**前言**

实习期间针对某车企开展的一次攻防演练，过程很曲折，当时的记录没有了只是简单的总结一下。

**攻击路径**

收集资产发现shiro→shiro反序列化→权限维持tsh→主机发现→漏洞扫描→ms17010→连接3389→目标主机存在ldapadmin应用→通过应用拿到研发组成员的md5解密→登陆wiki和堡垒机→在WIKI上发现网络拓扑→网络拓扑定位到靶标→管理系统远程SSH靶标IP->docker逃逸获取宿主机权限

**存在问题**

* tsh上线的时候，无法创建tsh进程，不知道具体原因。
* 上线tsh：wget tshd;tshd。
* 查看进程：tasklist ｜ grep "tshd"。
* 使用错误重定向查看是否是系统版本问题：/tmp/bash 2>/tmp/1.txt
* 将目标下载到系统进行编译：下载成功之后，查看当前目录是否下载成功，发现没有文件。多次查看/tmp目录内容，发现两次查看的/tmp目录内容不一样。
* 负载均衡：使用hostname命令，根据每次回显示的主机名，查看是否具有负载均衡并查看均衡的机器有多少，多次尝试发现只有两台机器。
* 负载均衡的解决办法：既然有两台，每个命令尝试两次就可以。
* tsh压缩之后发现内容比较大，在burp执行命令，容易504。所以直接使用nc开启端口并使用bash反弹shell，下载tsh，使用tsh对目标进行控制。(bash反弹shell流量很明显，容易被发现)。

2、内网渗透

* 查看当前网段，10.0.1.0段，扫描b段、c段没有发现任何有价值的东西，都是一些ssh弱口令、redis未授权(可以拿shell，但是可能会影响数据)。
* 之前在拿权限的时候以及看到根目录下和/tmp目录下有很多文件，比如shell脚本、txt文件。爱挨个看。
* 第一个文件是一个shell脚本，使用curl请求了一个子域名地址，子域名为yunwei，直接访问404，之前那shell之前获取信息收集的时候查看进程有zabbix\_agent这个进程，猜想使用的运维工具是zabbix，所以直接在域名后+/zabbix/，访问成功，没有登陆按钮，但是可以直接游客登陆。无失去了注入。
* 其中有一个文件中，有很多IP地址。注释部分为：SVN git、ansible(自动化运维工具)等等，所以此时确定重要资产应该在10.130段。
* 扫10.130段资产的时候，发现大量的运维机器、安全管理平台、堡垒机、wiki、gitlab、流量审计平台，要么漏洞打，要么密码登陆。
* 尝试找密码，要么从运维文件找，要么登陆任意一台机器抓取密码。扫描MS17010，拿到一台机器。
* ms17010拿到shell，添加用户，连接3389，抓取密码，没有抓到任何密码，只抓到了所添加用户的密码，使用cs的hashdump功能获取密码，拿到administrator的密码。连接3389。
* 连接3389之后，翻电脑资料。在桌面的工具文件夹发现了一个ldapadmin工具。打开之后可以直接连接三个域控服务器。直接查看目标的组织架构，以及用户的密码。md5或者sha1加密之后的密码。直接导出域管理员账户。
* 开始解密各种用户的密码，其中主要解密三种角色的密码。

wiki的管理员组用户

confluence的管理员组用户

jira的管理员组用户

在整个公司组织中有一个安全组，其中有一个用户，该用户的密码md5加密，没有解密成功。唯一的办法就是复制粘贴已经解密出来的md5，将该安全组的成员的密码进行替换。但是可能会影响正。

* 拿到密码之后，就是登陆各种重要的平台，比如wiki、confluence、安恒的明御、自身waf管理平台。找重要记录、找靶标记录。

最后是可以直接登陆wiki的，直接搜云桌面、VPN、堡垒机、运维机。