Go Recon Yourself!

Discovering Your External Risk with Mostly Open Source Tools

Informal Title:

Should that be really open to the internet?

Disclaimer:

This presentation is for informational purposes **ONLY**. The conference organizers nor myself are responsible for any erroneous behavior.

Agenda

- Introduction
- Reconnaissance Tools/Phases
- Automation Ideas
- Live Demo
- Q&A

./about_me

You may have seen this...

LinkedIn (@jeredbare): Billy Madison picture

Twitter (@jeredbare): All over the place Tweets

Instagram (@jered.bare): Bodybuilder

GitHub (/jeredbare): Scripts and tools

I'm that and…

Father

Cyber Security Engineer for CarFax

6+ "official" years of experience in InfoSec. 13+ in IT overall.

Serve part-time in the Missouri Air National Guard

What are We Talking About

- Reconnaissance with Mostly Open Source or Low Cost tooling
  - Basic steps in running a reconnaissance campaign against your organization or target.
- Basic use of these reconnaissance tools
  - These tools are very powerful in their own. This presentation strives to teach you the basic commands to start a reconnaissance campaign.
- Determining risk from our reconnaissance campaign.
  - We can take the information given and determine what our risk posture may be.

Why you should use these tools

- Mostly free or low cost!
  - Takes a little bit of time to learn.
- Can help you build your asset list
  - Do you know your unknown unknowns? Reconnaissance can help you discover them.
- Easy to use and very well documented.
  - All of these have a big community and have a ton of features.
- You probably don’t know everything about your organization. It’s good to find out.
  - Using the steps outlined here, you can figure a bit more of your organization’s footprint.
- Cloud is messy
  - Resources can be spun up in a matter of seconds and misconfigured. These tools can help you identify some assets that should not be exposed to the internet.

How I do Reconnaissance

- Environment Discovery
  - Discovering hostnames.
  - Ports
  - DNS Records
- Perimeter Scanning
  - Scanning for current open ports and services.
  - Scanning for possible web vulnerabilities.
- Cloud Discovery
  - Recognizing cloud assets and misconfigurations to build our reconnaissance profile.
- Determining Risk
  - What exactly constitutes a risk?

List of Tools we are covering (in no certain order)

- Shodan
- Amass
- Paradigm
- Nmap
- Nikto
- Gray Hat Warfare

Environment Discovery

Amass

- Amass is a DNS reconnaissance and enumeration service that scrapes data from all over the web.
- One of the first steps in gathering information about your organization or target.
- Runs in Linux, Docker, and Mac OSX.
- Types of data it can provide
  - TLS Certificates
  - Whois Information
  - CIDR blocks
  - IPs
  - Cloud Providers
- Written by Jeff Foley (@caffix)
  - https://github.com/OWASP/Amass

Amass -- Data Sources

Information Gathering Techniques Used:

Technique	Data Sources
DNS	Brute forcing, Reverse DNS sweeping, NSEC zone walking, Zone transfers, FQDN alterations/permutations, FQDN Similarity-based Guessing
Scraping	Ask, Baidu, Bing, BuiltWith, DNSDumpster, DuckDuckGo, HackerOne, IPv4Info, RapidDNS, Riddler, SiteDossier, Yahoo
Certificates	Active pulls (optional), Censys, CertSpotter, Crtsh, FacebookCT, GoogleCT
APIs	AlienVault, Anubis, BinaryEdge, BGPView, BufferOver, C99, Chaos, CIRCL, Cloudflare, CommonCrawl, DNSDB, GitHub, HackerTarget, Hunter, IPinfo, Mnemonic, NetworksDB, PassiveTotal, RADb, ReconDev, Robtex, SecurityTrails, ShadowServer, Shodan, SonarSearch, Spyse, Sublist3rAPI, TeamCymru, ThreatBook, ThreatCrowd, ThreatMiner, Twitter, Umbrella, URLScan, VirusTotal, WhoisXMLAPI, ZETAlytics, ZoomEye
Web Archives	ArchiveIt, ArchiveToday, Wayback

Amass -- Installing Amass

- Requirements
  - GoLang
  - Docker
  - Unix distribution -- Built into Kali Linux

- How to install:

MacOSX

```
brew tap caffix/amass

brew install amass
```

Docker

```
docker pull caffix/amass

docker run -v OUTPUT_DIR_PATH:/.config/amass/ caffix/amass enum -share -d example.com
```

Amass -- Gathering Intel

- Intel
  - Gathers the WHOIS data in which domain is registered to an organization.
  - Works on any registered TLD: .com, .net, .org, .gov.
- This is one of my first steps in gathering reconnaissance data.
- Running the intel command
  - `docker run -v OUTPUT_DIR_PATH:/.config/amass/ caffix/amass intel -whos -d [domain]`
  - `amass intel -whois -d [domain]`

```
kali@kali:~$ amass intel -whois -d carfax.net
carfaxinc.com
carfaxinspection.biz
carfax-sa.net
carfax1-ownervehicles.net
carfaxespanol.us
carfax-italy.info
carfaxautoinspection.org
carfaxbulgaria.org
carfaxdriveradvantage.org
carfax1-ownercars.org
carfaxlownervehicles.com
carfaxcanada.biz
carfaxcar.net
car-fax.com
carcheck.biz
carfax-quebec.com
carfax-germany.info
carfaxnunavut.com
carfaxoneownervehicles.net
carfaxautoinspection.info
carfaxdistribution.com
carfaxhotlistings.com
car-total-loss.com
carfact.biz
carfaxaccount.com
carfaxdenmark.net
carfaxforclaims.net
carfax-france.org
carfax-spain.biz
carfax.io
carfaxforsalebyowner.org
crashdocs.org
carfax-bulgaria.info
carfaxhistoryreport.com
carfax-ontario.com
carfax-france.biz
carfax1-ownercars.us
carfaxconnexion.com
carfaxautoreports.org
carfaxdealerspotlight.info
carfaxforsalebyowner.net
autohistory.ca
carfax-germany.us
carfax-poland.info
carfax-austria.com
carfax1-owner.net
carfaxmobile.net
carfacthistoryreport.com
carfax-1-ownersale.biz
```

Amass -- Enumeration

- Enum
  - Scrapes data from the various data sources.
- Looks very similar to the intel command, however will list sub domains.
- Running the enum command
  - `docker run -v OUTPUT_DIR_PATH:/.config/amass/ caffix/amass enum -share -d example.com`
  - `amass enum -d [domain] -json [domain].json`

```
kali@kali:~$ ls carfax_net.json
carfax_net.json
kali@kali:~$ vi carfax_net.json
```


```
{"name":"alpha-price-plan-services.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.174","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag
:"api","sources":["BufferOver"]}
{"name":"beta-crmlistener.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.142","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","
ources":["AlienVault"]}
{"name":"alpha-summary-services.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.171","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"
pi","sources":["BufferOver"]}
{"name":"internal-redirect-d.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.165","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"ap
,"sources":["BufferOver"]}
{"name":"dvlpimobile.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.105.208","cidr":"216.117.105.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","sou
ces":["AlienVault"]}
{"name":"betareports.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.223","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","sourc
s":["AlienVault"]}
{"name":"vpn-va.carfax.net","domain":"carfax.net","addresses":[{"ip":"166.90.97.81","cidr":"166.90.97.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag":"api"
"sources":["AlienVault"]}
{"name":"vpn-mo.carfax.net","domain":"carfax.net","addresses":[{"ip":"64.193.21.81","cidr":"64.193.21.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag":"api"
"sources":["BufferOver"]}
{"name":"rememberme-d.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.89","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","sourc
s":["AlienVault"]}
{"name":"liveav.carfax.net","domain":"carfax.net","addresses":[{"ip":"166.90.97.113","cidr":"166.90.97.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag":"ap
,"sources":["AlienVault"]}
{"name":"beta-company-services.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.141","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"
i","sources":["BufferOver"]}
{"name":"internal-redirect-f.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.105.169","cidr":"216.117.105.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"
i","sources":["BufferOver"]}
{"name":"meet.carfax.net","domain":"carfax.net","addresses":[{"ip":"166.90.97.19","cidr":"166.90.97.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag":"api","
ources":["AlienVault"]}
{"name":"finance-services.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.175","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","
ources":["AlienVault"]}
{"name":"live.carfax.net","domain":"carfax.net","addresses":[{"ip":"166.90.97.124","cidr":"166.90.97.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag":"api",
sources":["AlienVault"]}
{"name":"betamymail.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.205","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","sourc
":["AlienVault"]}
{"name":"stagingemployees.carfax.net","domain":"carfax.net","addresses":[{"ip":"52.84.22.65","cidr":"52.84.16.0/21","asn":16509,"desc":"AMAZON-02 - Amazon.com, Inc."},{"ip":"
2.84.22.68","cidr":"52.84.16.0/21","asn":16509,"desc":"AMAZON-02 - Amazon.com, Inc."},{"ip":"52.84.22.51","cidr":"52.84.16.0/21","asn":16509,"desc":"AMAZON-02 - Amazon.com,
c."},{"ip":"52.84.22.128","cidr":"52.84.16.0/21","asn":16509,"desc":"AMAZON-02 - Amazon.com, Inc."}],"tag":"cert","sources":["CertSpotter"]}
{"name":"pocimobile.carfax.net","domain":"carfax.net","addresses":[{"ip":"166.90.97.160","cidr":"166.90.97.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag"
api","sources":["AlienVault"]}
{"name":"imobile-d.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.95","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","sources"
["AlienVault"]}
{"name":"betaimobile.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.94","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":"api","sourc
":["AlienVault"]}
{"name":"alpha-company-services.carfax.net","domain":"carfax.net","addresses":[{"ip":"216.117.25.140","cidr":"216.117.25.0/24","asn":62,"desc":"CYRS - CyrusOne LLC"}],"tag":
pi","sources":["BufferOver"]}
{"name":"coderepo.carfax.net","domain":"carfax.net","addresses":[{"ip":"64.193.21.77","cidr":"64.193.21.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag":"a
","sources":["AlienVault"]}
{"name":"jamfshare.carfax.net","domain":"carfax.net","addresses":[{"ip":"64.157.165.46","cidr":"64.157.165.0/24","asn":62723,"desc":"ACTUAL-AS - Actualize Tech, LLC"}],"tag"
api","sources":["AlienVault"]}
```

Amass -- Limitations

- Slow...sometimes very slow.
- Documentation is extensive, can be overwhelming.
- Support is pretty good, but a lot of what you'll be doing is on your own.
- Not completely accurate and may not have fresh data.

Paradigm

- Paradigm is a Web UI to analyze JSON files that are exported from Amass.
- The user can upload their .json file to the interface and see the results in real time.
- There is a small risk scoring system that determines how much of your environment is open to the internet.
  - For example, if the domains discovered and enumerated by Amass are all open to the internet; that is probably a bad thing.
  - Doesn’t account for compensating controls
- Written by myself and business partner Jordan Johnson.

Paradigm -- Installation

- Install Docker and docker-compose.
- Download the repository
  - https://github.com/jeredbare/paradigm
- Building the container
  - Unzip the repository.
  - Go into that directory and run `docker-compose build`
- Running the container and navigate to the web interface
  - `docker-compose up`
  - Go to http://localhost:3000 in a web browser

Paradigm -- How to Use

- Upload your JSON file created from Amass.
  - [domain_enum].json
- Click on Get Score
  - See the Scan Results for score and list of assets.

127.0.0.1:3000

Paradigm

Drag File Here

Drag and drop your file here

127.0.0.1:3000

Paradigm

Drag File Here

Drag and drop your file here

GET SCORE

CLEAR DATA

AMASS Data

Search

Name	Domain	IP	CIDR	ASN	Description	Tag
alpha-price-plan-services.carfax.net	carfax.net	216.117.25.174	216.117.25.0/24	62	CYRS - CyrusOne LLC	dns
internal-redirect-d.carfax.net	carfax.net	216.117.25.169	216.117.25.0/24	62	CYRS - CyrusOne LLC	api
crmlistener.carfax.net	carfax.net	216.117.25.144	216.117.25.0/24	62	CYRS - CyrusOne LLC	api
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	CYRS - [illegible]	[illegible]

Paradigm

Drag File Here

Drag and drop your file here

GET SCORE

CLEAR DATA

Scan Score:

5 %

Scan Results

Search

FQDN	Domain	IP	CIDR	HTTP Response	HTTPS Response	Description	Date and Time
alpha-price-plan-services.carfax.net	carfax.net	216.117.25.174	216.117.25.0/24	No Response	No Response	CYRS - CyrusOne LLC	----
internal-redirect-d.carfax.net	carfax.net	216.117.25.169	216.117.25.0/24	No Response	No Response	CYRS - CyrusOne LLC	----
crmlistener.carfax.net	carfax.net	216.117.25.144	216.117.25.0/24	No Response	No Response	CYRS - CyrusOne LLC	----
dvlpimobile.carfax.net	carfax.net	216.117.105.208	216.117.105.0/24	No Response	No Response	CYRS - CyrusOne LLC	----

Scan Results

Search

FQDN	Domain	IP	CIDR	HTTP Response	HTTPS Response	Description	Date and Time
jamfshare.carfax.net	carfax.net	64.157.165.46	64.157.165.0/24	No Response	No Response	ACTUAL-AS - Actualize Tech, LLC	----
revproxy.carfax.net	carfax.net	166.90.97.12	166.90.97.0/24	No Response	No Response	ACTUAL-AS - Actualize Tech, LLC	----
dvlpimobile-f.carfax.net	carfax.net	216.117.105.208	216.117.105.0/24	No Response	No Response	CYRS - CyrusOne LLC	----
stagingemployees.carfax.net	carfax.net	13.35.90.98	13.35.90.0/23	200	200	AMAZON-02 - Amazon.com, Inc.	31/08/2021 23:11:59
five9recs.carfax.net	carfax.net	166.90.97.27	166.90.97.0/24	No Response	No Response	ACTUAL-AS - Actualize Tech, LLC	----

5 rows 21-25 of 42

Paradigm -- Limitations

- Pretty buggy
  - A properly formatted JSON file will not be accepted.
  - Can only accept json files from Amass using the -json flag.
- Doesn’t account for compensating controls
  - It only counts the number of 200 HTTP response out of the number of domains for discovered.
- Scoring is a little confusing
  - If 95% of your environment is open to the internet and has compensating controls; that poses very little risk.

Shodan

- A search engine that scans the entire internet for internet connected devices.
- Gained notoriety for IP Cameras connected to the internet.
- Port scans and sweeps the entire internet:
  - Scans all known and unknown ports.
  - Banner grabs from these ports.
  - Also determines what vulnerabilities may exist on the host.

SHODAN | Explore | Downloads | Pricing | Search... | Account

Dashboard

Getting Started

What is Shodan?

Search Query Fundamentals

Working with Shodan Data Files

LEARN MORE

>_ ASCII Videos

Setting up Real-Time Network Monitoring

Measuring Public SMB Exposure

Analyzing the Vulnerabilities for a Network

VISIT THE CHANNEL

</> Developer Access

How to Download Data with the API

Looking up IP Information

Working with Shodan Data Files

DEVELOPER PORTAL

// QUICK LINKS

SETUP NETWORK MONITORING

BROWSE IMAGES

MAP VIEW

Enterprise Access

Need bulk data access? Check out our enterprise offering which includes full, unlimited access to the entire Shodan platform:

Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	2-letter Country code	Open ports in the United States
http.title	Title of the website	"Hacked" Websites
net	Network range or IP in CIDR notation	Services in the range of 8.8.0.0 to 8.8.255.255

SHODAN | Explore | Downloads | Pricing | Search... | Account

Explore

// CATEGORIES

// TOP VOTED

Webcam
best ip cam search I have found yet.
12,519 webcam surveillance cams

Cams
admin admin
5,290 cam webcam

Netcam
Netcam
2,697 netcam

default password
Finds results with "default password" in the ban...
2,111 router default password

ufanet
":80:":8080:
1,413 ufanet

MORE

// RECENTLY SHARED

Seagate.com
...
1 iis

80
...
1

Saferoads Variable Message Signs
Electronic highway message signs
2 iot signs

ADB Remote Access
...
3 adb port:5555

shodan
shodan.io result
1

MORE

// FILTERS

Search shared queries...

Popular Tags

webcam cam camera ip router scada ftp server http iot test password cisco web default login ssh 1 nas ipcam

Shodan 2000

Explore the Internet in style using an 80's retro-futuristic interface to synthwave music.

2000.SHODAN.IO

Internet Observatory

How exposed to the Internet is your country? What is the most common vulnerability? Get a high-level view of the Internet using our Observatory.

EXPOSURE.SHODAN.IO

// PRODUCTS
Monitor
Bulk Data

// PRICING
Membership

// CONTACT US
support@shodan.io

SHODAN | Explore | Downloads | Pricing

Server: SQ-WEBCAM

TOTAL RESULTS

41

TOP COUNTRIES

Hungary	7
Italy	6
Japan	5
Czechia	4
India	3

More...

TOP PORTS

80	12
83	5
8080	4
443	3
52869	3

More...

TOP ORGANIZATIONS

139.162.0.0/16	5
Telecom Italia S.p.A.	4
DigitalOcean, LLC	3
Magyar Telekom plc.	3
DIGI Tavkozlesi es Szolgaltato Kft.	2

More...

TOP PRODUCTS

dvr1614n web-cam httpd	22
Apache httpd	1

View Report | Download Results | View on Map

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

90.49.35.92
ltbn-nan-1-186-92.w90-49.abo.wanadoo.fr
France, Mayenne

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002
```

2021-

Windows Download AP.
217.121.176.207
217-121-176-207.cable.dynamic.v4.ziggo.nl
Ziggo Consumers
Netherlands, Steenwijk

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2706
```

2021-

217.235.255.50
pd9ebff32.dip0.t-ipconnect.de
Deutsche Telekom AG
Germany, Bergisch Gladbach

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002
```

2021-

84.236.16.6
84-236-16-6.pool.digikabel.hu
DIGI Tavkozlesi es Szolgaltato Kft.
Hungary, Budapest

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002
```

2021-

78.199.73.88
piq03-2_migr-78-199-73-88.fbx.proxad.net
Free SAS
France, Paris

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:518
```

2021-

140.114.36.128
pc128.stat.nthu.edu.tw
Ministry of Education Computer Centern12F, No 106, Sec.2,Hoping E. Rd.,nTaipei Taiwan
Taiwan, Hsinchu

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2307
```

2021-

5.187.151.118
05BB9776.catv.pool.telekom.hu
Magyar Telekom plc.
Hungary, Gyál

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
```

2021-

shodan.io/search?query="VCenter"

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | "VCenter" | Account

View Report | Download Results | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

5,699

TOP COUNTRIES

United States	1,224
Germany	419
China	368
France	349
Turkey	297

More...

TOP PORTS

443	4,571
389	248
636	214
135	103
8443	93

More...

TOP ORGANIZATIONS

Hetzner Online GmbH	192
OVH SAS	114
Amazon.com, Inc.	105
Amazon Technologies Inc.	65
SoftLayer Technologies, Inc.	63

More...

TOP PRODUCTS

VMware vCenter Server	4,841
Microsoft RPC Endpoint Mapper	103
Apache httpd	21
MS-SQL Server	10
SAProuter	9

More...

TOP OPERATING SYSTEMS

MikroTik RouterOS 6.48.1	9
MikroTik RouterOS 6.48.2	5

" + ID_VC_Welcome + "

2021-08-30T15:04:12.245346

187.72.121.162
mail.lufflogistics.com
ALGAR TELECOM S/A
Brazil, São Paulo

SSL Certificate

Issued By:
|- Common Name:
lfspapp23.luftfarma.com.br CA 20748b76
|- Organization:
VMware, Inc.

Issued To:
|- Common Name:
lfspapp23.luftfarma.com.br
|- Organization:
VMware, Inc.

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Mon, 30 Aug 2021 15:01:06 GMT
Connection: Keep-Alive
Content-Security-Policy: block-all-mixed-content
Content-Type: text/html
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1
Content-Length: 3415
...
```

" + ID_VC_Welcome + "

2021-08-30T15:04:00.078267

212.97.32.172
172.32.97.212.host.static.ip.kpnqwest.it
STARDATA S.R.L.
Italy, Milan

SSL Certificate

Issued By:
|- Common Name:
vcenter.blasting.mng CA e0fdab13
|- Organization:
VMware, Inc.

Issued To:
|- Common Name:
vcenter.blasting.mng
|- Organization:
VMware, Inc.

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Mon, 30 Aug 2021 14:42:13 GMT
Connection: Keep-Alive
Content-Security-Policy: block-all-mixed-content
Content-Type: text/html
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1
Content-Length: 3415
...
```

" + ID_VC_Welcome + "

2021-08-30T15:03:08.954703

185.147.24.209
vcenter.physics.science.az
Institute of Information Technologies of National Academy of Science Azerbaijan
Azerbaijan, Baku

SSL Certificate

Issued By:
|- Common Name:
CA
|- Organization:
vcenter.physics.science.az

Issued To:
|- Common Name:
vcenter.physics.science.az

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
date: Mon, 30 Aug 2021 18:58:44 GMT
content-security-policy: block-all-mixed-content
content-type: text/html
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1
content-length: 3618
x-envoy-upstream-service...
```

" + ID_VC_Welcome + "

2021-08-30T15:03:01.340807

47.180.55.188
Frontier Communications of America, Inc.
United States, Malibu

SSL Certificate

Issued By:
|- Common Name:
CA
|- Organization:
vcsa.sl.malibu.ca.us

Issued To:
|- Common Name:
vcsa.sl.malibu.ca.us

```
HTTP/1.1 200 OK
date: Mon, 30 Aug 2021 15:03:16 GMT
content-security-policy: block-all-mixed-content
content-type: text/html
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1
content-length: 3618
```

Shodan | Maps | Images | Monitor | Developer | More..

SHODAN | Explore | Downloads | Pricing | Search... | Account

187.72.121.162

Regular View | Raw Data | History

// TAGS: self-signed starttls

// LAST UPDATE: 2021-08-30

General Information

Hostnames	mail.luftlogistics.com
Domains	LUFTLOGISTICS.COM
Country	Brazil
City	São Paulo
Organization	ALGAR TELECOM S/A
ISP	ALGAR TELECOM S/A
ASN	AS16735

Web Technologies

JQUERY | SWFOBJECT

Open Ports

25 | 53 | 143 | 443 | 465 | 587 | 993 | 995 | 2222 | 8080 | 9443

// 25 / TCP

-1636940839 | 2021-08-28T06:37:08.179239

Postfix smtpd

```
220 mail.luftlogistics.com ESMTP Postfix (Debian/GNU)
250-mail.luftlogistics.com
250-PIPELINING
250-SIZE 10864000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH CRAM-MD5 LOGIN PLAIN
250-AUTH=CRAM-MD5 LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            b3:57:00:4c:45:5a:0d:96
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=BR, ST=SP, L=Sao Paulo, O=bomifarma.com.br, OU=TI, CN=smtp.bomifarma.com.br/emailAddress=postmaster@bomifarma.com.br
        Validity
            Not Before: Sep 29 05:31:49 2005 GMT
            Not After : Jul 29 23:03:33 1969 GMT
        Subject: C=BR, ST=SP, L=Sao Paulo, O=bomifarma.com.br, OU=TI, CN=smtp.bomifarma.com.br/emailAddress=postmaster@bomifarma.com.br
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c6:c2:a5:57:8d:f4:e2:7d:69:4e:c7:4c:14:4d:
                    34:2a:15:00:48:05:7c:e5:e5:d3:4a:65:e7:a5:b1:
                    70:19:6e:2d:6e:72:34:35:e7:80:79:b1:bc:33:87:
                    e1:44:de:40:e3:55:73:b0:56:e2:1d:af:b3:45:82:
                    0d:36:3f:f7:db:64:8c:83:02:b7:42:e7:57:fd:1d:
                    e1:6c:f9:19:14:95:1a:54:de:a2:76:dc:91:28:0b:
                    d3:52:ab:2a:0c:01:ba:c4:a6:ec:b5:16:0c:00:63:
                    04:48:e5:04:69:f5:6c:e3:46:4b:c0:53:01:c8:35:
                    c6:f4:d4:c0:ad:00:63:a2:42:54:40:bd:10:6c:b8:
                    23:3c:9c:12:60:ef:20:44:2e:06:fa:22:2b:db:23:
                    89:6e:23:7a:79:00:98:1b:58:7e:33:76:45:31:f2:
                    86:7e:0b:d2:69:62:53:cc:8c:9f:90:9e:e1:65:0c:
                    f0:3c:cb:c8:65:35:46:3d:35:e3:81:96:34:ce:99:
                    4d:af:f5:fc:dc:e1:b5:fa:8b:ad:6c:c5:61:5f:21:
                    fd:56:ca:e3:dc:82:59:eb:73:77:70:97:f1:b1:1c:
                    97:9c:34:24:6d:6b:76:98:9e:70:aa:0b:91:25:12:
                    c8:de:bb:07:94:9d:1c:ee:99:cb:a5:de:c6:91:99:
```

Download Results

Search Query: **"VCenter"**

Number of results

5700

100 query credits available.

DOWNLOAD

Note: Downloads may take several hours to complete

FAQ

1. Downloads consume query credits which reset at the start of every month.
2. The maximum number of results that can be downloaded for a search query is 300,000.
3. Query credits are only deducted for data that was actually downloaded.

You can also download data using the official Shodan command-line interface (CLI):

LEARN MORE

// PRODUCTS

Monitor
Search Engine
Developer API
Maps
Bulk Data
Images
Snippets

// PRICING

Membership
API Subscriptions
Enterprise

// CONTACT US

support@shodan.io

5d252997-cea0-4058-a231-0951f6b65577....	8/30/2021 10:32 AM	GZ File	71 KB

Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	2-letter Country code	Open ports in the United States
http.title	Title of the website	"Hacked" Websites
net	Network range or IP in CIDR notation	Services in the range of 8.8.0.0 to 8.8.255.255
org	Name of the organization that owns the IP space	Devices at Google
port	Port number for the service that is running	SSH servers
product	Name of the software that is powering the service	Samsung Smart TVs
screenshot.label	Label that describes the content of the image	Screenshots of Industrial Control Systems
state	U.S. State	Devices in Texas

VIEW ALL FILTERS

MORE EXAMPLES

Filters and Examples:

city:"Columbia" -- Must be a [string]

country: "US" -- Must be a [string]

http.title:"Hacked by" -- Can be [string] or [float]

net:198.209.10.0/27 -- Has to be a [float]

org:"CenturyLink" -- Has to be a [string]

port:445 -- Has to be an [int]

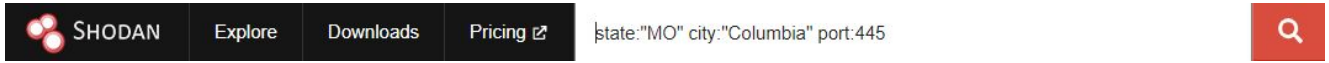
product:"Exchange" -- Can be a [string] and/or [float]

screenshot.label:ics -- Can be a [string] and/or [float]

state:"MO"

Let’s apply it locally -- Apologies ahead of time

- Filters we’ll be using
  - “City”, “state”, “port”



SHODAN | Explore | Downloads | Pricing | state:"MO" city:"Columbia" port:445 | Account

TOTAL RESULTS

54

TOP ORGANIZATIONS

[redacted]	13
	9
	8
	3
	3

More...

TOP OPERATING SYSTEMS

Windows Server 2016 Standard 14393	10
Windows 6.1	6
Windows Server 2012 R2 Standard 9600	4
Windows Server 2008 R2 Standard 7601 Service Pack 1	3
Windows 7 Professional 7601 Service Pack 1	1

More...

View Report | Download Results | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]

2021-08-30T10:19:02.124005

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2016 Standard 14393
  Software: Windows Server 2016 Standard 6.3
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode
```

[redacted]

2021-08-30T10:03:05.970547

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2016 Standard 14393
  Software: Windows Server 2016 Standard 6.3
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode
```

[redacted]

United States, Columbia

2021-08-30T06:22:20.049541

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2012 R2 Standard 9600
  Software: Windows Server 2012 R2 Standard 6.3
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode
```

[redacted]

2021-08-29T22:11:24.172895

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
  Software: Windows Server 2008 R2 Standard 6.1
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode
```

[redacted]

2021-08-29T18:22:22.634629

```
SMB Status:
  Authentication: enabled
  SMB Version: 2
  Capabilities: raw-mode
```

[redacted]

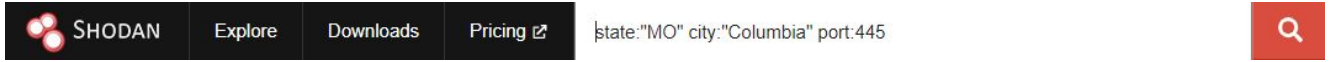
2021-08-29T17:58:28.274882

```
SMB Status:
  Authentication: disabled
  SMB Version: 1
  Capabilities: dfs, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api, unicode, unix

Shares
Name                Type       Comments
---------------------------------------------------------------------
IPC$                IPC        IPC Service (Samba 3.0.37-(Optimized by Tuxera Inc, 3015.10.21))
```

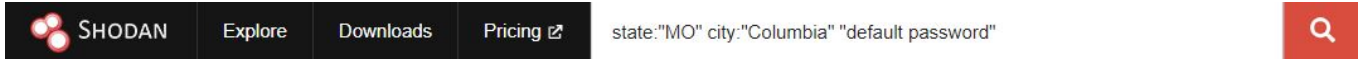
[redacted]

Let’s apply it locally -- Apologies ahead of time

- Finding SMB1 Host Locally [Filters we’ll be using below]
  - “City”, “state”, “port”
  - state:”MO” city:”Columbia” port:445



- Finding Default Passwords Locally [Filters we’ll be using below]
  - “state”, “city”, “[string]”
  - state:”MO” city:”Columbia” “default password”



SHODAN | Explore | Downloads | Pricing | state:"MO" city:"Columbia" "default password" | Account

TOTAL RESULTS

2

TOP PORTS

23	1
8081	1

View Report | Download Results | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

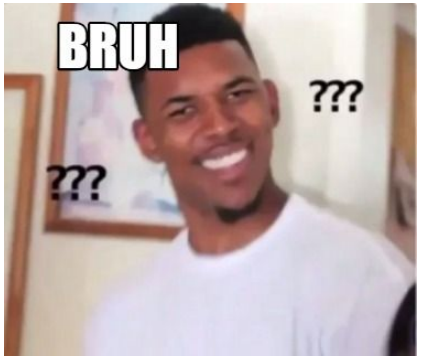
2021-08-28T09:59:05.548261

```
[2J[H

****** Important Banner Message ******

Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "password".
Please change them immediately.
The ethernet 0/1 interface is enabled with an address of 10.10....
```

United States, Columbia


```
[2J[H

****** Important Banner Message ******

Enable and Telnet passwords are configured to "password".
rd is "password".

****** Important Banner Message ******

of 10.10....
```


```
Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "password".
Please change them immediately.
The ethernet 0/1 interface is enabled with an address of 10.10....
```



Let’s apply it locally -- Apologies ahead of time

- Finding Hacked Websites in the United States [Filters we’ll be using below]
  - “country”, “http.title”
  - *country:”US” http.title:”Hacked by”*

SHODAN | Explore | Downloads | Pricing | country:"US" http.title:"Hacked by" | Account

TOTAL RESULTS

439

TOP CITIES

Atlanta	87
Los Angeles	31
Chamblee	25
Ashburn	23
Hilliard	22

More...

TOP PORTS

80	274
443	152
8080	4
8000	3
8443	3

More...

TOP ORGANIZATIONS

NationalNet, Managed Services	83
Unified Layer	46
DigitalOcean, LLC	34
Amazon Technologies Inc.	28
Performive LLC	25

More...

TOP PRODUCTS

Apache httpd	352
nginx	48
LiteSpeed httpd	13
Microsoft IIS httpd	7

View Report | Download Results | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

This Site Hacked By HackingTruths Team

2021-08-30T21:11:28.143707

65.99.237.127
uscentral19.myserverhosts.com
A Small Orange LLC
United States, Dallas

compromised

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Mon, 30 Aug 2021 21:11:27 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```

HackeD By Desert Warriors

2021-08-30T21:10:20.211616

69.50.133.252
Performive LLC
United States, Chamblee

compromised

```
HTTP/1.1 200 OK
Date: Mon, 30 Aug 2021 21:10:19 GMT
Server: Apache/2.2.16 (Debian) PHP/5.3.3-7+squeeze15 with Suhosin-Patch proxy_module/1.11.20
Last-Modified: Tue, 04 Sep 2018 19:51:05 GMT
ETag: "8672c-1433-57510fa6e1c40"
Accept-Ranges: bytes
Content-Length: 5171
Vary: Accept-Encoding
Con...
```

Hacked By MR.GREEN – Just another WordPress site

2021-08-30T20:59:40.603850

143.198.59.111
DigitalOcean, LLC
United States, Santa Clara

compromised | cloud | self-signed

SSL Certificate

Issued By:
- Common Name: openlitespeed-wordpress-v15
- Organization: LiteSpeedCommunity

Issued To:
- Common Name: openlitespeed-wordpress-v15
- Organization: LiteSpeedCommunity

Supported SSL Versions:
TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
link: <https://r.ocket.host/wp-json/>; rel="https://api.w.org/"
vary: Accept-Encoding
x-litespeed-cache: hit
date: Mon, 30 Aug 2021 20:59:40 GMT
server: LiteSpeed
transfer-encoding: chunked
alt-svc: h3=":443"; ma=2592000, h3-29=":443"...
```

Hacked By M4DI~UciH4

2021-08-30T20:21:50.402230

192.249.117.136
InMotion Hosting, Inc.
United States, Los Angeles

compromised | self-signed

SSL Certificate

Issued By:
- Common Name: vills.biz

Issued To:
- Common Name: vills.biz

Supported SSL Versions:
TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Mon, 30 Aug 2021 20:21:50 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Thu, 17 Jun 2021 15:22:04 GMT
Accept-Ranges: bytes
Content-Length: 8434
Content-Type: text/html
```

HackeD By Desert Warriors

2021-08-30T20:08:03.767196

69.50.133.225
Performive LLC
United States, Chamblee

```
HTTP/1.1 200 OK
Date: Mon, 30 Aug 2021 20:08:03 GMT
Server: Apache/2.2.16 (Debian) PHP/5.3.3-7+squeeze15 with Suhosin-Patch proxy_module/1.11.20
```

Let’s apply it locally -- Apologies ahead of time

- Finding Hacked Websites in the United States [Filters we’ll be using below]
  - “country”, “http.title”
  - *country:“US” http.title:“Hacked by”*

- Finding ICS systems in the state of Missouri... [Filters we’ll be using below]
  - “screenshot.label”, “state”
  - *screenshot.label:ics state:“MO”*

Please please please be careful with this one.

SHODAN | Explore | Downloads | Pricing | screenshot.label:ics state:"MO" | Account

TOTAL RESULTS

7

TOP PORTS

80	5
81	1
5900	1

TOP ORGANIZATIONS

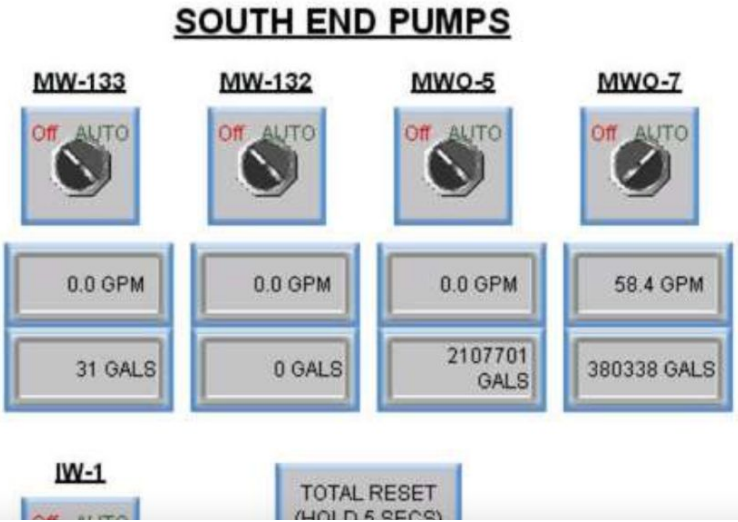
More...

View Report | Download Results | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

2021-08-30T06:38:29.315002

```
Last-Modified: Mon, 30 Aug 2021 05:21:27 GMT
ETag: "830002127"
Content-Type: text/html
Content-Length: 1520
```



Shodan Limitations

- Scans are old
  - About 1 - 2 weeks old.
- Little Expensive
  - Need to catch the $50 sale.
  - Real time monitoring cost $$$
- False positives
  - Due to the age of the scans, there can be false positives.
- Honeypots
  - Shodan cannot tell whether something is a honey pot or not.
- Doesn’t really give you the whole “picture”.
  - Compensating controls; Firewalls, WAFs, IDS/IPS

Perimeter Scanning

NMAP

- NMAP is a network port scanner that is compatible with all operating systems.
  - Windows
  - Mac OSX
  - Linux
  - Docker
- Used by Security Pros, Network Engineers, IT Pros.
- Has a robust scripting engine (LUA)
  - Checking for certificate ciphers.
  - Brute forcing engine.
  - Basic network vulnerability scanning.

NMAP -- Scanning the Perimeter

- Scanning a CIDR block, single IP, and domain.
  - `nmap -sV -A -T4 192.168.1.0/24`
  - `nmap -sV -A -T4 192.168.1.14`
  - `nmap -sV -A -T4 scanme.nmap.org`

NMAP -- Scanning the Perimeter

```
kali@kali:~$ nmap -sV -A -T4 nmap.scanme.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-31 21:28 UTC
Nmap scan report for nmap.scanme.org (45.33.32.156)
Host is up (0.054s latency).
Other addresses for nmap.scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
5431/tcp  filtered park-agent
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds
```

NMAP -- Scanning the Perimeter

- Scanning a CIDR block, single IP, and domain.
  - `nmap -sV -A -T4 192.168.1.0/24`
  - `nmap -sV -A -T4 192.168.1.14`
  - `nmap -sV -A -T4 scanme.nmap.org`
- Importing targets (Recon Profile)
  - `nmap -sV -A -T4 -iL targets.txt`

NMAP -- Scanning the Perimeter: Multiple Targets

```
kali@kali:~$ vi targets.txt
kali@kali:~$ cat targets.txt
scanme.nmap.org
10.0.0.2
kali@kali:~$
```

```
kali@kali:~$ nmap -sV -A -T4 -iL targets.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-31 21:35 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.054s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
5431/tcp  filtered park-agent
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.0.2
Host is up (0.00079s latency).
Not shown: 700 filtered ports, 295 closed ports
PORT    STATE SERVICE    VERSION
21/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=usg40_4C9EFF78DF46
| Subject Alternative Name: email:usg40_4C9EFF78DF46
| Not valid before: 2014-07-28T15:50:23
|_Not valid after:  2024-07-25T15:50:23
|_ssl-date: TLS randomness does not represent time
22/tcp  open  tcpwrapped
| ssh-hostkey:
|_  1024 cb:7a:b8:72:98:04:37:a0:4a:91:aa:17:56:b4:38:8b (RSA)
53/tcp  open  tcpwrapped
| dns-nsid:
|_  bind.version: ZyWALL DNS
80/tcp  open  tcpwrapped
|_http-title: Did not follow redirect to https://10.0.0.2:443/redirect.cgi?arip=10.0.0.2&original_url=http://10.0.0.2/
443/tcp open  tcpwrapped
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=usg40_4C9EFF78DF46
| Subject Alternative Name: email:usg40_4C9EFF78DF46
| Not valid before: 2014-07-28T15:50:23
|_Not valid after:  2024-07-25T15:50:23
|_ssl-date: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

NMAP -- Scanning the Perimeter

- Scanning a CIDR block, single IP, and domain.
  - `nmap -sV -A -T4 192.168.1.0/24`
  - `nmap -sV -A -T4 192.168.1.14`
  - `nmap -sV -A -T4 scanme.nmap.org`
- Importing targets
  - `nmap -sV -A -T4 -iL targets.txt`
- Exporting results
  - `nmap -sV -A -T4 -oN results.txt`

NMAP -- Limitations

- Sometimes can be slow.
- Noisy -- most IPS/IDS can pick up the port scanning activity.
  - You can manipulate packets to evade some IPS/IDS.
- Well known by attackers and defenders.
- Will sometimes break itself or other things.

Nikto

- Open source web vulnerability scanner.
- Built into Kali Linux, but can be used with Docker and other Linux flavors.
- Really good for quick scans to determine baseline vulnerabilities.
- https://cirt.net/Nikto2

Nikto -- Scanning Websites

- Running nikto (in Kali Linux)
  - `nikto -host [domain_or_ip]:[port]-o web_scan.txt`

```
kali@kali:~$ nikto -host 192.168.4.165:3000
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.4.165
+ Target Hostname:    192.168.4.165
+ Target Port:        3000
+ Start Time:         2021-08-31 21:02:04 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved access-control-allow-origin header: *
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'feature-policy' found, with contents: payment 'self'
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/ftp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ /site.jks: Potentially interesting archive/cert file found.
+ /site.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /192_168_4_165.jks: Potentially interesting archive/cert file found.
+ /192_168_4_165.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /backup.pem: Potentially interesting archive/cert file found.
+ /backup.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /168.jks: Potentially interesting archive/cert file found.
+ /168.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /168.alz: Potentially interesting archive/cert file found.
+ /168.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /backup.tgz: Potentially interesting archive/cert file found.
+ /backup.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /168.tar.lzma: Potentially interesting archive/cert file found.
+ /168.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /site.war: Potentially interesting archive/cert file found.
+ /site.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
+ /1921684165.egg: Potentially interesting archive/cert file found.
+ /1921684165.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).
```

Nikto -- Limitations

- Has a finite amount of signatures.
- VERY NOISY: Any basic IDS/IPS will pick up these activities.
- Does not replace commercial web vulnerability scanners, good for recon profiling.

Grayhat Warfare

- Online search for open AWS S3 Buckets, GCP Instances, and Azure blobs.
- You can find misconfigured cloud assets in this search engine.
- You can also find
  - Passwords
  - User accounts
  - Credit Card numbers
  - And….some other interesting stuff

buckets.grayhatwarfare.com

Buckets | Shorteners | Pricing | FAQ | Contact Us

GRAYHAT WARFARE

Login/Register

Home | Filter Buckets | Search Files | Docs / API | Top Keywords

Files
1.941 Of 6.736 Billion (?)

AWS Buckets
133108 Of 406159 (?)

Azure Blobs
7998 Of 47019 (?)

Last Update
09 August 2021

Search Public Buckets

Random Files

Wondering what is this website ? Read details here: How to search for Open Amazon s3 Buckets and their contents

Keywords - Stopwords (start with minus -) (?)

passwords

Order By

Order By Direction

Descending

Full Path (?) Treat as regex (?) Do not autocorrect regex (?)

Filename Extensions (php, xlsx, docx, pdf)

php, xlsx, docx, pdf

Include Exclude

Search

Notes

- A little more info about the tool: How to search for Open Amazon s3 Buckets and their contents
- All keywords are treated as logical AND. If you want a keyword excluded you could add -keyword.
  - ***secret*** - returns all files containing *secret* in filename.
  - ***secret -html*** - returns all files containing *secret* and do not contain *html* in filename.

Hand-crafted & made with ♥ with Symfony PHP Framework, golang and all databases known to man ☺

Buckets Shorteners

Pricing FAQ Contact Us

GRAYHAT WARFARE

carfax

Login/Register

Home | Filter Buckets | Search Files | Docs / API | Top Keywords

As a free user you are searching in 1940 from the 6735 million files in the index. Registered users have double limits. Finally Premium users also have sorting enabled, full path search instead of only filename and file listing enabled for all buckets. Upgrade your account to enable all features and remove all limitations. More info about packages here

Search File

Random Files

Keywords - Stopwords (start with minus -) (?)

carfax

Order By

Order By Direction

Descending

Full Path (?) Treat as regex (?)

Filename Extensions (php, xlsx, docx, pdf)

php, xlsx, docx, pdf

Include Exclude

Search

Results for "carfax"

1 - 20 of 612 results

Results might be less that usual, we are refreshing our indexes. This will take about 24h to completed.

Ignored Buckets

None (?)

#	Bucket	Filename	Container	Size	Last Modified
1	golden-media.s3.amazonaws.com	topics/225px-Carfax_Conduit_building.jpg		48.27kB	17-08-2017 13:44:04
2	golden-media.s3.amazonaws.com	to ... ilding__80x80.jpg		1.99kB	25-09-2017 20:08:58

Go to CARFAX/CARFAX-Promobar_01.png

2	aws	golden-media.s3.amazonaws.com	topics/225px-Carfax_Conduit_building__80x80.jpg	1.99kB	25-09-2017 20:08:58
3	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_01.png	21.49kB	21-06-2016 22:20:47
4	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_02.png	5.50kB	21-06-2016 22:20:47
5	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_03.png	6.85kB	21-06-2016 22:20:47
6	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_04.png	5.90kB	21-06-2016 22:20:47
7	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_05.png	5.13kB	21-06-2016 22:20:48
8	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_06.png	6.17kB	21-06-2016 22:20:48
9	aws	promobar.s3.amazonaws.com	CARFAX/CARFAX-Promobar_07.png	6.08kB	21-06-2016 22:20:49
10	aws	thebest.s3.amazonaws.com	reviews/103/carfax-used-cars.html	36.83kB	18-07-2016 17:27:54
11	aws	skunkworks-test.s3.amazonaws.com	089bff3cd5/carsgenius/static/images/carfax.png	6.27kB	02-07-2019 22:27:59
12	aws	skunkworks-test.s3.amazonaws.com	09ce9ffd7b/car_search/site_static/images/carfax.png	6.27kB	28-02-2019 00:24:54
13	aws	skunkworks-test.s3.amazonaws.com	0b59e502e9/carsgenius/static/images/carfax.png	6.27kB	20-06-2019 01:44:53
14	aws	skunkworks-test.s3.amazonaws.com	0ca069b4b8/carsgenius/static/images/carfax.png	6.27kB	11-06-2019 02:52:46
15	aws	skunkworks-test.s3.amazonaws.com	1167abd37c/car_search/site_static/images/carfax.png	6.27kB	02-05-2019 01:28:54
16	aws	skunkworks-test.s3.amazonaws.com	1252b0876e/carsgenius/static/images/carfax.png	6.27kB	12-06-2019 23:31:02
17	aws	skunkworks-test.s3.amazonaws.com	1304f6057c/carsgenius/static/images/carfax.png	6.27kB	08-06-2019 01:52:08
18	aws	skunkworks-test.s3.amazonaws.com	146a6efade/car_search/site_static/images/carfax.png	6.27kB	01-05-2019 02:28:45
19	aws	skunkworks-test.s3.amazonaws.com	14b88b5e37/car_search/site_static/images/carfax.png	6.27kB	13-03-2019 22:42:01
20	aws	skunkworks-test.s3.amazonaws.com	1694d02fca/car_search/site_static/images/carfax.png	6.27kB	30-04-2019 01:59:21

Automation

1. If I were to automate this it would look like so:
   1.1. Cron job or scheduled event would execute the job.
   1.2. The job would run Amass enum against your org's domain.
      1.2.1. `amass enum -d [your_org_domain} -json [your_org_domain_enum].json`
   1.3. As soon as the job is finished, it would upload the file to Paradigm for analysis and convert to text start nmap scanning.
      1.3.1. `POST to Paradigm back end`
      1.3.2. `nmap -sV -A -T4 -iL targets.txt`
   1.4. Paradigm records the date and time. For any changes that are unknown, I would investigate those immediately. I would use Nikto for any web services discovered.
   1.5. If any assets have a cloud infrastructure, I would test them using the providers CLI
      1.5.1. `aws s3 ls s3://$bucketname/ --region $region`
   1.6. Send updates and/or notifications to the SOC team, Slack/Email, or take care of them yourself.

Using this Information to Determine Risk

What Constitutes a Risk?

- Risk management is complicated, but it can be simplified.
- Risk is subjective. Most times a good organization will have compensating controls
  - Firewalls, rate limiting libraries, WAFs, IDS/IPS
- Risk is something you either address or accept.
- What I propose --->

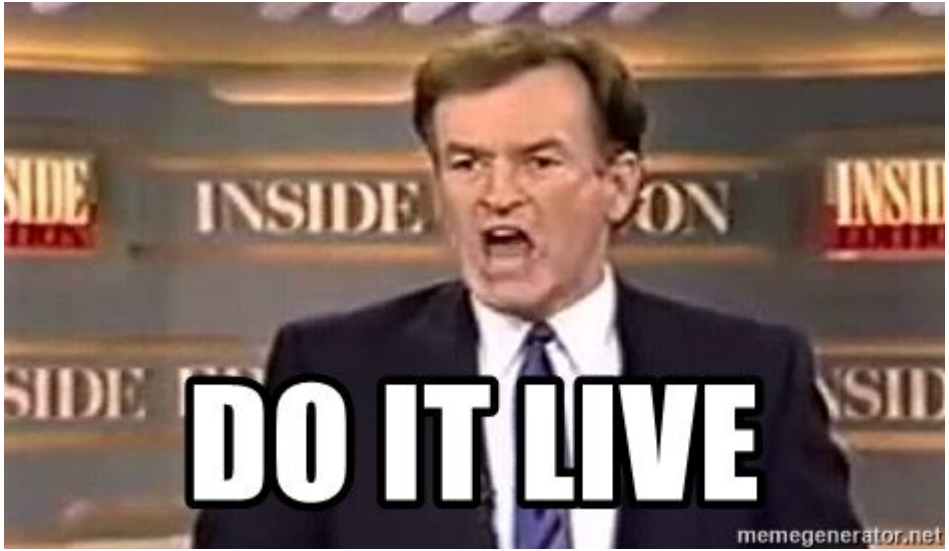
Simplified Reconnaissance Risk Management

Shodan	Shodan +2	Amass +1	Paradigm +1	NMAP/Nikto +1	Cloud (open instance) +5	**Total**
domain.com	+2	+1	+1	+1	0	5
example.com	+1	+1	+1	+1	+5	9
bigrisk.com	0	0	0	+1	0	1

References

- Shodan
  - https://shodan.io
- Paradigm
  - https://github.com/jeredbare/paradigm
- Amass
  - https://github.com/OWASP/Amass
- Grayhat Warfare
  - https://grayhatwarfare.com/

Live Recon Demo



Q&A

Let’s Connect!

- Twitter (@jeredbare)
- LinkedIn(jeredbare)
- Instagram (@jered.bare)
- GitHub (jeredbare)
- Discord (jeredbare)