
Bash History

ATT & CK 官网中主要说明了攻击中能够利用 Bash History 收集的一些信息，系统为 linux 系统和 MacOS 系统中。

在攻击中往往能够通过这个获得一些关键的点，比如通过这个主机使用密码登录过其他服务，编辑过的文件，而这些文件中可能就存在其他主机的账号密码等信息。

History 的查询

n:查询历史条数

```
140 history
root@kali:~# history 5
137 vim /etc/ssh/sshd_config
138 screen -ls
139 msfconsole
140 history
141 history 5
root@kali:~#
```

或者直接 history 查询历史所有记录

```
root@kali:~# history
1 history
2 vim ~/.bash_history
3 history
root@kali:~#
```

History 删除

History -c 可以看到使用-c 之后删除了历史记录

```
root@kali:~# history
1 history
2 vim ~/.bash_history
3 history
root@kali:~# history -c
root@kali:~# history
1 history
root@kali:~#
```

但是通过 ~/.bash_history 文件其实还是能够看到的

```
root@kali:~# cat ~/.bash_history
cd /opt
ls
python2
python2
python2
cd /
"
cd /
:s
rz
ls
curl -F "img
node --version
apt-get install node
ls
cd /demo
ls
rz sh
sz she
ls
cd /opt
ls
pyth
pyt
py
ls
ls servers/
ls logs/
rm -rf logs/*
```

其实 `history -c` 并没有完全删除，此时再通过 `history -r` 重新刷新缓存，又能够通过 `history` 查看到原来显示的 `history` 内容

```
root@kali:~# history -r
root@kali:~# history
 1 history
 2 vim ~/.bash_history
 3 cat ~/.bash_history
 4 history -r
 5 cd
 6 ls
 7
 8 python2
 9 python2
10 python2
11
12
13 cd /
14
15 rz
16 ls
17 curl -F
18 node --version
19 apt-get install node
```

如果希望删除部分历史命令可以编辑 `~/.bash_history` 文件进行删除然后使用 `history -r` 刷新，这样应该是最不容易被察觉的方式。