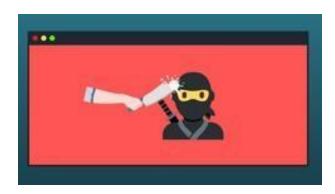
<u>Recon for Ethical Hacking / Penetration</u> <u>Testing & Bug Bounty</u>

Navigating the Art of Reconnaissance in Ethical Hacking, Penetration Testing & Bug Bounty Hunting



* Introduction

In the ever-evolving cybersecurity landscape, one truth remains constant: knowledge is power. Ethical hackers, penetration testers, and bug bounty hunters are driven by an insatiable curiosity to uncover vulnerabilities, safeguard systems, and contribute to a safer digital realm. Welcome to the enlightening Udemy course "Recon for Ethical Hacking / Penetration Testing & Bug Bounty." In this article, we invite you to embark on a journey of discovery through the intricacies of the reconnaissance foundation upon which effective cybersecurity strategies are built.

Introduction to Shodan

Shodan is a powerful tool used for online reconnaissance, like a search engine for internet-connected devices. It scans the web to find and index various devices, such as webcams, routers, servers, and more. Shodan reveals information about these devices, like open ports, vulnerabilities, and even the data they expose. It's often used by security professionals to identify potential weaknesses in a network's security. Shodan can be a valuable asset for assessing the security of your own systems or discovering vulnerabilities in other online devices, making it a key tool in the world of digital reconnaissance and cybersecurity.

Mastering Shodan Filters



Mastering Shodan filters involves refining your search queries to pinpoint specific devices or services. You can filter by criteria like location, port number, or even specific software versions to find vulnerable systems. Learning to use filters effectively allows you to uncover precise information about the devices and services you're interested in while minimizing noise in your search results. This skill is essential for targeted reconnaissance and security assessments.

Country Filter: This filter allows you to narrow down Shodan search results to devices or services located within a specific country, helping you focus on a particular geographic area for reconnaissance.

Filter: country:"Country Code"

Example: To find open webcams in the United States, use country:"US" port:80 webcam.

SHODAN Explore	Downloads	Pricing 2 country:"US" p	Acc				
0TAL RESULTS			owse Images				
			Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.				
OP CITIES Atlanta	7	SmarterGuard Remo 99.158.48.124 99.158.48.124 lightspeed.jc	Ste Viewing 12 2023-10-291705/25 26 662 #TTP/1.0 200 Date: Son, p2 Oct: 2023 00:35:26 6911				
Ashburn	2	snms.sbcglobal.net AT&T Corp.	Last-Modified: Sun, 29 Oct 2023 06:25:26 GMT				
remont	2	United States, Ocean Springs	Server: This is Smarteree's webcam server Accept-Ranges: bytes				
Morris Plains	2	spings	Content-Length: 5354 Content-Type: text/html				
Richardson	2						
More		170.187.149.164	2023-10-20104-55-56-210 HTTP/1.1.289:0K				
OP ORGANIZATIONS		ercontent.com	Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTEK UPNP/1.				
Linode	7	United States, Atlanta					
Asia Pacific Network Informat	ion Cente 3	۵					
Performive LLC	3	cloud honeypol					
WTS	2						
AT&T Corp. More	1	194.195.213.33 2 194-195-213-33.jp. Inodeuse roontent.com	NTTP/L1 2000 OK Server: 100 web server, 791/71644 HTTP Server version 1.0 - TELDAT 5.A., A1066/1.00, ADB Broadband HTTP Server, ADH-Meb, AD, ASUSTEK UP#P/L.				
OP PRODUCTS		United States, Atlanta					

Figure:- The above figure shows how we can get open ports of a particular country.

Port Filter: The port filter helps you find devices or services running on a specific port number, making it useful for identifying open ports and services on target systems.

Filter: port:Port Number

Example: To find MongoDB databases, use port:27017.

nodan Maps Images	s Monitor Develope	r More					
SHODAN Expl	ore Downloads	Pricing 2 port:27017.	٩	Account			
TOTAL RESULTS		甾 View Report 回 V	ew on Map				
121		Access Granted: W	Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.				
TOP COUNTRIES		43.153.58.105 Asia Pacific Network Information Center, Piy, Ltd. ■United States, Santa Citara	HTTP/L1 502 Proof Enner context-type: taxt/plain s-blackti-terror: Proof Enner connect ECOMBERGED 43.153.58.185:30 data: stat, 36 of 2002 22:32:42 OFT connection taxp-allee texp-allee: texpofs transfer-anoschage: chuskad >-2.per-port: 2007	2823-16-28722-32-42.946216			
United States	83						
China Germany Hong Kong Singapore	12 12 9 2	116.202.179.14 C static.14.179.202.116.client s.ycar-server.de Hetzner Chine GmbH Germany, Nümberg	WTTP/1.1 590 OK Bate: Med, 20 Jan 2021 05:55;41 GVT Contect-Type: text/jally, charateut-4 Context-Legar 4.6	2023-10-28720 08 34 055180			
More			Connection: keep-alive port expire 224.172.111.236 116.202.179.14:27017				
TOP PORTS 7071	71						
27017	43	43.154.70.51 🗹	НТТР/1.1 509 ОК	2023-10-28T18-47:20.201711			
8081	3	Information Center, Pty. Ltd. E Hong Kong, Hong Kong	Date: Wed, 20 Jan 2021 05:55:41 GWT Content-Type: text/plain; charset=utf-8				

Figure:- The above figure shows the result of port 27017.

Product Filter: This filter lets you search for devices or services based on the software or product they use, enabling you to discover systems running specific applications or versions.

Filter: product:"Product Name"

Example: To find Apache web servers, use the product:"Apache".

odan Maps Ima	ges Monitor Develo splore Downloads	Pricing & product."Apach	ie"	Q	Account	
TOTAL RESULTS		쏣 View Report @ Br	owse Images 🖽 View or	Map		
17,081,355		Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.				
TOP COUNTRIES		208.82.52.16 🗹	208.82.52.16 亿			
		Luther Seminary Luthed States, Sant Paul	HTTP/1.1 483 Forbidden Date: Sun, 20 Oct 2023 68: Serven: Apache Vary: Accept-Encoding Content-Length: 202 Content-Type: text/html; c <100CTYPE HTM, PUBLIC "-//	harset-110-8850-1		
United States	5,685,717					
Germany	1,611,537	<title>403 Forbidden</title> 				
Japan	1,558,721		<h1>Forbidden</h1>			
France	788,467					
China	764,339	Default Web Site Pa	je 🗹		2023-10-29708:35:14.340750	
More		162.241.76.8 cpanel.vps-126375.universid	SSL Certificate	HTTP/1.1 200 OK		
TOP PORTS		adjuguetron.mx cpcontacts.vps-126375.univ	Issued By: - Common Name:	Date: Sun, 29 Oct 2023 00:30:07 GMT Server: Apache		
80	8,739,776	ersidadjuguetron.mx mail.vps-126375.universidad	cPanel, Inc. Certification Authority	Transfer-Encoding: chunked Content-Type: text/html		
443	6,618,686	juguetron.mx cpcalendars.vps-126375.uni	- Organization			
8080	465,382	versidadjuguetron.mx whm.vps-126375.universida djuguetron.mx	cPanel, Inc. Issued To:			

Figure:- The above figure shows the result of ip address of Apache web sever

SSL Filter: With the SSL filter, you can locate devices or services that use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption, useful for identifying secure communication services.

Filter: ssl:"SSL Version"

Example: To find servers supporting SSLv2, use ssl:"SSLv2".

odan Maps Images	Monitor Devel	Pricing 12 ssl:"SSLv2"		٩	Accour		
TOTAL RESULTS		A View Report MV	inu op Mon				
109			論 View Report 印 View on Map Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.				
TOP COUNTRIES		197.96.219.150 2 transa online solvi II trarisa.oriine deskop trarisa.oriine solvi II trarisa.oriine Dimension Data E South Africa.ohannesburg	SSL Certificate Issued By: - Common Name: Go Daddy Secure Certificate Authority - G2 - Organization: GoDaddy.com, Inc.	HTTP/1.1 404 Hot Found Convection: class David Jone 20 002 2023 0736-23 601 Treasfer Society: classed	2023-10-29107/30/24 668216		
Brazil	104		Issued To: - Common Name:				
South Africa	4		tharisa.online				
France	1		Supported SSL Versions: TLSv1.2				
TOP PORTS							
443	106	404 Not Found 🗹			2023-10-29706.46:11.671832		
8443	2	161.148.173.68 treinasnor.serpro.gov.br	SSL Certificate	HTTP/1.1 484 Not Found			
9095	1	SERVICO FEDERAL DE PROCESSAMENTO DE DADOS - SERPRO	Issued By: - Common Name: Autoridade Certificadora do SERPRO Final SSLv2 -	Date: Sun, 20 Oct 2023 00:45:59 GMT Server: Apache/2.4.51 (codelt) OpenSSL/1.1.11 Content-Langth: 106 Content-Type: text/html; charset-iso-8859-1			
TOP ORGANIZATIONS SERVICO FEDERAL DE PRO	000000000000000000000000000000000000000		Hom				
JERVICO FEDERAL DE FRI	2 2		ICP-Brasil				

Figure:- The above figure shows the results server supporting SSL v2

- \succ
- Organization Filter: This filter allows you to search for devices associated with a specific organization or company, helping you find systems linked to a particular entity.

Filter: org:"Organization Name"

Example: To find devices belonging to a specific company, use org:"Example Company".

SHODAN Explore	Downloads Pricing 안 org:"exam	ple"	Q	Accou
TOTAL RESULTS	Si View Report	1) View on Map		
35	Access Granted	: Want to get more out of your e	xisting Shodan account? Check out everything you have access t	0.
TOP COUNTRES	26 9 10 24 24 autoincore hostparame mostparames com hostparames com wiccoretess com our source organisempte com wiccoretess com guard Example LC 10 24 10 24	ISSUED DY: I- Common Nama: R3 I- Organization: Lef's Encrypt Issued To: I- Common Name:	HTD/1.1.200 OF Carbi-Control.ins-carbo Progen: co-cable Context-Syst::nst/thdi; carsist-ucf-6 Context-Syst::nst/thdi; Carsest-fic::1370-8.4 Server: (Incostric-TS/SR-8 magnet:ds::1370-8.5 House:Share-Share	2023-16-04768, 17-04, SB378
80 443 500 53 25 More	B Document Move shi 0.4145 shi 0.4145 shi 0.4145 shi 0.4145 shi 0.4145 shi 0.4145 Digital Example LLC 2 Il United States, Viciabu	HTTP/1.1 302 Redirect Content-Type: text/html; ch Location: https://exchange. 9 Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET	Content-Integr:/encodenteel/UF-0 Location:https://encodenteel/UF-0 Awar: Microsoft:LISIA-0 X-Powere-6-yr:ADR-NET Date: Sony, 30 C 2020 5527:00 OFT	

Figure:- The above figure shows the results of a specific organization.

Host Name Filter: This filter enables you to search for devices by their hostname, making it easier to identify specific servers or domains within Shodan's database.

Filter: hostname:"Domain Name"

Example: To find devices associated with a specific domain, use hostname:"example.com".

🕕 Rect 🐴 NOV 🧮 Rect 🤅	🌀 med 🍽 The 🚥 Mas	en Bug en Mas en Und e	🖬 Corr 🔿 Gith 🔾 Gith	😋 meci 🕶 Ada; 🗰 Huri 😋 shoi: 🎮 Shoi 🎮 Inbi; 🥝 shoi				
\leftrightarrow \rightarrow X 🖷 shodan.io/s		🧿 🖈 🖬 🍘 E						
		All Bookmarks						
Shodan Maps Image	s Monitor Developer	More						
SHODAN Expl	lore Downloads F	Pricing 2 hostname:"exa	mple.com*	Q		Account		
TOTAL RESULTS		翁 View Report 🛛 🕮 Br	owse Images 🖽 View o	n Map				
106,940 Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.								
TOP COUNTRIES		3.71.131.223	,			5-10-29710-03-16-650058		
TOP COUNTRIES	•	ec2-3-71-131-223.eu-central -1.compute.amazonawa.com	SSL Certificate	HTTP/1.1 200 OK				
		example.com A100 ROW SmbH	Issued By: - Common Name:	Date: Sun, 29 Oct 2023 10:03:13 GMT Content-Type: text/html				
		Germany, Frankfurt am	example.com	Cache-Control: no-cache Pragna: no-cache				
		cloud self-signed	- Organization: My Company					
C .	. */		Issued To: - Common Name:	Set-Cookie: webvpnc=; expir	-			
Russian Federation	29,974 20,605		example.com					
Netherlands	20,605		- Organization: My Company					
Germany	6.311		Supported SSL Versions:					
Poland	5,596		TLSv1.2					
More	0,000	146.185.199.90			2021	5-10-29710:03:10.875684		
		m16.example.com EdgeCenter LLC	A SSL Certificate	SSL Error: TLSV1_ALERT_PROTOCOL_VERSION				
TOP PORTS			Issued By: - Common Name:					
443 80	17,675 15,154	Federation, Novosibirsk	m1-gcore-nsk- ca@1689670326					
22			Issued To:					
	14,689		- Common Name: m1.acore.osk@1689670326					
Search	🕂 👬 🙀 🙀	0 🖸 🖪 📆 😒	🚱 hostname: "example.c	🔇 Meeting notes - Goog 🍰 35°C S	moke 🛛 🗠 🔂 🖬	F (\$4) 🦟 3:37 PM 🗔		

Figure:- The above figure shows the output of a specific domain using Hostname filter.

References:-

- 1. Shodan:- https://www.shodan.io/
- 2. Medium :-<u>https://medium.com/@hexadefend/the-hackers-search-engine-shodan-part-2-6cf5c9b77ae</u> <u>7</u>