positive hack camp

Exploration in the customer's external infrastructure

positive education

CyberED

Rules

- You will work in **groups with your buddies** to make it easier for yourself to understand the material. Feel free to ask, help and prompt each other.

- There are **two teachers** in the classroom, one of them is always ready to help you at the computer if you have any problem.

- At the end of each day, **you will have a 30-minute section for questions** and discussion of the past material. Also, if you are not in a hurry, you can stay and ask the mentors a little more.

- Every day **we start our classes at 10.00 Moscow time**, and also strictly take into account the time of breaks. Try not to be late for classes.

Etiquette

→ **Turn off the sound on mobile phones.** If you need to answer a call, you can quietly leave the classroom and talk outside.

→ If you want **to ask a question, please raise your hand** and wait for the teacher to answer you.

→ Every day you will have new teachers and mentors, so **do not forget to introduce yourself** when you answer a question or speak.

→ **If you need to leave the classroom, you can quietly leave** the classroom without asking permission.

Requirements

To complete the course comfortably, you need:

- The art of "Googling"
- A notebook for notes
- Basic knowledge of Linux
- Basic knowledge about the work of the network
- Docker (?)
- Kali Linux Virtual Machine (?)

Ethic

→ **A white hacker or pentester** is an information security specialist who researches computer systems for vulnerabilities that can be used by intruders (black hackers) to access, influence, and steal sensitive data.

→ **In other words:** a white hacker helps companies identify potential threats in the IT infrastructure in a timely manner and, thus, prevent real hacker attacks.

→ **That's why white hackers are called ethical.** You may also come across the definition of "white hat", which also indicates that pentesters belong to the light side.

Legal regulation

Options for the activities of white hackers

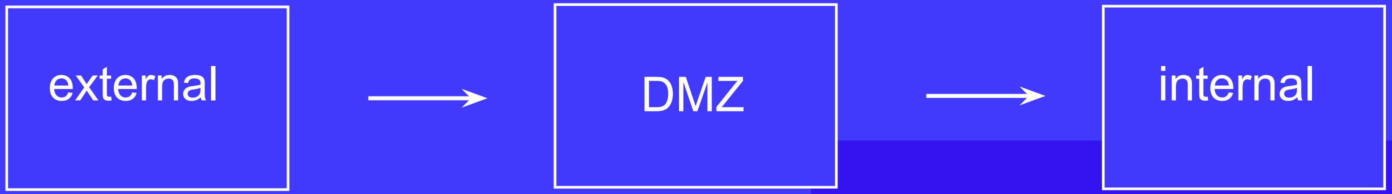
A white hacker can work both under signed contracts and without a contract (based on public policies of companies).

- **Contract work in companies specializing in information security services**
- **Work under an agreement with the owner of information systems**
- **Works without an explicitly signed contract (according to the contract offer)**

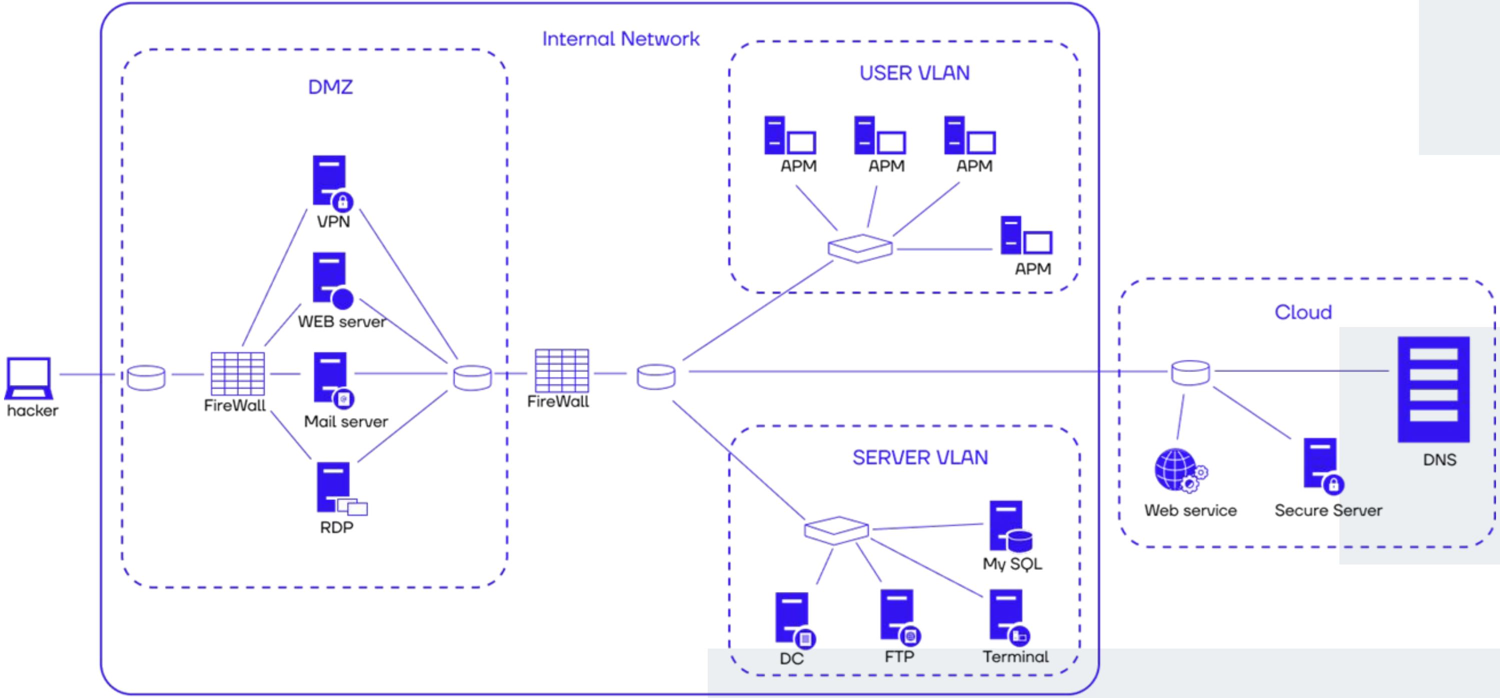
What kind of regulation do you have in your countries?

Basic Concepts

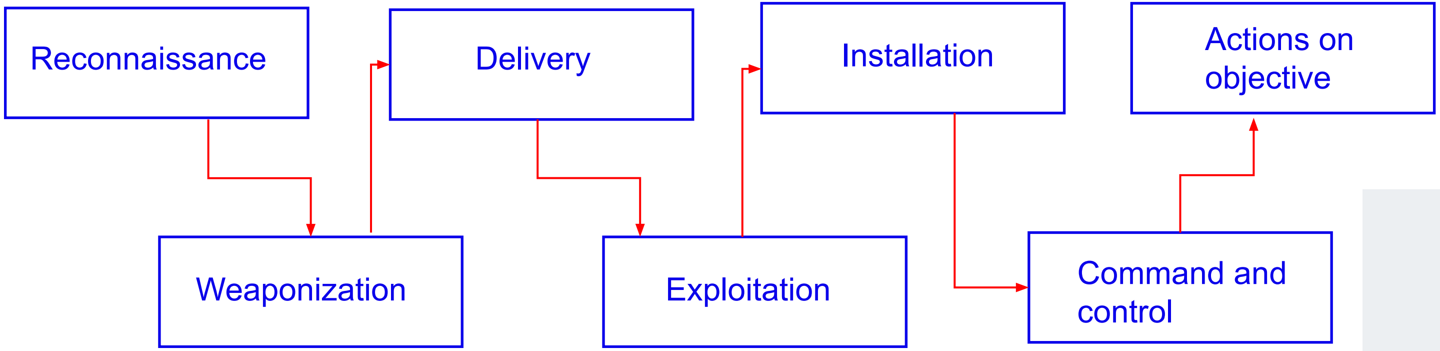
Typical company infrastructure



Company IT infrastructure in details



Set of actions to compromise the infrastructure looks this:



Basic Concepts

Network reconnaissance

Systematic discovery of internet-exposed assets and services.

Purpose: Map attack surfaces, identify vulnerabilities, and support penetration testing workflows.

A Company’s infrastructure

Public-facing components accessible via the internet:
- Network devices (routers, firewalls, VPN gateways)
- Web servers, APIs, and cloud instances
- DNS records and mail servers

A network scanner

Automated tool for:
- Host discovery (live IPs/Domains)
- Port/service enumeration (TCP/UDP)
- Vulnerability fingerprinting (e.g., banner grabbing)

Basic Concepts

A domain name

A human-readable identifier (e.g., example.com) that maps to an IP address.

▪ Hierarchical structure: [subdomain].[second-level domain].[top-level domain]

▪ Managed by domain registrars and governed by ICANN.

Domain Name System (DNS)

A decentralized, hierarchical database that resolves domain names to IP addresses.

▪ Uses record types: A (IPv4), AAAA (IPv6), MX (mail servers), CNAME (aliases).

▪ Relies on recursive resolvers (user queries) → authoritative nameservers (domain records).

Basic Concepts

A Secure Sockets Layer (SSL) certificate

A digital document that:

- Authenticates a server's identity (via trusted Certificate Authorities/CAs).
- Encrypts data in transit using asymmetric cryptography.
- Uses X.509 standard and binds a public key to a domain/organization.

A network port

A 16-bit integer (0-65535) identifying a transport-layer endpoint for TCP/UDP communications.

- Purpose: Enables multiplexing of services on a single IP address.

Basic Concepts

A host or node

Term	Definition	Examples
Node	Any device with a network interface (NIC)	Routers, switches, printers
Host	An endpoint node running applications	Servers, workstations, IoT devices

- **Critical Distinction:** Hosts process data; nodes forward/transport data.

General principles

- **OSINT (Open Source Intelligence)** is a methodology for gathering, analyzing, and utilizing publicly available information from various sources to generate intelligence or insights that aid in decision-making.

- **Open sources** may include internet resources, social media, newspapers, magazines, television, radio, public databases, and other accessible platforms that do not require special permissions or privileges. ess.

The primary objective of this information-gathering process is to collect as much relevant data as possible about the target organization.

General techniques of information gathering

Active
involve direct interaction with information sources

Passive
based on the analysis of publicly available information

Examples of Information To Collect:

Domain names registered to the organization

Active hosts on the network along with their IP addresses

Current status of **network ports** for the listed nodes

Type and version of the **operating systems** on the examined machines

Versions of software or services associated with network ports

Details about the **technologies** employed on the website

Active methods of information gathering

In the active method, network requests are sent directly from your systems to the target's systems, making them visible to the IT owner.

Examples of active methods include:

Port scanning is a method that allows you to determine which ports on a company's servers are open to outside access. Port scanning can help you determine what services are available on the servers and what operating system is installed on the servers.

Domain name enumerations and domain name prediction are ways of determining the domain names used by a company or organization. This process may involve the use of various methods, such as enumerating the names of subdomains used in the company name and various variations of domain zones (e.g., .com, .org, .net).

Site visits and analysis involve a detailed examination of sites to understand their functions, the technologies they use, and to uncover debugging and technical information about an organization's internal network or software design.

Passive methods of information gathering

These are methods that do not require direct interaction with the source of information, but rely on analyzing open sources of information.

Examples of passive methods of information gathering include:

Internet monitoring is the process of tracking and analyzing information published in online resources, including repositories, blogs, forums, and other Internet sites.

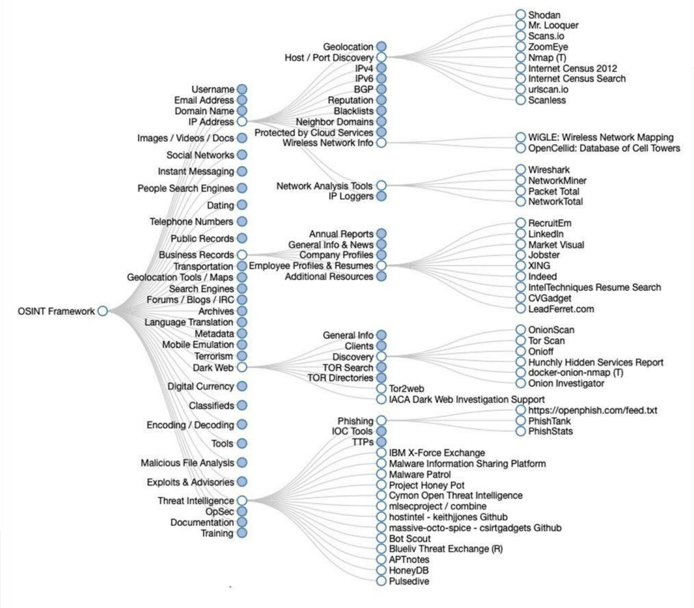
Open database analysis is the process of collecting information from public databases such as government registries, company databases, directories, etc.

Open source analysis is the process of collecting and analyzing information from various open sources, such as data leak aggregator sites, sites that collect DNS name change information and DNS history, sites that research the Internet and the services published on it.

OSINT Framework

The **OSINT framework** is a structured collection of references to OSINT tools, organized by task and type of information required, and presented in a hierarchical tree format.

https://osintframework.com/



Searching for Information in WHOIS

Protocol Fundamentals

Legacy WHOIS

TCP-based protocol (port 43) for querying domain/IP/ASN registration databases.

Limitations: Unencrypted, unstructured plain-text responses, inconsistent formatting.

Modern Replacement: RDAP

RESTful protocol (HTTPS/443) with JSON-structured responses.

Supports access control, internationalization, and redaction (GDPR-compliant).

Searching for Information in WHOIS

Protocol Fundamentals

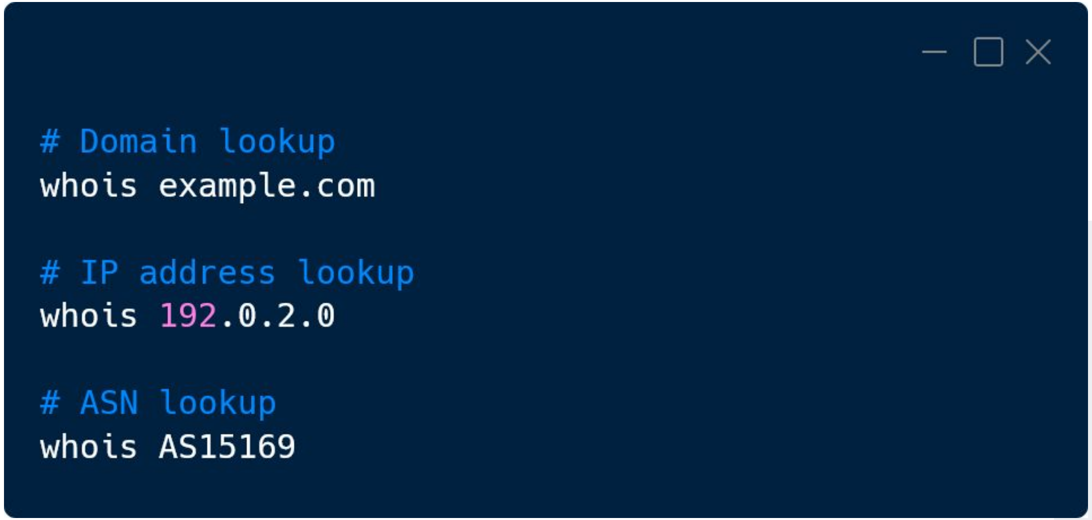
Legacy WHOIS

TCP-based protocol (port 43) for querying domain/IP/ASN registration databases.

Limitations: Unencrypted, unstructured plain-text responses, inconsistent formatting.

Record Type	Typical Data	Redaction Status
Domain	Registrar, creation/expiry dates, nameservers	Owner/contact details hidden
IP Address	RIR (e.g., ARIN), allocation block, ISP	Partially visible
ASN	Holder organization, routing policies	Fully visible

Searching for Information in WHOIS



```
# Domain lookup
whois example.com

# IP address lookup
whois 192.0.2.0

# ASN lookup
whois AS15169
```

Searching for Information in DNS

DNS (Domain Name System) is a hierarchical and decentralized naming system used to translate domain names into IP addresses and vice versa. DNS queries can provide various types of information about domain names, including IP addresses, mail servers, and name servers.

Common DNS Record Types:
A Record: Maps a domain name to an IPv4 address.
AAAA Record: Maps a domain name to an IPv6 address.
MX Record: Specifies mail exchange servers for the domain.
NS Record: Lists the name servers for the domain.
CNAME Record: Provides an alias for a domain name.
TXT Record: Holds text information, often used for verification and SPF records.

Searching for Information in DNS

DNS (Domain Name System) is a **How to Search for DNS Information:**

Using dig Command: A powerful DNS lookup tool available on most Unix-based systems.

Retrieves the A record for example.com.

```
dig example.com A
```

- Retrieves the MX records for example.com.

```
dig example.com MX
```

Using nslookup Command: A command-line tool used for querying DNS.

- Retrieves the A record for example.com.

```
nslookup -type=A example.com
```

- Retrieves the MX records for example.com.

```
nslookup -type=MX example.com
```

Online DNS Lookup Tools: Websites that provide DNS query services through a web interface.

•**Example**: Using services like MXToolbox or DNSstuff to perform various DNS queries.

Searching for subdomains

Subdomain enumeration is the process of identifying subdomains associated with a domain name. Subdomains are extensions of a primary domain and can reveal additional information about a website’s structure and services.

Methods for Searching Subdomains:

DNS Zone Transfer: A zone transfer is a mechanism by which DNS servers share their zone files, which can include information about subdomains.
DNS Brute Forcing: Automated tools perform a dictionary attack against the DNS records to discover subdomains by trying a list of common names.
Publicly Available Resources: Leverage publicly available resources such as search engines, certificate transparency logs, and subdomain databases.
Web-Based Tools and Services: Online services that provide subdomain enumeration and analysis.
Examples: VirusTotal, Shodan, SecurityTrails

Searching for subdomains - tools

Amass

```
amass enum -d example.com
```

theHarvester

```
theHarvester -d example.com -b all
```

Subfinder

```
subfinder -d example.com
```

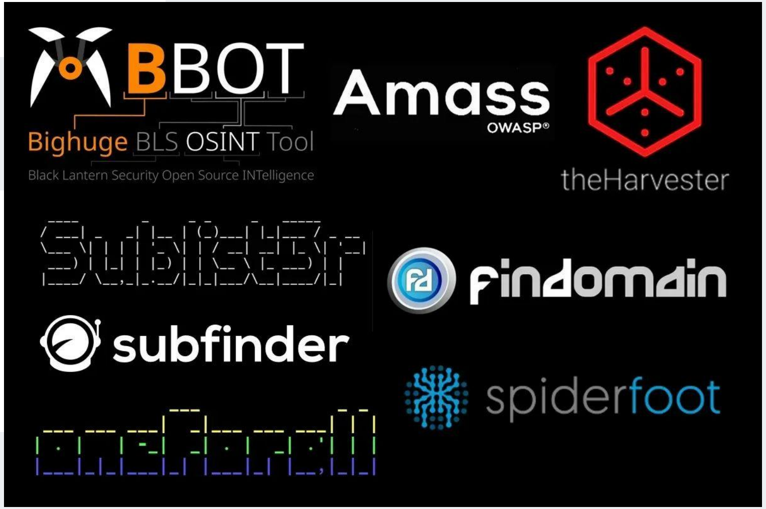
Sublist3r:

```
sublist3r -d example.com
```

Using dig for zone transfer:

```
dig axfr @<DNS_Server> example.com
```

https://blog.blacklanternsecurity.com/p/subdomain-enumer ation-tool-face-off-4e5



Other OSINT tools

Google Dork https://www.exploit-db.com/google-hacking-database

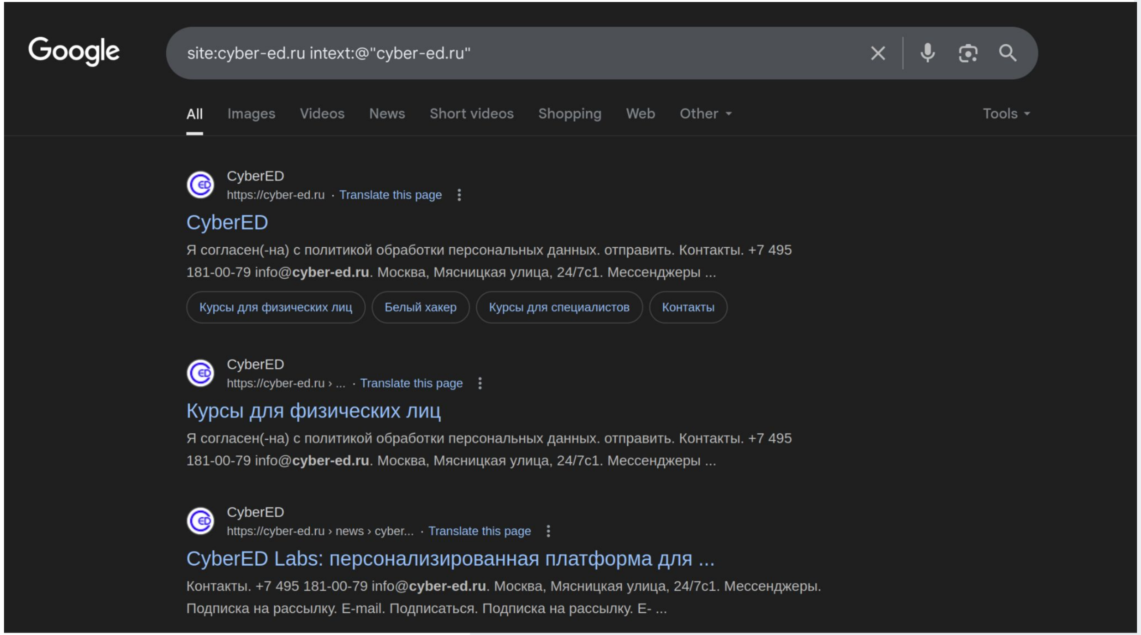
SHODAN https://www.shodan.io

WayBackMachine https://archive.org/web/

VirusTotal https://virustotal.com

Other OSINT tools

Google Dork



site:cyber-ed.ru intext:@"cyber-ed.ru"

CyberED
https://cyber-ed.ru · Translate this page

CyberED

Я согласен(-на) с политикой обработки персональных данных. отправить. Контакты. +7 495 181-00-79 info@**cyber-ed.ru**. Москва, Мясницкая улица, 24/7с1. Мессенджеры ...

Курсы для физических лиц · Белый хакер · Курсы для специалистов · Контакты

CyberED
https://cyber-ed.ru › ... · Translate this page

Курсы для физических лиц

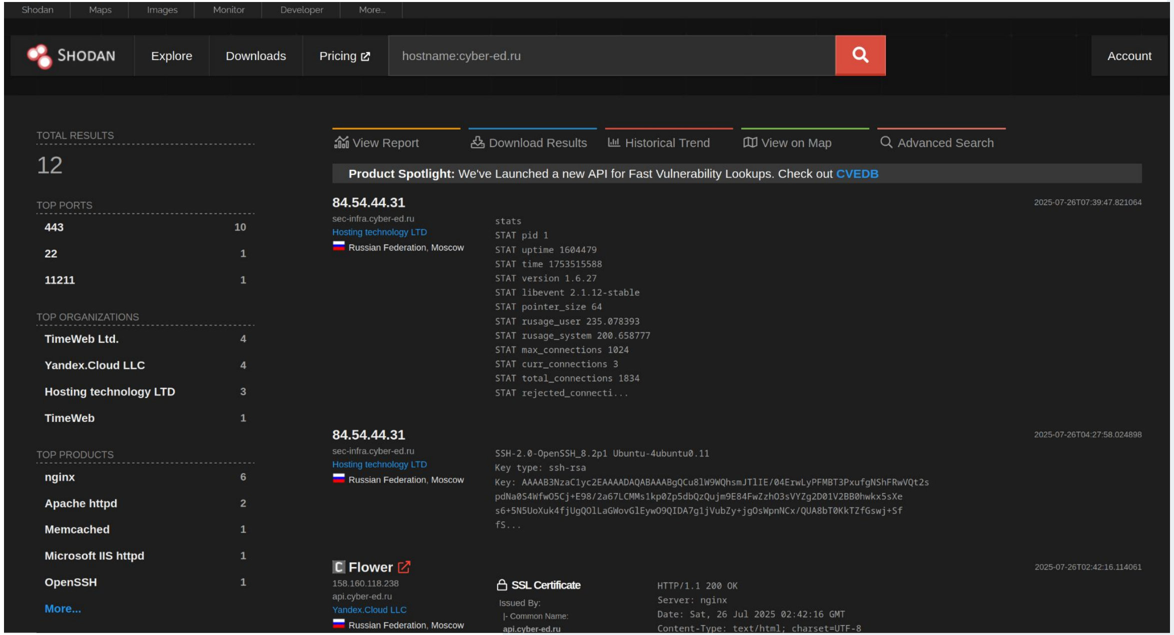
Я согласен(-на) с политикой обработки персональных данных. отправить. Контакты. +7 495 181-00-79 info@**cyber-ed.ru**. Москва, Мясницкая улица, 24/7с1. Мессенджеры ...

CyberED
https://cyber-ed.ru › news › cyber... · Translate this page

CyberED Labs: персонализированная платформа для ...

Контакты. +7 495 181-00-79 info@**cyber-ed.ru**. Москва, Мясницкая улица, 24/7с1. Мессенджеры. Подписка на рассылку. E-mail. Подписаться. Подписка на рассылку. E- ...

Other OSINT tools



hostname:cyber-ed.ru

TOTAL RESULTS

12

TOP PORTS

443	10
22	1
11211	1

TOP ORGANIZATIONS

TimeWeb Ltd.	4
Yandex.Cloud LLC	4
Hosting technology LTD	3
TimeWeb	1

TOP PRODUCTS

nginx	6
Apache httpd	2
Memcached	1
Microsoft IIS httpd	1
OpenSSH	1

More...

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

84.54.44.31
sec-infra.cyber-ed.ru
Hosting technology LTD
Russian Federation, Moscow

2025-07-26T07:39:47.821064

```
stats
STAT pid 1
STAT uptime 1604479
STAT time 1753515588
STAT version 1.6.27
STAT libevent 2.1.12-stable
STAT pointer_size 64
STAT rusage_user 235.078393
STAT rusage_system 200.658777
STAT max_connections 1024
STAT curr_connections 3
STAT total_connections 1834
STAT rejected_connecti...
```

84.54.44.31
sec-infra.cyber-ed.ru
Hosting technology LTD
Russian Federation, Moscow

2025-07-26T04:27:58.024898

```
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCu8lW9WQhsmJTlIE/04ErwLyPFMBT3PxufgNShFRwVQt2s
pdNa0S4WfwO5Cj+E98/2a67LCMMs1kp0Zp5dbQzQujm9E84FwZzhO3sVYZg2D01V2BB0hwkx5sXe
s6+5N5UoXuk4fjUgQOlLaGWovGlEywO9QIDA7g1jVubZy+jgOsWpnNCx/QUA8bT0KkTZfGswj+Sf
fS...
```

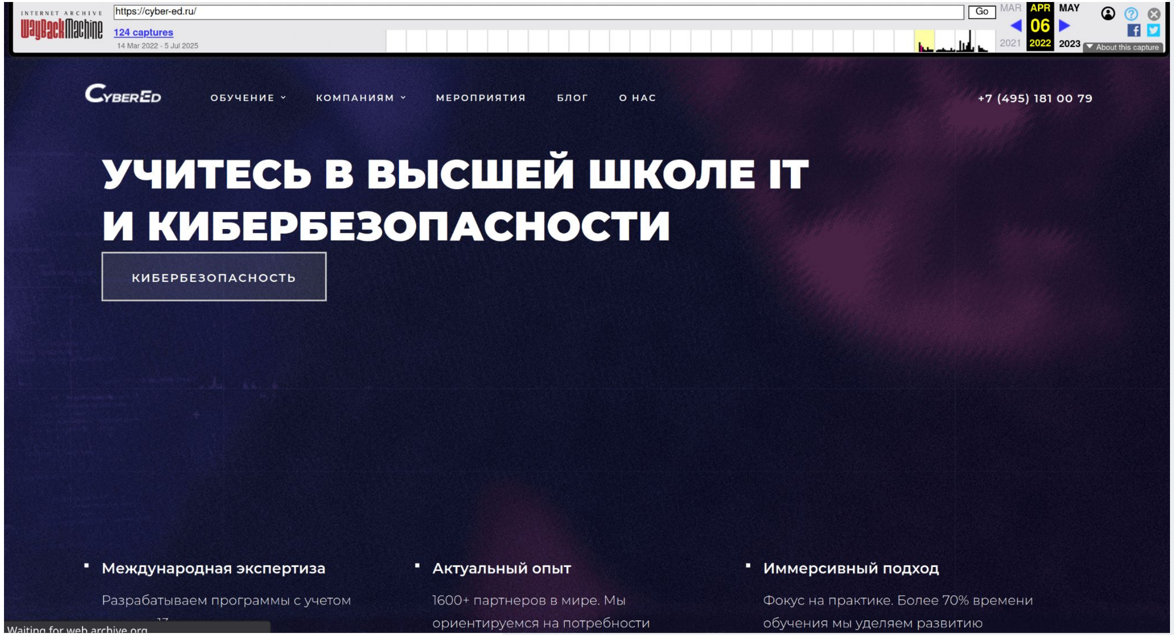
Flower
158.160.118.238
api.cyber-ed.ru
Yandex.Cloud LLC
Russian Federation, Moscow

2025-07-26T02:42:16.114061

SSL Certificate
Issued By:
|- Common Name:
api.cyber-ed.ru

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 26 Jul 2025 02:42:16 GMT
Content-Type: text/html; charset=UTF-8
```

Other OSINT tools



https://cyber-ed.ru/

124 captures

14 Mar 2022 - 5 Jul 2025

+7 (495) 181 00 79

УЧИТЕСЬ В ВЫСШЕЙ ШКОЛЕ IT И КИБЕРБЕЗОПАСНОСТИ

- **Международная экспертиза**

  Разрабатываем программы с учетом

- **Актуальный опыт**

  1600+ партнеров в мире. Мы ориентируемся на потребности

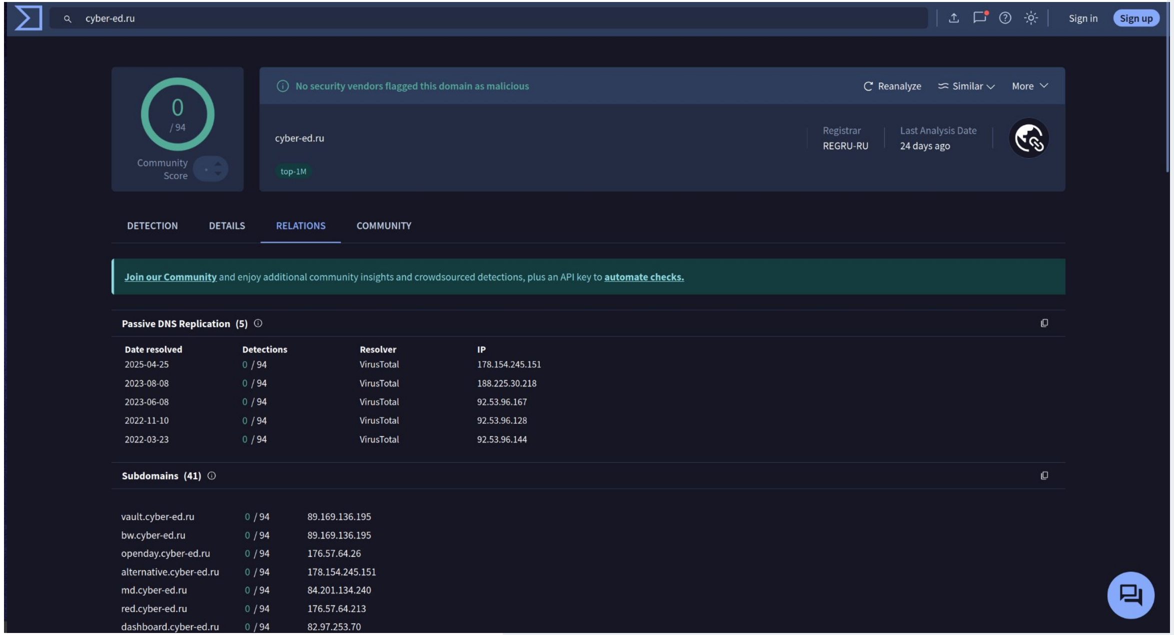
- **Иммерсивный подход**

  Фокус на практике. Более 70% времени обучения мы уделяем развитию

positive hack camp

Other OSINT tools

VirusTotal



0 / 94 Community Score

No security vendors flagged this domain as malicious

cyber-ed.ru

top-1M

Registrar: REGRU-RU

Last Analysis Date: 24 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (5)

Date resolved	Detections	Resolver	IP
2025-04-25	0 / 94	VirusTotal	178.154.245.151
2023-08-08	0 / 94	VirusTotal	188.225.30.218
2023-06-08	0 / 94	VirusTotal	92.53.96.167
2022-11-10	0 / 94	VirusTotal	92.53.96.128
2022-03-23	0 / 94	VirusTotal	92.53.96.144

Subdomains (41)

vault.cyber-ed.ru	0 / 94	89.169.136.195
bw.cyber-ed.ru	0 / 94	89.169.136.195
openday.cyber-ed.ru	0 / 94	176.57.64.26
alternative.cyber-ed.ru	0 / 94	178.154.245.151
md.cyber-ed.ru	0 / 94	84.201.134.240
red.cyber-ed.ru	0 / 94	176.57.64.213
dashboard.cyber-ed.ru	0 / 94	82.97.253.70

positive education

CyberED

Digital leaks

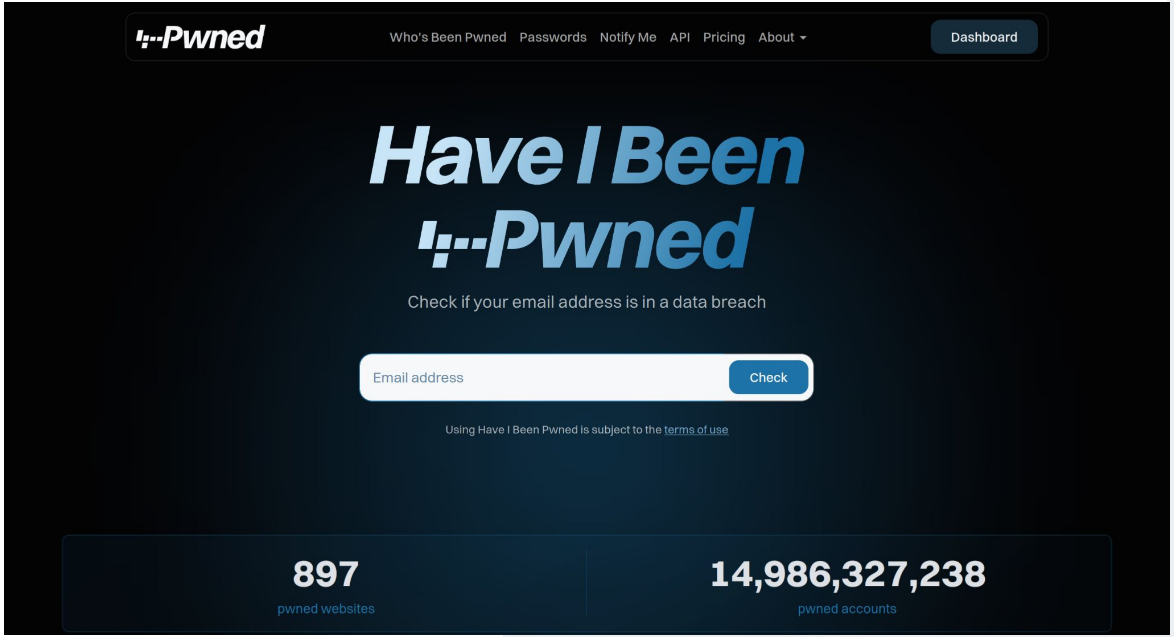
';--have i been pwned? https://haveibeenpwned.com

SnusBase https://snusbase.com

_IntelligenceX https://intelx.io

Digital leaks

';--have i been pwned?



Have I Been ';--Pwned

Check if your email address is in a data breach

Email address | Check

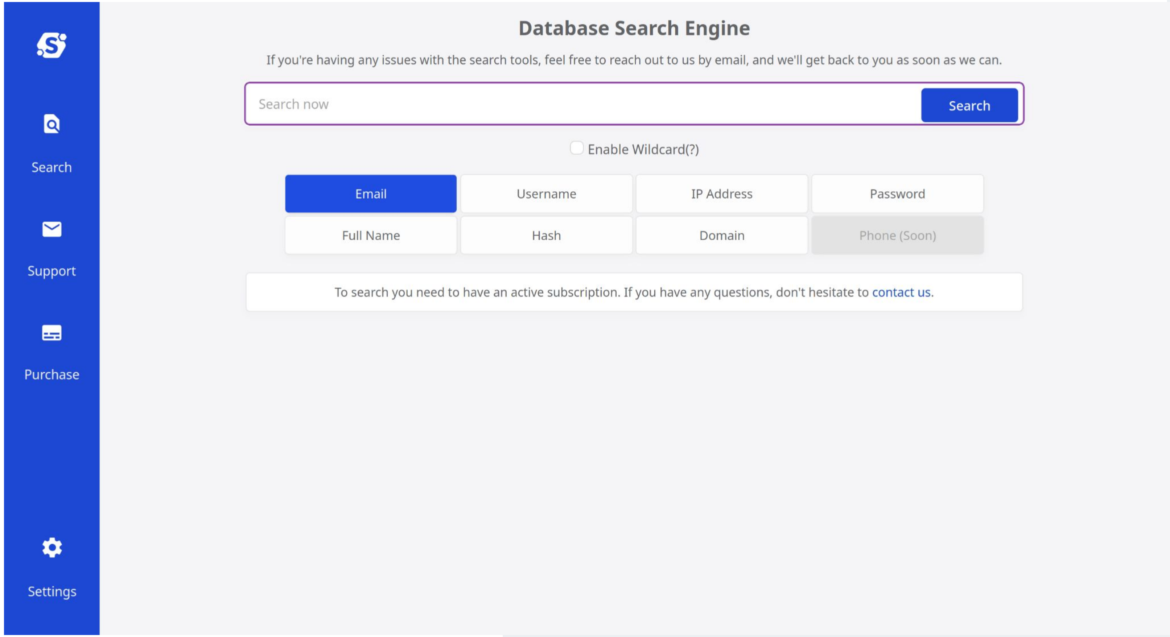
Using Have I Been Pwned is subject to the terms of use

897 pwned websites

14,986,327,238 pwned accounts

Digital leaks

SnusBase



Database Search Engine

If you're having any issues with the search tools, feel free to reach out to us by email, and we'll get back to you as soon as we can.

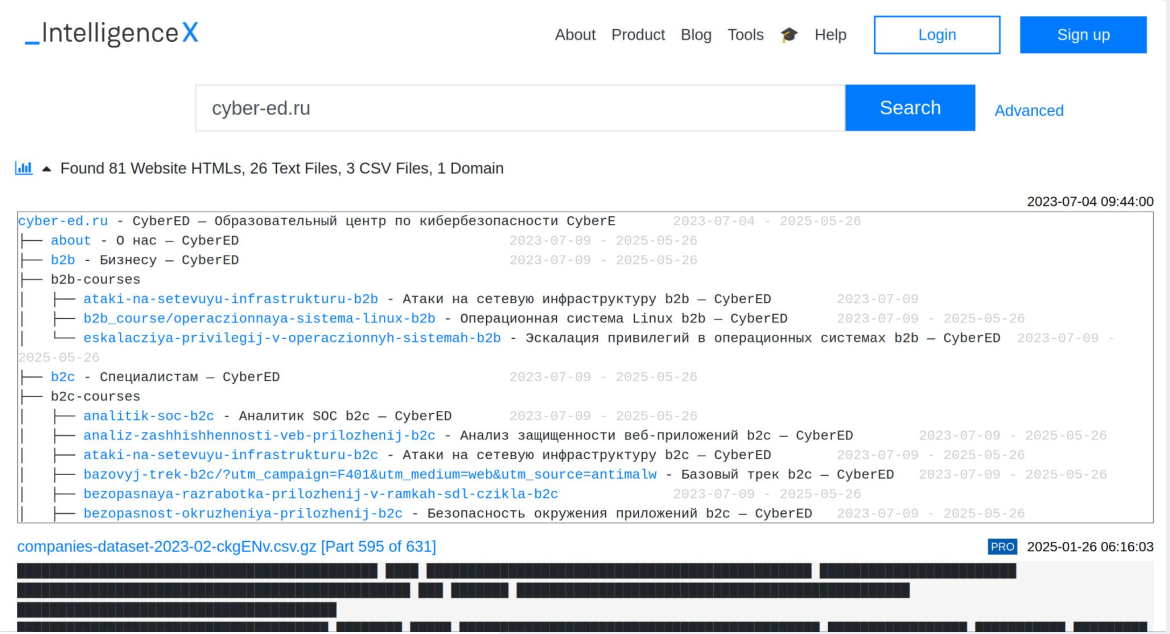
□ Enable Wildcard(?)

To search you need to have an active subscription. If you have any questions, don't hesitate to contact us.

positive hack camp

Digital leaks

_IntelligenceX



Found 81 Website HTMLs, 26 Text Files, 3 CSV Files, 1 Domain

2023-07-04 09:44:00

```
cyber-ed.ru - CyberED — Образовательный центр по кибербезопасности CyberE       2023-07-04 - 2025-05-26
├── about - О нас — CyberED                                  2023-07-09 - 2025-05-26
├── b2b - Бизнесу — CyberED                                  2023-07-09 - 2025-05-26
├── b2b-courses
│   ├── ataki-na-setevuyu-infrastrukturu-b2b - Атаки на сетевую инфраструктуру b2b — CyberED       2023-07-09
│   ├── b2b_course/operaczionnaya-sistema-linux-b2b - Операционная система Linux b2b — CyberED      2023-07-09 - 2025-05-26
│   └── eskalacziya-privilegij-v-operaczionnyh-sistemah-b2b - Эскалация привилегий в операционных системах b2b — CyberED  2023-07-09 -
2025-05-26
├── b2c - Специалистам — CyberED                             2023-07-09 - 2025-05-26
├── b2c-courses
│   ├── analitik-soc-b2c - Аналитик SOC b2c — CyberED       2023-07-09 - 2025-05-26
│   ├── analiz-zashhishhennosti-veb-prilozhenij-b2c - Анализ защищенности веб-приложений b2c — CyberED       2023-07-09 - 2025-05-26
│   ├── ataki-na-setevuyu-infrastrukturu-b2c - Атаки на сетевую инфраструктуру b2c — CyberED       2023-07-09 - 2025-05-26
│   ├── bazovyj-trek-b2c/?utm_campaign=F401&utm_medium=web&utm_source=antimalw - Базовый трек b2c — CyberED   2023-07-09 - 2025-05-26
│   ├── bezopasnaya-razrabotka-prilozhenij-v-ramkah-sdl-czikla-b2c          2023-07-09 - 2025-05-26
│   ├── bezopasnost-okruzheniya-prilozhenij-b2c - Безопасность окружения приложений b2c — CyberED   2023-07-09 - 2025-05-26
```

companies-dataset-2023-02-ckgENv.csv.gz [Part 595 of 631] PRO 2025-01-26 06:16:03

[redacted]

positive education

CyberED

Filtering out irrelevant data

After applying various methods and techniques to collect information, all the information obtained **needs to be validated.**

In general, white hat hackers provide the collected information to the organization and collaborate with the customer to determine which data will remain on the list of all received information, ensuring that systems not intended for further investigation or testing are excluded from the scope.

Examples of commonly used network scanners

Nmap
the most popular

Zenmap
GUI for nmap.

Masscan
a network scanner designed to increase the speed of scanning large network segments, including the entire IPv4 address space.

Network scanning

Network scanners are used to find network nodes and open ports and services on them, allowing us to answer the questions:
which nodes available to us in the target network?
what services are published on a node?
what network ports do they use?

When scanning a network, first we try to find all the **nodes available to us** considering our initial point of access. This step is named “**host discovery**”

Second step of network scanning is “**port scan**”. It’s essential to identify what services are running on any open ports on the nodes available, and it’s crucial to learn how to find these **ports and services** effectively.
To understand how scanning open ports and services operates, it’s crucial to grasp the **network protocols** that facilitate these functions. For a comprehensive understanding, we recommend studying the underlying network communication protocols on your own: TCP, UDP, IP, and ICMP.

Port Scanning

Port Scanning is a technique used to identify open ports and services available on a networked device. This process involves sending various types of packets to a range of ports on a target system and analyzing the responses to determine which ports are open, closed, or filtered. Key aspects of port scanning include:

Identifying Open Ports: Determining which ports are accepting connections, which can reveal services running on those ports (e.g., HTTP on port 80, SSH on port 22).

Service Detection: Identifying the services and applications running on the open ports, which can provide insights into potential vulnerabilities or misconfigurations.

Port scanning helps in mapping the network topology, assessing security posture, and identifying potential attack vectors by revealing which services are exposed and potentially vulnerable.

Port Scanning

Port Types:

TCP Ports: Scanning TCP ports involves establishing a connection with the target port. Common techniques include SYN scan (half-open scan) and ACK scan.
UDP Ports: Scanning UDP ports is more challenging due to the connectionless nature of UDP. Techniques include sending UDP packets and analyzing responses or lack thereof.

Port Scanning

Here's a breakdown of basic network scan types along with corresponding nmap commands:

Ping Scan (-sn): Determines live hosts without scanning ports.

TCP Connect Scan (-sT): Full TCP handshake to identify open ports.
SYN Scan (-sS): Sends SYN packets for stealthier port detection.
UDP Scan (-sU): Detects open UDP ports using UDP packets.

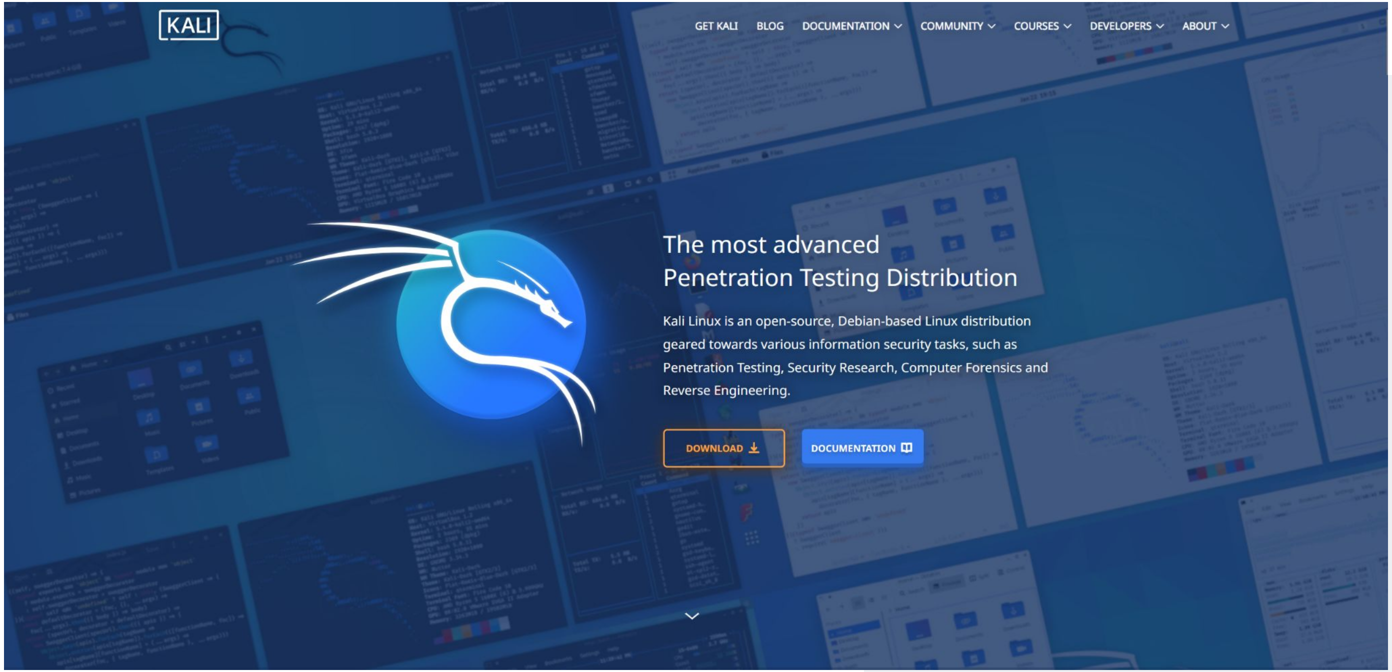
Version Detection (-sV): Identify versions of services running on open ports. **Run Default Scripts (-sC):** Execute default NSE scripts for additional information. **OS Detection (-O):** Determine the operating system of the target.

Port Range (-p): Specify range of ports on the target.

Lunch break

Let’s prepare your infra

Kali Linux



The most advanced
Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

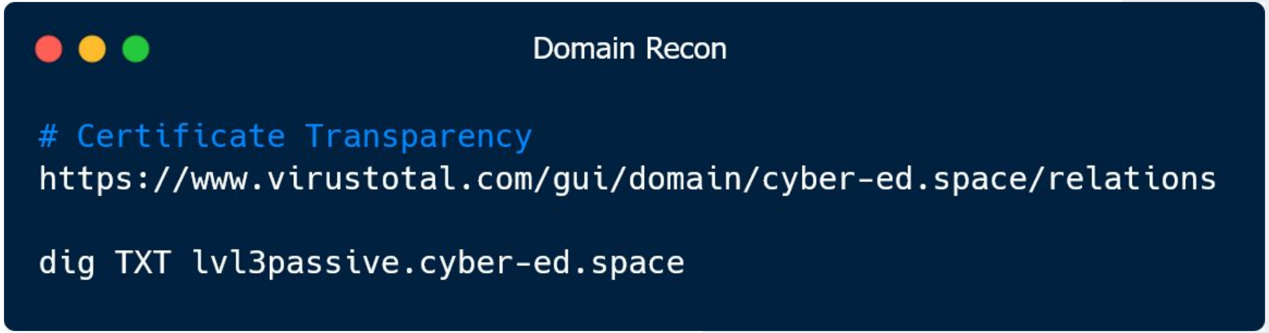
Domain Recon

Tools

- VirusTotal

- dig

Domain Recon



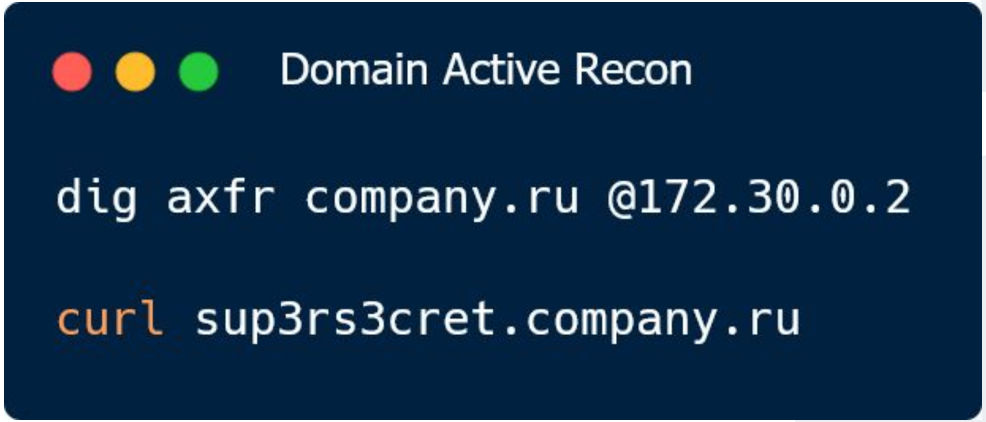
```
# Certificate Transparency
https://www.virustotal.com/gui/domain/cyber-ed.space/relations

dig TXT lvl3passive.cyber-ed.space
```

Domain Active Recon

Tools

- dig(Zone Transfer)

Domain Active Recon



Domain Active Recon

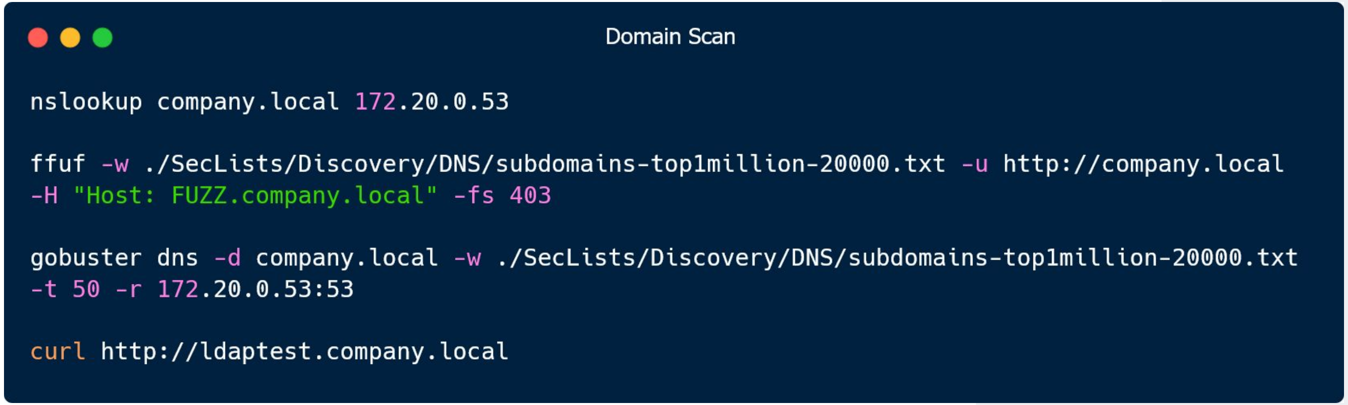
```
dig axfr company.ru @172.30.0.2

curl sup3rs3cret.company.ru
```

Domain Scan

Tools

- nslookup
- ffuf/gobuster
- curl

Domain Scan



Domain Scan

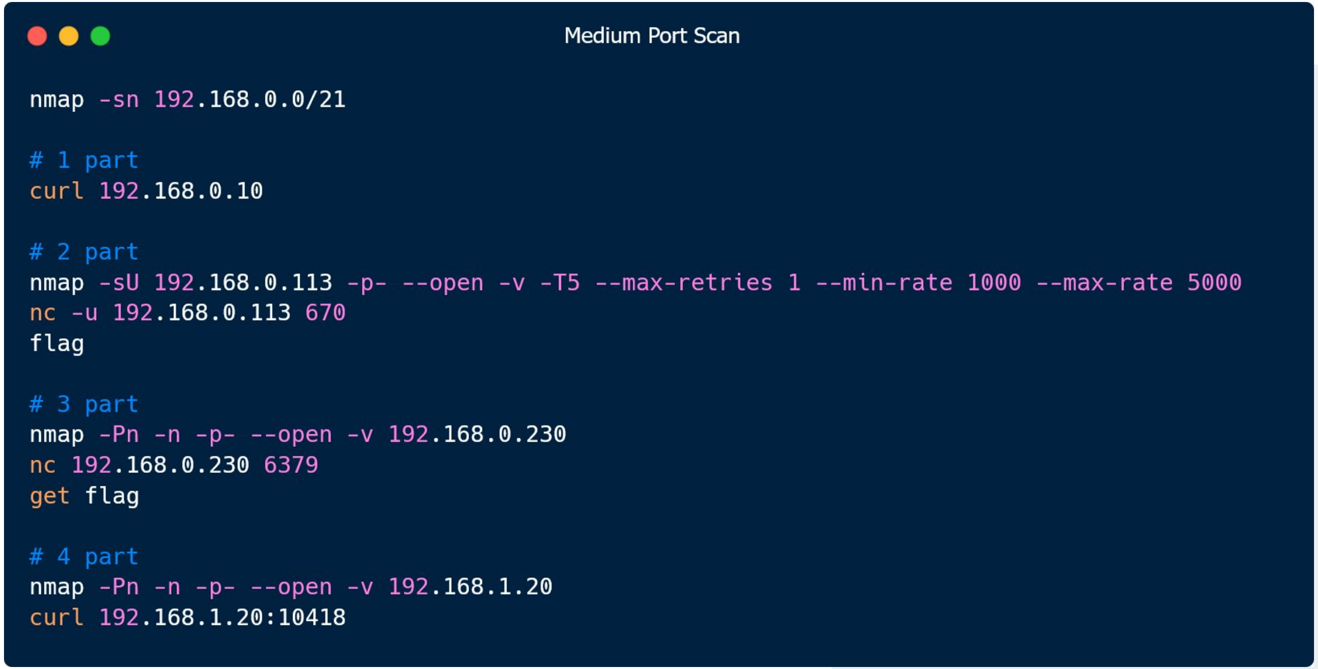
```
nslookup company.local 172.20.0.53

ffuf -w ./SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u http://company.local
-H "Host: FUZZ.company.local" -fs 403

gobuster dns -d company.local -w ./SecLists/Discovery/DNS/subdomains-top1million-20000.txt
-t 50 -r 172.20.0.53:53

curl http://ldaptest.company.local
```

Medium Port Scan

Tools

- curl
- nmap
- netcat

Medium Port Scan



```
nmap -sn 192.168.0.0/21

# 1 part
curl 192.168.0.10

# 2 part
nmap -sU 192.168.0.113 -p- --open -v -T5 --max-retries 1 --min-rate 1000 --max-rate 5000
nc -u 192.168.0.113 670
flag

# 3 part
nmap -Pn -n -p- --open -v 192.168.0.230
nc 192.168.0.230 6379
get flag

# 4 part
nmap -Pn -n -p- --open -v 192.168.1.20
curl 192.168.1.20:10418
```

positive hack camp

QUESTIONS AND DISCUSSION

positive education

CyberED