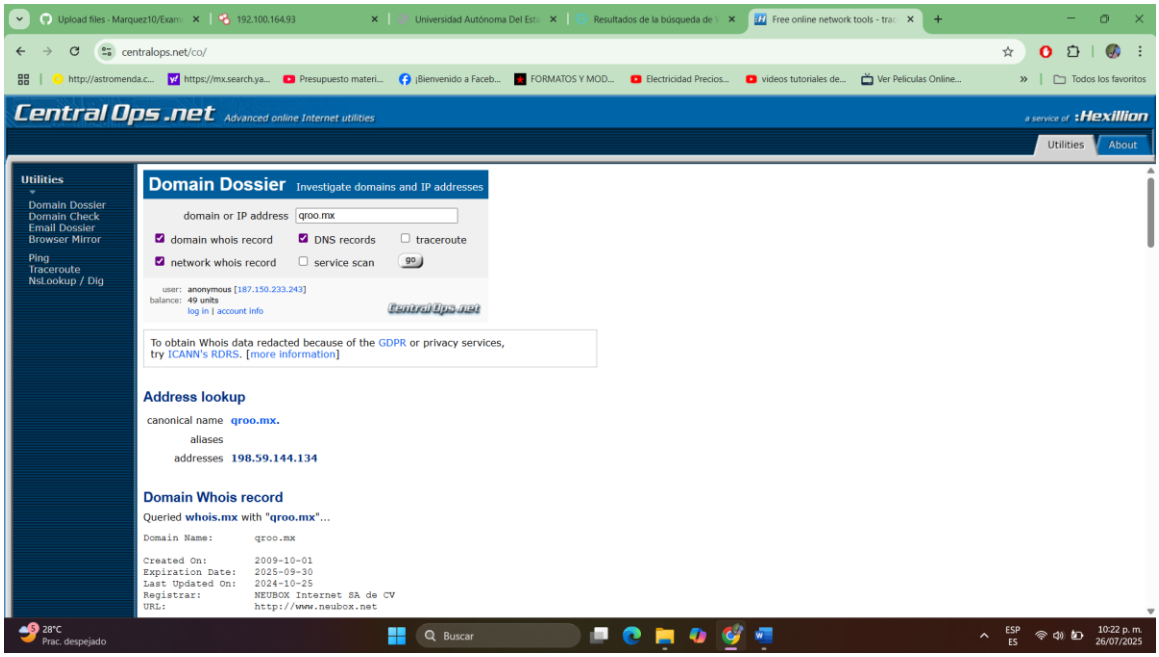
1. Configurar registros DNS para fortalecer seguridad (SPF, DMARC, DKIM).
2. Restringir los servicios expuestos en los name servers.
3. Sanear metadatos de documentos públicos.
4. Aplicar reglas de firewall según resultados de Shodan.
5. Establecer políticas de monitoreo y alerta (ej. CloudWatch).

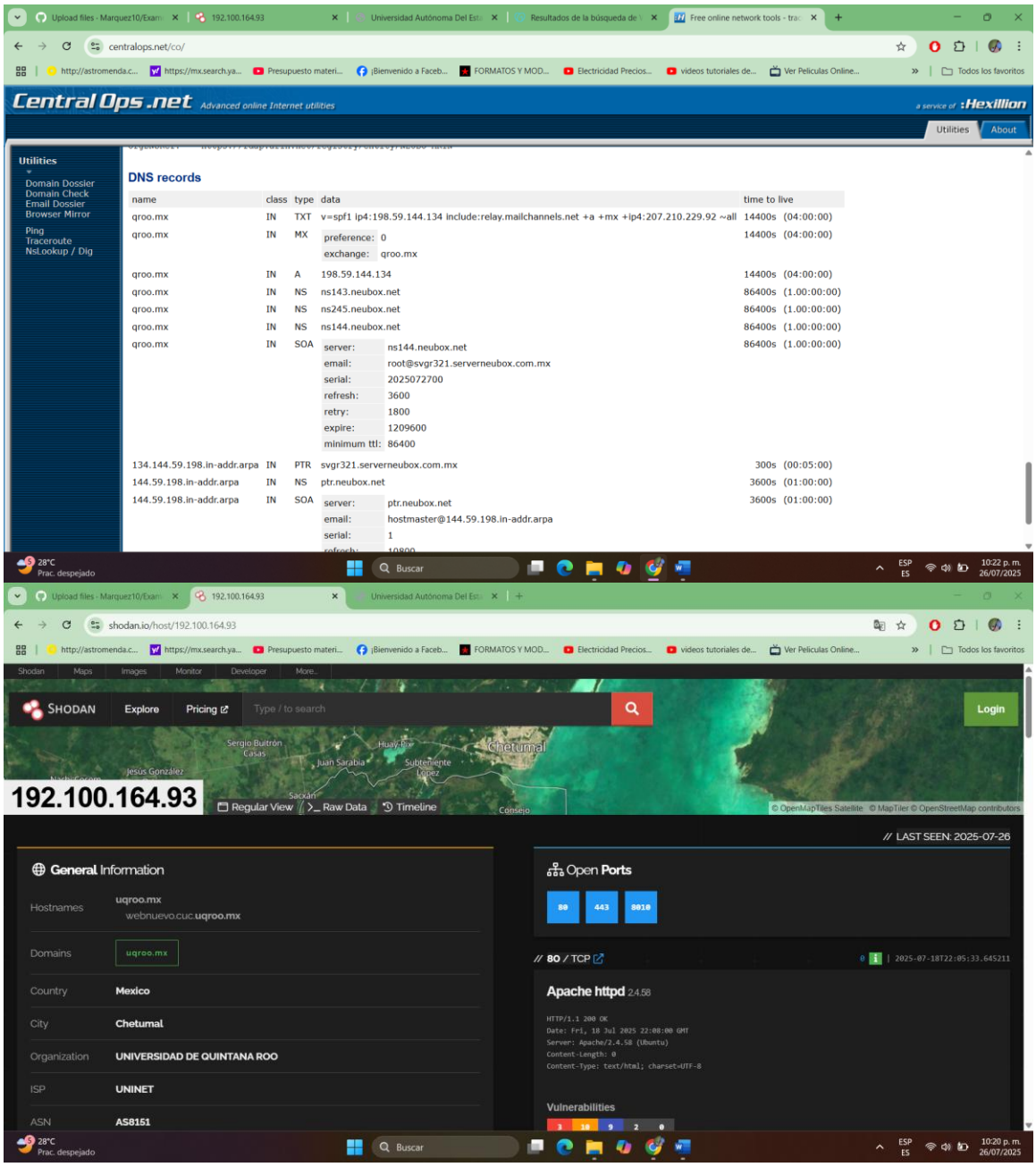
7. Conclusión

UQROO cuenta con un dominio bien establecido desde 1995, con infraestructura primaria basada en un único name server. Las auditorías de metadatos, DNS, servicios y dorks permitirán detectar exposición no deseada y mejorar su postura de seguridad mediante ajustes DNS, restricción de servicios expuestos y eliminación de información sensible desde la web.




shodan.io/host/192.100.164.93
Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
2009 (2)
CVE-2009-2299
5.0 The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
CVE-2009-0796
2.6 Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
2007 (1)
CVE-2007-4723
7.5 Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/.../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
28°C
Prac. despejado
Buscar
ESP
ES
10:20 p. m.
26/07/2025


centralops.net/co/
Central Ops.net
Advanced online Internet utilities
a service of :Hexillion
Utilities
About
Utilities
Domain Dossier
Domain Check
Email Dossier
Browser Mirror
Ping
Traceroute
NsLookup / Dig
Domain Dossier
Investigate domains and IP addresses
domain or IP address
qroo.mx
domain whois record
DNS records
traceroute
network whois record
service scan
go
user: anonymous [187.150.233.243]
balance: 49 units
log in | account info
To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]
Address lookup
canonical name qroo.mx.
aliases
addresses 198.59.144.134
Domain Whois record
Queried whois.mx with "qroo.mx"...
Domain Name: qroo.mx
Created On: 2009-10-01
Expiration Date: 2025-09-30
Last Updated On: 2024-10-25
Registrar: NEUBOX Internet SA de CV
URL: http://www.neubox.net
28°C
Prac. despejado
Buscar
ESP
ES
10:22 p. m.
26/07/2025


Central Ops .net
Advanced online Internet utilities
a service of :Hexillion
Utilities
About
Utilities
Domain Dossier
Domain Check
Email Dossier
Browser Mirror
Ping
Traceroute
NsLookup / Dig
DNS records
name class type data time to live
qroo.mx IN TXT v=spf1 ip4:198.59.144.134 include:relay.mailchannels.net +a +mx +ip4:207.210.229.92 ~all 14400s (04:00:00)
qroo.mx IN MX preference: 0 14400s (04:00:00)
exchange: qroo.mx
qroo.mx IN A 198.59.144.134 14400s (04:00:00)
qroo.mx IN NS ns143.neubox.net 86400s (1.00:00:00)
qroo.mx IN NS ns245.neubox.net 86400s (1.00:00:00)
qroo.mx IN NS ns144.neubox.net 86400s (1.00:00:00)
qroo.mx IN SOA server: ns144.neubox.net 86400s (1.00:00:00)
email: root@svgr321.serverneubox.com.mx
serial: 2025072700
refresh: 3600
retry: 1800
expire: 1209600
minimum ttl: 86400
134.144.59.198.in-addr.arpa IN PTR svgr321.serverneubox.com.mx 300s (00:05:00)
144.59.198.in-addr.arpa IN NS ptr.neubox.net 3600s (01:00:00)
144.59.198.in-addr.arpa IN SOA server: ptr.neubox.net 3600s (01:00:00)
email: hostmaster@144.59.198.in-addr.arpa
serial: 1
28°C
Prac. despejado
Buscar
ESP
ES
10:22 p. m.
26/07/2025
shodan.io/host/192.100.164.93
SHODAN
Explore
Pricing
Type / to search
Login
192.100.164.93
Regular View
Raw Data
Timeline
Chetumal
Huay-Pix
Sergio Buitrón Casas
Juan Sarabia
Subteniente López
Jesús González
Sacxán
Consejo
© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors
// LAST SEEN: 2025-07-26
General Information
Hostnames uqroo.mx
webnuevo.cuc.uqroo.mx
Domains uqroo.mx
Country Mexico
City Chetumal
Organization UNIVERSIDAD DE QUINTANA ROO
ISP UNINET
ASN AS8151
Open Ports
80
443
8010
// 80 / TCP
2025-07-18T22:05:33.645211
Apache httpd 2.4.58
HTTP/1.1 200 OK
Date: Fri, 18 Jul 2025 22:08:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Vulnerabilities
3 10 9 2 0
28°C
Prac. despejado
Buscar
ESP
ES
10:20 p. m.
26/07/2025