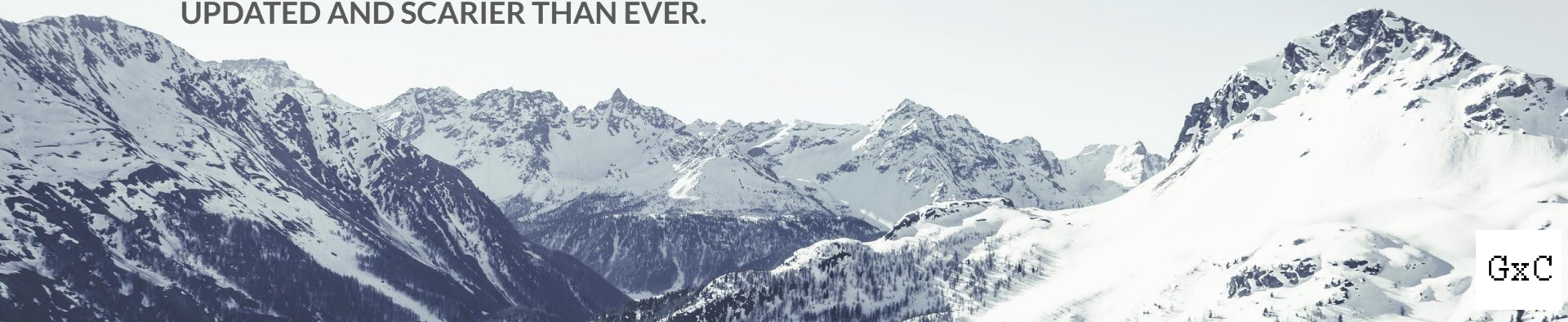
Go Recon Yourself! 2.0

Discovering your external risk using mostly open source tools.
UPDATED AND SCARIER THAN EVER.



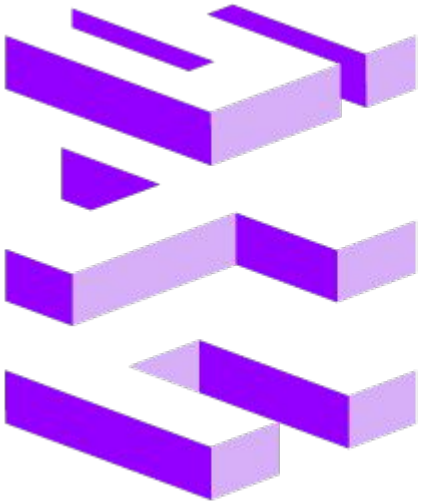
GxC

Informal Title

Just unplug the internet cord and start a farm.

Thank You

SecureData TECHNOLOGIES



springfield tech council

GxC

Disclaimer:

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

Today's Agenda

1. Estimated Time: 40 - 60 Minutes

Presentation

May run the full time.

2. Estimated Time: 15 Minutes

Demo?

If time allows, demo.

3

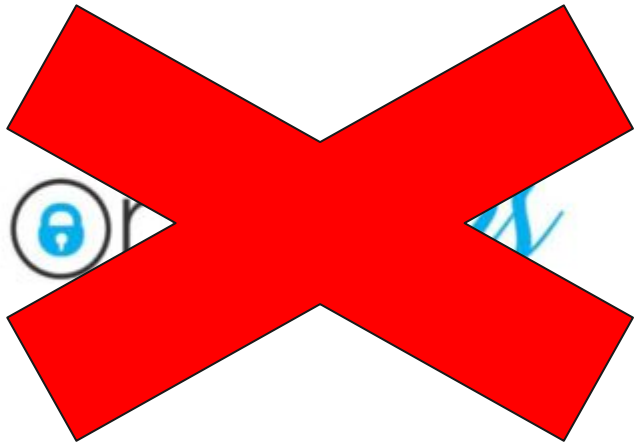
Q & A

If not, hit me up after

GxC

./about_me – What you may have seen or did your own Recon

- Cybe
  -
- Linke
  -
  -
- Twitt
  -
- Instag
  -
- GitHu
  -



The Problem

TLS every where is great.

The cloud is great.

For an attack surface: not so great.

Why?

Every certificate is registered with a CA (certificate authority)

Most cloud infrastructures use TLS (https://www.yourcompany.com)

GxC

The Big Question?

How can an organization know their attack surface in today's world?

Reconnaissance - A Four Step Process

- Environment Discovery
  - TLS Certificates
  - Networking Information
  - CIDR Blocks
  - Cloud Providers
- Perimeter Scanning
  - Using tools to determine what is live vs not live.
- Cloud Scanning
  - Using tools and techniques to recognize misconfigurations.
- Monitoring and Determining Risk
  - Monitoring for changes within the environment using tools that scan the internet.


Environment Discovery

AMASS - https://github.com/OWASP/Amass

Developed by Jeff Foley (@jeff_foley) and OWASP to help organizations discover their attack surface. Focused on asset discovery, DNS enumeration, and attack surface mapping.

Jeff Foley
caffix

OWASP®

GxC

Data Sources Used and API Integrations

Technique	Data Sources
DNS	Brute forcing, Reverse DNS sweeping, NSEC zone walking, Zone transfers, FQDN alterations/permutations, FQDN Similarity-based Guessing
Scraping	AbuseIPDB, Ask, AskDNS, Baidu, Bing, DNSDumpster, DuckDuckGo, Gists, HackerOne, HyperStat, IPv4Info, PKey, RapidDNS, Riddler, Searchcode, Searx, SiteDossier, SpyOnWeb, Yahoo
Certificates	Active pulls (optional), Censys, CertSpotter, Crtsh, Digitorus, FacebookCT, GoogleCT
APIs	360PassiveDNS, ARIN, Ahrefs, AlienVault, AnubisDB, BinaryEdge, BGPView, BufferOver, BuiltWith, C99, Chaos, CIRCL, Cloudflare, CommonCrawl, DNSDB, DNSlytics, DNSRepo, Detectify, FOFA, FullHunt, GitHub, GitLab, Greynoise, HackerTarget, Hunter, IntelX, IPdata, IPinfo, Maltiverse, Mnemonic, N45HT, NetworksDB, ONYPHE, PassiveTotal, PentestTools, Quake, RADb, Robtex, SecurityTrails, ShadowServer, Shodan, SonarSearch, Spamhaus, Spyse, Sublist3rAPI, TeamCymru, ThreatBook, ThreatCrowd, ThreatMiner, Twitter, Umbrella, URLScan, VirusTotal, WhoisXMLAPI, ZETAlytics, ZoomEye
Web Archives	ArchiveIt, Arquivo, HAW, UKWebArchive, Wayback

Installing AMASS

- Windows
  - Download and install the binary.
  - https://github.com/OWASP/Amass/releases/download/v3.16.0/amass_windows_amd64.zip
- Kali Linux or Ubuntu
  - `sudo apt install amass`
- Mac OSX using Homebrew
  - `brew tap caffix/amass`
  - `brew install amass`
- Docker
  - `docker pull caffix/amass`

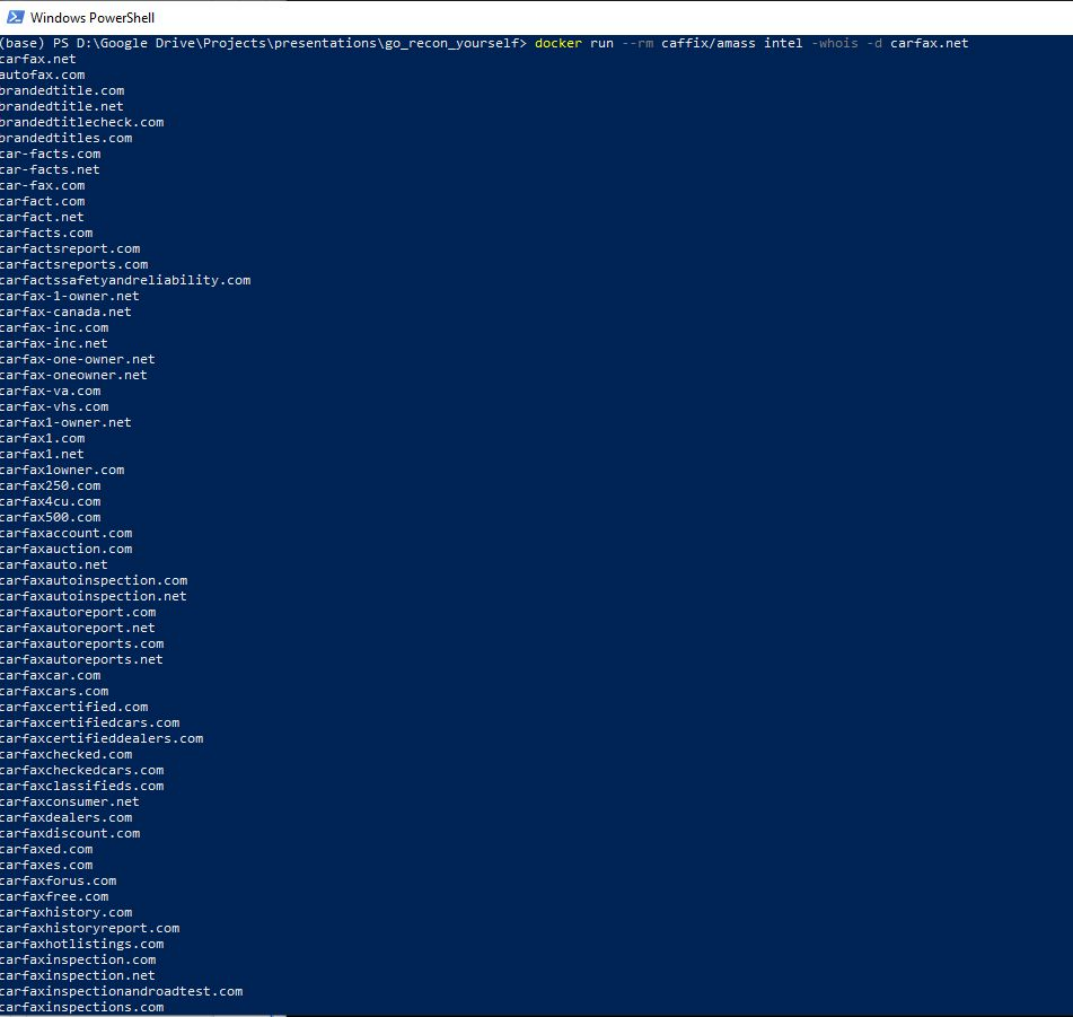
AMASS Commands

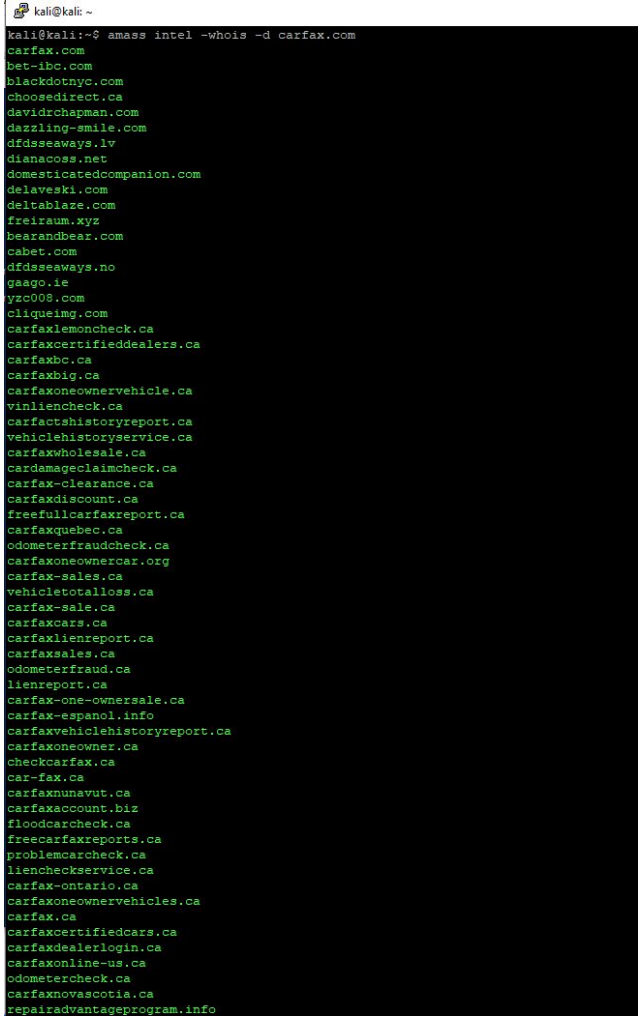
- intel
  - Gathers open source intelligence.
    i. WHOIS Data
  - Example
    i. `amass intel -whois -d [target_domain]`
- enum
  - Enumerates DNS and network maps systems that are exposed to the internet.
  - Example
    i. `amass enum -d [target_domain]`
- viz
  - Create network graph visualizations
  - HTML, Maltego, Graphistry
  - Example
    i. `amass viz -d3 -d [target_domain]`
- db
  - Manages the databases storing enumeration information.
  - Example
    i. `amass db -show -ip -d [target_domain]`
- track
  - Compares the results of multiple targets.
  - Good for global organizations and multiple domains.
    - `amass track -df [target_domains].txt`

GxC

1. AMASS Intel (using docker)

- Gather WHOIS data against the target
  - Windows + Docker
    - `docker run -rm caffix/amass intel -whois -d example.com`
  - Using the binary (Windows, Linux, Mac)
    - `amass intel -whois -d example.com`


Windows PowerShell
(base) PS D:\Google Drive\Projects\presentations\go_recon_yourself> docker run --rm caffix/amass intel -whois -d carfax.net
carfax.net
autofax.com
brandedtitle.com
brandedtitle.net
brandedtitlecheck.com
brandedtitles.com
car-facts.com
car-facts.net
car-fax.com
carfact.com
carfact.net
carfacts.com
carfactsreport.com
carfactsreports.com
carfactssafetyandreliability.com
carfax-1-owner.net
carfax-canada.net
carfax-inc.com
carfax-inc.net
carfax-one-owner.net
carfax-oneowner.net
carfax-va.com
carfax-vhs.com
carfax1-owner.net
carfax1.com
carfax1.net
carfax1owner.com
carfax250.com
carfax4cu.com
carfax500.com
carfaxaccount.com
carfaxauction.com
carfaxauto.net
carfaxautoinspection.com
carfaxautoinspection.net
carfaxautoreport.com
carfaxautoreport.net
carfaxautoreports.com
carfaxautoreports.net
carfaxcar.com
carfaxcars.com
carfaxcertified.com
carfaxcertifiedcars.com
carfaxcertifieddealers.com
carfaxchecked.com
carfaxcheckedcars.com
carfaxclassifieds.com
carfaxconsumer.net
carfaxdealers.com
carfaxdiscount.com
carfaxed.com
carfaxes.com
carfaxforus.com
carfaxfree.com
carfaxhistory.com
carfaxhistoryreport.com
carfaxhotlistings.com
carfaxinspection.com
carfaxinspection.net
carfaxinspectionandroadtest.com
carfaxinspections.com


kali@kali: ~
kali@kali:~$ amass intel -whois -d carfax.com
carfax.com
bet-ibc.com
blackdotnyc.com
choosedirect.ca
davidrchapman.com
dazzling-smile.com
dfdsseaways.lv
dianacoss.net
domesticatedcompanion.com
delaveski.com
deltablaze.com
freiraum.xyz
bearandbear.com
cabet.com
dfdsseaways.no
gaago.ie
yzc008.com
cliqueimg.com
carfaxlemoncheck.ca
carfaxcertifieddealers.ca
carfaxbc.ca
carfaxbig.ca
carfaxoneownervehicle.ca
vinliencheck.ca
carfactshistoryreport.ca
vehiclehistoryservice.ca
carfaxwholesale.ca
cardamageclaimcheck.ca
carfax-clearance.ca
carfaxdiscount.ca
freefullcarfaxreport.ca
carfaxquebec.ca
odometerfraudcheck.ca
carfaxoneownercar.org
carfax-sales.ca
vehicletotalloss.ca
carfax-sale.ca
carfaxcars.ca
carfaxlienreport.ca
carfaxsales.ca
odometerfraud.ca
lienreport.ca
carfax-one-ownersale.ca
carfax-espanol.info
carfaxvehiclehistoryreport.ca
carfaxoneowner.ca
checkcarfax.ca
car-fax.ca
carfaxnunavut.ca
carfaxaccount.biz
floodcarcheck.ca
freecarfaxreports.ca
problemcarcheck.ca
lienscheckservice.ca
carfax-ontario.ca
carfaxoneownervehicles.ca
carfax.ca
carfaxcertifiedcars.ca
carfaxdealerlogin.ca
carfaxonline-us.ca
odometercheck.ca
carfaxnovascotia.ca
repairadvantageprogram.info

GxC

2. AMASS Enumeration (using docker)

- Enumerate the public Network data
  - `docker run -rm caffix/amass enum -d example.com`
  - `amass enum -d example.com`

Windows PowerShell

```
(base) PS D:\Google Drive\Projects\presentations\go_recon_yourself> docker run --rm caffix/amass enum -d carfax.net -timeout 30
meet.carfax.net
proxy.carfax.net
v-fw-vpn-1.carfax.net
expe.carfax.net
revproxy.carfax.net
pocreports.carfax.net
selfservice.carfax.net
dam.carfax.net
finance-services.carfax.net
pocimobile.carfax.net
imobile.carfax.net
reports.carfax.net
alpha-price-plan-services.carfax.net
betaimobile.carfax.net
brochure.carfax.net
_collab-edge._tls.carfax.net
alpha-crmlistener.carfax.net
price-plan-services.carfax.net
jamf.carfax.net
employees.carfax.net
beta-price-plan-services.carfax.net
alpha-finance-services.carfax.net
crmlistener.carfax.net
internal-redirect-d.carfax.net
beta-crmlistener.carfax.net
_sips._tcp.carfax.net
exteam.carfax.net
rememberme-d.carfax.net
beta-finance-services.carfax.net
jamfshare.carfax.net
a-fw-vpn-1.carfax.net
beta-summary-services.carfax.net
live.carfax.net
myshare.carfax.net
alpha-company-services.carfax.net
beta-rememberme.carfax.net
imobile-d.carfax.net
rememberme.carfax.net
adfs.carfax.net
company-services.carfax.net
airwatch.carfax.net
alpha-summary-services.carfax.net
mydesktop.carfax.net
webim.carfax.net
betamymail.carfax.net
betareports.carfax.net
vpn-va2.carfax.net
dev.imobile.carfax.net
dialin.carfax.net
summary-services.carfax.net
stagingdam.carfax.net
liveav.carfax.net
vpn-mo.carfax.net
carfax.net
vidyo.carfax.net
five9recs.carfax.net
stagingemployees.carfax.net
dvlpimobile-f.carfax.net
ctmweb.carfax.net
dvlpimobile.carfax.net
workspace.carfax.net
pass-f.carfax.net.carfax.net
beta-rememberme-d.carfax.net
internal-redirect-f.carfax.net
www.carfax.net
okta.carfax.net
pass.carfax.net
vpn-va.carfax.net
pass-f.carfax.net
beta-company-services.carfax.net
coderepo.carfax.net
analytics.carfax.net
quote.cloud.carfax.net
foxnet.carfax.net
catalog.cloud.carfax.net
quote-alpha.cloud.carfax.net
update.carfax.net
catalog-beta.cloud.carfax.net
confluence-dev.carfax.net
landscape.carfax.net
```

```
OWASP Amass v3.18.3                                https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
86 names discovered - scrape: 9, dns: 9, cert: 14, archive: 6, api: 48
--------------------------------------------------------------------------------
ASN: 62723 - ACTUAL-AS - Actualize Tech, LLC
        166.90.97.0/24          25   Subdomain Name(s)
        64.157.165.0/24         2    Subdomain Name(s)
        64.193.21.0/24          4    Subdomain Name(s)
        139.60.112.0/24         1    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        108.156.120.0/21        4    Subdomain Name(s)
        13.226.26.0/23          4    Subdomain Name(s)
        15.197.192.0/20         1    Subdomain Name(s)
        35.160.0.0/13           1    Subdomain Name(s)
        35.80.0.0/12            2    Subdomain Name(s)
        54.70.0.0/15            1    Subdomain Name(s)
        34.208.0.0/12           1    Subdomain Name(s)
        13.225.220.0/22         4    Subdomain Name(s)
        3.33.240.0/20           1    Subdomain Name(s)
        44.224.0.0/11           5    Subdomain Name(s)
        54.68.0.0/15            1    Subdomain Name(s)
        52.24.0.0/14            1    Subdomain Name(s)
        108.159.224.0/21        4    Subdomain Name(s)
ASN: 62 - CYRS - CyrusOne LLC
        216.117.105.0/24        5    Subdomain Name(s)
        216.117.25.0/24         28   Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        23.20.0.0/14            3    Subdomain Name(s)
        18.204.0.0/14           2    Subdomain Name(s)
        18.232.0.0/14           1    Subdomain Name(s)
        54.237.0.0/16           2    Subdomain Name(s)
        3.208.0.0/12            2    Subdomain Name(s)
        52.86.0.0/15            1    Subdomain Name(s)
ASN: 8075 - MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation
        52.224.0.0/11           1    Subdomain Name(s)
```

GxC

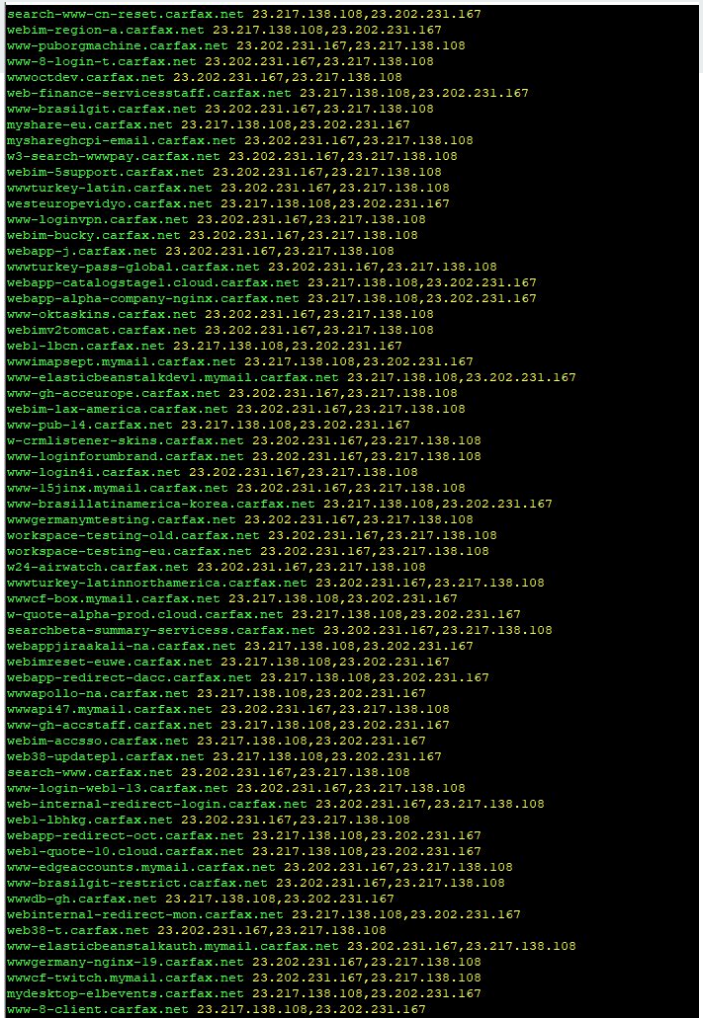
```
kali@kali:~$ amass enum -d carfax.net -json carfax_net.json -timeout 30
ctmweb.carfax.net
vpn-mo.carfax.net
expe.carfax.net
proxy.carfax.net
stagingdam.carfax.net
price-plan-services.carfax.net
revproxy.carfax.net
alpha-crmlistener.carfax.net
finance-services.carfax.net
crmlistener.carfax.net
reports.carfax.net
betaimobile.carfax.net
brochure.carfax.net
pocreports.carfax.net
beta-price-plan-services.carfax.net
okta-f.carfax.net
internal-redirect-f.carfax.net
adfs.carfax.net
beta-rememberme-d.carfax.net
www-pub9-mon.carfax.net
selfservice.carfax.net
dialin.carfax.net
webim-accengine.carfax.net
pocimobile.carfax.net
pass-f.carfax.net
five9recs.carfax.net
beta-crmlistener.carfax.net
internal-redirect-d.carfax.net
workspace.carfax.net
dam.carfax.net
w3-wwwpay-loadbalancer.carfax.net
mydesktop-staging-merchjeurope.carfax.net
dev.imobile.carfax.net
live.carfax.net
mydesktop.carfax.net
analytics.carfax.net
wwwpay-w2.carfax.net
airwatch.carfax.net
webim.carfax.net
internal-redirect.carfax.net
meet.carfax.net
vidyo.carfax.net
alpha-summary-services.carfax.net
www-jamfshare-repoengine-brasil.carfax.net
summary-services.carfax.net
okta.carfax.net
imobile.carfax.net
dvlpimobile-f.carfax.net
rememberme-d.carfax.net
landscape.carfax.net
beta-finance-services.carfax.net
catalog-alpha.cloud.carfax.net
quote.cloud.carfax.net
employees.carfax.net
coderepo.carfax.net
wwwfirewallsearchpriv.carfax.net
alpha-finance-services.carfax.net
pass-f.carfax.net.carfax.net
imobile-d.carfax.net
```

```
OWASP Amass v3.16.0                                https://github.com/OWASP/Amass
-------------------------------------------------------------------------------
136 names discovered - archive: 9, api: 34, cert: 26, alt: 55, scrape: 1, dns: 11
-------------------------------------------------------------------------------
ASN: 8075 - MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation
       52.224.0.0/11            1    Subdomain Name(s)
ASN: 62723 - ACTUAL-AS - Actualize Tech, LLC
       139.60.112.0/24          1    Subdomain Name(s)
       64.193.21.0/24           3    Subdomain Name(s)
       166.90.97.0/24           23   Subdomain Name(s)
       64.157.165.0/24          2    Subdomain Name(s)
ASN: 16509 - AMAZON-IAD - Amazon Data Services NoVa
       54.70.0.0/15             1    Subdomain Name(s)
       54.68.0.0/15             1    Subdomain Name(s)
       35.80.0.0/12             2    Subdomain Name(s)
       13.227.36.0/22           3    Subdomain Name(s)
       3.33.128.0/17            1    Subdomain Name(s)
       15.197.128.0/17          1    Subdomain Name(s)
       54.230.248.0/21          4    Subdomain Name(s)
       34.208.0.0/12            1    Subdomain Name(s)
       35.160.0.0/13            1    Subdomain Name(s)
       18.66.192.0/24           4    Subdomain Name(s)
       54.192.48.0/20           4    Subdomain Name(s)
       52.24.0.0/14             1    Subdomain Name(s)
       44.224.0.0/11            5    Subdomain Name(s)
ASN: 19384 - GRAMTEL001
       216.117.0.0/18           26   Subdomain Name(s)
ASN: 62 - CONE CyrusOne, TX USA - CyrusOne - Proxy for Customer
       216.117.105.0/24         6    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
       54.144.0.0/14            52   Subdomain Name(s)
       3.208.0.0/12             3    Subdomain Name(s)
       18.204.0.0/14            3    Subdomain Name(s)
       52.20.0.0/14             4    Subdomain Name(s)
       54.84.0.0/15             1    Subdomain Name(s)
       52.200.0.0/13            2    Subdomain Name(s)
       3.224.0.0/12             4    Subdomain Name(s)
       54.160.0.0/14            1    Subdomain Name(s)
       44.192.0.0/11            1    Subdomain Name(s)
       18.208.0.0/13            1    Subdomain Name(s)
       18.232.0.0/14            1    Subdomain Name(s)
       52.86.0.0/15             1    Subdomain Name(s)
       54.90.0.0/15             2    Subdomain Name(s)
       54.156.0.0/14            1    Subdomain Name(s)
       23.20.0.0/14             3    Subdomain Name(s)
       54.237.0.0/16            3    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

GxC

2. AMASS Database (using docker)

- Enumerate the public Network data
  - `docker run -rm caffix/amass db -show -ip -d example.com`
  - `amass db -show -ip -d example.com`


search-www-cn-reset.carfax.net 23.217.138.108,23.202.231.167
webim-region-a.carfax.net 23.217.138.108,23.202.231.167
www-puborgmachine.carfax.net 23.202.231.167,23.217.138.108
www-8-login-t.carfax.net 23.202.231.167,23.217.138.108
wwwoctdev.carfax.net 23.202.231.167,23.217.138.108
web-finance-servicesstaff.carfax.net 23.217.138.108,23.202.231.167
www-brasilgit.carfax.net 23.202.231.167,23.217.138.108
myshare-eu.carfax.net 23.217.138.108,23.202.231.167
myshareghcpi-email.carfax.net 23.202.231.167,23.217.138.108
w3-search-wwwpay.carfax.net 23.202.231.167,23.217.138.108
webim-5support.carfax.net 23.202.231.167,23.217.138.108
wwwturkey-latin.carfax.net 23.202.231.167,23.217.138.108
westeuropevidyo.carfax.net 23.217.138.108,23.202.231.167
www-loginvpn.carfax.net 23.202.231.167,23.217.138.108
webim-bucky.carfax.net 23.202.231.167,23.217.138.108
webapp-j.carfax.net 23.202.231.167,23.217.138.108
wwwturkey-pass-global.carfax.net 23.202.231.167,23.217.138.108
webapp-catalogstagel.cloud.carfax.net 23.217.138.108,23.202.231.167
webapp-alpha-company-nginx.carfax.net 23.217.138.108,23.202.231.167
www-oktaskins.carfax.net 23.202.231.167,23.217.138.108
webimv2tomcat.carfax.net 23.202.231.167,23.217.138.108
web1-lbcn.carfax.net 23.217.138.108,23.202.231.167
wwwimapsept.mymail.carfax.net 23.217.138.108,23.202.231.167
www-elasticbeanstalkdev1.mymail.carfax.net 23.217.138.108,23.202.231.167
www-gh-acceurope.carfax.net 23.202.231.167,23.217.138.108
webim-lax-america.carfax.net 23.202.231.167,23.217.138.108
www-pub-14.carfax.net 23.217.138.108,23.202.231.167
w-crmlistener-skins.carfax.net 23.202.231.167,23.217.138.108
www-loginforumbrand.carfax.net 23.202.231.167,23.217.138.108
www-login4i.carfax.net 23.202.231.167,23.217.138.108
www-15jinx.mymail.carfax.net 23.202.231.167,23.217.138.108
www-brasillatinamerica-korea.carfax.net 23.217.138.108,23.202.231.167
wwwgermanymtesting.carfax.net 23.202.231.167,23.217.138.108
workspace-testing-old.carfax.net 23.202.231.167,23.217.138.108
workspace-testing-eu.carfax.net 23.202.231.167,23.217.138.108
w24-airwatch.carfax.net 23.202.231.167,23.217.138.108
wwwturkey-latinnorthamerica.carfax.net 23.202.231.167,23.217.138.108
wwwcf-box.mymail.carfax.net 23.217.138.108,23.202.231.167
w-quote-alpha-prod.cloud.carfax.net 23.217.138.108,23.202.231.167
searchbeta-summary-servicess.carfax.net 23.202.231.167,23.217.138.108
webappjiraakali-na.carfax.net 23.217.138.108,23.202.231.167
webimreset-euwe.carfax.net 23.217.138.108,23.202.231.167
webapp-redirect-dacc.carfax.net 23.217.138.108,23.202.231.167
wwwapollo-na.carfax.net 23.217.138.108,23.202.231.167
wwwapi47.mymail.carfax.net 23.202.231.167,23.217.138.108
www-gh-accstaff.carfax.net 23.217.138.108,23.202.231.167
webim-accsso.carfax.net 23.217.138.108,23.202.231.167
web38-updatepl.carfax.net 23.217.138.108,23.202.231.167
search-www.carfax.net 23.202.231.167,23.217.138.108
www-login-web1-13.carfax.net 23.202.231.167,23.217.138.108
web-internal-redirect-login.carfax.net 23.202.231.167,23.217.138.108
web1-lbhkg.carfax.net 23.202.231.167,23.217.138.108
webapp-redirect-oct.carfax.net 23.217.138.108,23.202.231.167
web1-quote-10.cloud.carfax.net 23.217.138.108,23.202.231.167
www-edgeaccounts.mymail.carfax.net 23.202.231.167,23.217.138.108
www-brasilgit-restrict.carfax.net 23.202.231.167,23.217.138.108
wwwdb-gh.carfax.net 23.217.138.108,23.202.231.167
webinternal-redirect-mon.carfax.net 23.217.138.108,23.202.231.167
web38-t.carfax.net 23.202.231.167,23.217.138.108
www-elasticbeanstalkauth.mymail.carfax.net 23.202.231.167,23.217.138.108
wwwgermany-nginx-19.carfax.net 23.202.231.167,23.217.138.108
wwwcf-twitch.mymail.carfax.net 23.202.231.167,23.217.138.108
mydesktop-elbevents.carfax.net 23.217.138.108,23.202.231.167
www-8-client.carfax.net 23.217.138.108,23.202.231.167

My favorite flags

- intel
  - -o
    - Outputs to a text file
  - Example
    - `docker run –rm caffix/amass intel -whois -d example.com -o example_WHOIS_com.txt`
    - `amass intel -whois -d [target_domain] -o example_WHOIS_com.txt`
- enum
  - -json [file.json] -o [file.txt]
    - Saves to json file.
  - Example
    - `docker run –rm caffix/amass enum -d example.com -json example_enum_com.json -o example_enum_com.txt`
    - `amass enum -d example.com -json example_enum_com.json -o example_enum_com.txt`

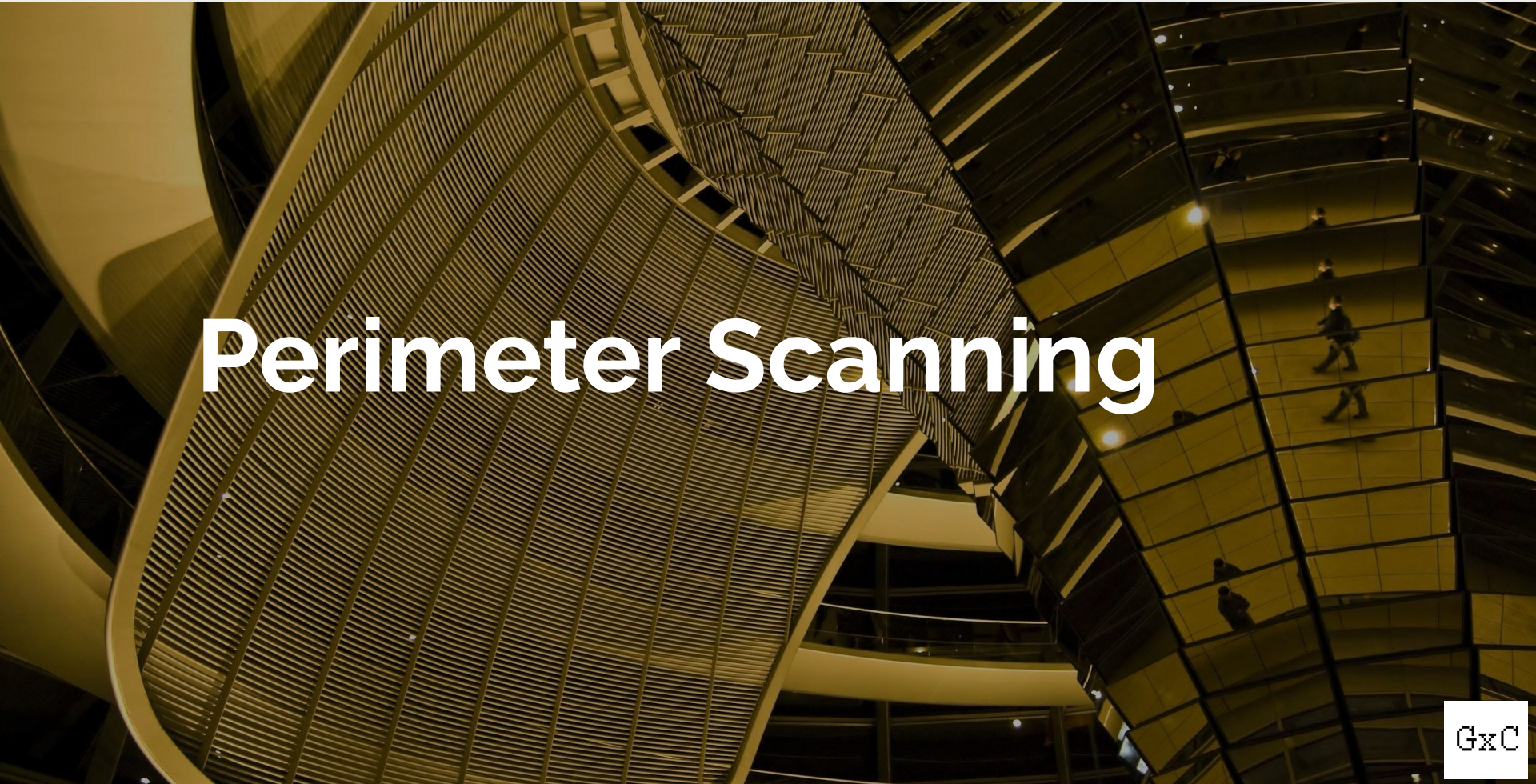
AMASS'ing yourself quickly (save this info):

- Using Docker
  - Run AMASS Intel command to gather the information and save to a text file.
    - `docker run -rm caffix/amass intel -whois -d example.com -o results.txt`
  - Run AMASS Enum, enumerate the domain, and save the information.
    - `docker run -rm caffix/amass enum -d example.com -json example_enum_com.json -o enum_example_com.txt`

Limitations

- Accuracy of data
  - Sometimes the data is not completely accurate.
  - What is live vs what is decommissioned?
- Slow
  - Data is scraped from a large amount of resources and consolidated into one place.
  - Need to add `-timeout` flag to every command invoked.
  - `docker run –rm caffix/amass enum -d example.com -json example_com.json -timeout 30`  *Minutes*
- No GUI
  - Easy to learn, but if someone is used to a GUI there is a bit of a learning curve.
- Risk Scoring
  - How do you risk score assets that may have compensating controls?

GxC


Perimeter Scanning

Recon Profile Check

1. Text file of WHOIS Intel domains in `example_whois_com.txt`
2. Enumerated services in our `example_com.json` file AND `example_enum_com.txt`

Paradigm

- Open source tool that analyzes discovered assets and reports if they are available to the public internet.
- Web UI that analyzes the enumeration JSON files you save from AMASS.
- Small risk scoring system that tells you what percentage of your discovered environment is open to the internet.
- https://github.com/jeredbare/paradigm

master · 4 branches · 0 tags · Go to file · Add file · Code

jeredbare update readme.md — f71a9a5 on Jul 21, 2021 — 55 commits

paradigm-ui	Bump postcss from 7.0.35 to 7.0.36 in /paradigm-ui	8 months ago
src	Update inetaccess.py	8 months ago
tests	Testing and repo organization	12 months ago
.gitignore	Added git ignore	12 months ago
README.md	update readme.md	8 months ago
docker-compose.yml	fixed docker network to talk between containers on docker-compose	12 months ago

README.md

Paradigm

About

Paradigm wanted to provide a web interface to parse the json file Amass outputs to json from the enumeration command. The tool will also go through the domain list and get the HTTP Status code of each domain. The 200 HTTP responses will then be calculated into a score and reported back to the user. Amass is an Open Source DNS Recon and Enumeration tool developed by the talented Jeff Foley. The user can then compare the results reported from the Amass json to the scanned JSON file. This tool is geared towards to those who may not feel comfortable with the commandline and/or would like an interface to see the json output.

Purpose

Paradigm provides an user interface to analyze the json output from `enum` command from Amass. The goal of this project is to notify Security and IT teams of assets they may not know is open to the internet. Hence, we've built in a scoring system to check the HTTP Response codes of all assets found from the `enum` command from Amass.

Why?

TLS everywhere is probably one of the greatest things to happen in the InfoSec and IT space. However, with the rise of cloud technologies TLS everywhere and automation means something a bit different in the environment. Engineers, developers, and any other IT team can spin up cloud assets within a matter of seconds and most public cloud assets have a registered TLD and associated TLS certificate. Sometimes team members will forget about assets open to the web and the goal of this tool is to discover those. You can use this just for more than cloud assets, but

determines what is actually accessible via the internet.

Readme
14 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Contributors 3

jeredbare Jered Bare
jstanford2013 Jordan
dependabot[bot]

Languages

TypeScript 46.7% · JavaScript 20.5% · Python 16.6% · CSS 13.1% · Dockerfile 3.1%

GxC

Paradigm Yourself

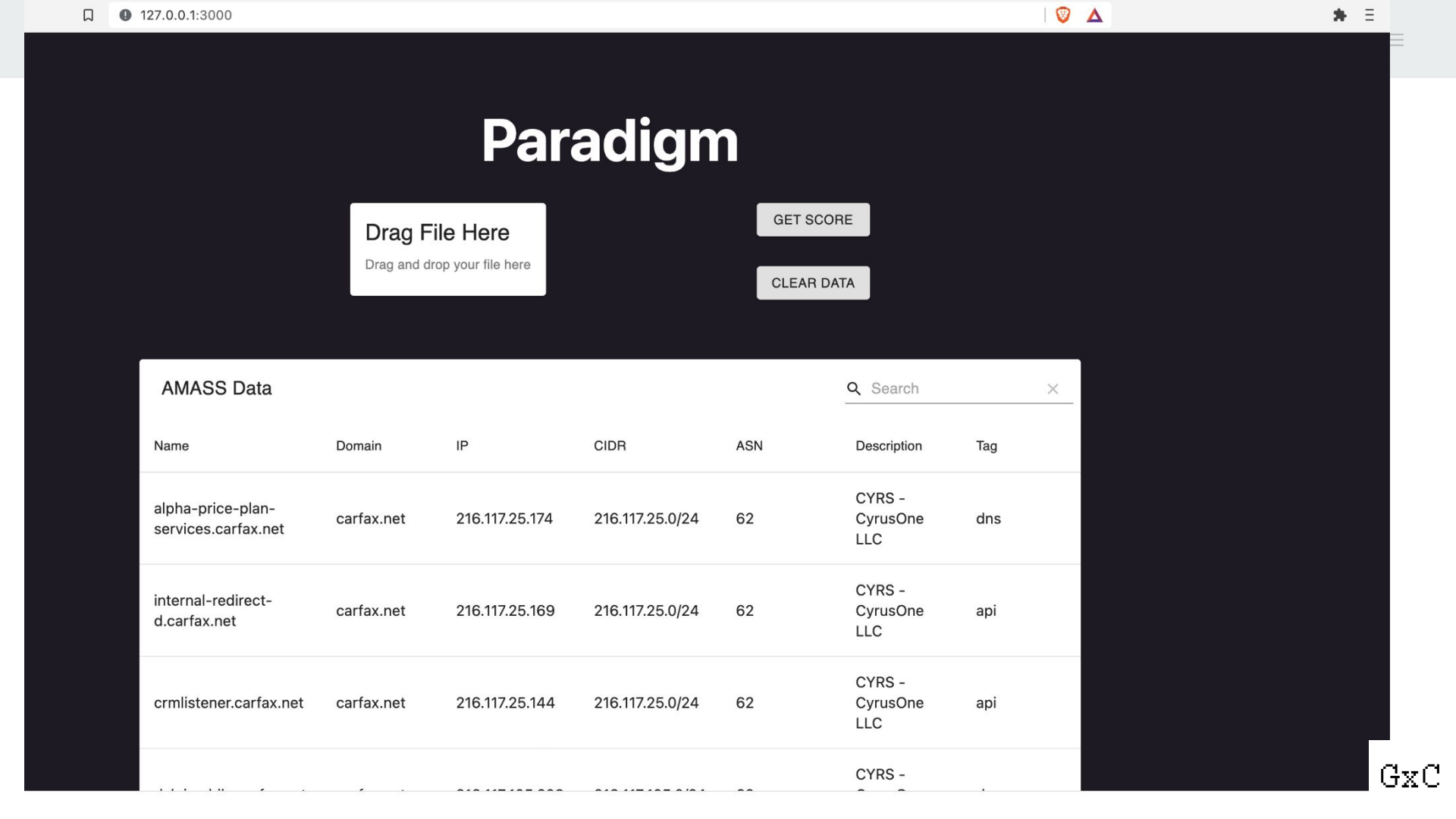
- Download and install Docker + docker-compose
  - https://docs.docker.com/get-docker/
- Download the repository
  - https://github.com/jeredbare/paradigm
- Build the container
  - Unzip the repository.
  - Go into that directory and run `docker-compose build`
- Running the container and navigate to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

```
(base) PS C:\Users\PC\Downloads\paradigm-master (3)\paradigm-master> docker-compose build
Building paradigm-ui
[+] Building 63.3s (12/12) FINISHED
 => [internal] load build definition from Dockerfile
 => => transferring dockerfile: 374B
 => [internal] load .dockerignore
 => => transferring context: 2B
 => [internal] load metadata for docker.io/library/node:alpine
 => [1/8] FROM docker.io/library/node:alpine@sha256:e4a152d1564f2e89d5fa46d74b9f5a050a601322aa10bc405a32faaf1085c5f0
 => => resolve docker.io/library/node:alpine@sha256:e4a152d1564f2e89d5fa46d74b9f5a050a601322aa10bc405a32faaf1085c5f0
 => => sha256:a9be95b9b1033aa59b5a5e538339f917c353199390d7ce8fb9e28ce99d17e429 2.34MB / 2.34MB
 => => sha256:8741045a91b18c4fb13f8d66bf6ff633167f6b1a0c99c53f3e5159f03bb394ee 450B / 450B
 => => sha256:e4a152d1564f2e89d5fa46d74b9f5a050a601322aa10bc405a32faaf1085c5f0 1.43kB / 1.43kB
 => => sha256:56d1a2b5d6d0e5927e567239b1762ac3aa1f0ddd3e95dc04b1c4bb8f8f4da06a 1.16kB / 1.16kB
 => => sha256:15c6163d954cb637f5f7af9752a393d1cdb14ad5f14f1745bdc3ecc342dea93f 6.58kB / 6.58kB
 => => sha256:3398e5f67ab61d75ec71ed8ab3226657e8ff8c3db169eb863957c3cbc8b6bdee 45.84MB / 45.84MB
 => => extracting sha256:3398e5f67ab61d75ec71ed8ab3226657e8ff8c3db169eb863957c3cbc8b6bdee
 => => extracting sha256:a9be95b9b1033aa59b5a5e538339f917c353199390d7ce8fb9e28ce99d17e429
 => => extracting sha256:8741045a91b18c4fb13f8d66bf6ff633167f6b1a0c99c53f3e5159f03bb394ee
 => [internal] load build context
 => => transferring context: 152.16kB
 => [2/8] RUN mkdir -p /usr/src/app
 => [3/8] WORKDIR /usr/src/app
 => [4/8] COPY ./paradigm-ui/package.json /usr/src/app
 => [5/8] COPY ./paradigm-ui/yarn.lock /usr/src/app
 => [6/8] RUN yarn install --production
 => [7/8] COPY ./paradigm-ui /usr/src/app
 => ERROR [8/8] RUN yarn build
------
 > [8/8] RUN yarn build:
#12 0.737 yarn run v1.22.18
#12 0.797 $ next build
#12 1.528 Browserslist: caniuse-lite is outdated. Please run:
#12 1.528 npx browserslist@latest --update-db
#12 1.528
#12 1.528 Why you should do it regularly:
#12 1.528 https://github.com/browserslist/browserslist#browsers-data-updating
#12 1.609 node:internal/errors:465
#12 1.609     ErrorCaptureStackTrace(err);
#12 1.609     ^
#12 1.609
#12 1.609 Error [ERR_PACKAGE_PATH_NOT_EXPORTED]: Package subpath './lib/parser' is not defined by "exports" in /usr/src/app/node_modules/next/node_modules/postcss/package.json
#12 1.609     at new NodeError (node:internal/errors:372:5)
#12 1.609     at throwExportsNotFound (node:internal/modules/esm/resolve:448:9)
#12 1.609     at packageExportsResolve (node:internal/modules/esm/resolve:727:3)
#12 1.609     at resolveExports (node:internal/modules/cjs/loader:482:36)
#12 1.609     at Function.Module._findPath (node:internal/modules/cjs/loader:522:31)
#12 1.609     at Function.Module._resolveFilename (node:internal/modules/cjs/loader:919:27)
#12 1.609     at Function.Module._load (node:internal/modules/cjs/loader:778:27)
#12 1.609     at Module.require (node:internal/modules/cjs/loader:999:19)
#12 1.609     at require (node:internal/modules/cjs/helpers:102:18)
#12 1.609     at Object.552 (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:11590)
#12 1.609     at __nccwpck_require__ (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:11735)
#12 1.609     at Object.270 (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:400)
#12 1.609     at __nccwpck_require__ (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:11735)
#12 1.609     at Object.327 (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:260)
#12 1.609     at __nccwpck_require__ (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:11735)
#12 1.609     at Object.845 (/usr/src/app/node_modules/next/dist/compiled/postcss-scss/scss-syntax.js:1:3733) {
#12 1.609   code: 'ERR_PACKAGE_PATH_NOT_EXPORTED'
#12 1.609 }
#12 1.609
#12 1.609 Node.js v17.8.0
#12 1.629 error Command failed with exit code 1.
#12 1.629 info Visit https://yarnpkg.com/en/docs/cli/run for documentation about this command.
------
executor failed running [/bin/sh -c yarn build]: exit code: 1
ERROR: Service 'paradigm-ui' failed to build : Build failed
(base) PS C:\Users\PC\Downloads\paradigm-master (3)\paradigm-master> docker-compose up
Recreating paradigm-master_paradigm-ui_1 ... done
Recreating paradigm-master_paradigm_1    ... done
Attaching to paradigm-master_paradigm_1, paradigm-master_paradigm-ui_1
paradigm-ui_1  | yarn run v1.22.5
paradigm-ui_1  | $ next start
paradigm_1     |  * Environment: production
paradigm_1     |    WARNING: This is a development server. Do not use it in a production deployment.
paradigm_1     |    Use a production WSGI server instead.
paradigm_1     |  * Debug mode: off
paradigm_1     |  * Running on all addresses.
paradigm_1     |    WARNING: This is a development server. Do not use it in a production deployment.
paradigm_1     |  * Running on http://172.20.0.3:5000/ (Press CTRL+C to quit)
paradigm-ui_1  | ready - started server on 0.0.0.0:3000, url: http://localhost:3000
paradigm-ui_1  | info  - Using webpack 4. Reason: future.webpack5 option not enabled https://nextjs.org/docs/messages/webpack5
```

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
CYRS -

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	----

GxC

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

GxC

Paradigm Limitations

- Buggy
  - Application will crash with a properly formatted JSON file.
  - Have to upload files saved from `amass enum -d [target_domain] -json [target_domain].json`
- Risk Score does not account for compensating controls
  - Every domain available to the internet is not a risk.

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.

GxC

NMAP Commands – Scanning Yourself

- Scanning a Single IP
  - `nmap -sV -A -T4 192.168.1.2`
- Scanning a CIDR Block
  - `nmap -sV -A -T4 192.168.1.0/24`
- Scanning a FQDN
  - `nmap -sV -A -T4 scanme.nmap.org`

```
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
```

GxC

NMAP Commands – Scanning The Perimeter

- Scanning a Single IP
  - `nmap -sV -A -T4 192.168.1.2`
- Scanning a CIDR Block
  - `nmap -sV -A -T4 192.168.1.0/24`
- Scanning a FQDN
  - `nmap -sV -A -T4 scanme.nmap.org`
- Scan a list of targets (importing our Recon evidence)
  - `nmap -sV -A -T4 -iL example_enum_com.txt`

```
kali@kali:~$ vi carfax_enum_net.txt
kali@kali:~$ cat carfax_enum_net.txt
carfactreport.com
carfax-slovenia.com
carfaxdriveradvisor.org
carfaxkroatia.info
carfaxcars.com
carfaxconnections.info
carfaxdriveradvisor.info
carfaxhistorybasedprice.com
carfax4salebyowner.net
carfaxadvantage.com
carfaxautofinance.com
carfaxoneownervehicles.info
carfaxcustom.org
carfaxmembership.com
carfaxnewbrunswick.com
carfaxoneownervehicle.us
carfaxonline-us.com
carfax-italy.us
carfax-sale.us
carfaxlownersale.net
carfaxforowners.com
carfaxmembership.org
carfax-latvia.us
carfax-lithuania.info
carfax-poland.biz
carfaxadvantage.net
carfaxcanada.net
carfax-one-ownersale.us
carfax-portugal.com
carfaxczech-republic.org
carfax-reports.com
carfaxluxembourg.biz
carcheck.biz
carfax-sweden.org
carfaxconnexion.com
carfaxnorthamerica.info
carfaxl-ownercar.com
carfaxautoinspection.info
carfax-oneowner.ca
carfaxessentials.com
carfaxitaly.org
carfaxlithuania.biz
carfaxfsbo.net
carfaxnorway.com
carfaxmobile.info
carfax-hungary.com
carfax4salebyowner.info
carfaxonlien.com
carfax-europe.us
carfaxaccount.com
carfaxlownercar.us
```

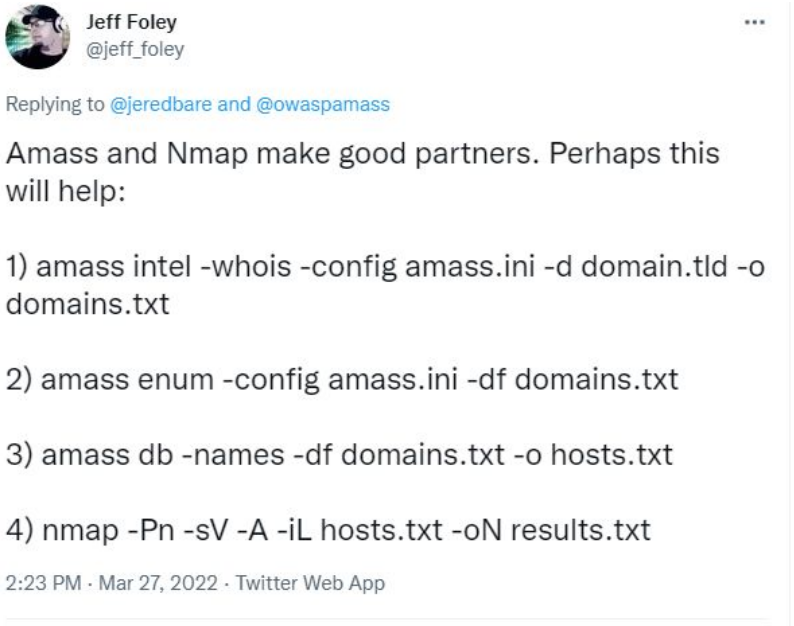
```
# Nmap 7.92 scan initiated Sat Mar 26 18:16:17 2022 as: nmap -sV -A -T4 -iL carfax_net.txt -oN carfax_net_results_portscan.txt
Nmap scan report for carfax.io (216.117.25.99)
Host is up (0.045s latency).
rDNS record for 216.117.25.99: redirect.gslb.carfax.com
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE    SERVICE    VERSION
80/tcp   open     http-proxy F5 BIG-IP load balancer http proxy
|_http-server-header: BigIP
|_http-title: Did not follow redirect to https://www.carfax.com
|_http-open-proxy: Proxy might be redirecting requests
161/tcp  filtered snmp
443/tcp  open     ssl/https?
| ssl-cert: Subject: commonName=*.carfax.com/organizationName=Carfax, Inc./stateOrProvinceName=Virginia/countryName=US
| Subject Alternative Name: DNS:*.carfax.com, DNS:carfax.com
| Not valid before: 2022-03-03T00:00:00
|_Not valid after:  2023-03-31T23:59:59
|_ssl-date: ERROR: Script execution failed (use -d to debug)
5431/tcp filtered park-agent
Service Info: Device: load balancer

Nmap scan report for carfaxnorthamerica.com (216.117.25.99)
Host is up (0.045s latency).
rDNS record for 216.117.25.99: redirect.gslb.carfax.com
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE    SERVICE    VERSION
80/tcp   open     http-proxy F5 BIG-IP load balancer http proxy
|_http-title: Did not follow redirect to https://www.carfax.com
|_http-server-header: BigIP
|_http-open-proxy: Proxy might be redirecting requests
161/tcp  filtered snmp
443/tcp  open     ssl/https?
| ssl-cert: Subject: commonName=*.carfax.com/organizationName=Carfax, Inc./stateOrProvinceName=Virginia/countryName=US
| Subject Alternative Name: DNS:*.carfax.com, DNS:carfax.com
| Not valid before: 2022-03-03T00:00:00
|_Not valid after:  2023-03-31T23:59:59
|_ssl-date: TLS randomness does not represent time
5431/tcp filtered park-agent
Service Info: Device: load balancer

Nmap scan report for carfaxforinsurers.com (216.117.25.99)
Host is up (0.045s latency).
rDNS record for 216.117.25.99: redirect.gslb.carfax.com
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE    SERVICE    VERSION
80/tcp   open     http-proxy F5 BIG-IP load balancer http proxy
|_http-server-header: BigIP
|_http-title: Did not follow redirect to https://www.carfaxforinsurers.com
|_http-open-proxy: Proxy might be redirecting requests
161/tcp  filtered snmp
443/tcp  open     ssl/https?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.carfax.com/organizationName=Carfax, Inc./stateOrProvinceName=Virginia/countryName=US
| Subject Alternative Name: DNS:*.carfax.com, DNS:carfax.com
| Not valid before: 2022-03-03T00:00:00
|_Not valid after:  2023-03-31T23:59:59
5431/tcp filtered park-agent
Service Info: Device: load balancer

Nmap scan report for carfaxoneownersale.net (216.117.25.99)
Host is up (0.045s latency).
rDNS record for 216.117.25.99: redirect.gslb.carfax.com
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE    SERVICE    VERSION
"carfax_net_results_portscan.txt" 21565L, 994861B
```

GxC

NMAP Commands – Adding to our Recon Profile

- Scanning a Single IP
  - `nmap -sV -A -T4 192.168.1.2`
- Scanning a CIDR Block
  - `nmap -sV -A -T4 192.168.1.0/24`
- Scanning a FQDN
  - `nmap -sV -A -T4 scanme.nmap.org`
- Scan a list of targets (importing our Recon evidence)
  - `nmap -sV -A -T4 -iL example_com.txt`
- Saving the port scan results
  - `nmap -sV -A -T4 -iL example_com.txt -oN example_com_results.txt`

NMAP Commands – Adding to our Recon Profile



Jeff Foley
@jeff_foley

Replying to @jeredbare and @owaspamass

Amass and Nmap make good partners. Perhaps this will help:

1) amass intel -whois -config amass.ini -d domain.tld -o domains.txt

2) amass enum -config amass.ini -df domains.txt

3) amass db -names -df domains.txt -o hosts.txt

4) nmap -Pn -sV -A -iL hosts.txt -oN results.txt

2:23 PM · Mar 27, 2022 · Twitter Web App

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.

Recon Profile Check

1. Text file of WHOIS Intel domains in `example_whois_com.txt`
2. Enumerated services in our `example_com.json` file AND `example_enum_com.txt`
3. We know which domains respond to GET requests (200 Code)
4. Ports scanned by NMAP and saved in `example_com_results.txt`

Nikto – Scanning the Perimeter (Web Apps)

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

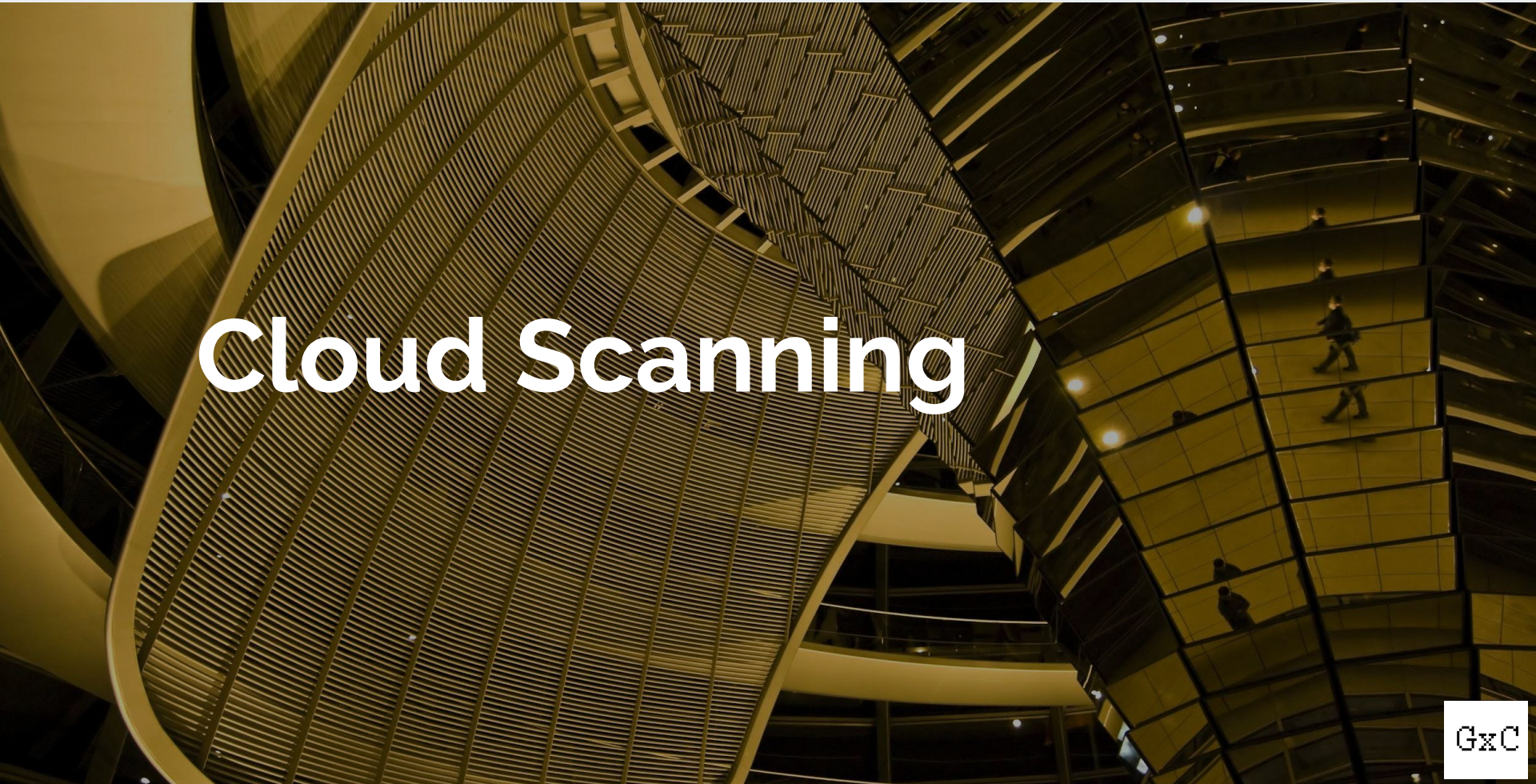
GxC

```
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).
```

GxC

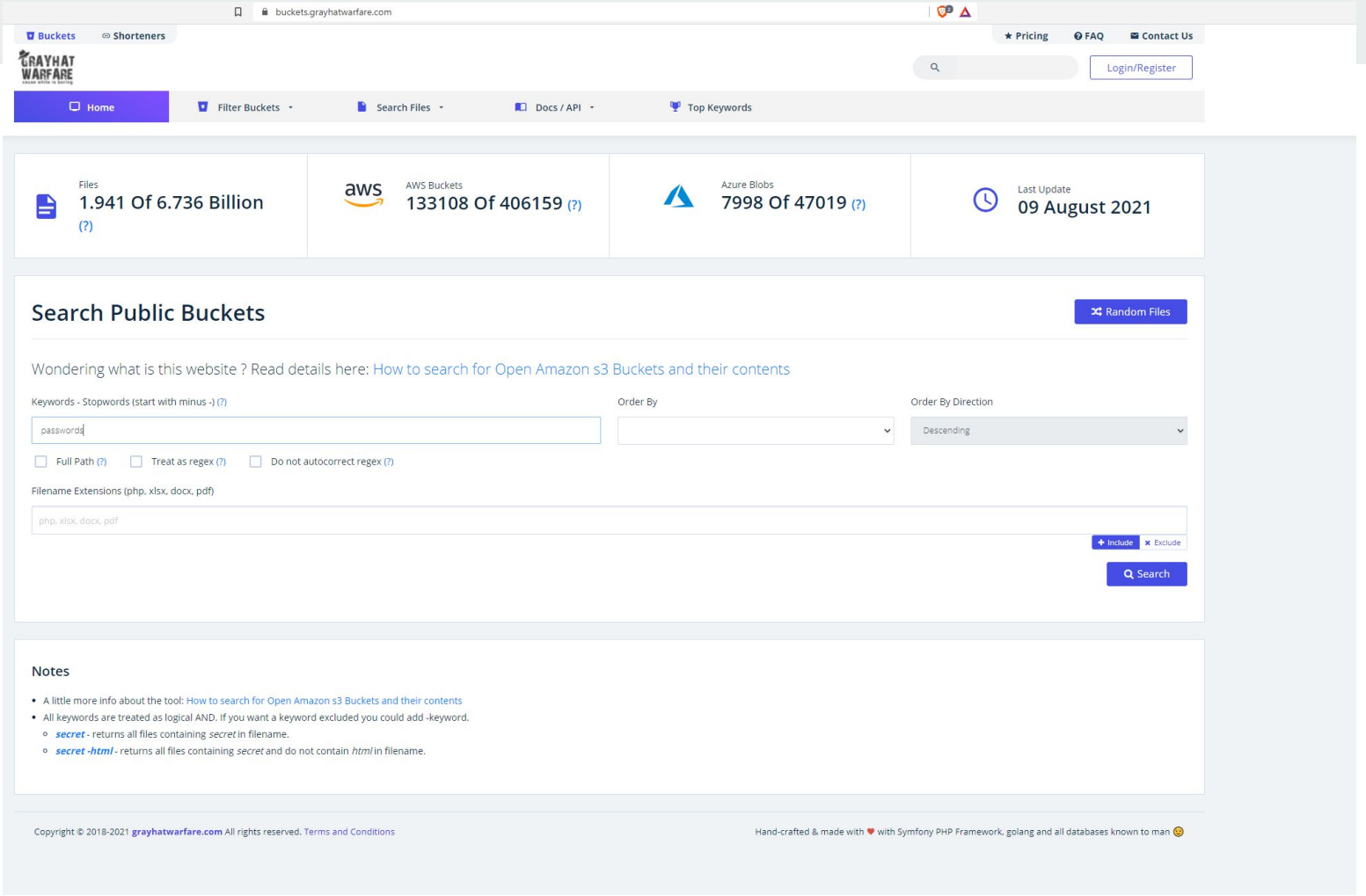
Nikto – Limitations

- 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.


Cloud Scanning

GrayHat Warfare - Cloud Recon

- 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
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.
Copyright © 2018-2021 grayhatwarfare.com All rights reserved. Terms and Conditions
Hand-crafted & made with ♥ with Symfony PHP Framework, golang and all databases known to man

GxC

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

GxC

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

GxC

GrayHat Warfare - Limitations

- Cost some money.
- Only looks for certain misconfigured items and ignores different tech stacks.
  - Serverless
  - Lamda
- Limited query searches

Recon Profile Check

1. Text file of WHOIS Intel domains in `example_whois_com.txt`
2. Enumerated services in our `example_com.json` file AND `example_enum_com.txt`
3. Ports scanned by NMAP and saved in `example_com_results.json`
4. Scanned our web applications for vulnerabilities (if any).
5. Determined our cloud assets that may be misconfigured.

GxC


Monitoring

Shodan – Monitoring your External Assets

- 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

GxC

SHODAN | Explore | Downloads | Pricing | "VCenter"

TOTAL RESULTS

5,134

TOP COUNTRIES

United States	812
Korea, Republic of	452
France	359
China	352
Germany	331

More...

TOP PORTS

443	2,867
389	616
636	560
9443	197
135	167

More...

TOP ORGANIZATIONS

Asia Pacific Network Information Centre	357
Hetzner Online GmbH	174
OVH SAS	106
Jumpline Inc	67
SoftLayer Technologies, Inc.	57

More...

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

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

" + ID_VC_Welcome + "

54.38.205.93
ip93.ip-54-38-205.eu
spolka jawna Technivo
Poland, Warsaw

SSL Certificate
Issued By:
|- Common Name:
CA
|- Organization:
ip93.ip-54-38-205.eu
Issued To:
|- Common Name:
ip93.ip-54-38-205.eu
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
date: Sat, 26 Mar 2022 19:51:01 GMT
content-security-policy: upgrade-insecure-requests
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-servi...
```

" + ID_VC_Welcome + "

54.38.99.165
vcenter.esx01.alx.host
ip165.ip-54-38-99.eu
ALIXANS Service Technique
France, Paris

SSL Certificate
Issued By:
|- Common Name:
CA
|- Organization:
vcenter.esx01.alx.host
Issued To:
|- Common Name:
vcenter.esx01.alx.host
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Date: Sat, 26 Mar 2022 19:46:34 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: 4251
...
```

" + ID_VC_Welcome + "

103.139.103.61
vcsa7.easternsun.vn
VietNam Eastern Sun Joint Stock Company
Viet Nam, Ho Chi Minh City

SSL Certificate
Issued By:
|- Common Name:
CA
|- Organization:
vcsa7.easternsun.vn
Issued To:
|- Common Name:
vcsa7.easternsun.vn
Supported SSL Versions:

```
HTTP/1.1 200 OK
date: Sun, 27 Mar 2022 02:44:56 GMT
content-security-policy: upgrade-insecure-requests
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-servi...
```

GxC

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

GxC

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 2021-
lfbn-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
```

Windows Download AP. 2021-
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
```

217.235.255.50 2021-
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
```

84.236.16.6 2021-
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
```

78.199.73.88 2021-
piq63-2_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
```

140.114.36.128 2021-
pc128.stat.nthu.edu.tw
Ministry of Education Computer Centerm12F, 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
```

5.187.151.118 2021-
05BB9776.catv.pool.telekom.hu
Magyar Telekom plc.
Hungary, Gyál

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

GxC

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:Springfield -- 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]

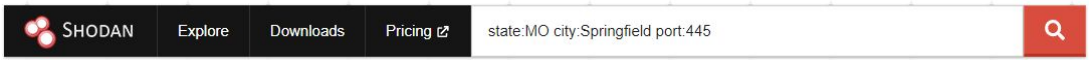
screenshot.label:ics -- Can be a [string] and/or [float]

state:"MO"

GxC

Shodan – Let's apply it locally – Apologies ahead of time

- Let's find all the servers that have SMB1 enabled.
- Filters we're using
  - state, city, port
  - Our query
    - state:MO city:Springfield port:445



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

TOTAL RESULTS

42

TOP ORGANIZATIONS

[redacted] 2

[redacted] 2

[redacted] 2

More...

TOP PRODUCTS

Samba	4
smbx	1

TOP OPERATING SYSTEMS

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

More...

View Report | Download Results | Historical Trend | View on Map

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

[redacted]
Joe's Datacenter, LLC
United States, Springfield

2022-03-26T13:43:08.945960

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2012 R2 Datacenter 9600
  Software: Windows Server 2012 R2 Datacenter 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]
SpringNet
United States, Springfield

2022-03-26T13:00:51.068426

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Server 2012 R2 Standard 9600
  Software: Windows Server 2012 R2 Standard 6.3
  Capabilities: dfs, 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]
jamkinggr.com
mail.jamkinggr.com
Critical Hosting, Inc
United States, Springfield

2022-03-26T01:22:54.013304

```
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]
SpringNet
United States, Springfield

2022-03-26T00:37:10.378138

```
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, 3015.11.5_1))
```

[redacted]
Joe's Datacenter, LLC
United States, Springfield

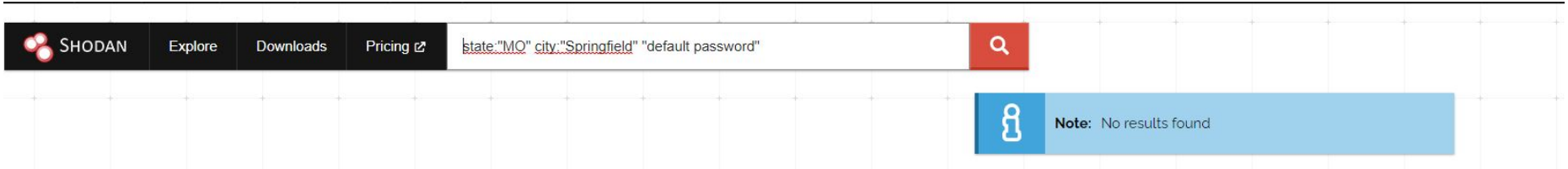
2022-03-25T16:29:43.001804

```
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
```

GxC

Shodan – Let's apply it locally – Apologies ahead of time

- Let's find all the servers that have a default password locally
- Filters we're using
  - state, city, [string]
  - Our query
    - state:"MO" city:"Springfield" "default password"



GxC

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

TOTAL RESULTS

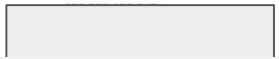
2

TOP PORTS

23	1
8081	1

View Report | Download Results | View on Map

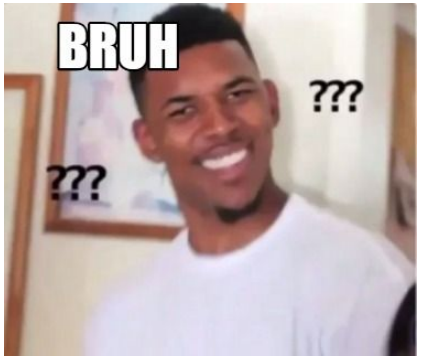
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor



```
[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....
```


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

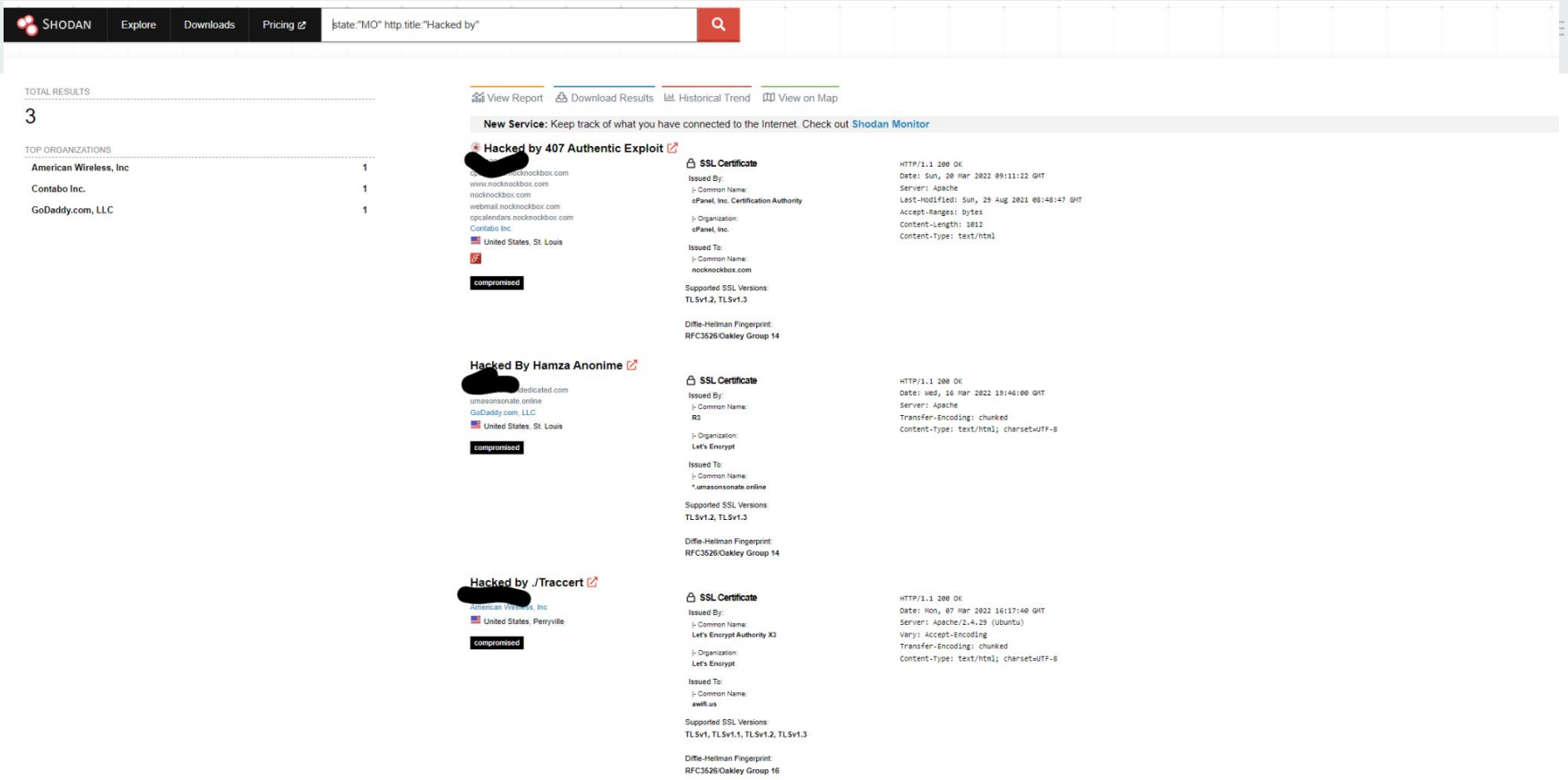
Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "password".
Please change them immediately.
The ethernet 0/1 interface is enabled with an address of 10.10....



GxC

Shodan – Let's apply it locally – Apologies ahead of time

- Let's find all the servers that have potentially been hacked in the state of Missouri.
- Filters we're using
  - state, http.title
  - Our query
    - state:"MO" http.title:"hacked by"


SHODAN
Explore
Downloads
Pricing
state:"MO" http.title:"Hacked by"
TOTAL RESULTS
3
TOP ORGANIZATIONS
American Wireless, Inc 1
Contabo Inc. 1
GoDaddy.com, LLC 1
View Report
Download Results
Historical Trend
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
Hacked by 407 Authentic Exploit
www.nocknockbox.com
nocknockbox.com
webmail.nocknockbox.com
cpcalendars.nocknockbox.com
Contabo Inc.
United States, St. Louis
compromised
SSL Certificate
Issued By:
|- Common Name:
cPanel, Inc. Certification Authority
|- Organization:
cPanel, Inc.
Issued To:
|- Common Name:
nocknockbox.com
Supported SSL Versions:
TLSv1.2, TLSv1.3
Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14
HTTP/1.1 200 OK
Date: Sun, 20 Mar 2022 09:11:22 GMT
Server: Apache
Last-Modified: Sun, 29 Aug 2021 08:48:47 GMT
Accept-Ranges: bytes
Content-Length: 1012
Content-Type: text/html
Hacked By Hamza Anonime
umasonsonate.online
GoDaddy.com, LLC
United States, St. Louis
compromised
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
*.umasonsonate.online
Supported SSL Versions:
TLSv1.2, TLSv1.3
Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14
HTTP/1.1 200 OK
Date: Wed, 16 Mar 2022 19:46:00 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Hacked by ./Traccert
American Wireless, Inc
United States, Perryville
compromised
SSL Certificate
Issued By:
|- Common Name:
Let's Encrypt Authority X3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
awifi.us
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 16
HTTP/1.1 200 OK
Date: Mon, 07 Mar 2022 16:17:40 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

GxC

Shodan – Let's apply it locally – Apologies ahead of time

- Let's find all the ICS systems in the state of Missouri.
- Filters we're using
  - state, screenshot.label
  - Our query
    - state:"MO" screenshot.label:ics

Disclaimer x 2:

Please be careful with this information. Remember, I nor the conference organizers are responsible for what you do with this presentation. Be good. Do good. If not…


I will find you...

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

TOTAL RESULTS

6

TOP COUNTRIES

United States	3
Uruguay	3

TOP PORTS

80	3
5900	3

TOP ORGANIZATIONS

[redacted]	3
[redacted]	2
[redacted]	1

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

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

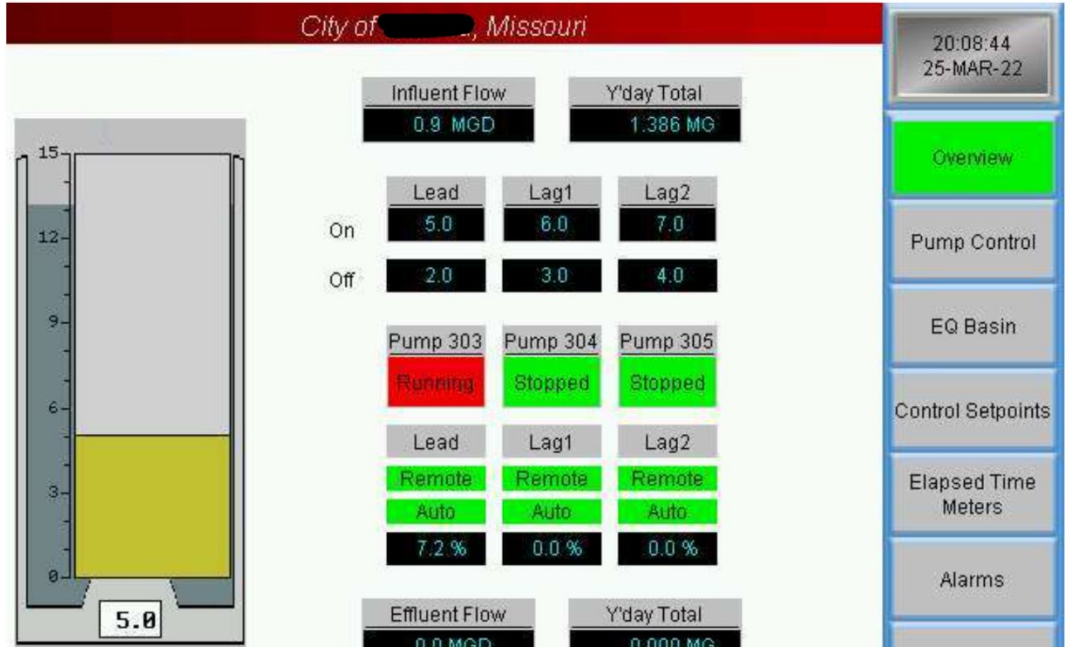
C-more -- the best HMI presented by AutomationDirect

[redacted]

United States, Sedalia

```
HTTP/1.1 200 OK
Server: EA-HTTP/1.0
Date: Sat, 26 Mar 2022 04:08:26 GMT
Last-Modified: Sat, 26 Mar 2022 04:08:26 GMT
Etag: "32520802e"
Content-Type: text/html
Content-Length: 1520
```

2022-03-26T01:25:19.369930



GxC

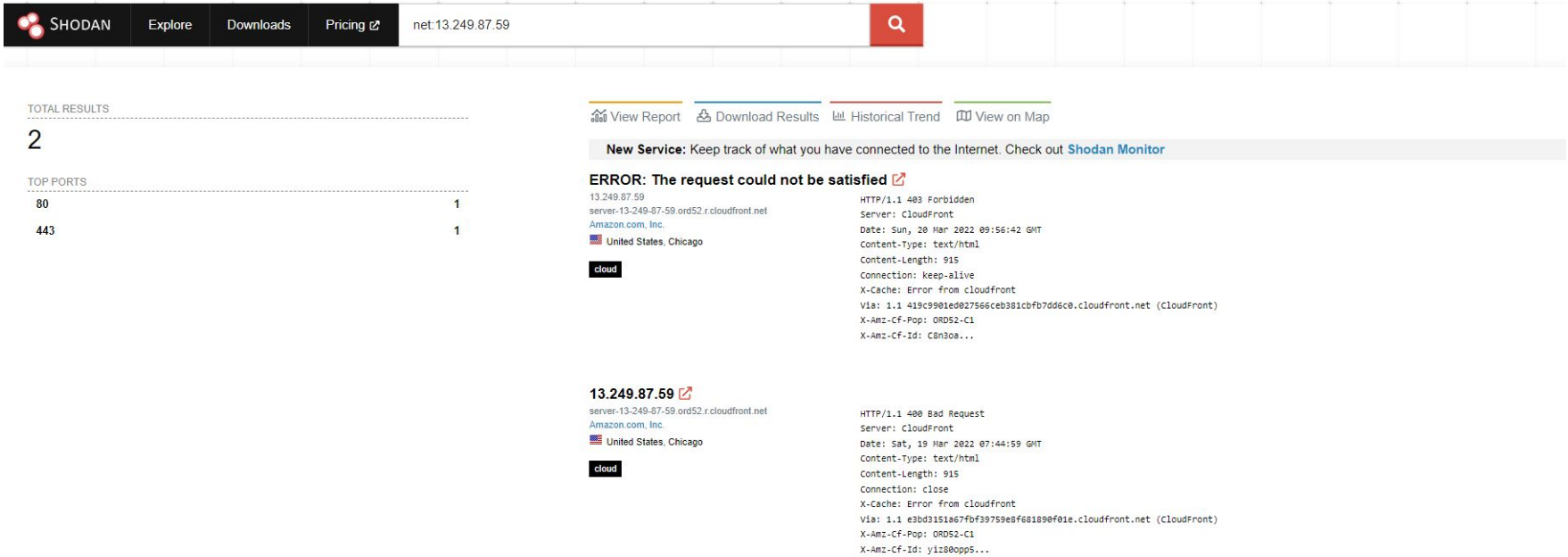
Recon Profile Check

1. Text file of WHOIS Intel domains in `example_whois_com.txt`
2. Enumerated services in our `example_com.json` file AND `example_enum_com.txt`
3. Ports scanned by NMAP and saved in `example_com_results.json`
4. Scanned our web applications for vulnerabilities (if any).
5. Determined our cloud assets that may be misconfigured.

GxC

Shodan – Let's apply it to us!

- Let's use the net and ip filters to find if our assets have been scanned
- Filter we're using
  - net
  - Our query
    - net: [ip or cidr]


SHODAN
Explore
Downloads
Pricing
net:13.249.87.59
TOTAL RESULTS
2
TOP PORTS
80 1
443 1
View Report
Download Results
Historical Trend
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
ERROR: The request could not be satisfied
13.249.87.59
server-13-249-87-59.ord52.r.cloudfront.net
Amazon.com, Inc.
United States, Chicago
cloud
HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Sun, 20 Mar 2022 09:56:42 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 419c9901ed027566ceb381cbfb7dd6c0.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ORD52-C1
X-Amz-Cf-Id: C8n3oa...
13.249.87.59
server-13-249-87-59.ord52.r.cloudfront.net
Amazon.com, Inc.
United States, Chicago
cloud
HTTP/1.1 400 Bad Request
Server: CloudFront
Date: Sat, 19 Mar 2022 07:44:59 GMT
Content-Type: text/html
Content-Length: 915
Connection: close
X-Cache: Error from cloudfront
Via: 1.1 e3bd3151a67fbf39759e8f681890f01e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ORD52-C1
X-Amz-Cf-Id: yiz80opp5...

Shodan – Let's apply it to us!

- Let's use the net and ip filters to find if our assets have been scanned
- Filter we're using
  - net
  - Our query
    - net: [ip or cidr]

Recon Profile Check

```
OWASP Amass v3.18.3                                https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
86 names discovered - scrape: 9, dns: 9, cert: 14, archive: 6, api: 48
--------------------------------------------------------------------------------
ASN: 62723 - ACTUAL-AS - Actualize Tech, LLC
        166.90.97.0/24          25   Subdomain Name(s)
        64.157.165.0/24         2    Subdomain Name(s)
        64.193.21.0/24          4    Subdomain Name(s)
        139.60.112.0/24         1    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        108.156.120.0/21        4    Subdomain Name(s)
        13.226.26.0/23          4    Subdomain Name(s)
        15.197.192.0/20         1    Subdomain Name(s)
        35.160.0.0/13           1    Subdomain Name(s)
        35.80.0.0/12            2    Subdomain Name(s)
        54.70.0.0/15            1    Subdomain Name(s)
        34.208.0.0/12           1    Subdomain Name(s)
        13.225.220.0/22         4    Subdomain Name(s)
        3.33.240.0/20           1    Subdomain Name(s)
        44.224.0.0/11           5    Subdomain Name(s)
        54.68.0.0/15            1    Subdomain Name(s)
        52.24.0.0/14            1    Subdomain Name(s)
        108.159.224.0/21        4    Subdomain Name(s)
ASN: 62 - CYRS - CyrusOne LLC
        216.117.105.0/24        5    Subdomain Name(s)
        216.117.25.0/24         28   Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        23.20.0.0/14            3    Subdomain Name(s)
        18.204.0.0/14           2    Subdomain Name(s)
        18.232.0.0/14           1    Subdomain Name(s)
        54.237.0.0/16           2    Subdomain Name(s)
        3.208.0.0/12            2    Subdomain Name(s)
        52.86.0.0/15            1    Subdomain Name(s)
ASN: 8075 - MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation
        52.224.0.0/11           1    Subdomain Name(s)
```

GxC

SHODAN | Explore | Downloads | Pricing | net:108.156.120.0/21

TOTAL RESULTS

4,038

TOP COUNTRIES

United States	2,288
Korea, Republic of	1,750

TOP PORTS

80	2,031
443	2,007

TOP PRODUCTS

CloudFront httpd	3,998
Microsoft IIS httpd	3
Apache httpd	2

View Report | Download Results | Historical Trend | View on Map

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

ERROR: The request could not be satisfied

108.156.126.45
server-108-156-126-45.ord56.r.cloudfront.net
Amazon.com, Inc.
United States, Chicago

cloud

```
HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Sat, 26 Mar 2022 20:06:16 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 85d9c09ca046a4310056e6148b05256e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ORD56-P3
X-Amz-Cf-Id: rALV59...
```

ERROR: The request could not be satisfied

108.156.126.194
healthcheck.staging.armorlabsaws.net
server-108-156-126-194.ord56.r.cloudfront.net
Amazon.com, Inc.
United States, Chicago

cloud

SSL Certificate

Issued By:
|- Common Name:
Amazon
|- Organization:
Amazon

Issued To:
|- Common Name:
healthcheck.staging.armorlabsaws.net

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

```
HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Sat, 26 Mar 2022 20:04:50 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 879577459c816cd0d14ed39ecb78fa32.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ORD56-P3
X-Amz-Cf-Id: QnW2Mj...
```

ERROR: The request could not be satisfied

108.156.127.122
cloudfront.edge.classic.dm.amplience-qa.net
akamai.edge.classic.dm.amplience-qa.net
classic.cdn.media.amplience-qa.net
classic.dm.amplience-qa.net
i1-qa.adis.ws
Amazon.com, Inc.
United States, Chicago

cloud

SSL Certificate

Issued By:
|- Common Name:
DigiCert TLS RSA SHA256 2020 CA1
|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
classic.dm.amplience-qa.net
|- Organization:
Amplience (UK) Limited

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

```
HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Sat, 26 Mar 2022 20:03:44 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 c829b3e651886a9824004bb6e7296c143a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ORD56-P3
X-Amz-Cf-Id: nvRbNB...
```

ERROR: The request could not be satisfied

108.156.126.169
robinhood.com
server-108-156-126-169.ord56.r.cloudfront.net
Amazon.com, Inc.
United States, Chicago

cloud

SSL Certificate

Issued By:
|- Common Name:
DigiCert SHA2 Secure Server CA
|- Organization:
DigiCert Inc

Issued To:
|- Common Name:
*.robinhood.com
|- Organization:

```
HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Sat, 26 Mar 2022 19:58:43 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 192228dcba44aa7310059d7f976fd506.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ORD56-P3
X-Amz-Cf-Id: 4DBajS...
```

GxC

SHODAN | Explore | Downloads | Pricing | net:108.156.120.0/21 "200" | Account

TOTAL RESULTS

19

TOP COUNTRIES

Korea, Republic of	18
United States	1

View Report | Download Results | Historical Trend | View on Map

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

Why am I here?

2022-03-26T08:43:57.781641

108.156.120.107
msgf.net
msgfocus.com
server-108-156-120-107.ord56.r.cloudfront.net
Amazon.com, Inc.
United States, Chicago

cloud

SSL Certificate
Issued By:
|- Common Name:
Amazon
|- Organization:
Amazon
Issued To:
|- Common Name:
*.msgfocus.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 2662
Connection: keep-alive
Server: Apache
Last-Modified: Wed, 23 Dec 2020 19:02:09 GMT
Accept-Ranges: bytes
Date: Sat, 26 Mar 2022 05:29:47 GMT
Expires: Sat, 26 Mar 2022 07:29:46 GMT
Cache-Control: max-age=7200
ETag...
```

Auburn Tiger Women's Golf Camps | at Auburn University | Auburn, AL

2022-03-25T21:01:11.072500

108.156.120.106
www.auburntigergolfcamps.com
auburntigergolfcamps.com
server-108-156-120-106.ord56.r.cloudfront.net
Amazon.com, Inc.
Korea, Republic of, Seoul

cloud

SSL Certificate
Issued By:
|- Common Name:
Amazon
|- Organization:
Amazon
Issued To:
|- Common Name:
www.auburntigergolfcamps.com
Supported SSL Versions:
TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: private
Date: Fri, 25 Mar 2022 20:55:54 GMT
Expires: {ts '2022-03-25 15:55:54'}
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Cache: Miss from cloudfront
Via: 1.1 0...
```

Auburn Tiger Women's Golf Camps | at Auburn University | Auburn, AL

2022-03-25T20:02:23.630335

108.156.120.55
www.auburntigergolfcamps.com
auburntigergolfcamps.com
server-108-156-120-55.ord56.r.cloudfront.net
Amazon.com, Inc.
Korea, Republic of, Seoul

cloud

SSL Certificate
Issued By:
|- Common Name:
Amazon
|- Organization:
Amazon
Issued To:
|- Common Name:
www.auburntigergolfcamps.com
Supported SSL Versions:
TLSv1.1, TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: private
Date: Fri, 25 Mar 2022 19:57:06 GMT
Expires: {ts '2022-03-25 14:57:06'}
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Cache: Miss from cloudfront
Via: 1.1 f...
```

Why am I here?

2022-03-25T13:04:15.171188

108.156.120.34
msgf.net
msgfocus.com
server-108-156-120-34.ord56.r.cloudfront.net
Amazon.com, Inc.
Korea, Republic of, Seoul

cloud

SSL Certificate
Issued By:
|- Common Name:
Amazon
|- Organization:
Amazon
Issued To:
|- Common Name:
*.msgfocus.com
Supported SSL Versions:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 2662
Connection: keep-alive
Server: Apache
Last-Modified: Wed, 23 Dec 2020 19:02:09 GMT
Accept-Ranges: bytes
Date: Fri, 25 Mar 2022 11:29:56 GMT
Expires: Fri, 25 Mar 2022 13:29:41 GMT
Cache-Control: max-age=7200
ETag...
```

GxC

Disclaimer x 3:

The darker side of Shodan

What I’m about to show you is the exact reason why we need to get recon and infosec right. Your organization could possibly be here someday. Again: Be good. Do good.

GxC

[REDACTED]

[REDACTED]

[REDACTED]

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


Determining Risk

Risk…is complicated and subjective

- Just because something is connected to the internet doesn't mean it's inherently risky.

1. Risk Analysis with Reconnaissance

http://www.example.com

Ports Open
80

Web Vulnerabilities
Open Redirect

Manual Validation
Front end and Static website.
No calls to backend APIs.
No WAF.

Hosting
AWS

https://employeereports.example.com

Ports Open
443

Web Vulnerabilities
Medium Reflected XSS

Manual Validation
Site that has a full stack framework: front, back, DB.
Calls to backend APIs.
Outdated WAF

Hosting
AWS

https://creditcards.example.com

Ports Open
443, 80 (301)

Web Vulnerabilities
None

Manual Validation
Site that has a full stack framework: front, back, DB.
Calls to backend Auth APIs.
WAF, DMZ, Up to date code.

Hosting
On Prem

GxC

2. Risk Analysis with Reconnaissance

http://www.example.com

Ports Open
80

Web Vulnerabilities
Open Redirect

Manual Validation
Front end and Static website.
No calls to backend APIs.
No WAF.

Hosting
AWS

https://employeereports.example.com

Ports Open
443

Web Vulnerabilities
Medium Reflected XSS

Manual Validation
Site that has a full stack framework: front, back, DB.
Calls to backend APIs.
Outdated WAF

Hosting
AWS

https://creditcards.example.com

Ports Open
443, 80 (301), 3306

Web Vulnerabilities
None

Manual Validation
Site that has a full stack framework: front, back, DB.
Calls to backend Auth APIs.
WAF, DMZ, Up to date code.

Hosting
On Prem

GxC

3. Risk Analysis with Reconnaissance

http://www.example.com

Ports Open
80

Web Vulnerabilities
Open Redirect

Manual Validation
Front end and Static website.
No calls to backend APIs.
No WAF.

Hosting
AWS

https://employeereports.example.com

Ports Open
443

Web Vulnerabilities
None

Manual Validation
Site that has a full stack framework: front, back, DB.
Calls to backend APIs.
Outdated WAF

Hosting
AWS

https://creditcards.example.com

Ports Open
443, 80 (301)

Web Vulnerabilities
None

Manual Validation
Site that has a full stack framework: front, back, DB.
Calls to backend Auth APIs.
WAF, DMZ, Up to date code.

Hosting
On Prem

GxC

How to Recon Yourself tldr; version

1. Environment Discovery
    a. AMASS Yourself
        i. Intel and Enum
2. Perimeter Scanning
    a. Paradigm Yourself
    b. Nmap your gathered information
    c. Nikto your web targets
3. Cloud Scanning
    a. Grayhat Warfare Search for Cloud Assets
4. Monitoring and Determining Risk
    a. Check commercial and open source tools for your assets connected to the internet.
    b. Shodan Yourself
    c. What needs to be addressed vs not addressed
    d. Build your asset list.

Coming Soon

1. Automated Reconnaissance
2. Open Source Tool
3. Risk Framework based upon reconnaissance discoveries.

References and Links

- AMASS
  - https://github.com/OWASP/Amass
- Paradigm
  - https://github.com/jeredbare/paradigm
- Nmap
  - https://nmap.org/
- Nikto
  - https://cirt.net/Nikto2
- GrayHat Warfare
  - https://buckets.grayhatwarfare.com/
- This talk
  - https://github.com/jeredbare/talks/reconyourself2

Thank you

jeredbare@gmail.com
Cell: 573-355-0676
Twitter - @jeredbare IG: jered.bare
LinkedIn - /in/jeredbare
Github - jeredbare

GxC

Q & A