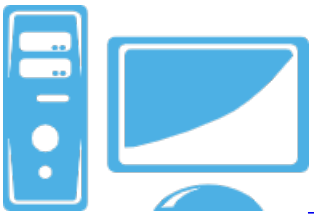
记某次CTF中经典组合拳

原创

网络¥安全联盟站 于 2021-09-03 09:26:10 发布 9455 收藏 9

分类专栏： Toolbar&CTF 文章标签： redis CTF

本文链接：https://blog.csdn.net/weixin_44309905/article/details/120042090



Toolbar&CTF 专栏收录该内容

15 篇文章 1 订阅

订阅专栏

redis未授权访问利用

- □出题思路
- □解题技巧
- □ 总结
- □ 涉及的工具

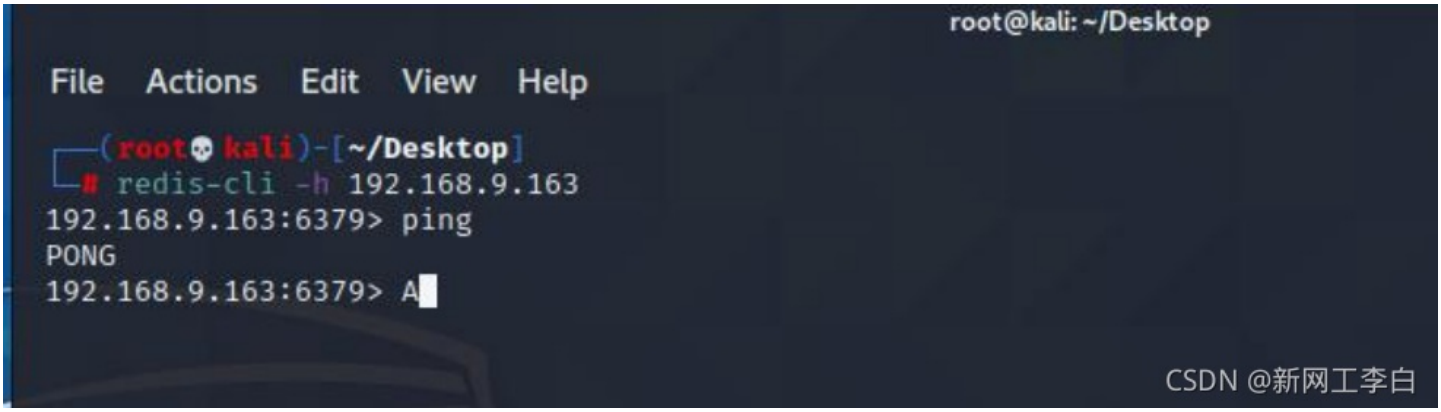
□出题思路

题目考核的是Windows环境下的redis未授权利用场景，包括基本信息收集能力以及基础漏洞利用，部分内网中的禅道环境未删除默认的phpinfo页面，同时安装有redis服务，可以获取绝对路径后写入webshell，是实战环境中多次遇到的经典技法。

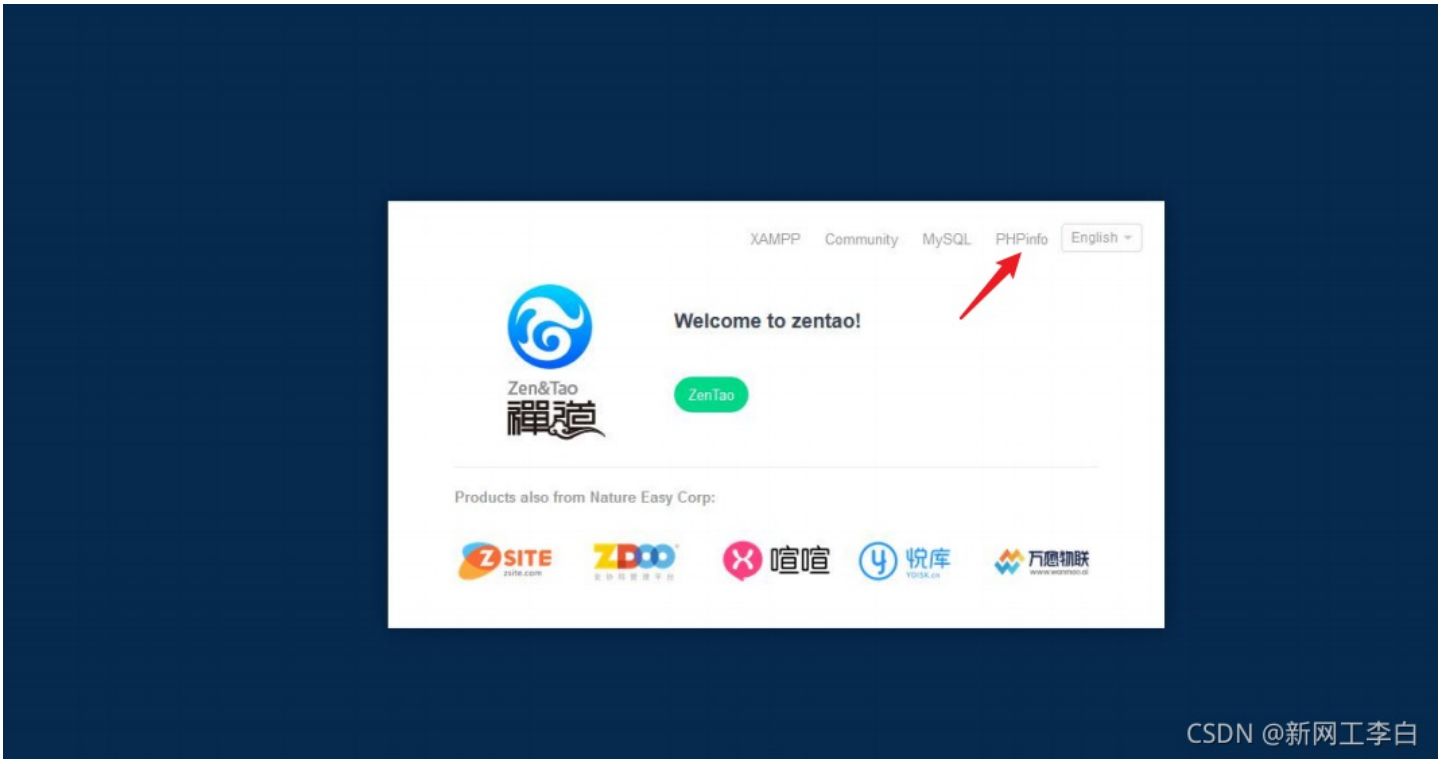
□解题技巧

Nmap扫描发现开启两个端口 通过 banner 可知其中之一为 redis 另一个为禅道。

Redis

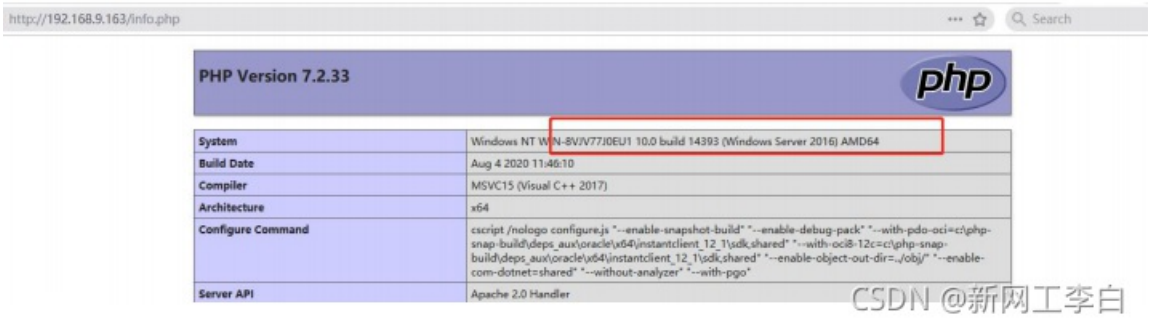


禅道



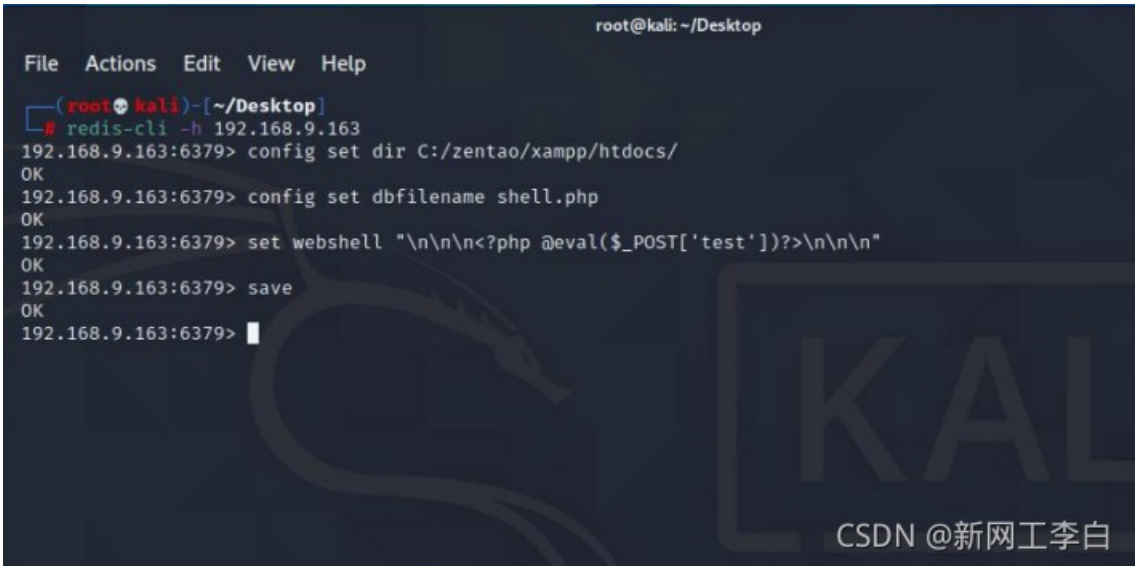
可以看到禅道存在 phpinfo

访问phpinfo有系统信息及绝对路径：



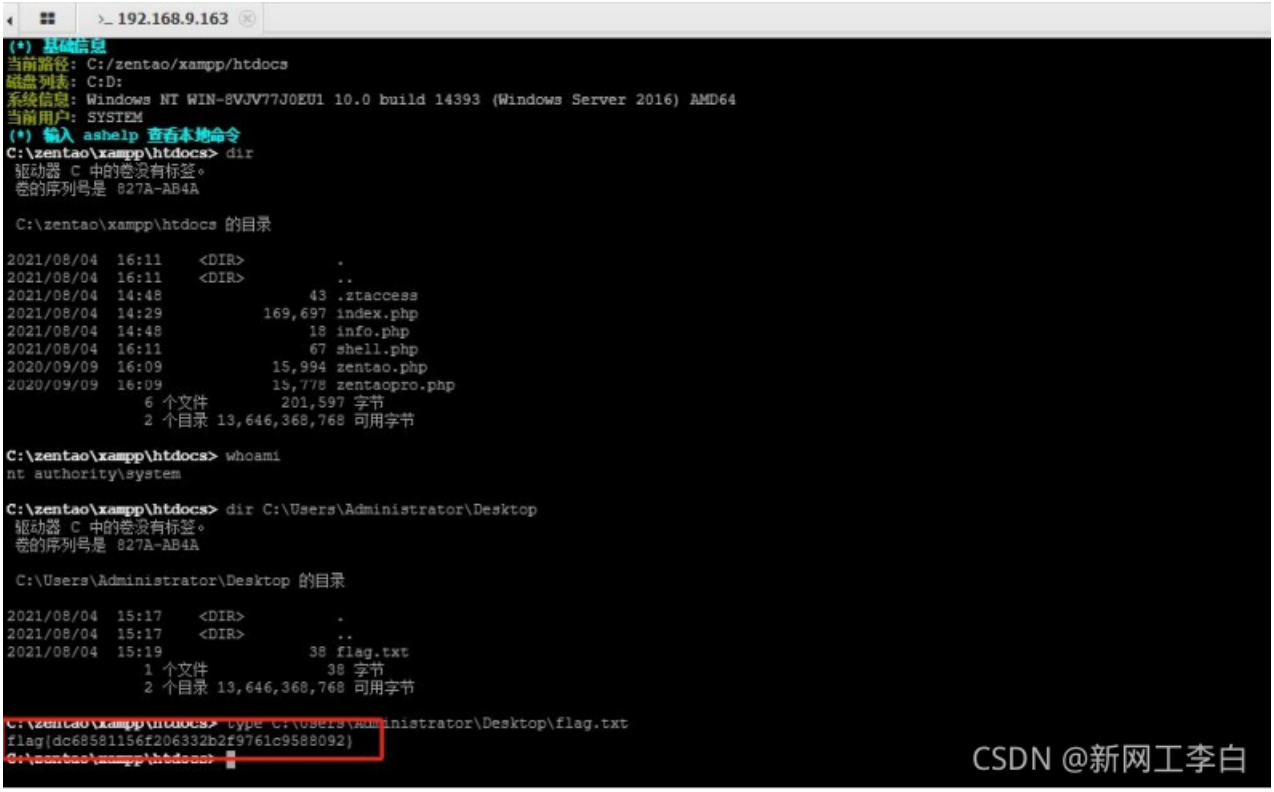
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_REFERER	http://192.168.9.163/
HTTP_DNT	1
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
PATH	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Redis\;C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\WindowsApps
SystemRoot	C:\Windows
COMSPEC	C:\Windows\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
WINDIR	C:\Windows
SERVER_SIGNATURE	*no value*
SERVER_SOFTWARE	Apache
SERVER_NAME	192.168.9.163
SERVER_ADDR	192.168.9.163
SERVER_PORT	80
REMOTE_ADDR	192.168.9.1
DOCUMENT_ROOT	C:/zentao/xampp/htdocs
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*

直接通过 redis 写入 webshell



蚁剑连接取得 flag

```
flag{dc68581156f206332b2f9761c9588092}
```



总结

- 基本信息收集
- redis未授权利用场景

涉及的工具

- kali
- 蚁剑