whois:

Purpose: WHOIS is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system.

dns:

Purpose: DNS (Domain Name System) is a system that translates human-readable domain names into IP addresses. It's a critical component of the internet infrastructure.

fierce:

Purpose: Fierce is a domain scanner that helps in DNS reconnaissance. It attempts to discover non-contiguous IP address space and identify network infrastructure.

host:

Purpose: The host command is used for DNS lookups to convert domain names to IP addresses and vice versa. It also provides information about various DNS records associated with a domain.

Dmitry:

Purpose: Dmitry is a command-line tool that combines different techniques to gather information about a target, including DNS information, subdomains, and more. It's useful for reconnaissance during penetration testing.

Traceroute:

Purpose: Traceroute is a network diagnostic tool used to track the route that packets take across an IP network to reach a destination. It shows the IP addresses of the routers in the path.

p0f:

Purpose: p0f is a passive OS fingerprinting tool. It identifies the operating system of a target host by analyzing packets passively rather than actively sending probes.

hping3/arping/fping/npin:

> **hping3**: A versatile tool for network testing, including packet crafting, firewall testing, and TCP/IP stack analysis.
>
> **arping**: Used to discover hosts on a network using ARP requests.
>
> **fping**: Similar to ping but allows for sending ICMP echo requests to multiple hosts simultaneously.
>
> **npin**: A tool for sending ICMP, TCP, and UDP packets to network hosts for discovering hosts and open ports.
>
> **nbtscan**:

Purpose: nbtscan is a NetBIOS scanner that identifies devices on a local network, providing information about NetBIOS names and services.

PART 4

Task 1

OS fingerprinting is a method used in cybersecurity to determine the operating system (OS) running on a remote device. The primary goal is to gather information about the unique characteristics and behaviors of the target OS, enabling tailored security measures or attacks based on the identified vulnerabilities and features.

Here's a simplified explanation of the technical concept behind OS fingerprinting:

Analysis of Network Packets:

OS fingerprinting involves scrutinizing the network packets exchanged between the probing system and the target. This analysis usually occurs during network scanning or communication activities.

Examination of Packet Headers:

Different operating systems implement network protocols with slight variations. OS fingerprinting tools examine details in packet headers, such as TCP/IP stack implementation, differences in TCP handshake behavior, and specific flags set in packets.

Response Evaluation:

Specific probes or requests are sent to the target system, and the responses are analyzed. The way a system responds to ICMP requests or TCP SYN packets can unveil information about the OS.

Consideration of Timing and Behavior:

Attention is given to the timing and behavior of responses. For instance, the time taken for a system to respond to requests or the order in which it responds to various probes can be indicative of a particular operating system.

Comparison with Database:

OS fingerprinting tools compare observed characteristics with a database of known OS fingerprints. This database contains profiles of various operating systems, each with its unique network behavior. By matching observed behavior with entries in the database, the tool can make an informed guess about the target OS.

Passive Fingerprinting:

In certain cases, OS fingerprinting can be performed passively by analyzing patterns of network traffic without directly interacting with the target. This may involve monitoring and analyzing packets as they traverse the network.

Task2

Why OS fingerprinting can be important for security?

OS fingerprinting holds significance in cybersecurity for various reasons:

Assessment of Vulnerabilities:

Determining the operating system of a target system allows security professionals to evaluate potential vulnerabilities specific to that OS. Each operating system has distinct security flaws, enabling the customization of security measures to address these weaknesses.

Tailoring of Attacks:

Malicious actors often customize their attacks based on the target's operating system. OS fingerprinting provides crucial information for adapting attacks to maximize their effectiveness. Consequently, security measures can be implemented to defend against these tailored threats.

Configuration of Network Security:

Understanding the OS of devices within a network is essential for configuring network security settings. This knowledge enables the optimization of firewalls, intrusion detection/prevention systems, and other security measures based on the characteristics of the operating systems present.

Effective Incident Response:

In the event of a security incident or breach, knowledge of the target OS is crucial for an effective incident response. Security teams can quickly identify affected systems, comprehend the nature of the attack, and implement appropriate remediation measures.

Enforcement of Security Policies:

Security policies and access controls within organizations often align with specific operating systems. OS fingerprinting assists in enforcing these policies by ensuring that security measures are consistent with the characteristics of devices and systems in the network.

Facilitation of Forensic Analysis:

During forensic analysis of security incidents, knowing the operating system of affected systems is essential. This information aids investigators in reconstructing the timeline of events, understanding attack vectors, and determining the extent of the compromise.

Network Monitoring and Anomaly Detection:

OS fingerprinting can be integrated into ongoing network monitoring efforts. Any deviation from expected OS behavior can trigger alerts, aiding security teams in detecting potential anomalies or suspicious activities in real-time.

Enhancement of Security Awareness and Training:

OS fingerprinting contributes to security awareness and training programs by highlighting the diversity of operating systems within an organization's network. This information can be used to educate users and IT staff about specific security considerations associated with different operating systems.

Optimization of Resource Allocation:

Organizations can allocate resources more effectively by prioritizing security efforts based on the distribution of operating systems. This ensures prompt addressing of the most critical vulnerabilities, ultimately improving the overall security posture.

Task 3

What is a difference between passive and active OS fingerprinting?

Passive and active OS fingerprinting are two approaches used to gather information about the operating system running on a remote system. The key difference lies in how the information is collected:

Active OS Fingerprinting:

Definition: Active OS fingerprinting involves sending specific probes or requests to the target system and analyzing the responses.

How it Works: In this method, the fingerprinting tool actively interacts with the target by sending packets and observing how the target system responds. The tool may send crafted packets, such as ICMP (Internet Control Message Protocol) requests or TCP SYN packets, and analyze the responses to deduce information about the target's operating system.

Advantages:

- Provides more detailed and accurate information.
- Enables real-time interaction with the target system.

Disadvantages:

- Can be more easily detected by intrusion detection systems or firewalls.
- May generate additional network traffic and potentially impact system performance.

Passive OS Fingerprinting:

Definition: Passive OS fingerprinting involves analyzing patterns of network traffic without directly interacting with the target system.

How it Works: Instead of actively sending probes, passive OS fingerprinting tools observe and analyze the natural network traffic between the target and other systems. The characteristics of this traffic, such as packet timing, size, and sequence, are used to make educated guesses about the operating system without actively engaging with the target.

Advantages:

- More stealthy and less likely to be detected.
- Does not generate additional network traffic.

Disadvantages:

- Provides less detailed information compared to active fingerprinting.
- Relies on the availability of sufficient network traffic for analysis

Task 4

Is it possible to protect your systems from OS fingerprinting?

Safeguarding systems from OS fingerprinting presents challenges, as it involves mitigating techniques employed by attackers or security professionals to determine the operating system of a target system. While it may not be possible to completely eliminate the risk, you can adopt measures to diminish the likelihood of successful OS fingerprinting:

Firewall Configuration:

Adequately configure firewalls to filter and block unnecessary or malicious network traffic. Firewalls can be set up to intercept packets associated with common OS fingerprinting techniques.

Intrusion Detection/Prevention Systems (IDS/IPS):

Deploy IDS/IPS systems to identify and respond to suspicious network activity, including attempts at OS fingerprinting. Configure these systems to issue alerts to administrators or automatically thwart identified fingerprinting activities.

Traffic Encryption:

Utilize encrypted communication protocols like TLS/SSL to safeguard sensitive information during transit. Encrypted traffic complicates the analysis of packet headers, making it more challenging for attackers to gather information about the operating system.

Network Anonymization:

Implement techniques such as network address translation (NAT) to conceal the actual IP addresses and network configurations of internal systems. This can heighten the difficulty for attackers attempting to accurately fingerprint systems.

Randomized Responses:

Configure systems to deliver randomized responses to specific types of probes or requests. This introduces variability in the responses, confusing OS fingerprinting tools and making it more challenging to accurately identify the operating system.

Traffic Padding:

Introduce additional, non-essential network traffic to obscure patterns that OS fingerprinting tools may attempt to detect. This can be achieved using traffic generators or network emulation tools.

Regular Patching and Updates:

Ensure systems are regularly updated with the latest security patches. OS fingerprinting often relies on exploiting known vulnerabilities, and keeping systems patched reduces the chances of successful identification.

Task 5

Is it possible to fool intruder and to show him that your host is not alive?

Yes, you can use tricks to make it seem like your computer is not active or not responsive to outsiders. These tricks are part of keeping your computer safe, but keep in mind they're not perfect, and smart attackers might still figure out what's really going on.

Here are some simple tricks to make it look like your computer is not doing much:

Firewall Setup:

Adjust the settings of your firewall to ignore certain types of messages. This makes it seem like your computer is not responding to specific types of checks.

Quiet TCP Mode:

Make your computer respond less to certain types of connections. This can confuse attackers trying to see if your computer is working.

Fake Ports:

Set up pretend services on different ports. This might trick attackers into thinking they've found something, when really, they're just interacting with fake stuff.

Fake Network Activity:

Simulate some bursts of online activity every so often. This makes it hard for attackers to tell when your computer is actually busy.

Slow Responses:

Make your computer take a bit longer to answer certain kinds of online requests. This can make it seem like your computer is slow or not working well.

Fake Vulnerable Services:

Create pretend systems or services that seem easy to attack. These fakes can attract attackers, letting you watch what they do without risking your real stuff.

Changeable IP Addresses:

Every so often, switch your computer's IP address. This makes it tricky for attackers to keep track of what your computer is up to.

TASK 6

What is DNS zone transfer and what is a risk related to this mechanism?

DNS zone transfer is a mechanism used in the Domain Name System (DNS) to replicate and synchronize DNS databases across multiple DNS servers. It allows a secondary DNS server to request a copy of the DNS zone information from a primary DNS server. This transfer of zone information helps in distributing the DNS load, improving fault tolerance, and ensuring that multiple DNS servers have consistent and up-to-date information about a domain.

The process typically involves a primary DNS server (master server) that holds the authoritative copy of the DNS zone, and one or more secondary DNS servers (slave servers) that request and receive updates from the primary server.

Risks related to DNS Zone Transfer:

Unauthorized Access to DNS Data:

> One of the significant risks associated with DNS zone transfers is the potential for unauthorized access to sensitive DNS data. If an attacker gains access to a zone transfer, they can obtain a comprehensive list of domain names, IP addresses, and other critical DNS information, which could be valuable for reconnaissance in preparation for a cyber-attack.

Information Disclosure:

> DNS zone transfers, if not properly secured, can lead to information disclosure. Attackers may use the information obtained from zone transfers to identify potential targets, understand the network structure, and gather intelligence that can be exploited in subsequent attacks.

Data Integrity Concerns:

> If an attacker gains control of a secondary DNS server, they could manipulate the DNS zone data received during zone transfers. This could lead to data integrity issues, causing disruptions in DNS resolution and potentially redirecting legitimate traffic to malicious destinations.

Mitigation Strategies:

To mitigate the risks associated with DNS zone transfers, consider implementing the following best practices:

Limit Zone Transfer Access:

Restrict zone transfer access to authorized DNS servers. Only allow zone transfers to specific IP addresses, and avoid allowing transfers to arbitrary or unauthorized systems.

Use TSIG (Transaction Signature) Authentication:

Implement Transaction Signature (TSIG) authentication to secure the communication between primary and secondary DNS servers during zone transfers. TSIG helps ensure that only authorized servers can participate in the transfer process.

Firewall Rules:

Employ firewall rules to control and limit the traffic that can initiate or respond to DNS zone transfer requests. This helps prevent unauthorized systems from accessing sensitive DNS information.

Regular Monitoring:

Regularly monitor DNS logs and network traffic for any unusual or unauthorized activities. Detecting and responding to suspicious activities promptly can help mitigate potential risks.

DNSSEC (DNS Security Extensions):

Deploy DNSSEC to enhance the security of DNS data. DNSSEC helps in validating the authenticity and integrity of DNS information, reducing the risk of data tampering during zone transfers.

Task 7

Is it legal to use OSINT methods to get sensitive information?

The legality of using Open Source Intelligence (OSINT) methods to gather information depends on various factors, including the methods employed, the nature of the information sought, and the laws and regulations of the jurisdiction in question. OSINT itself refers to the collection and analysis of publicly available information from open sources, such as websites, social media, public records, and more.

Here are some general points to consider:

Publicly Available Information:

OSINT involves gathering information that is publicly accessible. If the information is freely available and does not involve unauthorized access to private systems or data, it is generally legal to collect.

Ethical Considerations:

While something may be legal, ethical considerations also come into play. It is important to use OSINT methods responsibly and avoid activities that could harm individuals or violate their privacy.

Respect for Terms of Service:

When conducting OSINT, it's essential to adhere to the terms of service of the platforms or websites from which you are gathering information. Violating terms of service could lead to legal consequences.

Privacy Laws:

Privacy laws vary by jurisdiction, and it's crucial to understand and comply with local regulations. In some cases, collecting and using certain types of information, especially personal or sensitive data, may be subject to privacy laws and require informed consent.

No Unauthorized Access:

OSINT methods should not involve unauthorized access to private systems, networks, or data. Unauthorized access is illegal and can lead to severe legal consequences.

Professional and Responsible Use:

Individuals and organizations conducting OSINT should act in a professional and responsible manner. Avoid activities that could be perceived as harassment, stalking, or any form of malicious intent.

Intellectual Property Rights:

Respect intellectual property rights when gathering and using information. Avoid copyright infringement and ensure compliance with intellectual property laws.

It's important to note that legal perspectives on OSINT can vary, and staying informed about the laws in your specific jurisdiction is crucial. Additionally, laws related to technology, privacy, and data protection are continually evolving, so it's advisable to seek legal advice when in doubt.

Task 8

What is the biggest threat in context of security and OSINT methods?

One of the significant threats in the context of security and Open Source Intelligence (OSINT) methods is the potential misuse of collected information for malicious purposes. While OSINT is a valuable tool for gathering publicly available information, it also poses risks when wielded by threat actors with malicious intent. Here are some key concerns:

Social Engineering Attacks:

Malicious actors can leverage OSINT to gather detailed information about individuals, organizations, or employees. This information can then be used in social engineering attacks, where attackers manipulate individuals into divulging sensitive information, such as login credentials or confidential data.

Targeted Attacks and Reconnaissance:

OSINT provides a wealth of information about potential targets, including network details, employee profiles, and infrastructure information. This information is valuable for attackers conducting targeted attacks and reconnaissance, helping them identify vulnerabilities and plan more effective and tailored cyberattacks.

Privacy Violations:

Collecting and aggregating information from various sources may lead to privacy violations. OSINT methods, if used irresponsibly, can compromise the privacy of individuals by exposing personal details, habits, or activities without their knowledge or consent.

Identity Theft:

OSINT can provide attackers with the necessary information to facilitate identity theft. By piecing together details from different sources, attackers can create a comprehensive profile of an individual, potentially leading to fraudulent activities using the stolen identity.

Corporate Espionage:

In the business context, OSINT can be used for corporate espionage. Competitors or malicious actors may gather information about an organization's strategies, partnerships, or proprietary technologies, leading to a competitive advantage or harm to the targeted company.

Stalking and Harassment:

OSINT can be misused for stalking and harassment purposes. Malicious actors may use gathered information to track and harass individuals, posing a significant threat to personal safety and well-being.

Information Warfare:

Nation-states and threat actors with geopolitical motives may use OSINT as part of information warfare campaigns. By manipulating and disseminating information, they can influence public opinion, create disinformation campaigns, or undermine trust in institutions.

Credential Stuffing Attacks:

OSINT can contribute to credential stuffing attacks where attackers use known information about individuals to attempt unauthorized access to various online accounts. This is especially effective if individuals reuse passwords across multiple platforms.

Task 9

How to protect your sensitive data from OSINT search?

Protecting sensitive data from Open Source Intelligence (OSINT) searches involves taking proactive measures to limit the availability of information and mitigate the risk of exposure. Here are some strategies to enhance the protection of sensitive data:

Review Online Presence:

Regularly review your online presence, including social media profiles, and adjust privacy settings to restrict the visibility of personal information. Be mindful of the details you share publicly.

Limit Personal Information:

Avoid sharing sensitive details, such as your home address, phone number, or specific financial information, on public platforms. Consider what information is necessary for others to know and limit disclosure accordingly.

Customize Privacy Settings:

Customize privacy settings on social media platforms and other online accounts to control who can access your information. Restrict access to personal details to only trusted individuals or contacts.

Be Mindful of Geotagging:

Disable geotagging features on photos and posts to prevent the inadvertent disclosure of your location. Geotagged information can be used in OSINT to track an individual's movements.

Use Pseudonyms:

Consider using pseudonyms or alternative names on public platforms to make it more challenging for OSINT analysts to link your online presence to your real identity.

Regularly Update Security Settings:

Regularly update and review the security settings of your online accounts. Platforms may introduce new features or settings that could impact your privacy.

Monitor Online Mentions:

Use online monitoring tools to keep track of mentions of your name, organization, or other sensitive information. This proactive approach allows you to be aware of any potential exposure and take corrective action.

Implement Email Security:

Use secure email practices, such as encrypted communication and secure email gateways, to protect sensitive information shared via email. Be cautious about sharing confidential details in unsecured communications.

Monitor and Remove Personal Information:

Regularly monitor online directories and public databases for personal information and request the removal of any unnecessary or outdated details. Many websites allow individuals to request the removal of personal data.

Legal Measures:

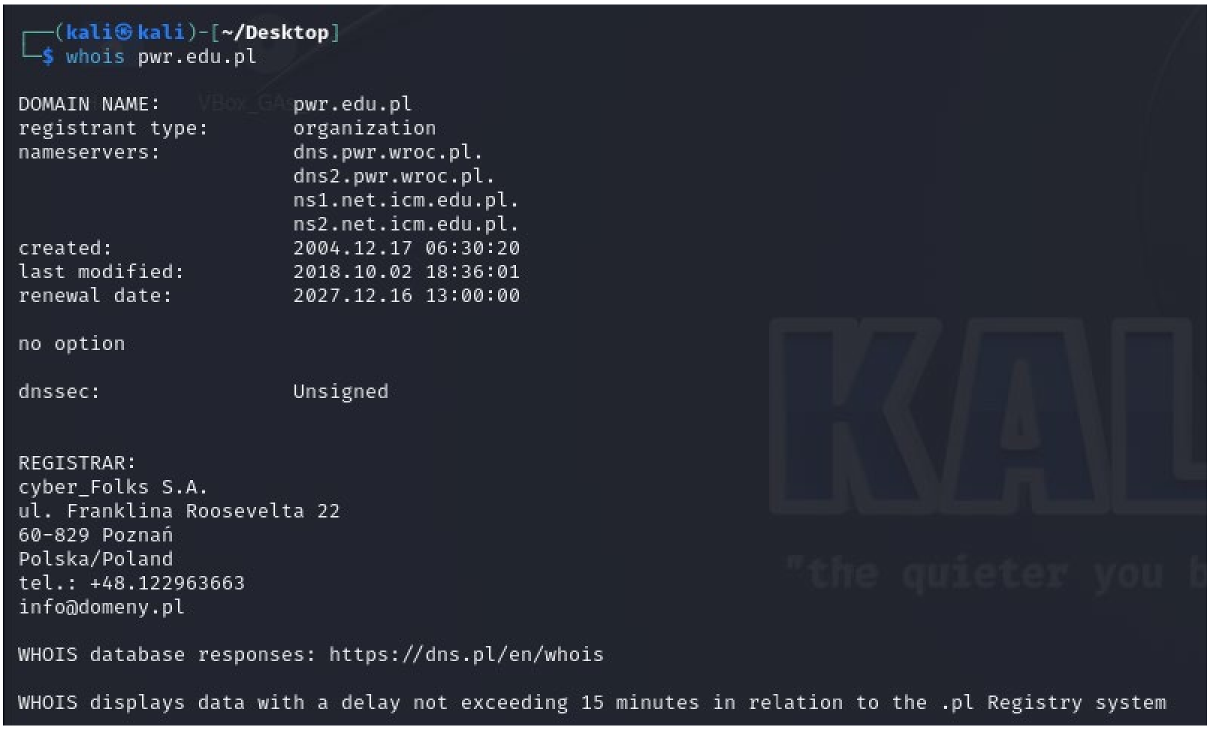
Familiarize yourself with privacy laws and regulations in your jurisdiction. If applicable, consider legal measures to request the removal of sensitive information from websites or databases.

Implement Network Security:

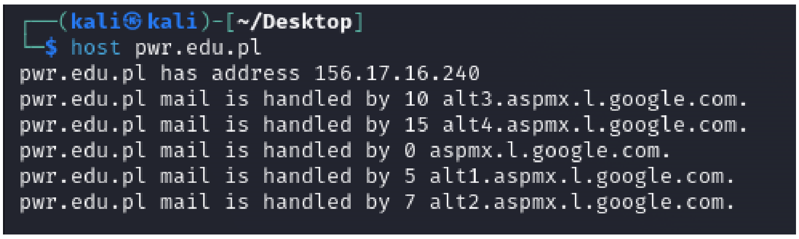
Ensure robust network security measures to protect against potential cyber threats. Use firewalls, intrusion detection/prevention systems, and other security tools to safeguard sensitive data.

Part 5

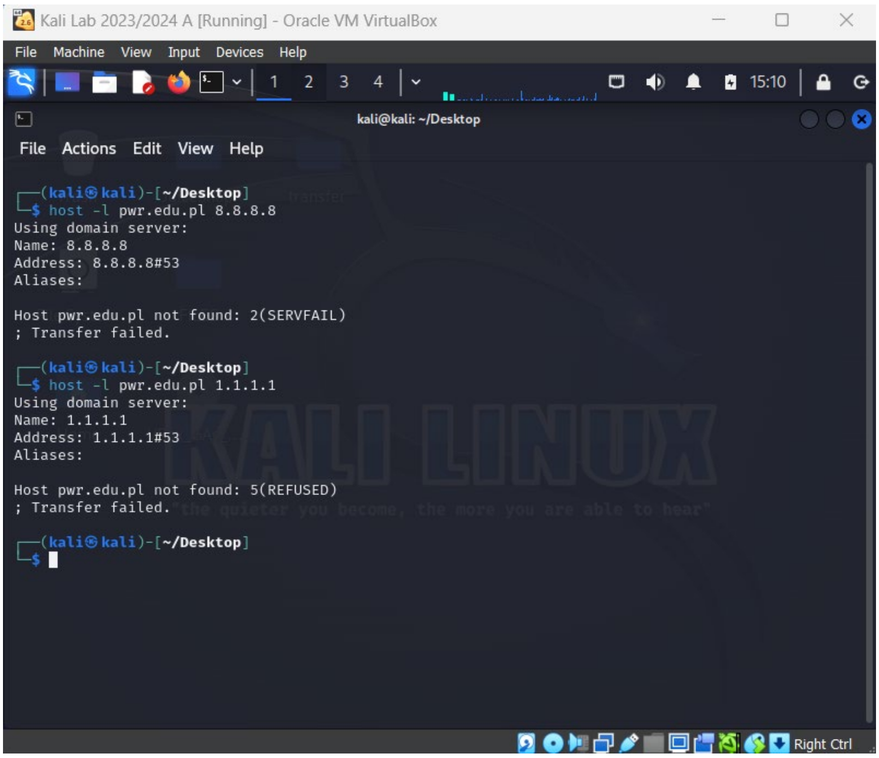
Analysed domain pwr.edu.pl



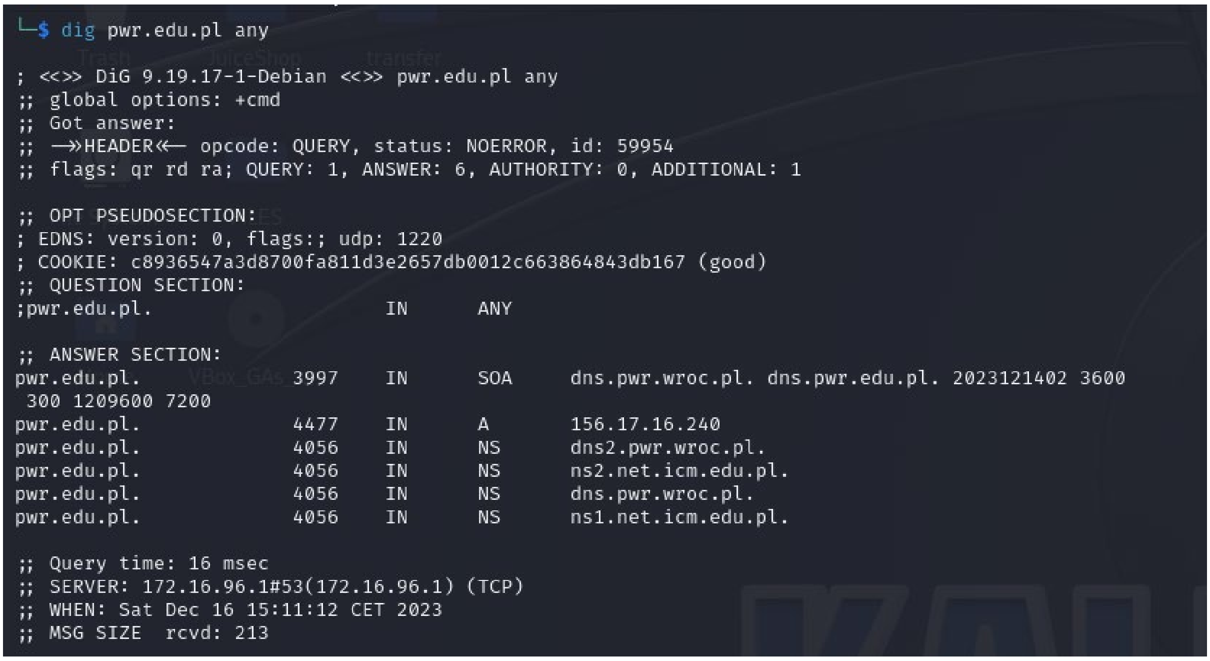
```
┌──(kali㉿kali)-[~/Desktop]
└─$ whois pwr.edu.pl

DOMAIN NAME:            pwr.edu.pl
registrant type:        organization
nameservers:            dns.pwr.wroc.pl.
                        dns2.pwr.wroc.pl.
                        ns1.net.icm.edu.pl.
                        ns2.net.icm.edu.pl.
created:                2004.12.17 06:30:20
last modified:          2018.10.02 18:36:01
renewal date:           2027.12.16 13:00:00

no option

dnssec:                 Unsigned


REGISTRAR:
cyber_Folks S.A.
ul. Franklina Roosevelta 22
60-829 Poznań
Polska/Poland
tel.: +48.122963663
info@domeny.pl

WHOIS database responses: https://dns.pl/en/whois

WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry system
```



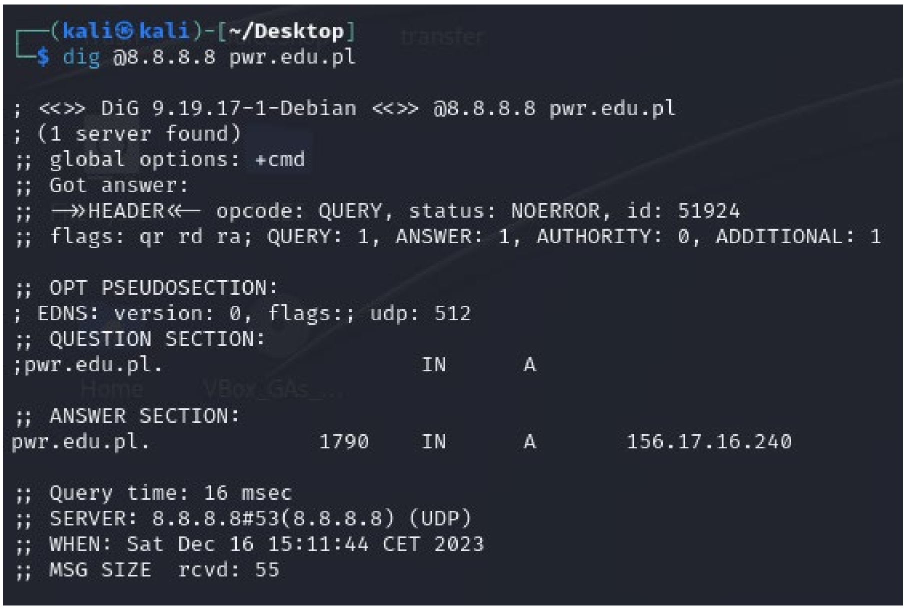
```
┌──(kali㉿kali)-[~/Desktop]
└─$ host pwr.edu.pl
pwr.edu.pl has address 156.17.16.240
pwr.edu.pl mail is handled by 10 alt3.aspmx.l.google.com.
pwr.edu.pl mail is handled by 15 alt4.aspmx.l.google.com.
pwr.edu.pl mail is handled by 0 aspmx.l.google.com.
pwr.edu.pl mail is handled by 5 alt1.aspmx.l.google.com.
pwr.edu.pl mail is handled by 7 alt2.aspmx.l.google.com.
```


Kali Lab 2023/2024 A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:10
kali@kali: ~/Desktop
File Actions Edit View Help
Right Ctrl

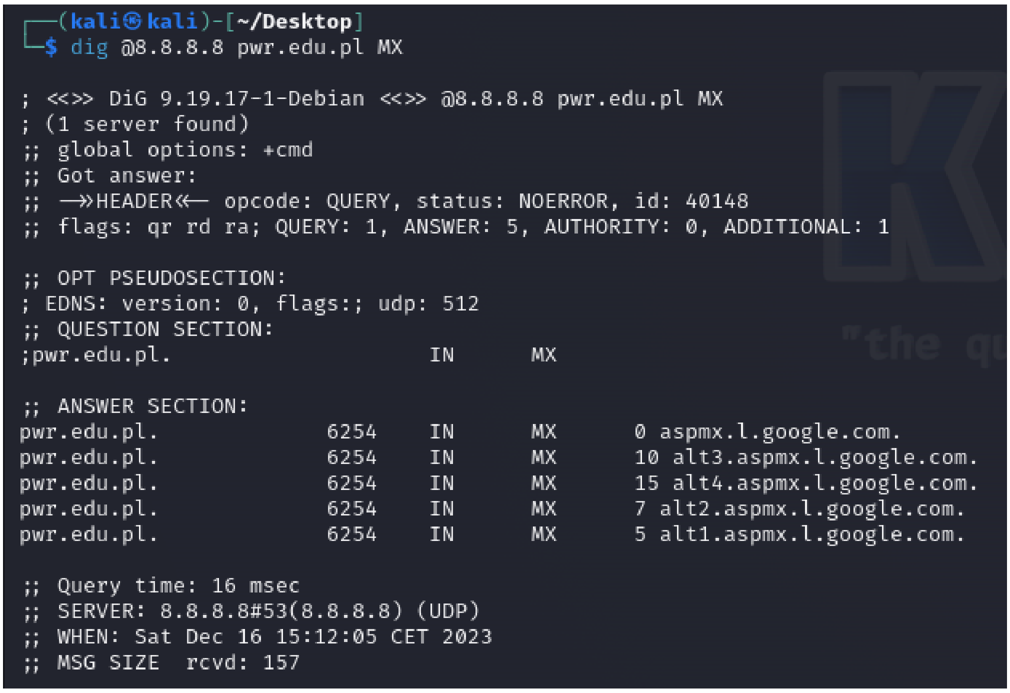
```
┌──(kali㉿kali)-[~/Desktop]
└─$ host -l pwr.edu.pl 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

Host pwr.edu.pl not found: 2(SERVFAIL)
; Transfer failed.

┌──(kali㉿kali)-[~/Desktop]
└─$ host -l pwr.edu.pl 1.1.1.1
Using domain server:
Name: 1.1.1.1
Address: 1.1.1.1#53
Aliases:

Host pwr.edu.pl not found: 5(REFUSED)
; Transfer failed.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```



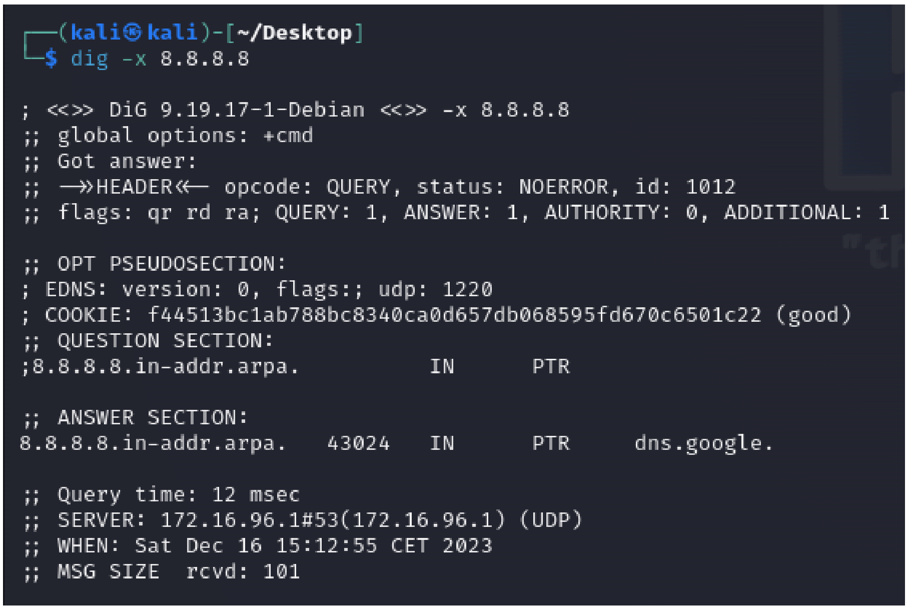
```
└─$ dig pwr.edu.pl any

; <<>> DiG 9.19.17-1-Debian <<>> pwr.edu.pl any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59954
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: c8936547a3d8700fa811d3e2657db0012c663864843db167 (good)
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      ANY

;; ANSWER SECTION:
pwr.edu.pl.             3997    IN      SOA     dns.pwr.wroc.pl. dns.pwr.edu.pl. 2023121402 3600
 300 1209600 7200
pwr.edu.pl.             4477    IN      A       156.17.16.240
pwr.edu.pl.             4056    IN      NS      dns2.pwr.wroc.pl.
pwr.edu.pl.             4056    IN      NS      ns2.net.icm.edu.pl.
pwr.edu.pl.             4056    IN      NS      dns.pwr.wroc.pl.
pwr.edu.pl.             4056    IN      NS      ns1.net.icm.edu.pl.

;; Query time: 16 msec
;; SERVER: 172.16.96.1#53(172.16.96.1) (TCP)
;; WHEN: Sat Dec 16 15:11:12 CET 2023
;; MSG SIZE  rcvd: 213
```



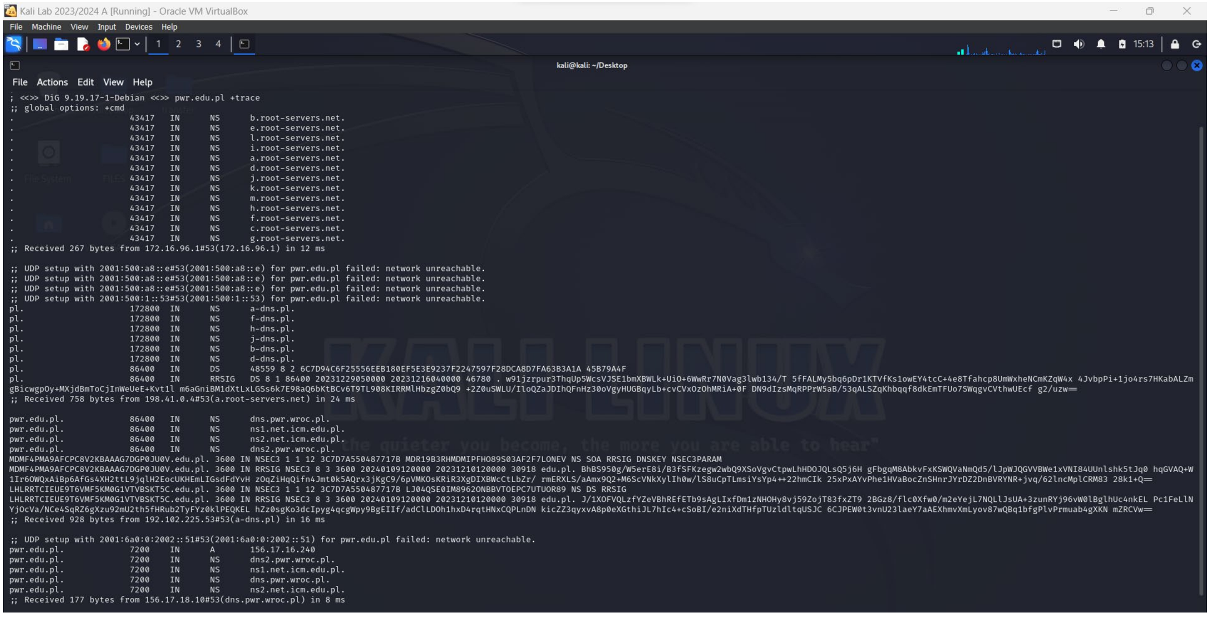
```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @8.8.8.8 pwr.edu.pl

; <<>> DiG 9.19.17-1-Debian <<>> @8.8.8.8 pwr.edu.pl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51924
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      A

;; ANSWER SECTION:
pwr.edu.pl.             1790    IN      A       156.17.16.240

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sat Dec 16 15:11:44 CET 2023
;; MSG SIZE  rcvd: 55
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @8.8.8.8 pwr.edu.pl MX

; <<>> DiG 9.19.17-1-Debian <<>> @8.8.8.8 pwr.edu.pl MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40148
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      MX

;; ANSWER SECTION:
pwr.edu.pl.             6254    IN      MX      0 aspmx.l.google.com.
pwr.edu.pl.             6254    IN      MX      10 alt3.aspmx.l.google.com.
pwr.edu.pl.             6254    IN      MX      15 alt4.aspmx.l.google.com.
pwr.edu.pl.             6254    IN      MX      7 alt2.aspmx.l.google.com.
pwr.edu.pl.             6254    IN      MX      5 alt1.aspmx.l.google.com.

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sat Dec 16 15:12:05 CET 2023
;; MSG SIZE  rcvd: 157
```

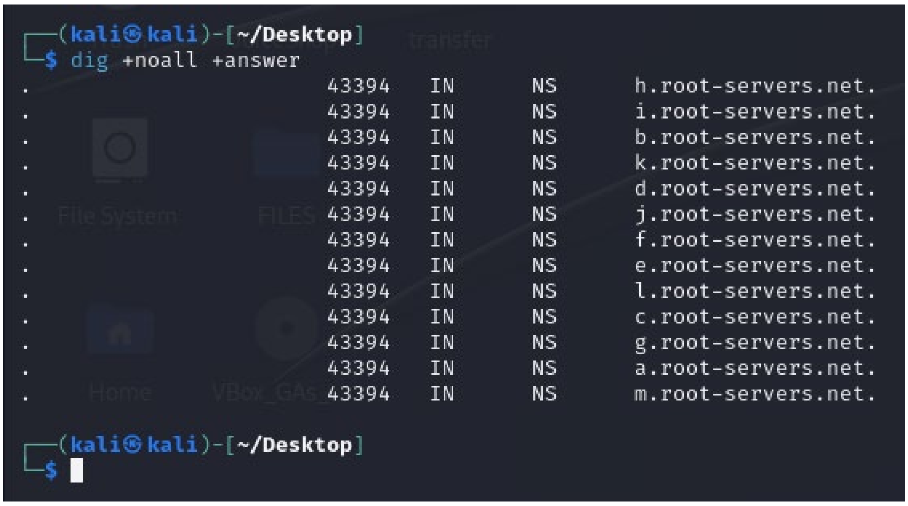


```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig -x 8.8.8.8

; <<>> DiG 9.19.17-1-Debian <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1012
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: f44513bc1ab788bc8340ca0d657db068595fd670c6501c22 (good)
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   43024   IN      PTR     dns.google.

;; Query time: 12 msec
;; SERVER: 172.16.96.1#53(172.16.96.1) (UDP)
;; WHEN: Sat Dec 16 15:12:55 CET 2023
;; MSG SIZE  rcvd: 101
```

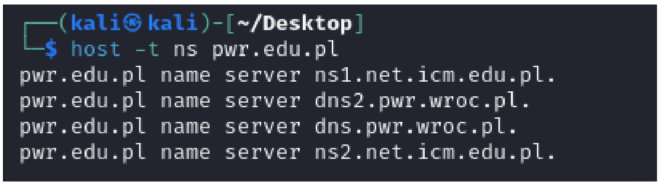


Kali Lab 2023/2024 A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:13
kali@kali: ~/Desktop
File Actions Edit View Help

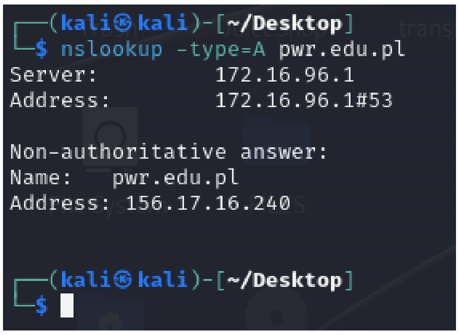
```
; <<>> DiG 9.19.17-1-Debian <<>> pwr.edu.pl +trace
;; global options: +cmd
.                       43417   IN      NS      b.root-servers.net.
.                       43417   IN      NS      e.root-servers.net.
.                       43417   IN      NS      l.root-servers.net.
.                       43417   IN      NS      i.root-servers.net.
.                       43417   IN      NS      a.root-servers.net.
.                       43417   IN      NS      d.root-servers.net.
.                       43417   IN      NS      j.root-servers.net.
.                       43417   IN      NS      k.root-servers.net.
.                       43417   IN      NS      m.root-servers.net.
.                       43417   IN      NS      h.root-servers.net.
.                       43417   IN      NS      f.root-servers.net.
.                       43417   IN      NS      c.root-servers.net.
.                       43417   IN      NS      g.root-servers.net.
;; Received 267 bytes from 172.16.96.1#53(172.16.96.1) in 12 ms

;; UDP setup with 2001:500:a8::e#53(2001:500:a8::e) for pwr.edu.pl failed: network unreachable.
;; UDP setup with 2001:500:a8::e#53(2001:500:a8::e) for pwr.edu.pl failed: network unreachable.
;; UDP setup with 2001:500:a8::e#53(2001:500:a8::e) for pwr.edu.pl failed: network unreachable.
;; UDP setup with 2001:500:1::53#53(2001:500:1::53) for pwr.edu.pl failed: network unreachable.
pl.                     172800  IN      NS      a-dns.pl.
pl.                     172800  IN      NS      f-dns.pl.
pl.                     172800  IN      NS      h-dns.pl.
pl.                     172800  IN      NS      j-dns.pl.
pl.                     172800  IN      NS      b-dns.pl.
pl.                     172800  IN      NS      d-dns.pl.
pl.                     86400   IN      DS      48559 8 2 6C7D94C6F25556EEB180EF5E3E9237F2247597F28DCA8D7FA63B3A1A 45B79A4F
pl.                     86400   IN      RRSIG   DS 8 1 86400 20231229050000 20231216040000 46780 . w91jzrpur3ThqUp5WcsVJSE1bmXBWLk+UiO+6WwRr7N0Vag3lwb134/T 5fFALMy5bq6pDr1KTVfKs1owEY4tcC+4e8Tfahcp8UmWxheNCmKZqW4x 4JvbpPi+1jo4rs7HKabALZm
gBicwgpOy+MXjdBmToCjInWeUeE+Kvt1l m6aGniBM1dXtLxLGSs6k7E98aQ6bKtBCv6T9TL908KIRRMlHbzgZ0bQ9 +2Z0uSWLU/IloQZaJDIhQFnHz30oVgyHUGBqyLb+cvCVxOzOhMRiA+0F DN9dIzsMqRPPrW5aB/53qALSZqKhbqqf8dkEmTFUo7SWqgvCVthwUEcf g2/uzw==
;; Received 758 bytes from 198.41.0.4#53(a.root-servers.net) in 24 ms

pwr.edu.pl.             86400   IN      NS      dns.pwr.wroc.pl.
pwr.edu.pl.             86400   IN      NS      ns1.net.icm.edu.pl.
pwr.edu.pl.             86400   IN      NS      ns2.net.icm.edu.pl.
pwr.edu.pl.             86400   IN      NS      dns2.pwr.wroc.pl.
MDMF4PMA9AFCPC8V2KBAAAG7DGP0JU0V.edu.pl. 3600 IN NSEC3 1 1 12 3C7D7A550487717B MDR19B3RHMDMIPFHO89S03AF2F7LONEV NS SOA RRSIG DNSKEY NSEC3PARAM
MDMF4PMA9AFCPC8V2KBAAAG7DGP0JU0V.edu.pl. 3600 IN RRSIG NSEC3 8 3 3600 20240109120000 20231210120000 30918 edu.pl. BhBS950g/W5erE8i/B3fSFKzegw2wbQ9XSoVgvCtpwLhHDOJQLsQ5j6H gFbgqM8AbkvFxKSWQVaNmQd5/lJpWJQGVVBWe1xVNI84UUnlshk5tJq0 hqGVAQ+W
1Ir6OWQxAiBp6AfGs4XH2ttL9jqlH2EocUKHEmLIGsdFdYvH zOqZiHqQifn4Jmt0k5AQrx3jKgC9/6pVMKOsKRiR3XgDIXBWcCtLbZr/ rmERXLS/aAmx9Q2+M6ScVNkXylIh0w/lS8uCpTLmsiYsYp4++22hmCIk 25xPxAYvPhe1HVaBocZnSHnrJYrDZ2DnBVRYNR+jvq/62lncMplCRM83 28k1+Q==
LHLRRTCIEUE9T6VMF5KM0G1VTVBSKT5C.edu.pl. 3600 IN NSEC3 1 1 12 3C7D7A550487717B LJ04QSE0IM8962ONBBVTOEPC7UTUOR89 NS DS RRSIG
LHLRRTCIEUE9T6VMF5KM0G1VTVBSKT5C.edu.pl. 3600 IN RRSIG NSEC3 8 3 3600 20240109120000 20231210120000 30918 edu.pl. J/1XOFVQLzfYZeVBhREfETb9sAgLIxfDm1zNHOHy8vj59ZojT83fxZT9 2BGz8/flc0Xfw0/m2eYejL7NQLlJsUA+3zunRYj96vW0lBglhUc4nkEL Pc1FeLlN
YjOcVa/NCe4SqRZ6gXzu92mU2th5fHRub2TyFYz0klPEQKEL hZz0sgKo3dcIpyg4qcgWpy9BgEIIf/adClLDOh1hxD4rqtHNxCQPLnDN kicZZ3qyxvA8p0eXGthiJL7hIc4+cSoBI/e2niXdTHfpTUzldltqUSJC 6CJPEW0t3vnU23laeY7aAEXhmvXmLyov87wQBq1bfgPlvPrmuab4gXKN mZRCVw==
;; Received 928 bytes from 192.102.225.53#53(a-dns.pl) in 16 ms

;; UDP setup with 2001:6a0:0:2002::51#53(2001:6a0:0:2002::51) for pwr.edu.pl failed: network unreachable.
pwr.edu.pl.             7200    IN      A       156.17.16.240
pwr.edu.pl.             7200    IN      NS      dns2.pwr.wroc.pl.
pwr.edu.pl.             7200    IN      NS      ns1.net.icm.edu.pl.
pwr.edu.pl.             7200    IN      NS      dns.pwr.wroc.pl.
pwr.edu.pl.             7200    IN      NS      ns2.net.icm.edu.pl.
;; Received 177 bytes from 156.17.18.10#53(dns.pwr.wroc.pl) in 8 ms
```



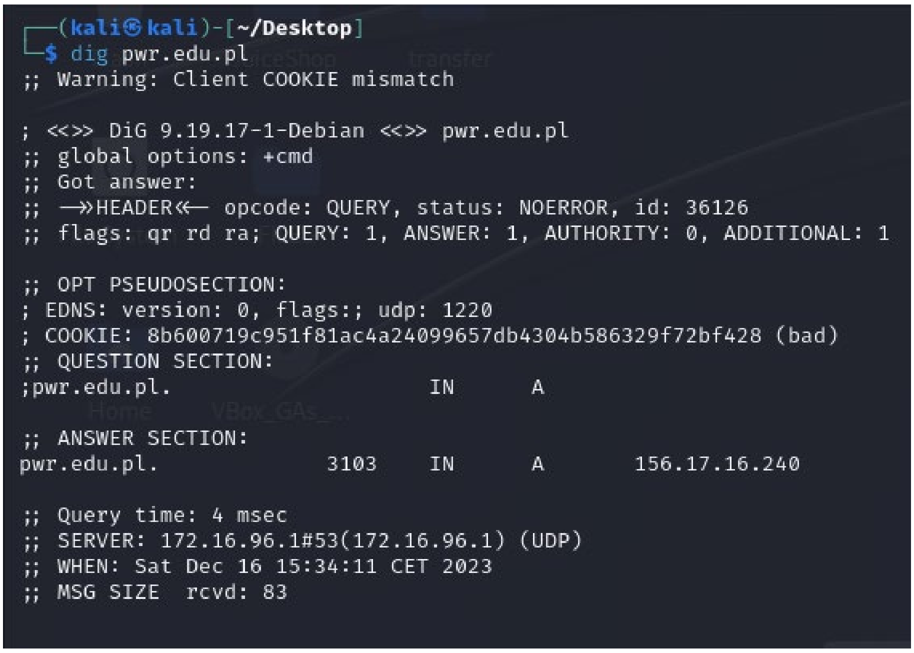
```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig +noall +answer
.                       43394   IN      NS      h.root-servers.net.
.                       43394   IN      NS      i.root-servers.net.
.                       43394   IN      NS      b.root-servers.net.
.                       43394   IN      NS      k.root-servers.net.
.                       43394   IN      NS      d.root-servers.net.
.                       43394   IN      NS      j.root-servers.net.
.                       43394   IN      NS      f.root-servers.net.
.                       43394   IN      NS      e.root-servers.net.
.                       43394   IN      NS      l.root-servers.net.
.                       43394   IN      NS      c.root-servers.net.
.                       43394   IN      NS      g.root-servers.net.
.                       43394   IN      NS      a.root-servers.net.
.                       43394   IN      NS      m.root-servers.net.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```



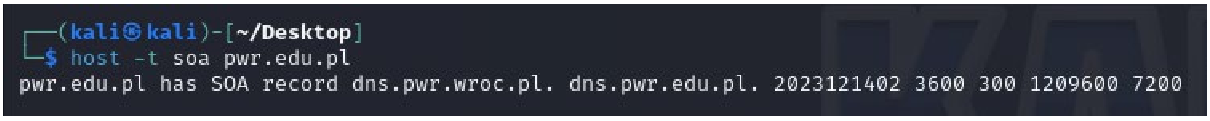
```
┌──(kali㉿kali)-[~/Desktop]
└─$ host -t ns pwr.edu.pl
pwr.edu.pl name server ns1.net.icm.edu.pl.
pwr.edu.pl name server dns2.pwr.wroc.pl.
pwr.edu.pl name server dns.pwr.wroc.pl.
pwr.edu.pl name server ns2.net.icm.edu.pl.
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup -type=A pwr.edu.pl
Server:         172.16.96.1
Address:        172.16.96.1#53

Non-authoritative answer:
Name:   pwr.edu.pl
Address: 156.17.16.240


┌──(kali㉿kali)-[~/Desktop]
└─$ ▮
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig pwr.edu.pl
;; Warning: Client COOKIE mismatch

; <<>> DiG 9.19.17-1-Debian <<>> pwr.edu.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36126
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 8b600719c951f81ac4a24099657db4304b586329f72bf428 (bad)
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      A

;; ANSWER SECTION:
pwr.edu.pl.             3103    IN      A       156.17.16.240

;; Query time: 4 msec
;; SERVER: 172.16.96.1#53(172.16.96.1) (UDP)
;; WHEN: Sat Dec 16 15:34:11 CET 2023
;; MSG SIZE  rcvd: 83
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ host -t soa pwr.edu.pl
pwr.edu.pl has SOA record dns.pwr.wroc.pl. dns.pwr.edu.pl. 2023121402 3600 300 1209600 7200
```

Domain Name:

pwr.edu.pl is the domain for which the SOA record is being queried.

SOA Record Information:

dns.pwr.wroc.pl. is the primary authoritative DNS server for the domain.

dns.pwr.edu.pl. is the email address of the domain administrator.

2023121402 is the serial number of the zone. This number is typically updated whenever there's a change to the DNS records within the domain. In this case, the serial number is represented as a date (December 14, 2023) followed by a two-digit increment (02).

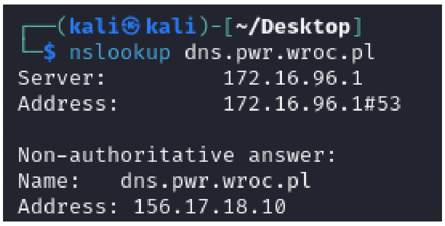
Timing Parameters:

3600 is the refresh interval. It indicates the time (in seconds) during which secondary DNS servers should check with the primary DNS server for updates. In this case, it's set to 1 hour.

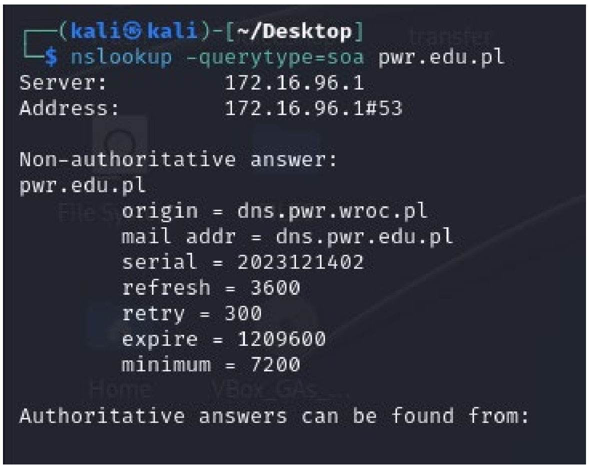
300 is the retry interval. It specifies the time (in seconds) secondary servers should wait before retrying a failed zone transfer. Here, it's set to 300 seconds.

1209600 is the expiry interval. It represents the maximum time (in seconds) a secondary server can use the zone data before considering it outdated. In this case, it's set to 14 days.

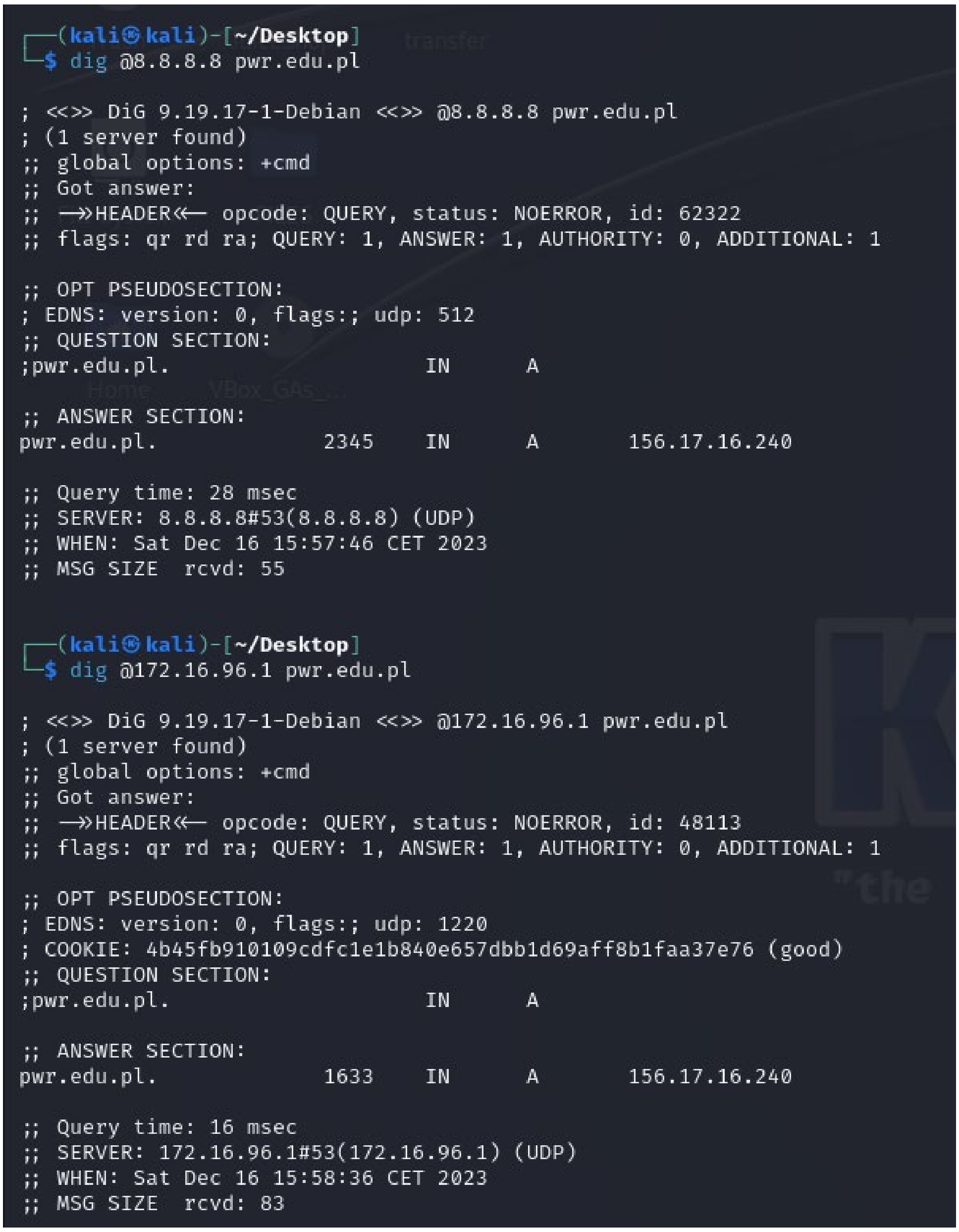
7200 is the minimum (default) TTL (Time to Live). It is the default TTL for resource records in the zone. In this example, it's set to 2 hours.



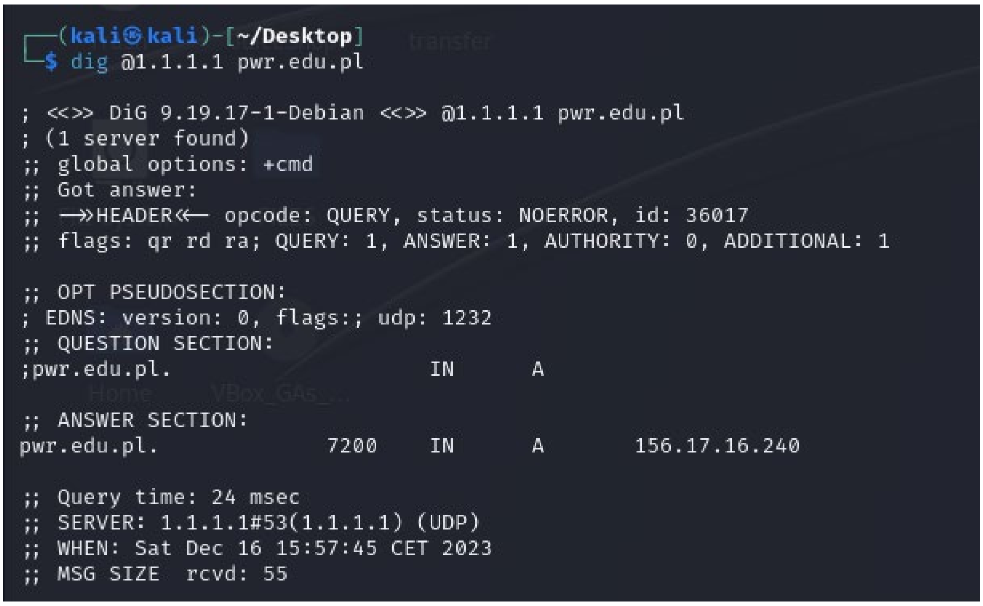
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup dns.pwr.wroc.pl
Server:         172.16.96.1
Address:        172.16.96.1#53

Non-authoritative answer:
Name:   dns.pwr.wroc.pl
Address: 156.17.18.10
```



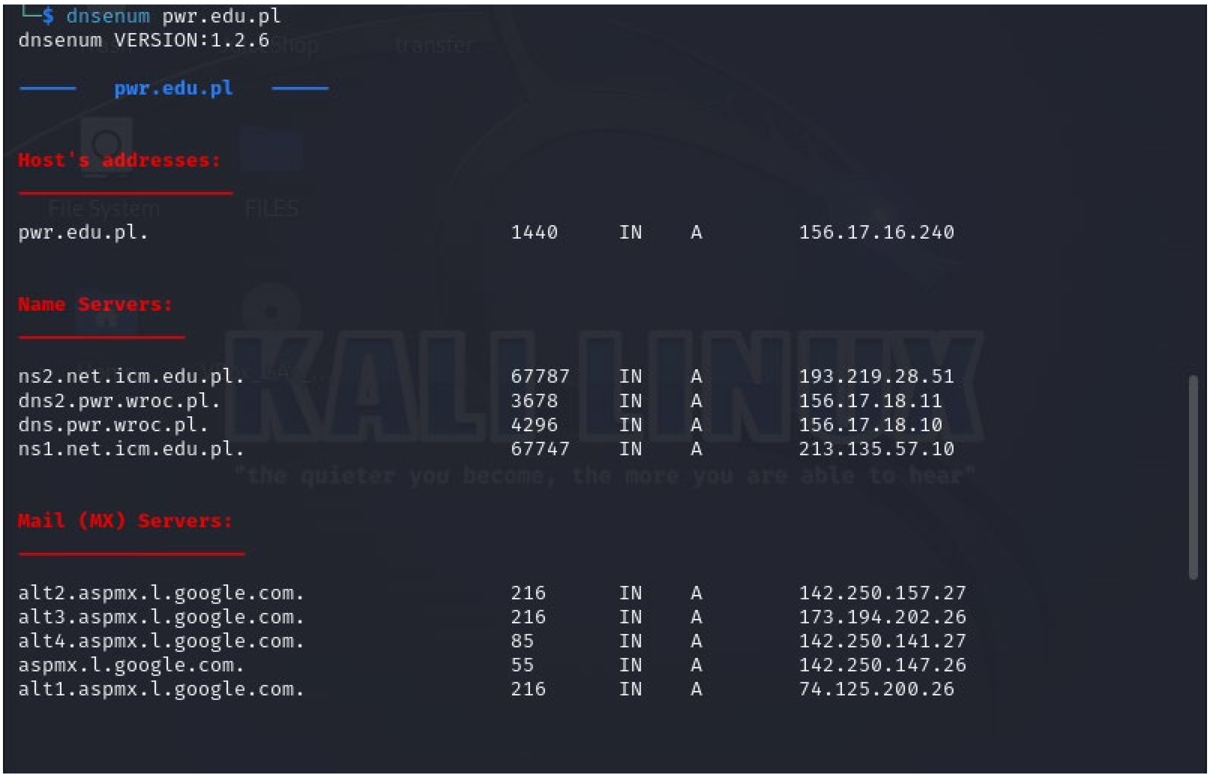
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup -querytype=soa pwr.edu.pl
Server:         172.16.96.1
Address:        172.16.96.1#53

Non-authoritative answer:
pwr.edu.pl
        origin = dns.pwr.wroc.pl
        mail addr = dns.pwr.edu.pl
        serial = 2023121402
        refresh = 3600
        retry = 300
        expire = 1209600
        minimum = 7200

Authoritative answers can be found from:
```



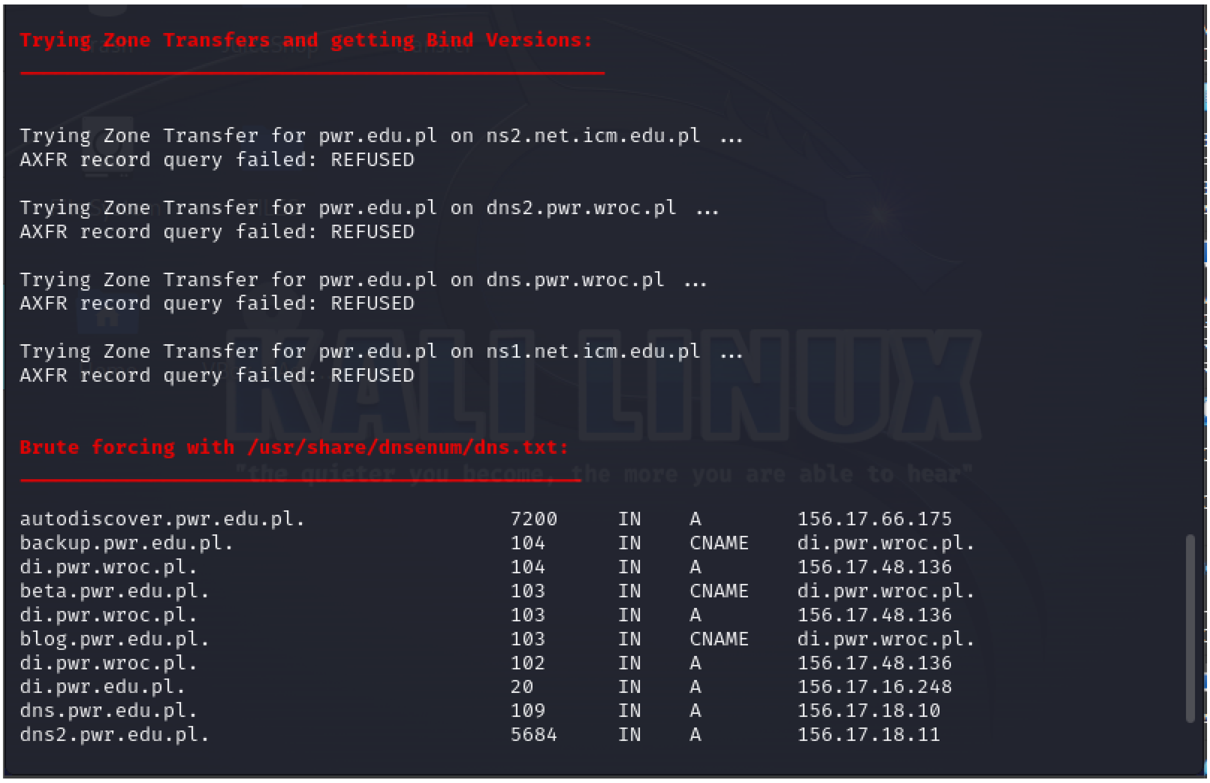
```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @8.8.8.8 pwr.edu.pl

; <<>> DiG 9.19.17-1-Debian <<>> @8.8.8.8 pwr.edu.pl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62322
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      A

;; ANSWER SECTION:
pwr.edu.pl.             2345    IN      A       156.17.16.240

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sat Dec 16 15:57:46 CET 2023
;; MSG SIZE  rcvd: 55


┌──(kali㉿kali)-[~/Desktop]
└─$ dig @172.16.96.1 pwr.edu.pl

; <<>> DiG 9.19.17-1-Debian <<>> @172.16.96.1 pwr.edu.pl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48113
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 4b45fb910109cdfc1e1b840e657dbb1d69aff8b1faa37e76 (good)
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      A

;; ANSWER SECTION:
pwr.edu.pl.             1633    IN      A       156.17.16.240

;; Query time: 16 msec
;; SERVER: 172.16.96.1#53(172.16.96.1) (UDP)
;; WHEN: Sat Dec 16 15:58:36 CET 2023
;; MSG SIZE  rcvd: 83
```



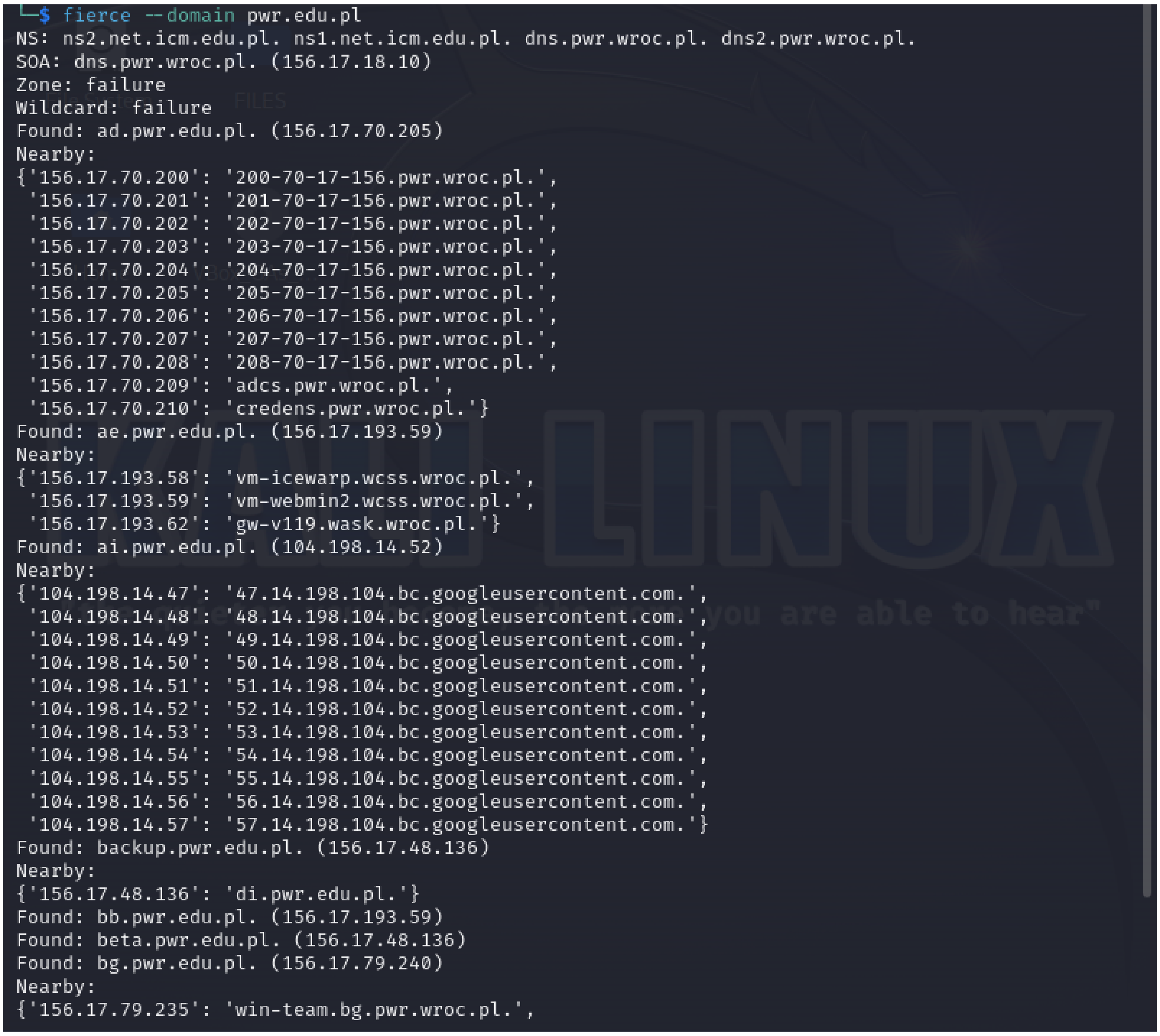
```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @1.1.1.1 pwr.edu.pl

; <<>> DiG 9.19.17-1-Debian <<>> @1.1.1.1 pwr.edu.pl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36017
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;pwr.edu.pl.                    IN      A

;; ANSWER SECTION:
pwr.edu.pl.             7200    IN      A       156.17.16.240

;; Query time: 24 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Sat Dec 16 15:57:45 CET 2023
;; MSG SIZE  rcvd: 55
```



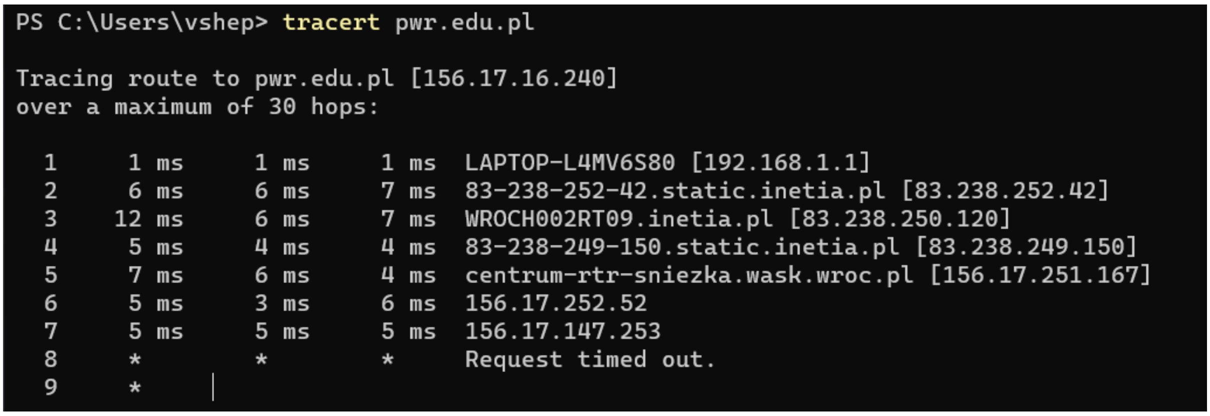
```
└─$ dnsenum pwr.edu.pl
dnsenum VERSION:1.2.6

-----   pwr.edu.pl   -----


Host's addresses:
__________________

pwr.edu.pl.                              1440     IN    A        156.17.16.240


Name Servers:
______________

ns2.net.icm.edu.pl.                      67787    IN    A        193.219.28.51
dns2.pwr.wroc.pl.                        3678     IN    A        156.17.18.11
dns.pwr.wroc.pl.                         4296     IN    A        156.17.18.10
ns1.net.icm.edu.pl.                      67747    IN    A        213.135.57.10


Mail (MX) Servers:
___________________

alt2.aspmx.l.google.com.                 216      IN    A        142.250.157.27
alt3.aspmx.l.google.com.                 216      IN    A        173.194.202.26
alt4.aspmx.l.google.com.                 85       IN    A        142.250.141.27
aspmx.l.google.com.                      55       IN    A        142.250.147.26
alt1.aspmx.l.google.com.                 216      IN    A        74.125.200.26
```



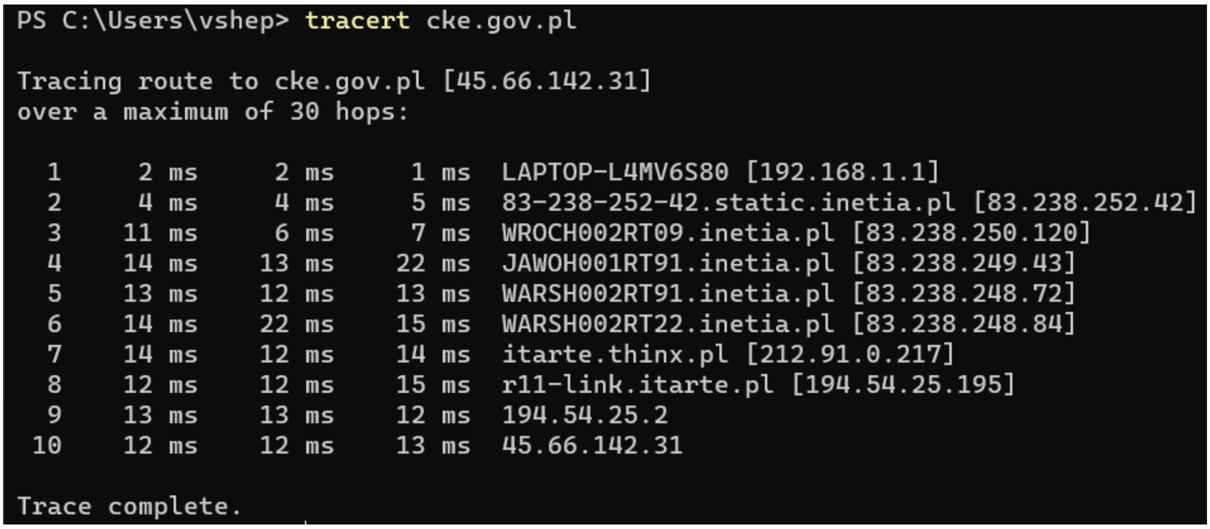
```
Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for pwr.edu.pl on ns2.net.icm.edu.pl ...
AXFR record query failed: REFUSED

Trying Zone Transfer for pwr.edu.pl on dns2.pwr.wroc.pl ...
AXFR record query failed: REFUSED

Trying Zone Transfer for pwr.edu.pl on dns.pwr.wroc.pl ...
AXFR record query failed: REFUSED

Trying Zone Transfer for pwr.edu.pl on ns1.net.icm.edu.pl ...
AXFR record query failed: REFUSED


Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

autodiscover.pwr.edu.pl.                 7200     IN    A        156.17.66.175
backup.pwr.edu.pl.                       104      IN    CNAME    di.pwr.wroc.pl.
di.pwr.wroc.pl.                          104      IN    A        156.17.48.136
beta.pwr.edu.pl.                         103      IN    CNAME    di.pwr.wroc.pl.
di.pwr.wroc.pl.                          103      IN    A        156.17.48.136
blog.pwr.edu.pl.                         103      IN    CNAME    di.pwr.wroc.pl.
di.pwr.wroc.pl.                          102      IN    A        156.17.48.136
di.pwr.edu.pl.                           20       IN    A        156.17.16.248
dns.pwr.edu.pl.                          109      IN    A        156.17.18.10
dns2.pwr.edu.pl.                         5684     IN    A        156.17.18.11
```



```
└─$ fierce --domain pwr.edu.pl
NS: ns2.net.icm.edu.pl. ns1.net.icm.edu.pl. dns.pwr.wroc.pl. dns2.pwr.wroc.pl.
SOA: dns.pwr.wroc.pl. (156.17.18.10)
Zone: failure
Wildcard: failure
Found: ad.pwr.edu.pl. (156.17.70.205)
Nearby:
{'156.17.70.200': '200-70-17-156.pwr.wroc.pl.',
 '156.17.70.201': '201-70-17-156.pwr.wroc.pl.',
 '156.17.70.202': '202-70-17-156.pwr.wroc.pl.',
 '156.17.70.203': '203-70-17-156.pwr.wroc.pl.',
 '156.17.70.204': '204-70-17-156.pwr.wroc.pl.',
 '156.17.70.205': '205-70-17-156.pwr.wroc.pl.',
 '156.17.70.206': '206-70-17-156.pwr.wroc.pl.',
 '156.17.70.207': '207-70-17-156.pwr.wroc.pl.',
 '156.17.70.208': '208-70-17-156.pwr.wroc.pl.',
 '156.17.70.209': 'adcs.pwr.wroc.pl.',
 '156.17.70.210': 'credens.pwr.wroc.pl.'}
Found: ae.pwr.edu.pl. (156.17.193.59)
Nearby:
{'156.17.193.58': 'vm-icewarp.wcss.wroc.pl.',
 '156.17.193.59': 'vm-webmin2.wcss.wroc.pl.',
 '156.17.193.62': 'gw-v119.wask.wroc.pl.'}
Found: ai.pwr.edu.pl. (104.198.14.52)
Nearby:
{'104.198.14.47': '47.14.198.104.bc.googleusercontent.com.',
 '104.198.14.48': '48.14.198.104.bc.googleusercontent.com.',
 '104.198.14.49': '49.14.198.104.bc.googleusercontent.com.',
 '104.198.14.50': '50.14.198.104.bc.googleusercontent.com.',
 '104.198.14.51': '51.14.198.104.bc.googleusercontent.com.',
 '104.198.14.52': '52.14.198.104.bc.googleusercontent.com.',
 '104.198.14.53': '53.14.198.104.bc.googleusercontent.com.',
 '104.198.14.54': '54.14.198.104.bc.googleusercontent.com.',
 '104.198.14.55': '55.14.198.104.bc.googleusercontent.com.',
 '104.198.14.56': '56.14.198.104.bc.googleusercontent.com.',
 '104.198.14.57': '57.14.198.104.bc.googleusercontent.com.'}
Found: backup.pwr.edu.pl. (156.17.48.136)
Nearby:
{'156.17.48.136': 'di.pwr.edu.pl.'}
Found: bb.pwr.edu.pl. (156.17.193.59)
Found: beta.pwr.edu.pl. (156.17.48.136)
Found: bg.pwr.edu.pl. (156.17.79.240)
Nearby:
{'156.17.79.235': 'win-team.bg.pwr.wroc.pl.',
```

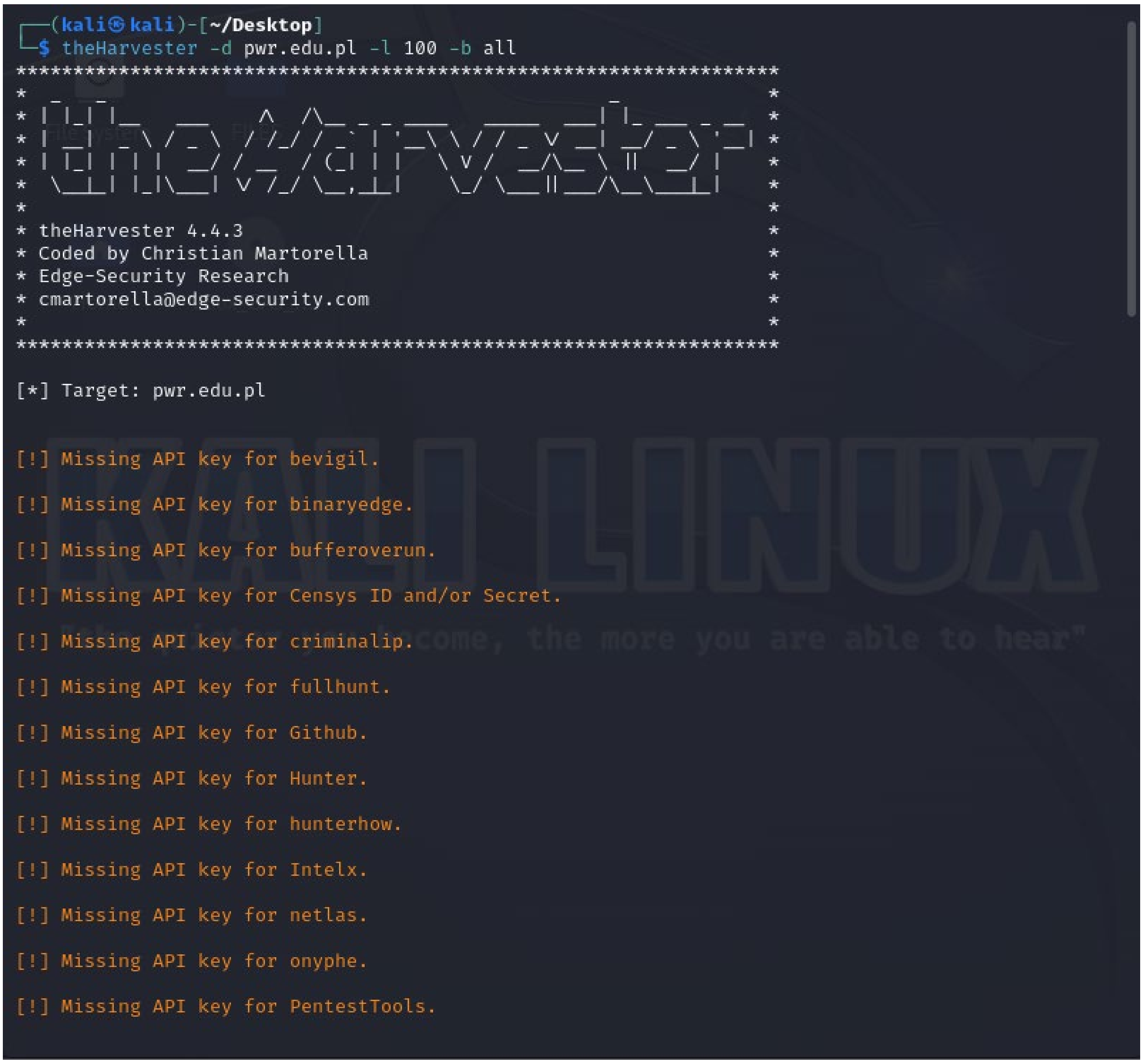


```
PS C:\Users\vshep> tracert pwr.edu.pl

Tracing route to pwr.edu.pl [156.17.16.240]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  LAPTOP-L4MV6S80 [192.168.1.1]
  2     6 ms     6 ms     7 ms  83-238-252-42.static.inetia.pl [83.238.252.42]
  3    12 ms     6 ms     7 ms  WROCH002RT09.inetia.pl [83.238.250.120]
  4     5 ms     4 ms     4 ms  83-238-249-150.static.inetia.pl [83.238.249.150]
  5     7 ms     6 ms     4 ms  centrum-rtr-sniezka.wask.wroc.pl [156.17.251.167]
  6     5 ms     3 ms     6 ms  156.17.252.52
  7     5 ms     5 ms     5 ms  156.17.147.253
  8     *        *        *     Request timed out.
  9     *
```

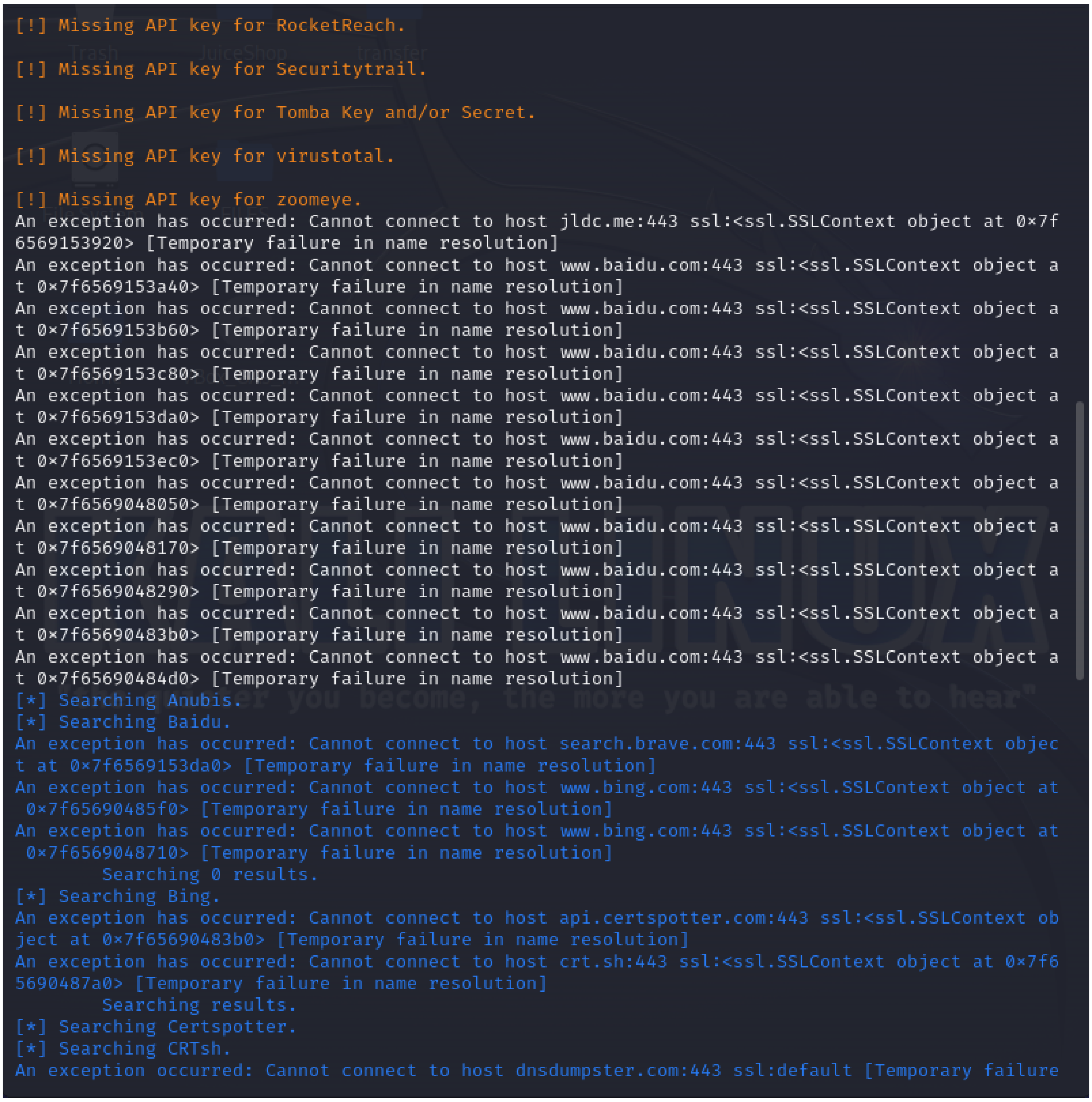


```
PS C:\Users\vshep> tracert cke.gov.pl

Tracing route to cke.gov.pl [45.66.142.31]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  LAPTOP-L4MV6S80 [192.168.1.1]
  2     4 ms     4 ms     5 ms  83-238-252-42.static.inetia.pl [83.238.252.42]
  3    11 ms     6 ms     7 ms  WROCH002RT09.inetia.pl [83.238.250.120]
  4    14 ms    13 ms    22 ms  JAWOH001RT91.inetia.pl [83.238.249.43]
  5    13 ms    12 ms    13 ms  WARSH002RT91.inetia.pl [83.238.248.72]
  6    14 ms    22 ms    15 ms  WARSH002RT22.inetia.pl [83.238.248.84]
  7    14 ms    12 ms    14 ms  itarte.thinx.pl [212.91.0.217]
  8    12 ms    12 ms    15 ms  r11-link.itarte.pl [194.54.25.195]
  9    13 ms    13 ms    12 ms  194.54.25.2
 10    12 ms    12 ms    13 ms  45.66.142.31

Trace complete.
```

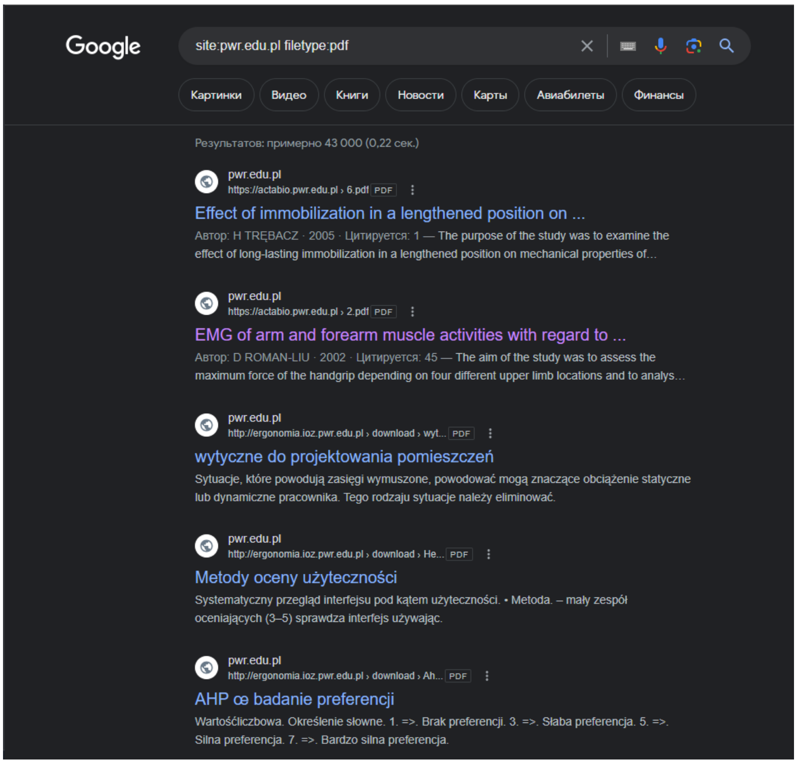
By leveraging a combination of powerful tools, we successfully gathered valuable insights about a given domain. Utilizing the 'whois' command, we obtained details about the domain registration, including registrant information. Employing 'dig,' we extracted the domain's IP address, while the 'host' command provided information about the DNS server associated with the domain. Additionally, we delved into the domain's hosted services using tools such as 'dnsenum' and 'fierce,' enabling us to uncover further details about the services running on the server



```
┌──(kali㉿kali)-[~/Desktop]
└─$ theHarvester -d pwr.edu.pl -l 100 -b all
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: pwr.edu.pl


[!] Missing API key for bevigil.

[!] Missing API key for binaryedge.

[!] Missing API key for bufferoverun.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for criminalip.

[!] Missing API key for fullhunt.

[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for hunterhow.

[!] Missing API key for Intelx.

[!] Missing API key for netlas.

[!] Missing API key for onyphe.

[!] Missing API key for PentestTools.
```



```
[!] Missing API key for RocketReach.

[!] Missing API key for Securitytrail.

[!] Missing API key for Tomba Key and/or Secret.

[!] Missing API key for virustotal.

[!] Missing API key for zoomeye.
An exception has occurred: Cannot connect to host jldc.me:443 ssl:<ssl.SSLContext object at 0x7f
6569153920> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569153a40> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569153b60> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569153c80> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569153da0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569153ec0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569048050> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569048170> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f6569048290> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f65690483b0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object a
t 0x7f65690484d0> [Temporary failure in name resolution]
[*] Searching Anubis.
[*] Searching Baidu.
An exception has occurred: Cannot connect to host search.brave.com:443 ssl:<ssl.SSLContext objec
t at 0x7f6569153da0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.bing.com:443 ssl:<ssl.SSLContext object at
 0x7f65690485f0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host www.bing.com:443 ssl:<ssl.SSLContext object at
 0x7f6569048710> [Temporary failure in name resolution]
        Searching 0 results.
[*] Searching Bing.
An exception has occurred: Cannot connect to host api.certspotter.com:443 ssl:<ssl.SSLContext ob
ject at 0x7f65690483b0> [Temporary failure in name resolution]
An exception has occurred: Cannot connect to host crt.sh:443 ssl:<ssl.SSLContext object at 0x7f6
5690487a0> [Temporary failure in name resolution]
        Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
An exception occurred: Cannot connect to host dnsdumpster.com:443 ssl:default [Temporary failure
```



site:pwr.edu.pl filetype:pdf

Результатов: примерно 43 000 (0,22 сек.)

pwr.edu.pl
https://actabio.pwr.edu.pl › 6.pdf PDF

Effect of immobilization in a lengthened position on ...

Автор: H TRĘBACZ · 2005 · Цитируется: 1 — The purpose of the study was to examine the effect of long-lasting immobilization in a lengthened position on mechanical properties of...

pwr.edu.pl
https://actabio.pwr.edu.pl › 2.pdf PDF

EMG of arm and forearm muscle activities with regard to ...

Автор: D ROMAN-LIU · 2002 · Цитируется: 45 — The aim of the study was to assess the maximum force of the handgrip depending on four different upper limb locations and to analys...

pwr.edu.pl
http://ergonomia.ioz.pwr.edu.pl › download › wyt... PDF

wytyczne do projektowania pomieszczeń

Sytuacje, które powodują zasięgi wymuszone, powodować mogą znaczące obciążenie statyczne lub dynamiczne pracownika. Tego rodzaju sytuacje należy eliminować.

pwr.edu.pl
http://ergonomia.ioz.pwr.edu.pl › download › He... PDF

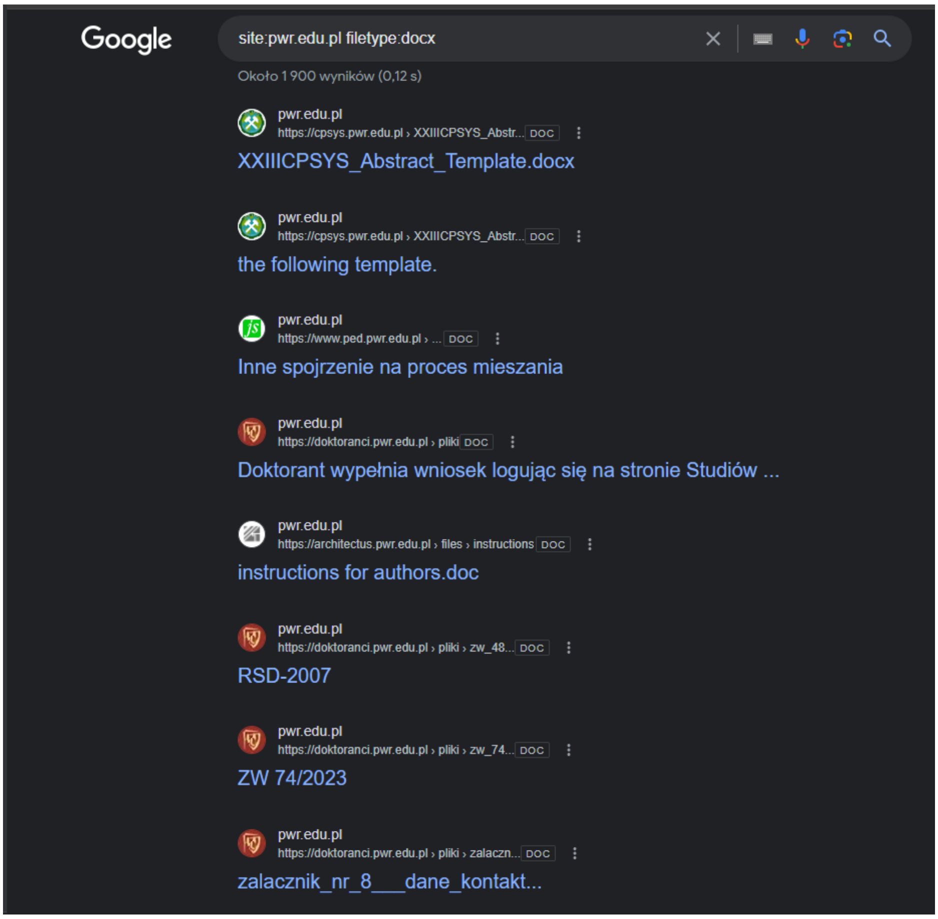
Metody oceny użyteczności

Systematyczny przegląd interfejsu pod kątem użyteczności. • Metoda. – mały zespół oceniających (3–5) sprawdza interfejs używając.

pwr.edu.pl
http://ergonomia.ioz.pwr.edu.pl › download › Ah... PDF

AHP œ badanie preferencji

Wartośćliczbowa. Określenie słowne. 1. =>. Brak preferencji. 3. =>. Słaba preferencja. 5. =>. Silna preferencja. 7. =>. Bardzo silna preferencja.



site:pwr.edu.pl filetype:docx

Około 1 900 wyników (0,12 s)

pwr.edu.pl
https://cpsys.pwr.edu.pl › XXIIICPSYS_Abstr... DOC

XXIIICPSYS_Abstract_Template.docx

pwr.edu.pl
https://cpsys.pwr.edu.pl › XXIIICPSYS_Abstr... DOC

the following template.

pwr.edu.pl
https://www.ped.pwr.edu.pl › ... DOC

Inne spojrzenie na proces mieszania

pwr.edu.pl
https://doktoranci.pwr.edu.pl › pliki DOC

Doktorant wypełnia wniosek logując się na stronie Studiów ...

pwr.edu.pl
https://architectus.pwr.edu.pl › files › instructions DOC

instructions for authors.doc

pwr.edu.pl
https://doktoranci.pwr.edu.pl › pliki › zw_48... DOC

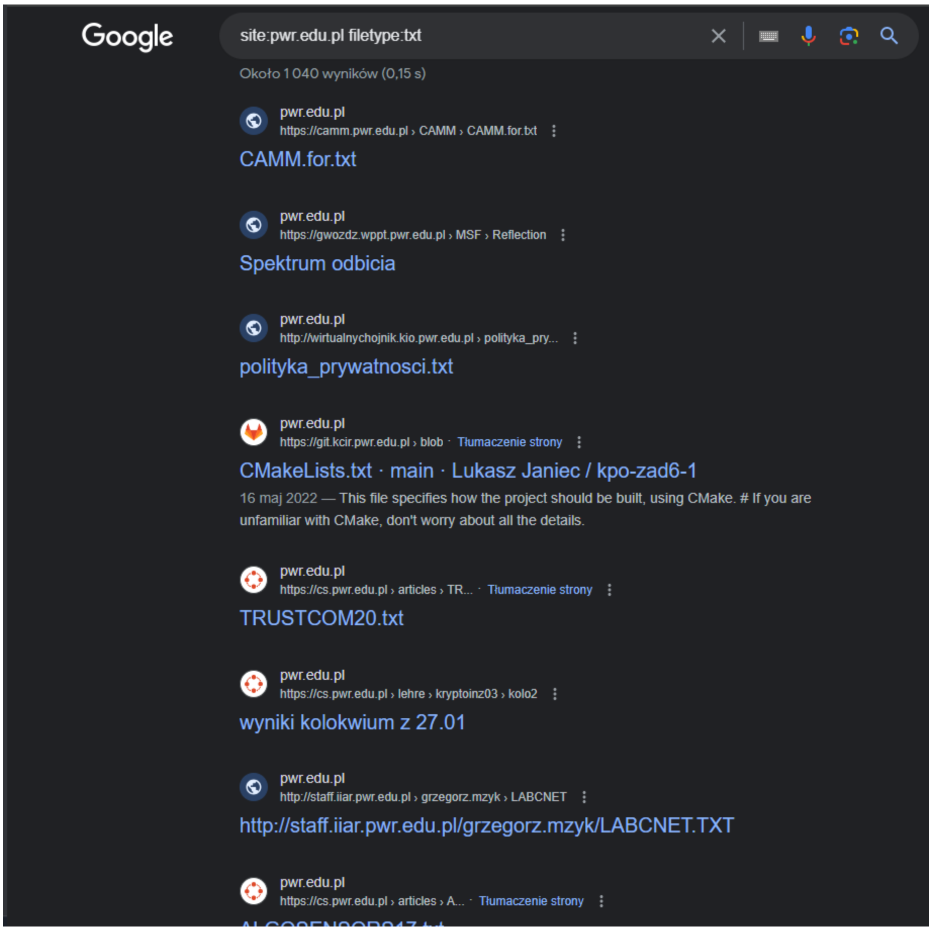
RSD-2007

pwr.edu.pl
https://doktoranci.pwr.edu.pl › pliki › zw_74... DOC

ZW 74/2023

pwr.edu.pl
https://doktoranci.pwr.edu.pl › pliki › zalaczn... DOC

zalacznik_nr_8___dane_kontakt...



Google

site:pwr.edu.pl filetype:txt

Około 1 040 wyników (0,15 s)

pwr.edu.pl
https://camm.pwr.edu.pl › CAMM › CAMM.for.txt

CAMM.for.txt

pwr.edu.pl
https://gwozdz.wppt.pwr.edu.pl › MSF › Reflection

Spektrum odbicia

pwr.edu.pl
http://wirtualnychojnik.kio.pwr.edu.pl › polityka_pry...

polityka_prywatnosci.txt

pwr.edu.pl
https://git.kcir.pwr.edu.pl › blob · Tłumaczenie strony

CMakeLists.txt · main · Lukasz Janiec / kpo-zad6-1

16 maj 2022 — This file specifies how the project should be built, using CMake. # If you are unfamiliar with CMake, don't worry about all the details.

pwr.edu.pl
https://cs.pwr.edu.pl › articles › TR... · Tłumaczenie strony

TRUSTCOM20.txt

pwr.edu.pl
https://cs.pwr.edu.pl › lehre › kryptoinz03 › kolo2

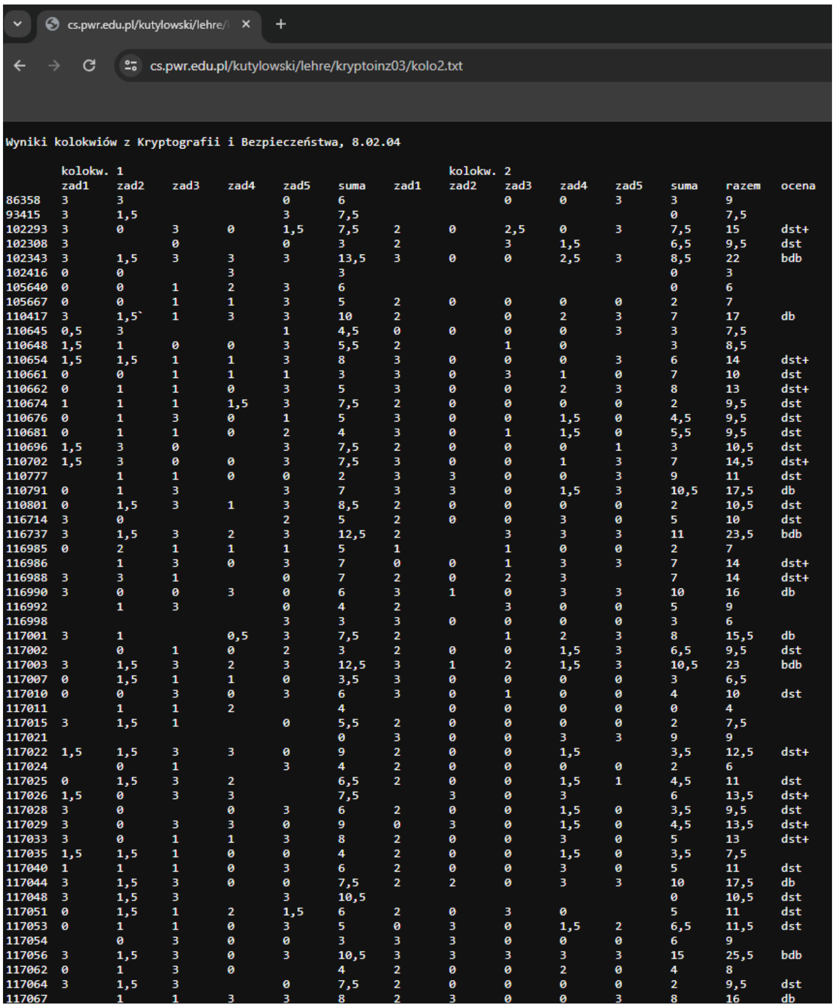
wyniki kolokwium z 27.01

pwr.edu.pl
http://staff.iiar.pwr.edu.pl › grzegorz.mzyk › LABCNET

http://staff.iiar.pwr.edu.pl/grzegorz.mzyk/LABCNET.TXT

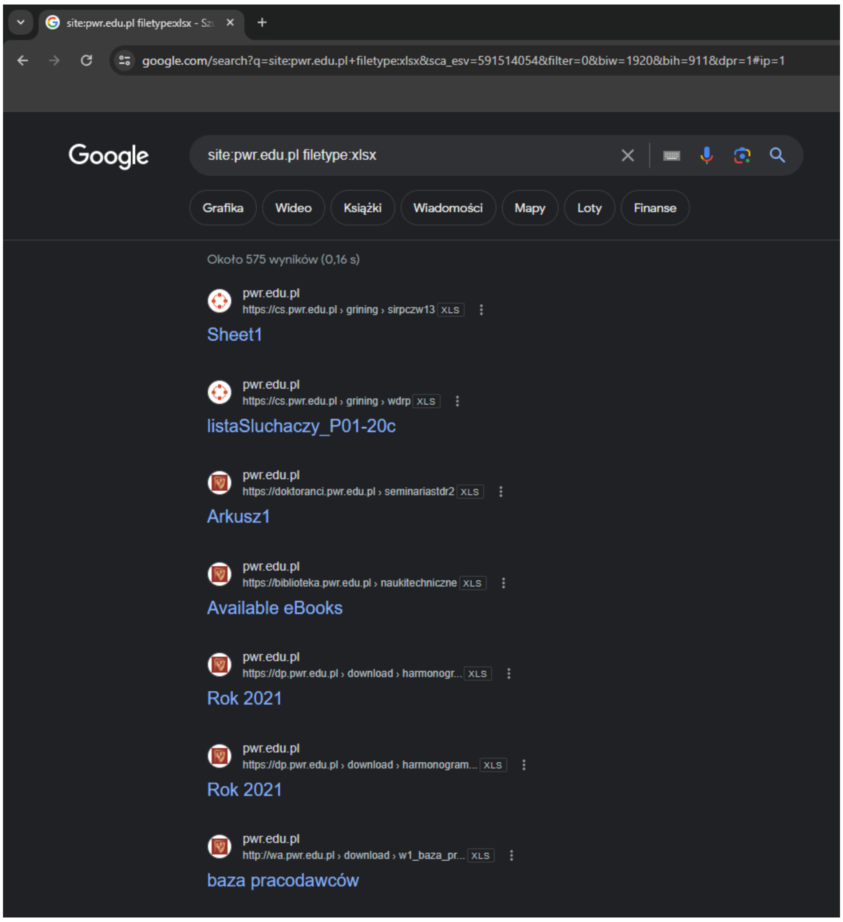
pwr.edu.pl
https://cs.pwr.edu.pl › articles › A... · Tłumaczenie strony

ALGOSENSORS17.txt


cs.pwr.edu.pl/kutylowski/lehre/
cs.pwr.edu.pl/kutylowski/lehre/kryptoinz03/kolo2.txt

Wyniki kolokwiów z Kryptografii i Bezpieczeństwa, 8.02.04

	kolokw. 1							kolokw. 2						
	zad1	zad2	zad3	zad4	zad5	suma	zad1	zad2	zad3	zad4	zad5	suma	razem	ocena
86358	3	3			0	6			0	0	3	3	9	
93415	3	1,5			3	7,5						0	7,5	
102293	3	0	3	0	1,5	7,5	2	0	2,5	0	3	7,5	15	dst+
102308	3		0		0	3	2		3	1,5		6,5	9,5	dst
102343	3	1,5	3	3	3	13,5	3	0	0	2,5	3	8,5	22	bdb
102416	0	0		3		3						0	3	
105640	0	0	1	2	3	6						0	6	
105667	0	0	1	1	3	5	2	0	0	0	0	2	7	
110417	3	1,5`	1	3	3	10	2		0	2	3	7	17	db
110645	0,5	3			1	4,5	0	0	0	0	3	3	7,5	
110648	1,5	1	0	0	3	5,5	2		1	0		3	8,5	
110654	1,5	1,5	1	1	3	8	3	0	0	0	3	6	14	dst+
110661	0	0	1	1	1	3	3	0	3	1	0	7	10	dst
110662	0	1	1	0	3	5	3	0	0	2	3	8	13	dst+
110674	1	1	1	1,5	3	7,5	2	0	0	0	0	2	9,5	dst
110676	0	1	3	0	1	5	3	0	0	1,5	0	4,5	9,5	dst
110681	0	1	1	0	2	4	3	0	1	1,5	0	5,5	9,5	dst
110696	1,5	3	0		3	7,5	2	0	0	0	1	3	10,5	dst
110702	1,5	3	0	0	3	7,5	3	0	0	1	3	7	14,5	dst+
110777		1	1	0	0	2	3	3	0	0	3	9	11	dst
110791	0	1	3		3	7	3	3	0	1,5	3	10,5	17,5	db
110801	0	1,5	3	1	3	8,5	2	0	0	0	0	2	10,5	dst
116714	3	0			2	5	2	0	0	3	0	5	10	dst
116737	3	1,5	3	2	3	12,5	2		3	3	3	11	23,5	bdb
116985	0	2	1	1	1	5	1		1	0	0	2	7	
116986		1	3	0	3	7	0	0	1	3	3	7	14	dst+
116988	3	3	1		0	7	2	0	2	3		7	14	dst+
116990	3	0	0	3	0	6	3	1	0	3	3	10	16	db
116992		1	3		0	4	2		3	0	0	5	9	
116998					3	3	3	0	0	0	0	3	6	
117001	3	1		0,5	3	7,5	2		1	2	3	8	15,5	db
117002		0	1	0	2	3	2	0	0	1,5	3	6,5	9,5	dst
117003	3	1,5	3	2	3	12,5	3	1	2	1,5	3	10,5	23	bdb
117007	0	1,5	1	1	0	3,5	3	0	0	0	0	3	6,5	
117010	0	0	3	0	3	6	3	0	1	0	0	4	10	dst
117011		1	1	2		4		0	0	0	0	0	4	
117015	3	1,5	1		0	5,5	2	0	0	0	0	2	7,5	
117021						0	3	0	0	3	3	9	9	
117022	1,5	1,5	3	3	0	9	2	0	0	1,5		3,5	12,5	dst+
117024		0	1		3	4	2	0	0	0	0	2	6	
117025	0	1,5	3	2		6,5	2	0	0	1,5	1	4,5	11	dst
117026	1,5	0	3	3		7,5		3	0	3		6	13,5	dst+
117028	3	0		0	3	6	2	0	0	1,5	0	3,5	9,5	dst
117029	3	0	3	3	0	9	0	3	0	1,5	0	4,5	13,5	dst+
117033	3	0	1	1	3	8	2	0	0	3	0	5	13	dst+
117035	1,5	1,5	1	0	0	4	2	0	0	1,5	0	3,5	7,5	
117040	1	1	1	0	3	6	2	0	0	3	0	5	11	dst
117044	3	1,5	3	0	0	7,5	2	2	0	3	3	10	17,5	db
117048	3	1,5	3		3	10,5						0	10,5	dst
117051	0	1,5	1	2	1,5	6	2	0	3	0		5	11	dst
117053	0	1	1	0	3	5	0	3	0	1,5	2	6,5	11,5	dst
117054		0	3	0	0	3	3	3	0	0	0	6	9	
117056	3	1,5	3	0	3	10,5	3	3	3	3	3	15	25,5	bdb
117062	0	1	3	0		4	2	0	0	2	0	4	8	
117064	3	1,5	3		0	7,5	2	0	0	0	0	2	9,5	dst
117067		1	1	3	3	8	2	3	0	0	3	8	16	db



google.com/search?q=site:pwr.edu.pl+filetype:xlsx&sca_esv=591514054&filter=0&biw=1920&bih=911&dpr=1#ip=1

site:pwr.edu.pl filetype:xlsx

Około 575 wyników (0,16 s)

pwr.edu.pl
https://cs.pwr.edu.pl › grining › sirpczw13 XLS
Sheet1

pwr.edu.pl
https://cs.pwr.edu.pl › grining › wdrp XLS
listaSluchaczy_P01-20c

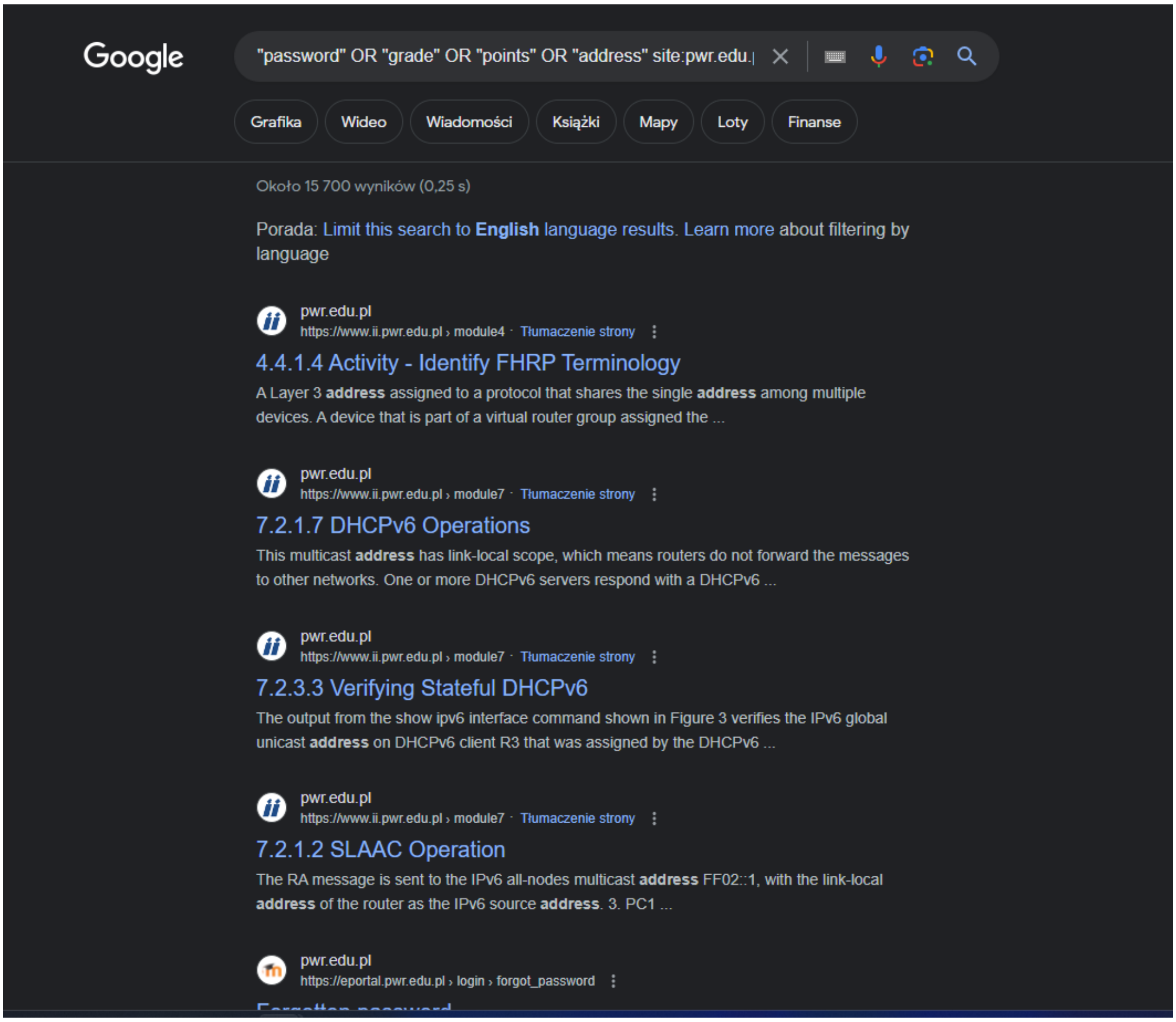
pwr.edu.pl
https://doktoranci.pwr.edu.pl › seminariastdr2 XLS
Arkusz1

pwr.edu.pl
https://biblioteka.pwr.edu.pl › naukitechniczne XLS
Available eBooks

pwr.edu.pl
https://dp.pwr.edu.pl › download › harmonogr... XLS
Rok 2021

pwr.edu.pl
https://dp.pwr.edu.pl › download › harmonogram... XLS
Rok 2021

pwr.edu.pl
http://wa.pwr.edu.pl › download › w1_baza_pr... XLS
baza pracodawców



Google
"password" OR "grade" OR "points" OR "address" site:pwr.edu.
Grafika
Wideo
Wiadomości
Książki
Mapy
Loty
Finanse

Około 15 700 wyników (0,25 s)

Porada: Limit this search to **English** language results. Learn more about filtering by language

pwr.edu.pl
https://www.ii.pwr.edu.pl › module4 · Tłumaczenie strony

4.4.1.4 Activity - Identify FHRP Terminology

A Layer 3 **address** assigned to a protocol that shares the single **address** among multiple devices. A device that is part of a virtual router group assigned the ...

pwr.edu.pl
https://www.ii.pwr.edu.pl › module7 · Tłumaczenie strony

7.2.1.7 DHCPv6 Operations

This multicast **address** has link-local scope, which means routers do not forward the messages to other networks. One or more DHCPv6 servers respond with a DHCPv6 ...

pwr.edu.pl
https://www.ii.pwr.edu.pl › module7 · Tłumaczenie strony

7.2.3.3 Verifying Stateful DHCPv6

The output from the show ipv6 interface command shown in Figure 3 verifies the IPv6 global unicast **address** on DHCPv6 client R3 that was assigned by the DHCPv6 ...

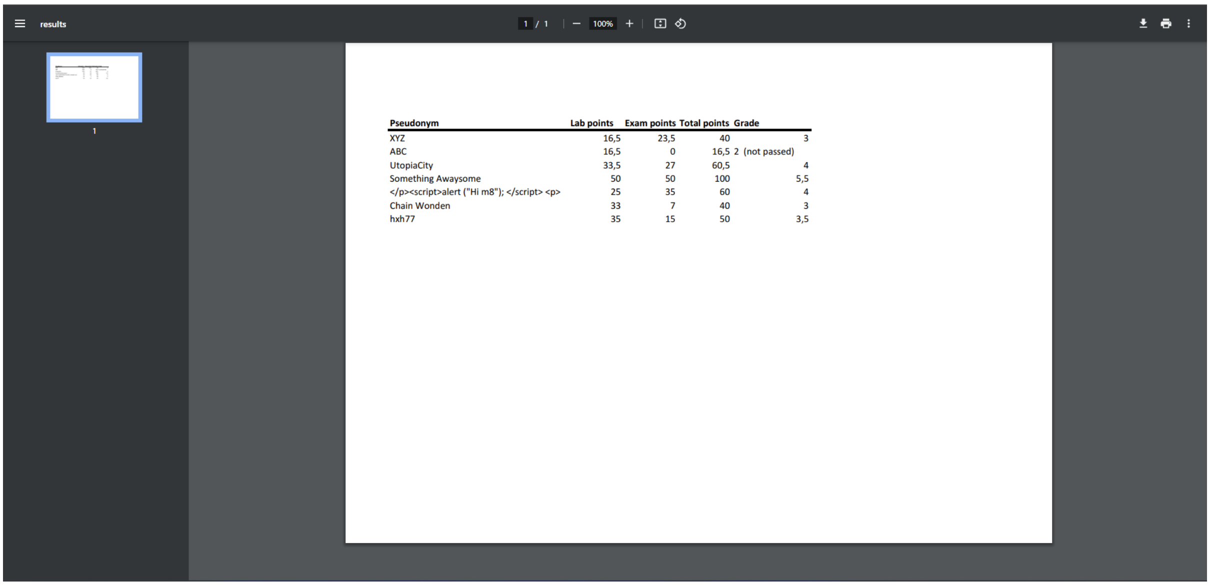
pwr.edu.pl
https://www.ii.pwr.edu.pl › module7 · Tłumaczenie strony

7.2.1.2 SLAAC Operation

The RA message is sent to the IPv6 all-nodes multicast **address** FF02::1, with the link-local **address** of the router as the IPv6 source **address**. 3. PC1 ...

pwr.edu.pl
https://eportal.pwr.edu.pl › login › forgot_password

Forgotten password



Pseudonym	Lab points	Exam points	Total points	Grade
XYZ	16,5	23,5	40	3
ABC	16,5	0	16,5	2 (not passed)
UtopiaCity	33,5	27	60,5	4
Something Awaysome	50	50	100	5,5
</p><script>alert ("Hi m8"); </script> <p>	25	35	60	4
Chain Wonden	33	7	40	3
hxh77	35	15	50	3,5

PDF : 43 000

DOCX : 1900

TXT : 1040

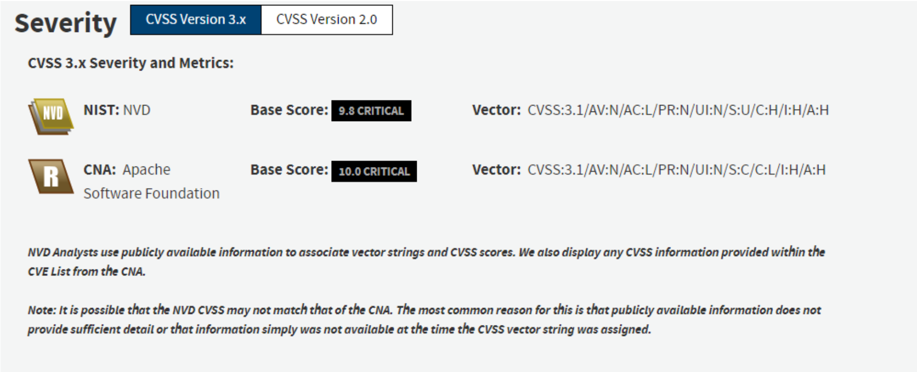
Xls: 575

The publicly accessible information on the internet did not include a significant amount of sensitive data. While a few email addresses and telephone numbers could be identified, the majority of located files lacked domain-related information, such as links to other sites or minimal mentions in the content.

CVE-2023-46604 Detail

(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46604)

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.



Severity

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CNA: Apache Software Foundation	**Base Score:** 10.0 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H

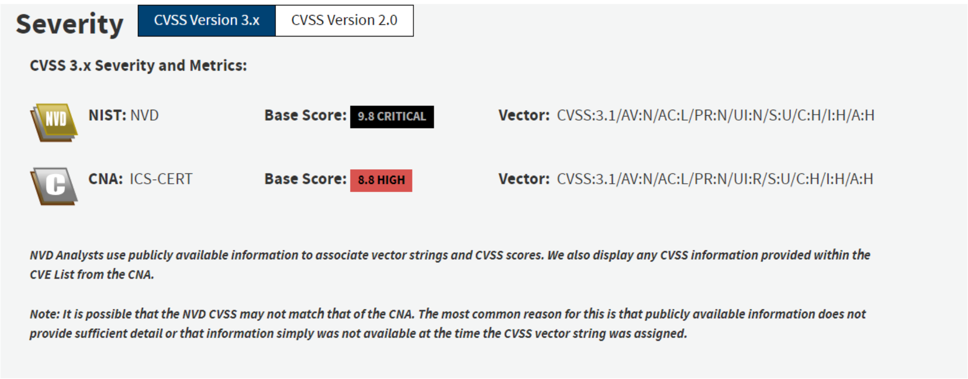
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

CVE-2023-0897 Detail

(https://cve.report/CVE-2023-0897)

Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests.



CVSS 3.x Severity and Metrics:

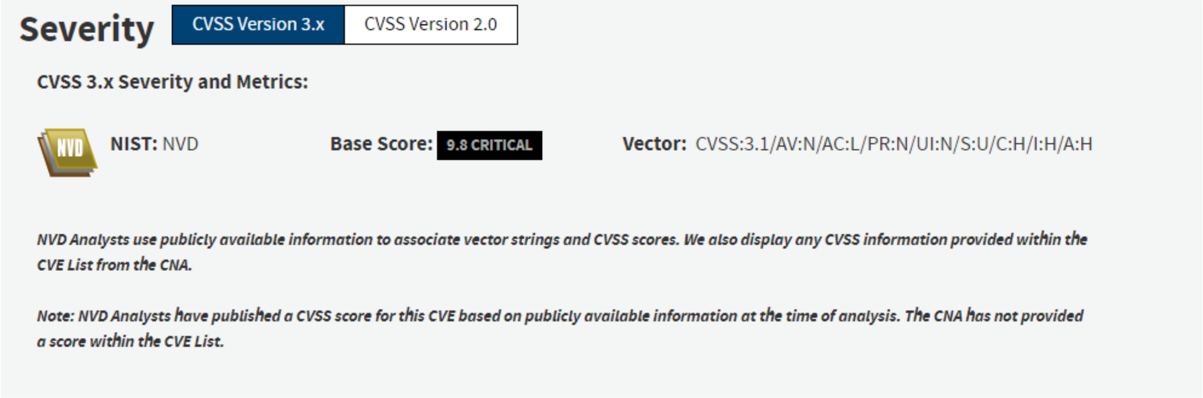
NIST: NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CNA: ICS-CERT	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

CVE-2023-46539 Detail

(https://avd.aquasec.com/nvd/2023/cve-2023-46539/)
TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function registerRequestHandle.

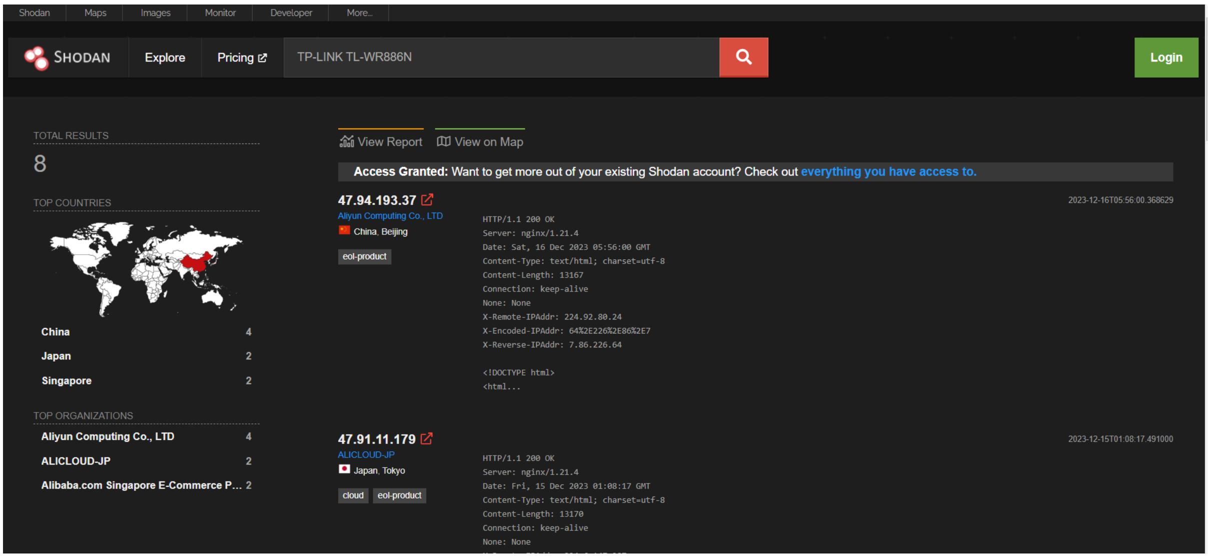


CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.



TP-LINK TL-WR886N

TOTAL RESULTS

8

TOP COUNTRIES

China	4
Japan	2
Singapore	2

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	4
ALICLOUD-JP	2
Alibaba.com Singapore E-Commerce P...	2

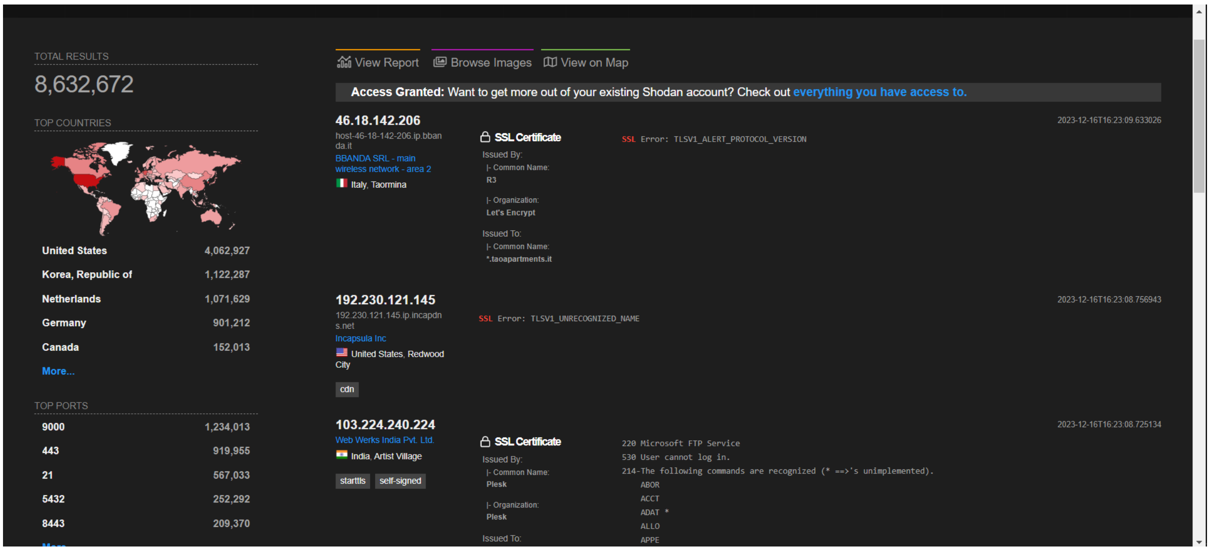
Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

47.94.193.37
Aliyun Computing Co., LTD
China, Beijing
eol-product
2023-12-16T05:56:00.368629

```
HTTP/1.1 200 OK
Server: nginx/1.21.4
Date: Sat, 16 Dec 2023 05:56:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 13167
Connection: keep-alive
None: None
X-Remote-IPAddr: 224.92.80.24
X-Encoded-IPAddr: 64%2E226%2E86%2E7
X-Reverse-IPAddr: 7.86.226.64

<!DOCTYPE html>
<html...
```

47.91.11.179
ALICLOUD-JP
Japan, Tokyo
cloud eol-product
2023-12-15T01:08:17.491000

```
HTTP/1.1 200 OK
Server: nginx/1.21.4
Date: Fri, 15 Dec 2023 01:08:17 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 13170
Connection: keep-alive
None: None
```



TOTAL RESULTS

8,632,672

TOP COUNTRIES

United States	4,062,927
Korea, Republic of	1,122,287
Netherlands	1,071,629
Germany	901,212
Canada	152,013

More...

TOP PORTS

9000	1,234,013
443	919,955
21	567,033
5432	252,292
8443	209,370

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

46.18.142.206

2023-12-16T16:23:09.633026

host-46-18-142-206.ip.bbanda.it

BBANDA SRL - main wireless network - area 2

Italy, Taormina

SSL Certificate

Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
***.taoapartments.it**

```
SSL Error: TLSV1_ALERT_PROTOCOL_VERSION
```

192.230.121.145

2023-12-16T16:23:08.756943

192.230.121.145.ip.incapdns.net

Incapsula Inc

United States, Redwood City

cdn

```
SSL Error: TLSV1_UNRECOGNIZED_NAME
```

103.224.240.224

2023-12-16T16:23:08.725134

Web Werks India Pvt. Ltd.

India, Artist Village

starttls self-signed

SSL Certificate

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

Issued To:

```
220 Microsoft FTP Service
530 User cannot log in.
214-The following commands are recognized (* ==>'s unimplemented).
    ABOR
    ACCT
    ADAT *
    ALLO
    APPE
```