

SHODAN DORKS - CHEATSHEET

BUSQUEDAS GENERALES		
Operador	Descripcion	Ejemplo
city:"nombre"	Dispositivos en una ciudad.	city:"New York"
country:"codigo"	Dispositivos en un pais.	country:"US"
geo:"lat,lon"	Ubicacion geografica especifica.	geo:"40.71,-74.00"
hostname:"host"	Dispositivos con hostname especifico.	hostname:"example.com"
net:"rango"	Rango de IPs.	net:"192.168.1.0/24"
os:"sistema"	Sistema operativo.	os:"Windows"
port:numero	Puerto abierto especifico.	port:22
org:"nombre"	Organizacion especifica.	org:"Google"
isp:"nombre"	Proveedor de internet.	isp:"Comcast"
product:"nombre"	Software/producto.	product:"Apache"
version:"ver"	Version de software.	version:"5.7"
has_screenshot:true	Dispositivos con captura de pantalla.	has_screenshot:true

WEB Y SSL		
Operador	Descripcion	Ejemplo
ssl.cert.subject.cn:"cn"	Certificado SSL con nombre comun.	ssl.cert.subject.cn:"example.com"
http.title:"titulo"	Paginas con titulo especifico.	http.title:"Welcome"
http.status_code:codigo	Codigo HTTP especifico.	http.status_code:404
ssl:"keyword"	Configuracion SSL especifica.	ssl:"SHA256"
before:"fecha" / after:"fecha"	Indexado antes/despues de fecha.	before:"2023-01-01"

APLICACIONES Y SERVICIOS		
Operador	Descripcion	Ejemplo
product:"nombre"	Producto especifico.	product:"Apache"
version:"ver"	Version de software.	version:"2.4.41"
"default password"	Credenciales por defecto (riesgo).	"default password"
webcam	Webcams conectadas a internet.	webcam
ftp	Servicios FTP.	ftp
"X-Powered-By: PHP/ver"	Servidores con version PHP.	"X-Powered-By: PHP/5.6"
iis:version	Version de Microsoft IIS.	iis:8.5
"MongoDB Server Information" port:27017	MongoDB expuesto en puerto 27017.	"MongoDB Server Information" port:27017

VULNERABILIDADES		
Operador	Descripcion	Ejemplo
vuln:"CVE-ID"	Dispositivos afectados por CVE.	vuln:"CVE-2021-26855"
ssl.cert.expired:true	Certificados SSL expirados.	ssl.cert.expired:true
"heartbleed" vuln	Vulnerables a Heartbleed.	"heartbleed" vuln
"Authentication: disabled"	Autenticacion deshabilitada.	"Authentication: disabled"
ssl:"TLSv1"	Usando protocolo TLSv1 (inseguro).	ssl:"TLSv1"
http.component:"Drupal" vuln:"CVE-2018-7600"	Drupal vulnerable a Drupalgeddon2.	http.component:"Drupal" vuln:"CVE-2018-7600"

EJEMPLOS COMPLEJOS	
Query	Descripcion
os:"Linux" port:22 country:"JP"	SSH Linux en Japon
product:"Apache" version:"2.4.7"	Apache 2.4.7 especifico
city:"New York" os:"Windows" port:3389	RDP Windows en NY
net:"192.168.1.0/24" webcam	Webcams en red especifica
org:"Google" ssl.cert.expired:true	Google con cert expirado
country:"DE" product:"MySQL" "default password"	MySQL Alemania con pass default