Linux安全运维丨OpenSSH安全浅析

xmirror / 2017-11-07 10:25:45 / 浏览数 2539 安全技术 技术讨论 顶(0) 踩(0)

本篇文章是悬镜安全实验室推出的第10篇原创安全技术文章

SSH 是建立在应用层基础上的安全协议，是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH
协议可以有效防止远程管理过程中的信息泄露问题。SSH最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。我们常用的OpenSSH就是SSH协议的开源实现。

IETF RFC 4251 到 4256 将 SSH 定义为 “经由一个不安全网络进行远程登录和其他安全网络服务的安全 shell 协议”。shell 由三个主要元素组成。

传输层协议：提供服务器身份验证、隐私和具有完美转发隐私的完整性。该层可以提供可选压缩且通过一个 TCP/IP
连接运行，但是也可用于任何其他可靠的数据流之上。

用户认证协议：从服务器到客户端进行身份验证，且通过传输层运行。

连接协议：多路传输加密隧道到多个逻辑通道，通过用户认证协议运行。

下面我们来看看如何让我们的OpenSSH更安全。

一、基础配置，服务端配置文件为/etc/ssh/sshd_config**

1、将 root 账户仅限制为控制台访问
PermitRootLogin no

2、仅使用 SSH Protocol 2

3、禁用空密码
PermitEmptyPasswords no

4、用户登录控制
AllowUsers user1@host1 user1@! @*
DenyUsers user2

5、配置 Idle Log Out Timeout 间隔
ClientAliveInterval 300
ClientAliveCountMax 0

6、禁用基于主机的身份验证
HostbasedAuthentication no

7、禁用用户的 .rhosts 文件
IgnoreRhosts yes

8、强密码策略（生成14位随机字符密码）
</dev/urandom tr -dc '!@#$%^&*()-+=0-9a-zA-Z' | head -c14; echo ""

9、pam_chroot
通过ssh远程登录的用户将被限制在jail环境中。

10、访问控制
tcpwrapper(/etc/hosts.allow，/etc/hosts.deny)
iptables（限制源IP等）

二、攻防对抗

一旦攻击者获取了相关权限，就可能安装openssh后门、或者隐身登录等。接下来我们看看如何让攻击者无所遁形。

1、隐身登录（登录后，不能通过w、who查看到）

```
■■ssh -T■■■■■-T■■■notty■ctrl+C■■■■■■
```

```
■■■■■■■■■■w■■■■■■utmp■■■log■■■■■■■■■■■■■■■■■■■■utmp■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■w■who■■■■■■■■■■■■■■■■■■■■■
```

当然，这样操作会造成整个utmp为空，如果是在管理员登录之后再操作的话，还是会发现异常的。

同时也要处理下wtmp，否则还是会被审计到。

那么如何快递排查呢，我们可以通过ps命令查看进程，如下图所示。

我们可以看到当攻击者处理掉自己的记录后，管理员虽然通过w、who看不到，但是进程中却存在着攻击者登录申请的TTY。

以上只是简单的隐藏，通常情况下，攻击者获取权限后，会安装openssh后门，成功运行后门后，攻击者通过后门登录将不记录任何日志，正常用户登录该主机或者通过该主

这里我们介绍如何利用操作系统自身的工具手工快速查找后门，主要用到strace、strings、grep。

通过openssh后门功能中会记录正常用户登录账号密码，因此猜测会用到open系统调用，只要在登录是用strace跟踪sshd打开的系统调用，然后过滤open，就应该能获取到

strace –o ssh –ff –p pid

可以看到记录文件中关键字为user:password，而且因为后门密码是硬编码在后门patch中的，因此我们通过关键字利用strings可以找到攻击者的openssh后门密码。

如果安全意识不高的攻击者使用了自己攻击机器的通用密码，通过抓包获取到攻击者攻击IP后，就有可能控制攻击者的机器。（意淫）

攻击者通过openssh后门登录后，w、who同样看不到登录信息，但ps查看进程，仍然可以看到申请到的TTY，也可以快速发现攻击行为。
以上只是最基础一些小tips，欢迎各位大佬拍砖。

本篇文章为悬镜安全实验室原创文章，如需转载请标注来源：http://lab.xmirror.cn/

上一篇：使用TensorFlow自动识别验... 下一篇：一步一步PWN路由器之环境搭建
1. 0 条回复
   - 动动手指，沙发就是你的了！