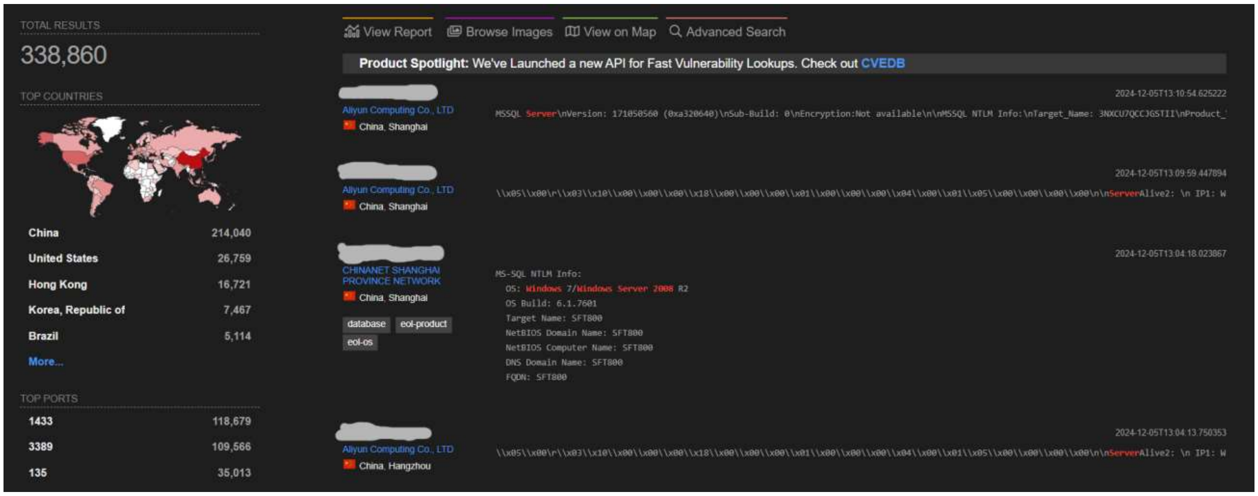
This project focuses on the importance of reconnaissance in ethical hacking and penetration testing. It covers passive information gathering techniques and tools used in the initial stages of the Cyber Kill Chain.

Using search engines for reconnaissance and footprinting

Shodan is a search engine for Internet-connected devices. This activity demonstrates how to use Shodan to find potentially vulnerable systems.



TOTAL RESULTS

338,860

TOP COUNTRIES

China	214,040
United States	26,759
Hong Kong	16,721
Korea, Republic of	7,467
Brazil	5,114
More...	

TOP PORTS

1433	118,679
3389	109,566
135	35,013

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

[redacted]
Aliyun Computing Co., LTD
China, Shanghai

2024-12-05T13:10:54.625222

```
MSSQL Server\nVersion: 171050560 (0xa320640)\nSub-Build: 0\nEncryption:Not available\n\nMSSQL NTLM Info:\nTarget_Name: 3NXCU7QCCJGSTII\nProduct_
```

[redacted]
Aliyun Computing Co., LTD
China, Shanghai

2024-12-05T13:09:59.447894

```
\\x05\\x00\r\\x03\\x10\\x00\\x00\\x00\\x18\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x04\\x00\\x01\\x05\\x00\\x00\\x00\\x00\n\nServerAlive2: \n IP1: W
```

[redacted]
CHINANET SHANGHAI PROVINCE NETWORK
China, Shanghai
database eol-product eol-os

2024-12-05T13:04:18.023867

```
MS-SQL NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: SFT800
  NetBIOS Domain Name: SFT800
  NetBIOS Computer Name: SFT800
  DNS Domain Name: SFT800
  FQDN: SFT800
```

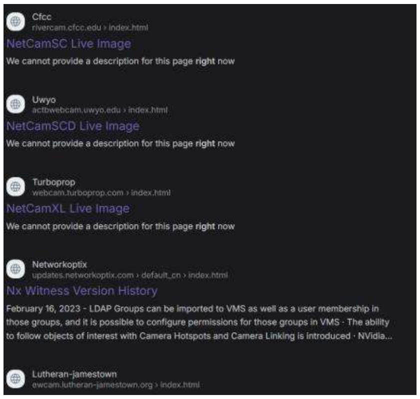
[redacted]
Aliyun Computing Co., LTD
China, Hangzhou

2024-12-05T13:04:13.750353

```
\\x05\\x00\r\\x03\\x10\\x00\\x00\\x00\\x18\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x04\\x00\\x01\\x05\\x00\\x00\\x00\\x00\n\nServerAlive2: \n IP1: W
```

Here is a screenshot of results for “windows server 2008.” IP addresses have been masked for security reasons. This shows that there are over 300,000 running Windows Server 2008 that have been discovered by Shodan.

Another way to use browsers for reconnaissance and footprinting is called Google Dorking. Google Dorking involves using advanced search operators to find sensitive information that may be inadvertently exposed on the internet.



Cfcc
rivercam.cfcc.edu › index.html
NetCamSC Live Image
We cannot provide a description for this page right now

Uwyo
actbwebcam.uwyo.edu › index.html
NetCamSCD Live Image
We cannot provide a description for this page right now

Turboprop
webcam.turboprop.com › index.html
NetCamXL Live Image
We cannot provide a description for this page right now

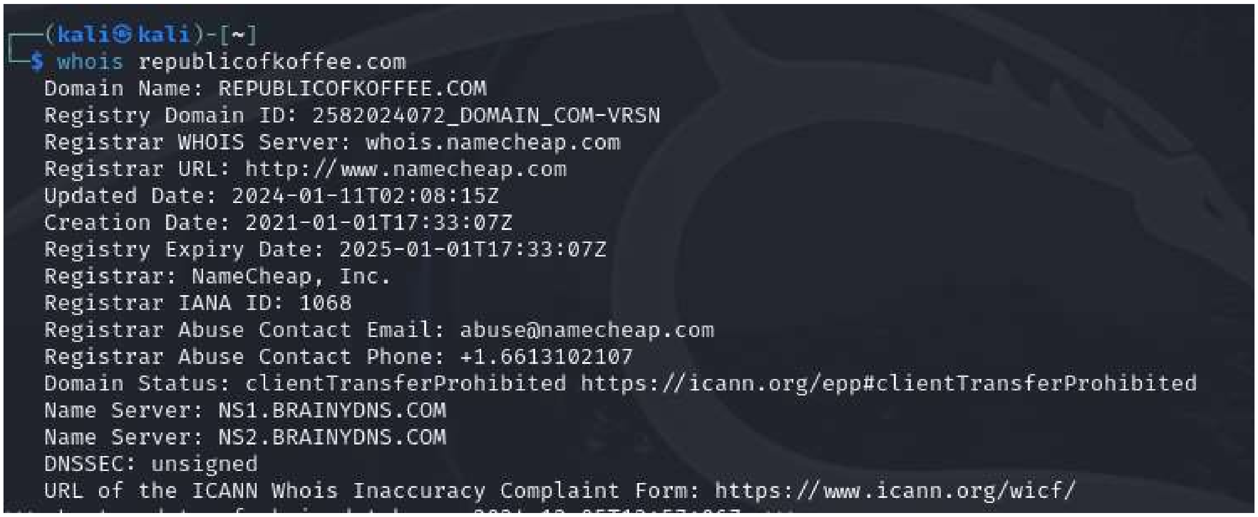
Networkoptix
updates.networkoptix.com › default_cn › index.html
Nx Witness Version History
February 16, 2023 – LDAP Groups can be imported to VMS as well as a user membership in those groups, and it is possible to configure permissions for those groups in VMS · The ability to follow objects of interest with Camera Hotspots and Camera Linking is introduced · NVidia...

Lutheran-jamestown
ewcam.lutheran-jamestown.org › index.html

Here are the results for entering in ‘“Pop-up” + “Live Image” inurl:index.html.’ It shows unsecured cameras and shows their live feed. This shows how powerful search engines can be used to find potentially sensitive information. It highlights the importance of proper access controls and careful consideration of what information is made public.

There are some command line commands that are helpful for reconnaissance and footprinting. The WHOIS command is a utility used to retrieve information about a domain name or an IP address. It queries the WHOIS database to provide details such as the registrant's contact information, registration date, and expiration date.

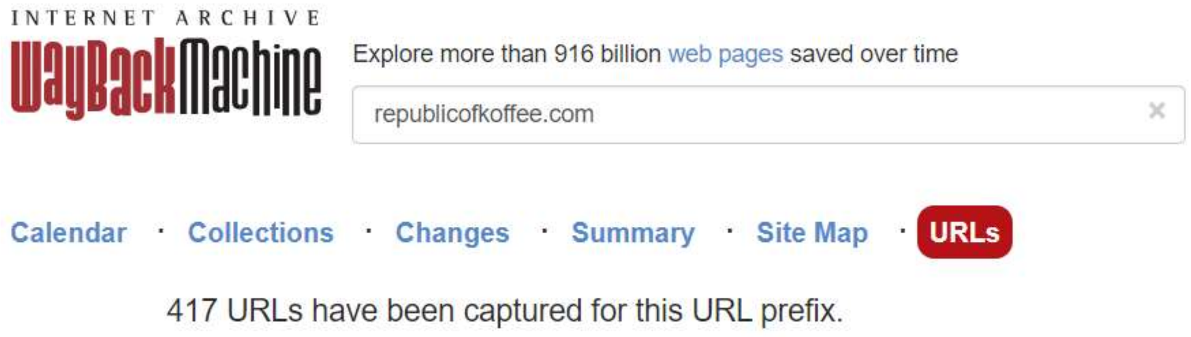
For example, if I wanted to do reconnaissance on the domain “republicofkoffee.com,” you would get something like this:



```
┌──(kali㉿kali)-[~]
└─$ whois republicofkoffee.com
   Domain Name: REPUBLICOFKOFFEE.COM
   Registry Domain ID: 2582024072_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2024-01-11T02:08:15Z
   Creation Date: 2021-01-01T17:33:07Z
   Registry Expiry Date: 2025-01-01T17:33:07Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.BRAINYDNS.COM
   Name Server: NS2.BRAINYDNS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

It includes a lot more information than just this. This is just a taste of it. It should be noted that the same information can be found at the whois website: https://www.whois.com/whois/republicofkoffee.com.

You can use the Internet Archive Wayback machine to see previous versions of this website.


INTERNET ARCHIVE
WayBackMachine
Calendar · Collections · Changes · Summary · Site Map · URLs

Explore more than 916 billion web pages saved over time

republicofkoffee.com

417 URLs have been captured for this URL prefix.

This project showcased systematic OSINT techniques for extracting domain intelligence, emphasizing the critical role of ethical, methodical information gathering in cybersecurity reconnaissance.