SaltStack 水平权限绕过漏洞 任意文件读写漏洞 CVE-2020-11651/CVE-2020-11651 漏洞复现

原创

ADummy_ 于 2021-02-28 22:25:11 发布 92 收藏

分类专栏： vulhub_Writeup 文章标签： 安全漏洞 网络安全 渗透测试

SaltStack 水平权限绕过漏洞（CVE-2020-11651）

by ADummy

0x00利用路线

exp直接打

0x01漏洞介绍

SaltStack 是基于 Python 开发的一套C/S架构配置管理工具。国外某安全团队披露了 SaltStack 存在认证绕过漏洞（CVE-2020-11651）和目录遍历漏洞（CVE-2020-11652）。

在 CVE-2020-11651 认证绕过漏洞中，攻击者通过构造恶意请求，可以绕过 Salt Master 的验证逻辑，调用相关未授权函数功能，从而可以造成远程命令执行漏洞：

ClearFuncs类会处理非认证的请求和暴露_send_pub()方法，可以用来直接在master publish服务器上对消息进行排队。这些消息可以用来触发minion来以root权限运行任意命令。

ClearFuncs类还会暴露 _prep_auth_info()方法，该方法会返回用来认证master服务器上本地root用户的命令的root key。然后root key就可以远程调用master 服务器的管理命令。这种无意的暴露提供给远程非认证的攻击者对salt master的与root权限等价的访问权限。

影响版本

```
SaltStack Version < 2019.2.4
SaltStack Version < 3000.2
```

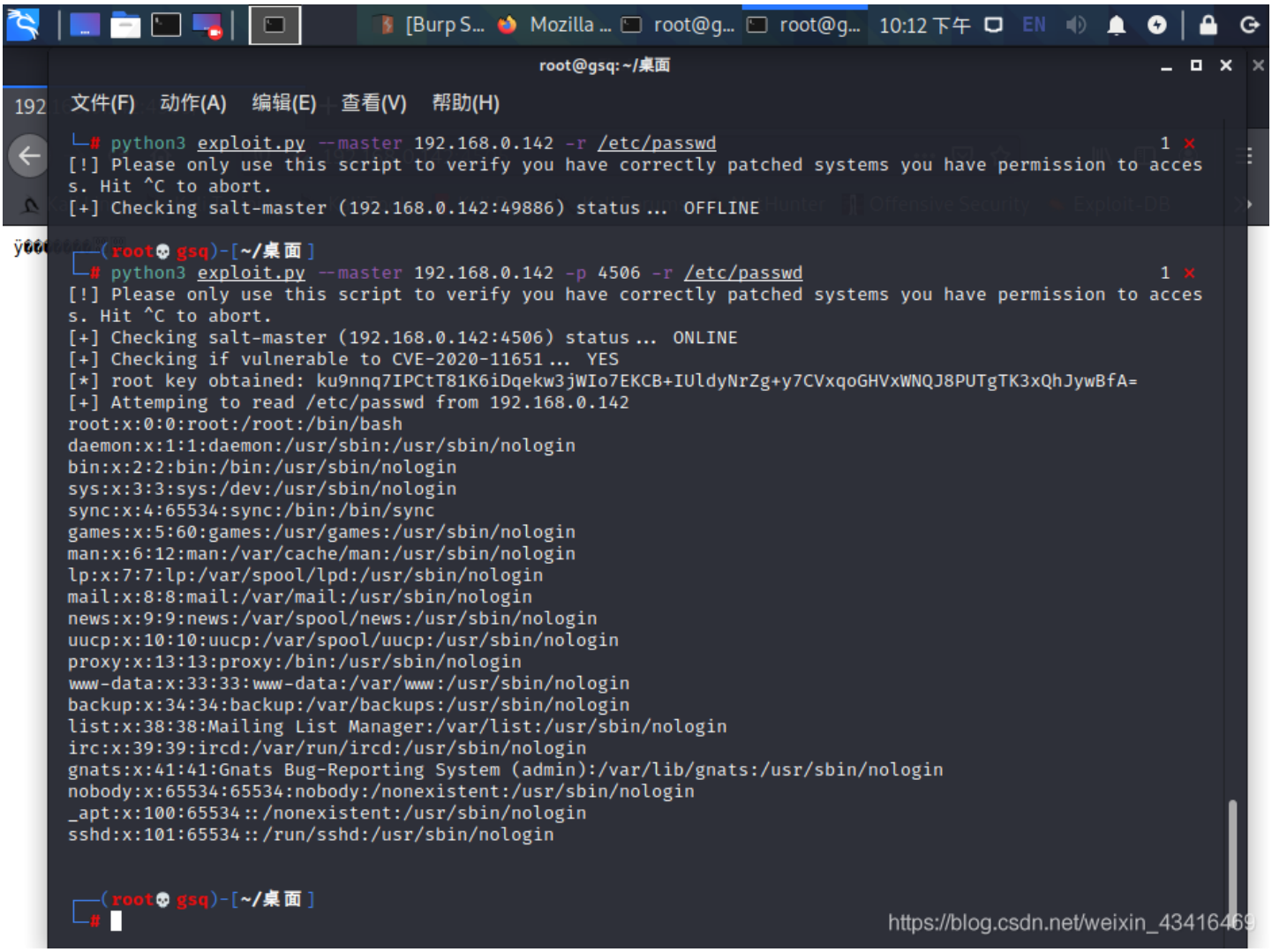
0x02漏洞复现

环境启动后，将会在本地监听如下端口：

```
4505/4506 这是SaltStack Master与minions通信的端口
8000 这是Salt的API端口
2222 这是容器内部的SSH服务器监听的端口
```

```
pip install salt==2019.2.3  //需要安装的包

python3 exploit.py --master  ip  -r /etc/passwd  // exp地址在末尾
```



exp：https://github.com/ADummmy/vulhub_Writeup/blob/main/code/SaltStack_CVE_2020_11651.py

0x03参考资料

https://www.cnblogs.com/Sylon/p/12935381.html