安全技术与应用

最佳实践

文档版本	01
发布日期	2024-10-10

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 华为账号使用的安全最佳实践

为保障您的华为账号安全，帮助您安全地访问华为云资源，请您遵循安全使用IAM的建议。

开启登录保护

开启登录保护后，您或者您账号中的用户登录时还需要通过虚拟MFA、短信或邮件验证，再次确认登录者身份，可以进一步提高账号安全性，有效避免钓鱼式攻击或者用户密码意外泄露。

步骤1 为账号开启登录保护，如表1-1所示。

表 1-1 用户角色

用户角色	操作指导
华为云账号	进入安全设置。选择“敏感操作 > 登录保护”，单击“立即设置”，选择“开启”。

说明

- 华为云账号是您首次使用华为云时，在华为云控制台创建的账号，该账号是您的华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限。
- 华为账号是您访问华为各网站的统一“身份标识”，您只需注册华为账号，即可访问所有华为服务。

步骤2 依次为账号下的**所有**IAM用户开启登录保护。

1. 选择“统一身份认证服务 > 用户”，单击IAM用户所在行的“安全设置”。

图 1-1 用户列表

2. 单击“登录保护”区域的 。

图 1-2 安全设置

3. 在弹出的“登录保护”对话框，根据需要，选择“验证方式”为“手机”、“邮件地址”或“虚拟MFA”，单击“确定”。

图 1-3 登录保护界面

----结束

开启敏感操作保护

开启敏感操作保护后，您或者您账号中的用户进行**敏感操作**时，例如删除资源、生成访问密钥等，需要输入密码和验证码进行验证，可以避免误操作带来的风险和损失。

步骤1 管理员**进入安全设置**。

步骤2 选择“敏感操作 > 操作保护”，单击“立即启用”。

图 1-4 敏感操作

步骤3 在“操作保护”所在行，单击“开启”，您可以选择“操作员验证”或“指定人员验证”。

- 操作员验证：触发敏感操作的账号或IAM用户进行二次验证。
- 指定人员验证：账号及IAM用户触发的敏感操作均由指定人员进行验证。支持手机号、邮件地址，不支持虚拟MFA验证。

图 1-5 敏感操作保护设置

步骤4 单击“确定”，开启操作保护。

----结束

设置登录验证策略

设置登录验证策略，例如会话超时、账号锁定策略、最近登录提示、登录验证提示，可以进一步提高账号安全性，避免账号忘记退出或钓鱼式攻击带来的用户密码意外泄露。

步骤1 管理员进入安全设置。

步骤2 选择“登录验证策略”，按照下图策略进行配置。

图 1-6 登录验证策略配置图

说明

用户可自行修改“登录验证提示”的自定义验证消息。

----结束

设置密码策略

设置密码策略，例如密码最小长度、密码中同一字符连续出现的最大次数、密码不能与历史密码相同，保证使用复杂程度高的强密码，可以进一步提高账号安全性。

步骤1 管理员**进入安全设置**。

步骤2 选择“密码策略”，按照下图策略进行配置。

图 1-7 密码策略配置图

----结束

2 高危端口开放策略的安全最佳实践

为保障您的华为云资源安全，帮助您安全地访问华为云资源，请您参考以下安全建议来设置高危端口的开放策略。

设置安全组和网络 ACL 控制入方向访问

用户可以通过在安全组和网络ACL中定义入方向的访问规则，保护加入该安全组的云服务器和该网络ACL关联的子网。

步骤1 进入安全组。

1. 登录管理控制台。
2. 单击左上角的，选择区域和项目。
3. 在左侧导航树中，单击，选择“网络 > 虚拟私有云”，进入“虚拟私有云”页面。
4. 在左侧导航树中，选择“访问控制 > 安全组”。

步骤2 逐个检查安全组，删除入方向规则中的高危端口策略。

1. 在安全组界面，单击“操作”列的“配置规则”，进入安全组详情界面，如图2-1所示。

图 2-1 安全组界面

2. 选择“入方向规则”，检查是否有表2-1中的“协议端口”，找到其对应“策略”为“允许”且“源地址”为“0.0.0.0/0”的策略，如图2-2所示。

图 2-2 检查安全组策略

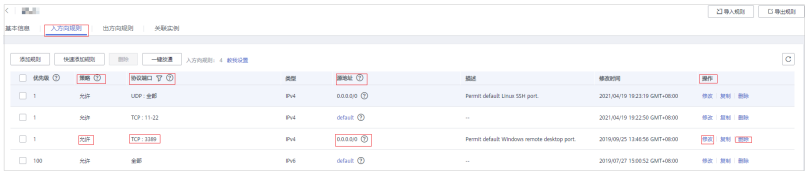
表 2-1 高危端口列表

协议端口（1）	服务	协议端口（2）	服务
TCP： 20、21	FTP（文件传输协议）	TCP: 3306	MySQL（数据库）
TCP：22	SSH（安全外壳协议）	TCP: 3389	Windows rdp（桌面协议）
TCP：23	Telnet（远程终端协议）	TCP: 3690	SVN（开放源代码的版本控制系统）
TCP：25	SMTP（简单邮件传输协议）	TCP: 4848	GlassFish（应用服务器）
TCP/UDP: 53	DNS（域名系统）	TCP: 5000	Sybase/DB2（数据库）
TCP：69	TFTP（简单文件传送协议）	TCP: 5432	PostgreSQL（数据库）
TCP：110	POP3（邮局协议版本3）	TCP: 5900-5902	VNC（虚拟网络控制台，远控）
TCP：111、2049	NFS（网络文件系统）	TCP: 5984	CouchDB（数据库）
TCP：137、139、445	SMB（NETBIOS协议）	TCP: 6379	Redis（数据库）
TCP：143	IMAP（邮件访问协议）	TCP: 7001-7002	WebLogic（WEB应用系统）
TCP：389	LDAP（轻量目录访问协议）	TCP: 7199、7000、7001、9160、9042	Apache Cassandra
TCP: 512-514	Linux rexec（远程登录）	TCP: 7778	Kloxo（虚拟主机管理系统）
TCP：873	Rsync（数据镜像备份工具）	TCP: 8000	Ajenti（Linux服务器管理面板）
TCP：1194	OpenVPN（虚拟专用通道）	TCP: 8069	Zabbix（系统网络监视）
TCP：1352	Lotus（Lotus软件）	TCP: 8443	Plesk（虚拟主机管理面板）

协议端口（1）	服务	协议端口（2）	服务
TCP：1433	SQL Server（数据库管理系统）	TCP：8080、28015、29015	RethinkDB
TCP：1521	Oracle（甲骨文数据库）	TCP：8080-8089	Jenkins、JBoss（应用服务器）
TCP：1500	ISPmanager（主机控制面板）	TCP：8088、50010、50020、50030、50070	Hadoop（分布式文件系统）
TCP：1723	PPTP（点对点隧道协议）	TCP：9080-9081、9090	WebSphere（应用服务器）
TCP：2082-2083	cPanel（虚拟机控制系统）	TCP：9200、9300	ElasticSearch（Lucene的搜索服务器）
TCP：2181	ZooKeeper（分布式系统的可靠协调系统）	TCP：11211	Memcached（缓存系统）
TCP：2601-2604	Zebra（zebra路由）	TCP：27017-27018	MongoDB（数据库）
TCP：3128	Squid（代理缓存服务器）	TCP：50000	SAP Management Console
TCP：3311-3312	kangle（web服务器）	TCP：60010、60030	HBase

3. 如存在此类高危端口策略，您可以根据您的业务需求，在“操作”列中，选择“修改”或“删除”。

图 2-3 安全组高危端口策略设置



说明

- 若不需要对外开放，建议您删除对应策略。
- 若需要对外指定“源地址”开放，建议您修改对应策略的“源地址”为“IP白名单内的地址”，可参考**仅允许特定IP地址远程连接弹性云服务器**。
- 不建议您对所有IP地址开放高危端口策略。

步骤3 在左侧导航树中，选择“访问控制 > 网络ACL”，进入网络ACL。

步骤4 逐个检查“状态”为“已开启”，且关联了子网的网络ACL，删除入方向规则中的高危端口策略。

1. 在网络ACL界面，单击“操作”列的“配置规则”，进入网络ACL详情界面，如**图2-4**所示。

图 2-4 网络 ACL 界面

2. 选择“入方向规则”，检查是否有**表2-1**中的“协议端口”，找到其对应“策略”为“允许”且“源地址”为“0.0.0.0/0”的策略，如**图2-5**所示。

图 2-5 检查网络 ACL 策略

3. 如存在此类高危端口策略，您可以根据您的业务需求，在“操作”列中，选择“修改”或“删除”。

说明

- 若不需要对外开放，建议您删除对应策略。
- 若需要对外指定“源地址”开放，建议您修改对应策略的“源地址”为“IP白名单内的地址”。
- 不建议您对所有IP地址开放高危端口。

----结束

使用 VPN/IPSec 保障端口的内部访问控制

默认情况下，在Virtual Private Cloud (VPC) 中的弹性云服务器无法与您自己的数据中心或私有网络进行通信。如果您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，建议您使用华为云的**虚拟专用网络（VPN）**。

使用华为云原生服务保障安全性

华为云原生服务提供多个特性来保障安全性。

数据库

云数据库服务RDS具有完善的性能监控体系和**多重安全防护措施**，并提供了专业的数据库管理平台，让用户能够在云上轻松的进行设置和扩展云数据库。通过云数据库

RDS服务的管理控制台，用户无需编程就可以执行所有必需任务，简化运营流程，减少日常运维工作量，从而专注于开发应用和业务发展。

应用中间件

分布式缓存服务DCS提供**多个特性**来保障租户数据的可靠性和安全性，例如VPC、安全组、白名单、公网访问SSL加密连接、自动备份、数据快照和跨可用区部署等。

3 对外发送垃圾邮件处置说明

3.1 垃圾邮件的定义及危害

什么是垃圾邮件?

垃圾邮件是指未经收件人允许而强行发送的电子邮件，以下是垃圾邮件的一些常见特征：

- 不显示标题、发件人身份或地址的电子邮件。
- 主题或内容包含虚假信息的电子邮件。
- 内容包含欺骗性信息的电子邮件。
- 内容违反法律法规的电子邮件。
- 携带有病毒等有害信息的电子邮件。

垃圾邮件有哪些危害?

电子邮件是当今社会的重要沟通工具之一，如果垃圾邮件泛滥将会对社会的稳定与发展产生严重影响：

- 降低通信质量：垃圾邮件占用大量网络带宽，影响网络传输速度，容易造成邮件服务器堵塞。
- 损害收件人利益：垃圾邮件常常包含隐蔽性极强的钓鱼信息，容易导致收件人的信息泄露，进而可能造成收件人被诈骗或商业机密被窃取，而且垃圾邮件反复性强、传播速度快，会耗费收件人大量的时间和金钱进行处理。
- 散布有害信息：垃圾邮件易被用于传播谣言、色情等有害信息，影响社会治安。

3.2 华为云对发送垃圾邮件的用户资源的处理

处理说明

对外发送垃圾邮件的行为违反了**《华为云用户协议》**及相关法律法规，且发送大量垃圾邮件的主机将会被国际反垃圾邮件组织列入黑名单，致使主机访问网站受限、发送邮件受限（邮件无法被接收），将极大的损害华为云的服务形象。因此华为云收到用

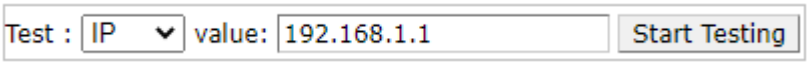
户的资源存在对外发送垃圾邮件的行为的外部投诉后，华为云将会向用户发送预警通知邮件并对用户的资源实施风险遏制措施（包括但不限于封禁端口、冻结IP）。

整改建议

针对不同的投诉类型，华为云会实施不同的风险遏制措施。

您可以打开**反垃圾邮件组织地址**，输入您的IP，单击“Start Testing”，查询有无IP记录，判断是否为反垃圾邮件组织的投诉，如**图 反垃圾邮件组织**所示，然后做出对应情况的处理。

图 3-1 反垃圾邮件组织



- 如果页面未显示任何IP记录并停留在初始页面，表示非反垃圾邮件组织投诉。

  请您尽快停止使用该IP地址的主机发送垃圾邮件，并对邮箱做好防护，防止他人恶意利用。若未在预警邮件规定的时间内整改完成，您的资源将会面临被拦截限制（包括但不限于封禁端口、冻结IP）的风险。
- 如果页面显示有您的IP记录，表示是反垃圾邮件组织投诉。

  反垃圾邮件组织已将您的IP列入黑名单，会限制绑定该IP地址的主机访问网站和对外发送邮件，请您尽快停止使用该IP地址的主机发送垃圾邮件，并对邮箱做好防护。

  被反垃圾邮件组织拉黑，将严重损害华为云的服务形象，华为云将永久冻结您的IP且无法解冻。请重新绑定新的IP地址使用。

4 UDP 反射放大攻击安全排查

4.1 简介

DDoS 攻击的原理

拒绝服务（Denial of Service，简称DoS）攻击也称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，服务暂时中断或停止，导致合法用户不能够访问正常网络服务的行为。当攻击者使用网络上多个被攻陷的电脑作为攻击机器向特定的目标发动DoS攻击时，称为分布式拒绝服务攻击（Distributed Denial of Service Attack，简称DDoS）。

UDP 反射放大攻击简介

UDP反射放大攻击，是一种具有超大攻击威力，且成本低廉，难以追踪的DDoS攻击方式。

基于UDP报文的反射DDoS攻击是这类攻击的一种实现形式，如图4-1所示。攻击者并不是直接发起对攻击目标的攻击，而是利用互联网的某些服务开放的服务器，通过伪造被攻击者的地址，向中间服务器发送基于UDP服务的特殊请求报文，而这些请求报文会形成成倍的数据发送到攻击目标，从而对后者间接形成DDoS攻击。

图 4-1 UDP 反射放大原理图

4.2 排查方法

本章节内容主要指导您：排查主机是否被作为UDP反射攻击的“放大器”利用。

1. 使用root账户登录服务器。

   说明

   本例中，该服务器正常运行情况下每秒发送10个长度为800Byte的UDP数据包。

2. 执行以下命令，查看当前的网络连接与进程。

   netstat -anput

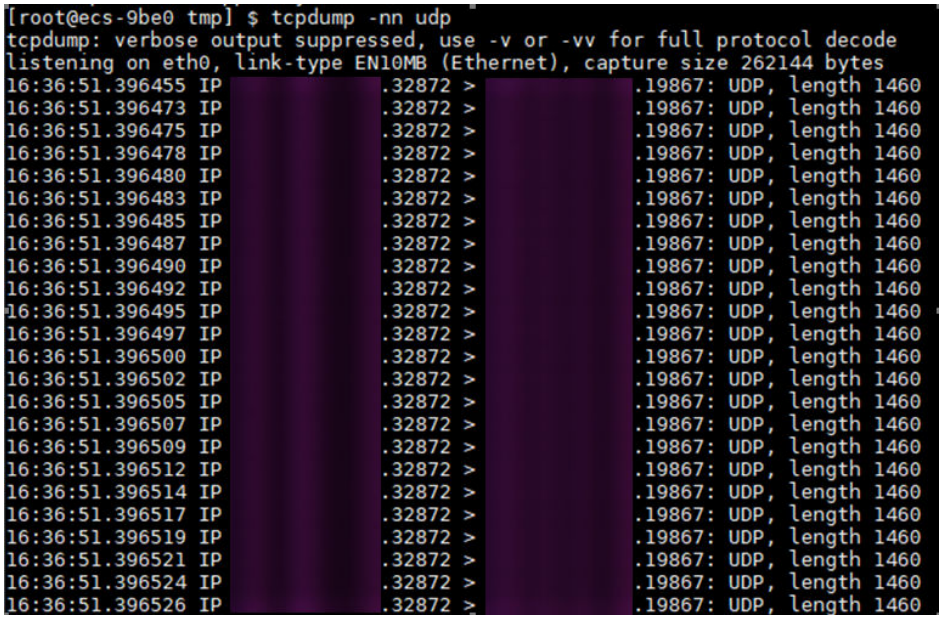
   分析当前的网络连接与进程是否存在异常，建议利用netstat -anpt命令进行查看；若当前连接与进程已停止或被隐藏，可以利用抓包方式进行分析，需要安装tcpdump抓包工具。

3. 执行以下命令抓包，分析UDP流量攻击。

   tcpdump -nn udp

   抓包结果如图4-2显示。

   图 4-2 UDP 对外攻击数据包

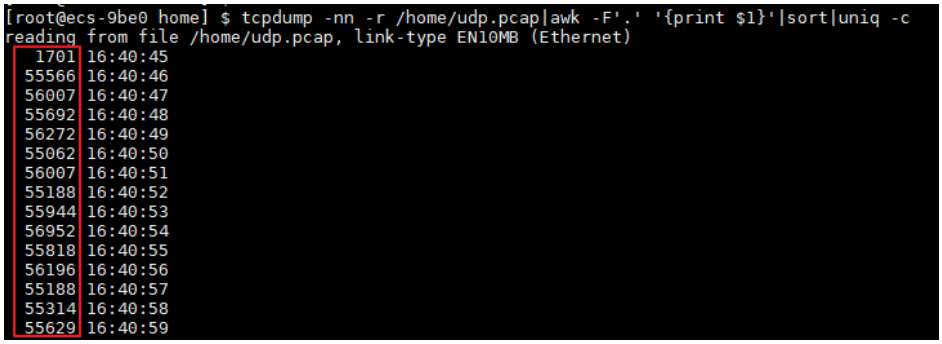
   a. 执行以下命令，将抓包分析结果暂存至/home文件夹中，文件名为udp.pcap。

      nohup tcpdump -nn udp -c 1000000 -w /home/udp.pcap &

   b. 执行以下命令，对抓包分析结果进行分析，结果如图4-3所示。

      tcpdump -nn -r /home/udp.pcap|awk -F'.' '{print $1}'|sort|uniq -c

图 4-3 抓包分析结果



根据步骤**3**可知，图中被检查的设备正在对另一个IP地址发送数十个UDP长度为1460Byte的数据包，明显超出正常业务数据包的范畴，说明该设备正在被利用为UDP反射攻击的“放大器”对外攻击。

通过步骤**b**可知，图中设备UDP连接次数每秒高达5万次以上，说明图中设备所提供的服务被攻击者利用实施UDP反射放大攻击，需要对设备采取必要的防护措施，避免设备资源被攻击行为占用，影响正常业务。

4.3 解决方案&防护措施

针对UDP反射放大攻击方式，您可根据业务的实际情况做出应对措施，下面提出几点建议性防护措施，供您参考。

- 关注网络安全防护设备和服务厂商发布的最新安全公告，及时对此类攻击做出针对性防护策略。
- 云服务器内通过防火墙对UDP端口进行限制。
- 通过安全组对UDP端口进行限制，华为云用户可参见**ECS配置安全组规则**。
- 启动绑定本地监听IP，禁止对外访问、禁用UDP协议、启用登录认证。
- 调整应用程序中的一些参数，并且重启服务器达成禁用UDP的效果。
- 通过对业务历史报文数据的统计学习，建立正常业务包大小的正态分布图，由此可以清晰识别出超大或超小包攻击报文。

5 主机安全排查

5.1 主机面临的安全问题

5.1.1 概述

数据、程序运行在主机上，一旦主机被黑客成功入侵，数据将面临被窃取或被篡改的风险，导致业务中断，造成重大损失，主机安全是业务安全的重中之重。

本文将重点介绍主机可能面临的以下几个安全问题：

- 对外攻击：端口扫描
- 挖矿
- 勒索

5.1.2 对外攻击：端口扫描

什么是端口扫描攻击

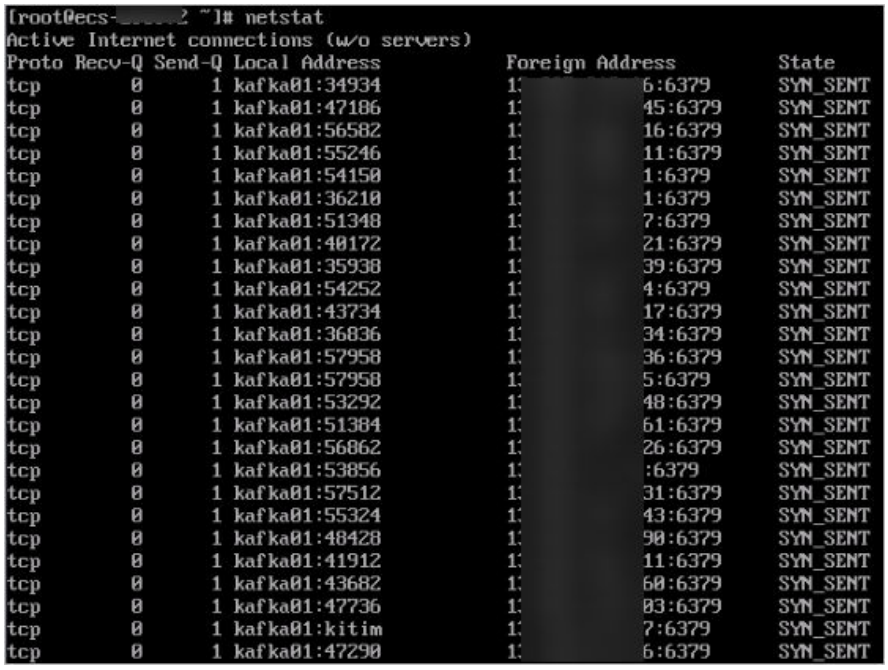
端口扫描攻击是一种攻击方式，攻击者将请求发送到目标服务器或工作站的IP地址，以发现主机开放的端口，并利用端口对应程序中的漏洞进行攻击。

案例

以下为主机被端口扫描攻击的几个案例：

- 案例一：
  a. 此机器正在对外大量扫描6379端口，示例如图5-1所示。

图 5-1 端口扫描



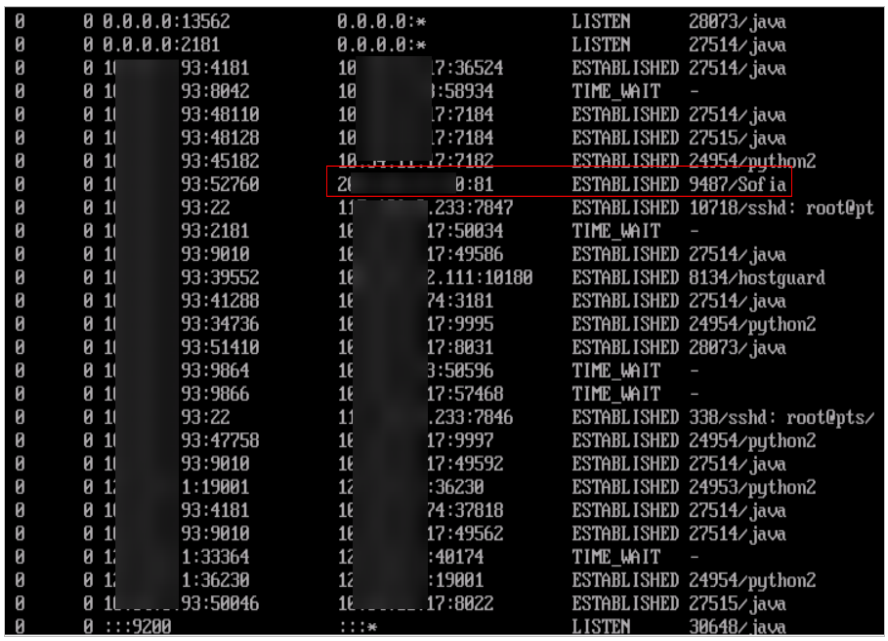
```
[root@ecs-      2 ~]# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      1 kafka01:34934           1          6:6379       SYN_SENT
tcp        0      1 kafka01:47186           1          45:6379      SYN_SENT
tcp        0      1 kafka01:56582           1          16:6379      SYN_SENT
tcp        0      1 kafka01:55246           1          11:6379      SYN_SENT
tcp        0      1 kafka01:54150           1          1:6379       SYN_SENT
tcp        0      1 kafka01:36210           1          1:6379       SYN_SENT
tcp        0      1 kafka01:51348           1          7:6379       SYN_SENT
tcp        0      1 kafka01:40172           1          21:6379      SYN_SENT
tcp        0      1 kafka01:35938           1          39:6379      SYN_SENT
tcp        0      1 kafka01:54252           1          4:6379       SYN_SENT
tcp        0      1 kafka01:43734           1          17:6379      SYN_SENT
tcp        0      1 kafka01:36836           1          34:6379      SYN_SENT
tcp        0      1 kafka01:57958           1          36:6379      SYN_SENT
tcp        0      1 kafka01:57958           1          5:6379       SYN_SENT
tcp        0      1 kafka01:53292           1          48:6379      SYN_SENT
tcp        0      1 kafka01:51384           1          61:6379      SYN_SENT
tcp        0      1 kafka01:56862           1          26:6379      SYN_SENT
tcp        0      1 kafka01:53856           1          :6379        SYN_SENT
tcp        0      1 kafka01:57512           1          31:6379      SYN_SENT
tcp        0      1 kafka01:55324           1          43:6379      SYN_SENT
tcp        0      1 kafka01:48428           1          90:6379      SYN_SENT
tcp        0      1 kafka01:41912           1          11:6379      SYN_SENT
tcp        0      1 kafka01:43682           1          60:6379      SYN_SENT
tcp        0      1 kafka01:47736           1          83:6379      SYN_SENT
tcp        0      1 kafka01:kitim           1          7:6379       SYN_SENT
tcp        0      1 kafka01:47290           1          6:6379       SYN_SENT
```

b. 查询发现这些IP地址均来自不同国家。

- 案例二：

a. 主机内发现异常进程，如图5-2所示。

图 5-2 异常进程

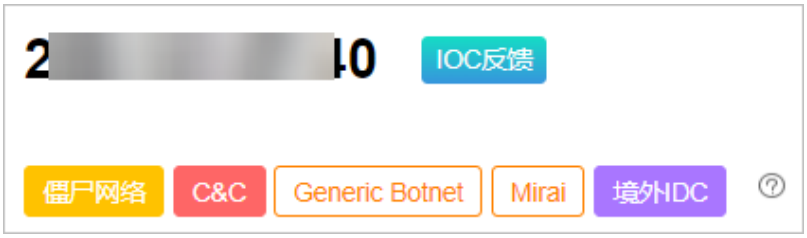


```
0      0 0.0.0.0:13562           0.0.0.0:*               LISTEN      28073/java
0      0 0.0.0.0:2181            0.0.0.0:*               LISTEN      27514/java
0      0 1          93:4181      10          .7:36524    ESTABLISHED 27514/java
0      0 1          93:8042      10          :58934      TIME_WAIT   -
0      0 1          93:48110     10          .7:7184     ESTABLISHED 27514/java
0      0 1          93:48128     10          .7:7184     ESTABLISHED 27515/java
0      0 1          93:45182     10          .7:7182     ESTABLISHED 24954/python2
0      0 1          93:52760     2           0:81        ESTABLISHED 9487/Sofia
0      0 1          93:22        1           .233:7847   ESTABLISHED 10718/sshd: root@pt
0      0 1          93:2181      1           17:50034    TIME_WAIT   -
0      0 1          93:9010      1           17:49586    ESTABLISHED 27514/java
0      0 1          93:39552     1           2.111:10180 ESTABLISHED 8134/hostguard
0      0 1          93:41288     1           74:3181     ESTABLISHED 27514/java
0      0 1          93:34736     1           17:9995     ESTABLISHED 24954/python2
0      0 1          93:51410     1           17:8031     ESTABLISHED 28073/java
0      0 1          93:9864      1           3:50596     TIME_WAIT   -
0      0 1          93:9866      1           17:57468    TIME_WAIT   -
0      0 1          93:22        1           .233:7846   ESTABLISHED 338/sshd: root@pts/
0      0 1          93:47758     1           17:9997     ESTABLISHED 24954/python2
0      0 1          93:9010      1           17:49592    ESTABLISHED 27514/java
0      0 1          1:19001      1           :36230      ESTABLISHED 24953/python2
0      0 1          93:4181      1           74:37818    ESTABLISHED 27514/java
0      0 1          93:9010      1           17:49562    ESTABLISHED 27514/java
0      0 1          1:33364      1           :40174      TIME_WAIT   -
0      0 1          1:36230      1           :19001      ESTABLISHED 24954/python2
0      0 1          93:50046     1           17:8022     ESTABLISHED 27515/java
0      0 :::9200                 :::*                    LISTEN      30648/java
```

b. 查询发现此IP地址连接C&C。

C&C是指command-and-control命令与控制。简单来说就是一种机器与机器之间的通讯方式。

C&C服务器是由攻击者的计算机将命令发送到受恶意软件入侵的系统，并从目标网络接收被盗的数据。



5.1.3 挖矿

什么是挖矿

数字货币因其技术去中性化和经济价值等属性，逐渐成为大众关注的焦点，同时，通过恶意挖矿获取数字货币是黑灰色产业获取收益的重要途径。

其中，挖矿是指通过大量计算机运算获取数字货币-虚拟货币奖励的过程。恶意挖矿攻击就是在用户不知情或未经允许的情况下，占用受害者的系统资源和网络资源进行挖矿，从而获取加密货币牟利。

肉鸡也称傀儡机，是指可以被黑客远程控制的机器。肉鸡可以是各种系统，如Windows、Linux、Unix等，更可以是一家公司、企业、学校甚至是政府军队的服务器。

主机被挖矿最直接的影响就是大量消耗系统资源，使系统其他软件或服务运行缓慢，性能变差。同时，黑客还可能通过挖矿程序窃取机密信息，比如机密文件、关键资产的用户名和密码等，导致资产遭受更进一步的损失。

案例

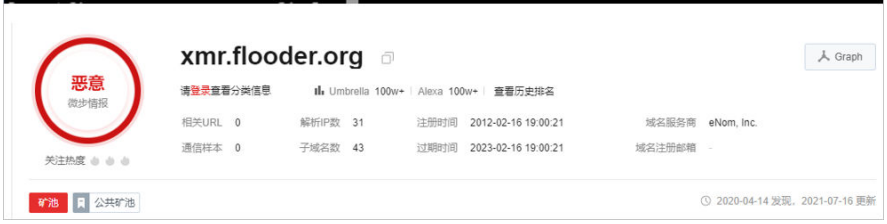
如下为主机被挖矿的几个案例：

- 案例一：
  a. 发现异常文件（一般带有**xmr**或**mine**的标识）。

```
[root@hecs      7 .config]# ll -art
total 13676
-rwxrwxrwx 1 oracle oinstall      54 Jan  9  2002 start
-rwxrwxrwx 1 oracle oinstall  838583 Jun 15  2018 h64
-rwxr-xr-x 1 oracle oinstall     337 Feb 14  2020 go
-rwx--x--x 1 oracle oinstall  215960 Dec 19  2020 arm
-rwx--x--x 1 oracle oinstall 5092504 Dec 19  2020 xmrigMiner
-rwxr-xr-x 1 oracle oinstall 7805520 Apr 28 13:30 logind
-rwxrwxrwx 1 oracle oinstall     243 Apr 28 13:31 update
drwxr-xr-x 2 oracle oinstall    4096 Jun 25 00:25 .
-rwxrwxrwx 1 oracle oinstall     392 Jun 25 00:31 libs
-rw-r--r-- 1 oracle oinstall      21 Jun 27 11:59 dir.dir
-rw-r--r-- 1 oracle oinstall      51 Jun 27 11:59 cron.d
-rwxr--r-- 1 oracle oinstall     212 Jun 27 11:59 upd
-rwxr-xr-x 1 oracle oinstall       6 Jun 27 11:59 bash.pid
-rw-r--r-- 1 oracle oinstall    2771 Jun 27 11:59 config.json
drwx------ 5 oracle oinstall    4096 Jun 28 16:44 ..
[root@hecs-      7 .config]# pwd
/home/oracle/.config
```

b. 对文件进行分析，发现矿池信息，URL进行检测为矿池。

```
[root@h          7 .config]# pwd
/home/oracle/.config
[root@           7 .config]# strings config.json |grep xmr
            "url": "xmr.flooder.org:80",
[root@r          7 .config]# pwd
/home/oracle/.config
```

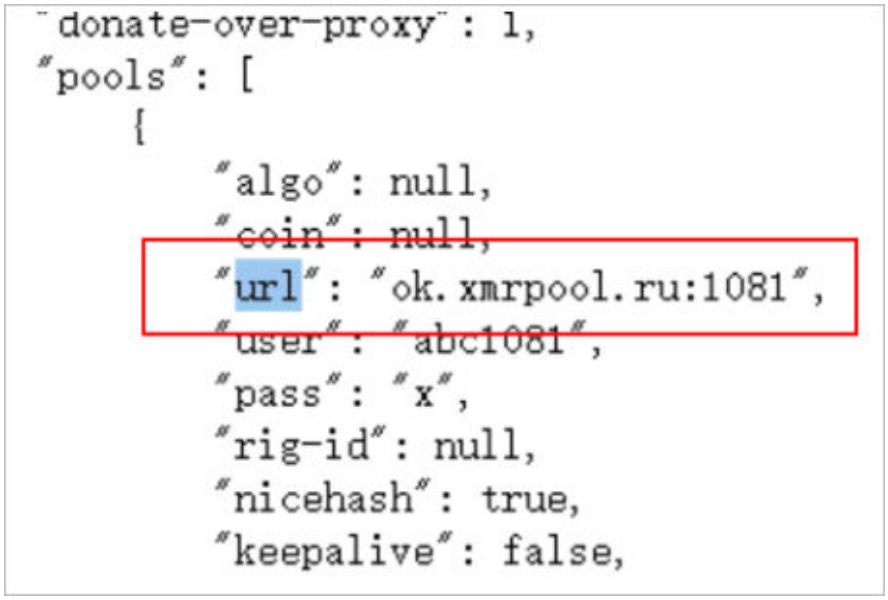


- 案例二：

a. Windows主机存在挖矿进程。

b. 主机内发现异常文件。

c. 对文件进行分析，发现矿池信息。



d. 检测URL为恶意矿池地址。

5.1.4 勒索

什么是勒索病毒

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑软件等多种形式进行传播。一旦遭受勒索病毒攻击，将会使绝大多数的关键文件被加密。被加密的关键文件无法通过技术手段解密，用户将无法读取资产中的文件，即使向黑客缴纳高昂的赎金，也不一定能将被加密的文件无损的还原。黑客通常要求通过数字货币支付赎金，一般无法溯源。

如果关键文件被加密，企业业务将受到严重影响；黑客索要高额赎金，也会带来直接的经济损失，因此，勒索病毒的入侵危害巨大。

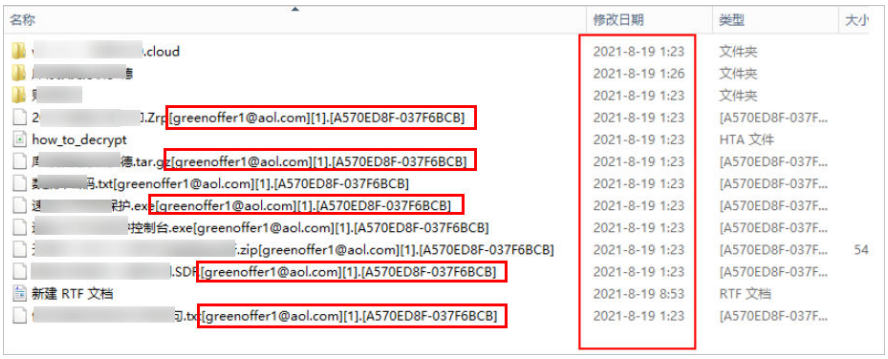
勒索病毒具有传播方式多样性和顽固的攻击性特征，一旦被勒索病毒入侵，资产和经济都将遭受重大损失。

案例

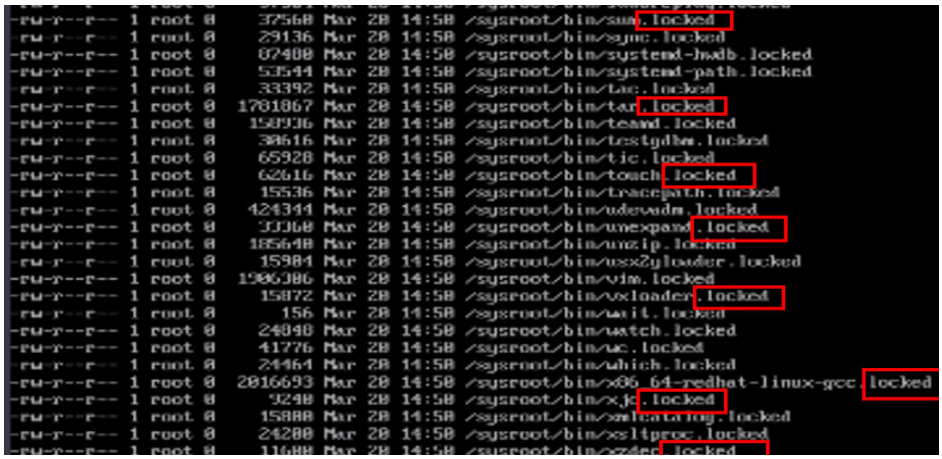
如下为主机被勒索的几个案例：

- 案例一：Windows主机文件加密，主机内存在勒索信条

- 案例二：Windows主机文件加密，主机内文件被添加后缀



- 案例三：Linux主机文件加密，主机文件被添加后缀



5.2 主机安全排查（Windows 操作系统）

5.2.1 排查思路

本文档为您介绍两种Windows主机排查方法，推荐选择“工具溯源排查”的方法：

- 方案一：**工具取证排查**（推荐）：使用Windows官方的进程/链接/自启动分析工具进行排查。
- 使用工具取证排查方案时，建议如下软件工具：

  表 5-1 软件工具

工具名称	下载地址
ProcessExplorer	https://docs.microsoft.com/zh-cn/sysinternals/downloads/process-explorer
Tcpview	https://docs.microsoft.com/zh-cn/sysinternals/downloads/tcpview
Autoruns	https://docs.microsoft.com/zh-cn/sysinternals/downloads/autoruns
busybox-x86_64	https://busybox.net/downloads/binaries/1.16.1/busybox-x86_64

- 方案二：**DOS系统命令排查**：通过Windows主机DOS系统命令排查。

5.2.2 排查过程

5.2.2.1 方案一：工具溯源排查

5.2.2.1.1 步骤 1：进程分析

本章节介绍如何通过Windows官方进程排查木马程序。

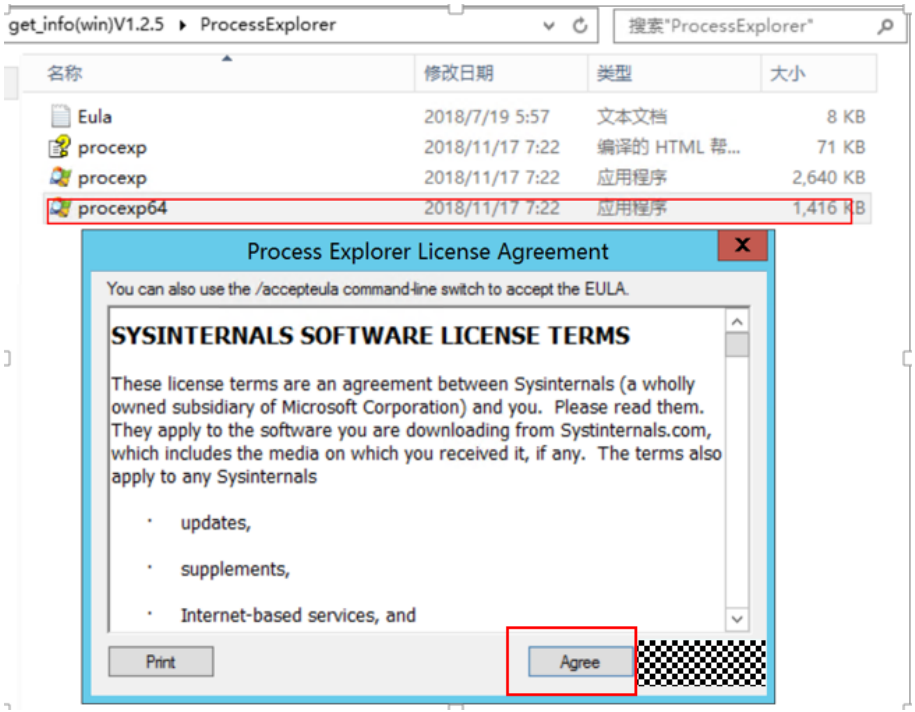
前提条件

推荐下载“ProcessExplorer”软件。

操作步骤

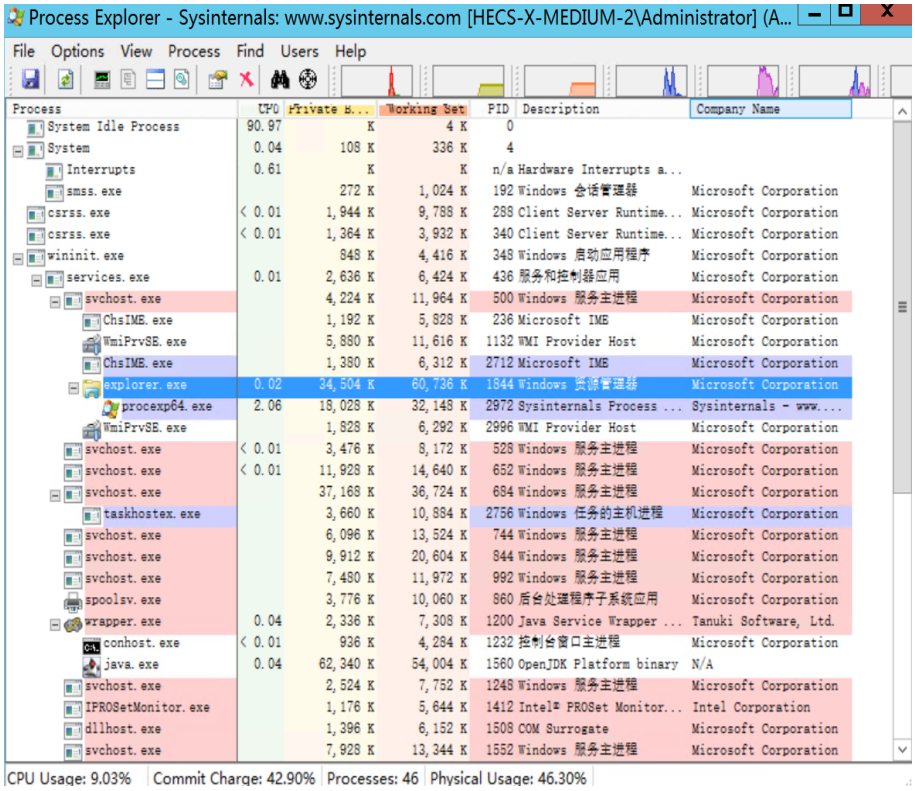
步骤1 打开“ProcessExplorer”文件夹，双击“procexp64.exe”文件。

图 5-3 processExplorer



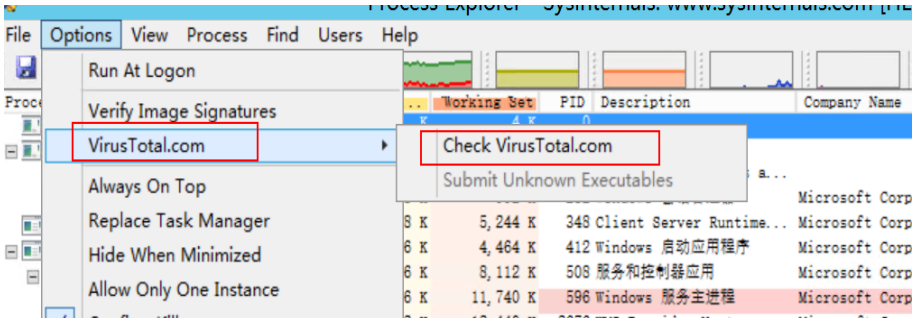
步骤2 在弹出的对话框中，单击“Agree”，查看进程信息，在线排查进程。

图 5-4 查看当前进程



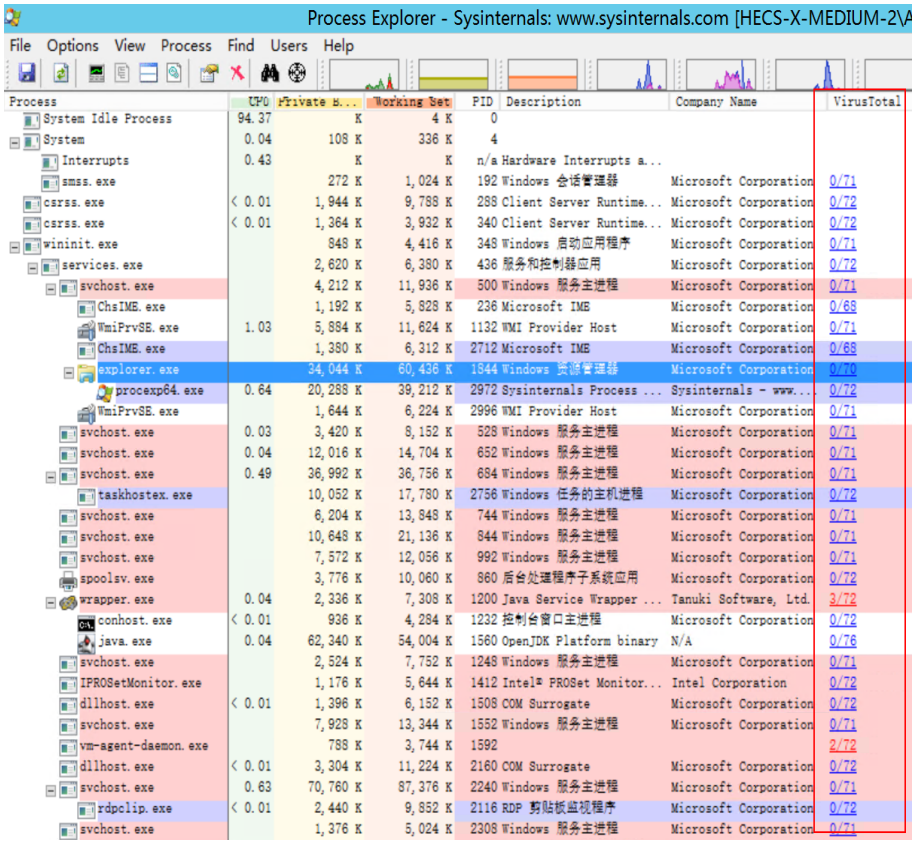
步骤3 在上方的菜单栏中，选择“Options > VirusTotal.com”，勾选“Check VirusTotal.com”和“Submit Unknown Executables”。

图 5-5 options > VirusTotal.com



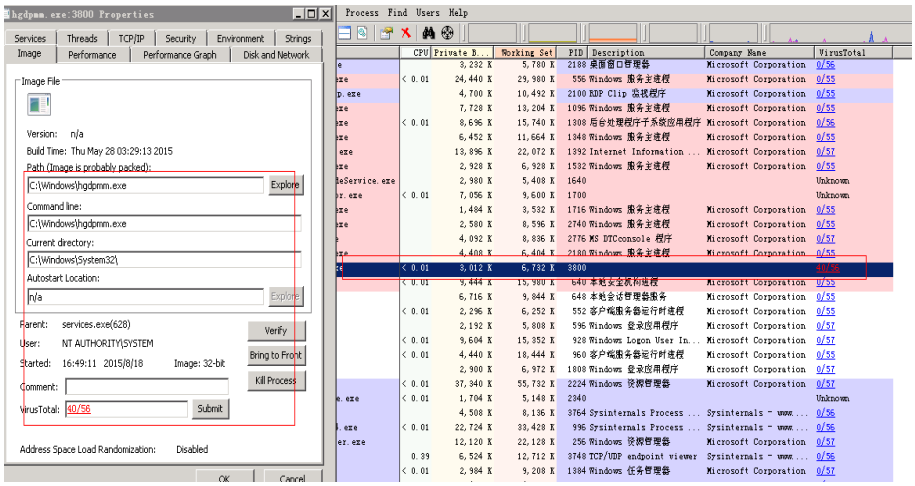
此时，系统会将当前进程的hash值同virustotal库比对，可快速发现木马进程。

图 5-6 Process Explore-Sysinternals



步骤4 检查“VirusTotal”值，右键单击进程名称，选择“Properties”，在弹出的页面中，单击“Image”可查看进程路径，进而再次判断该进程是否是木马程序。

图 5-7 判断是否为木马程序



----结束

5.2.2.1.2 步骤 2：自启动分析

该章节为您介绍如何通过Autoruns工具查看哪些程序被配置为在系统启动和登录时自动启动。

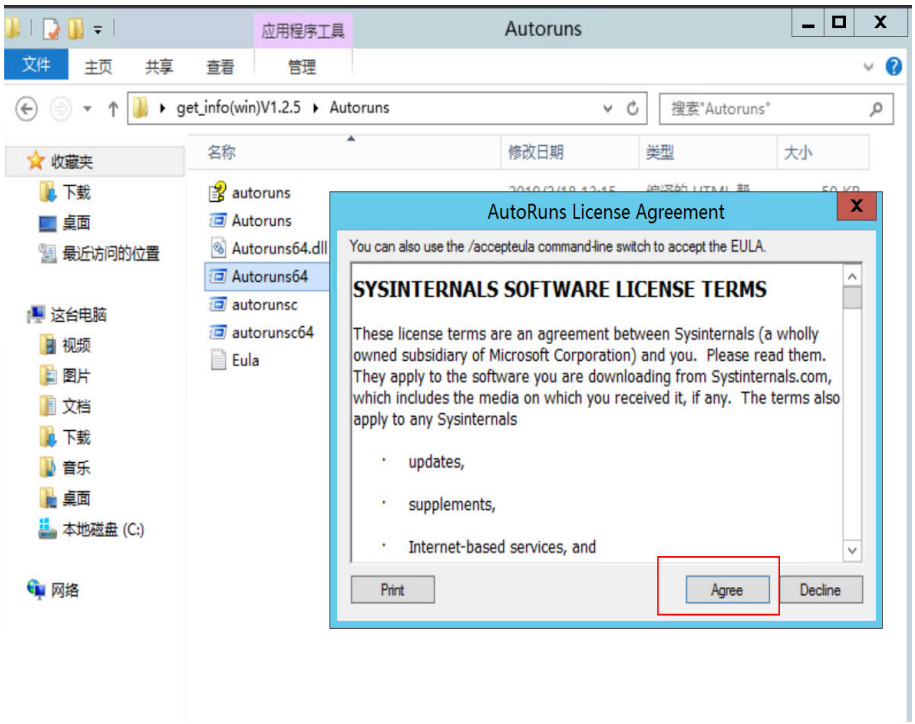
前提条件

推荐下载“Autoruns”工具。

操作步骤

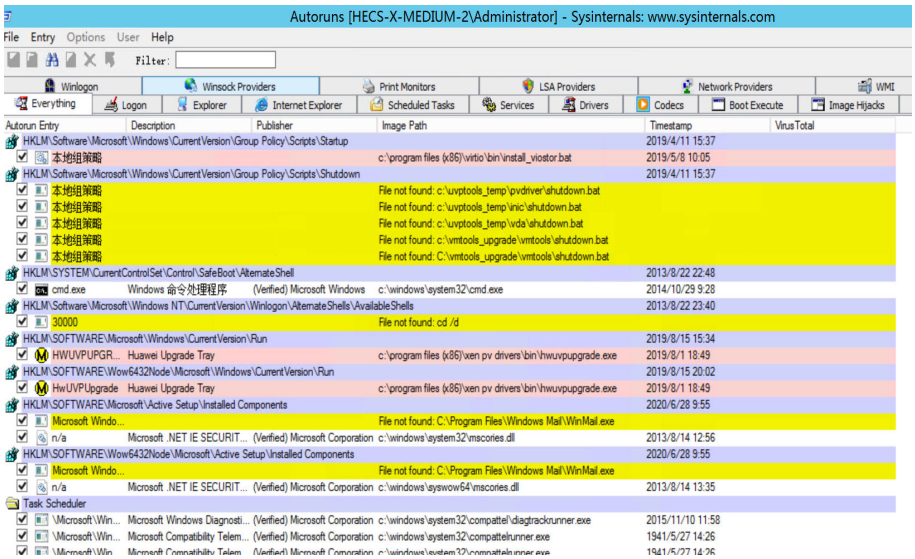
步骤1 打开“Autoruns”文件夹，双击“Autoruns.exe”文件。

图 5-8 打开 AutoRuns 文件夹

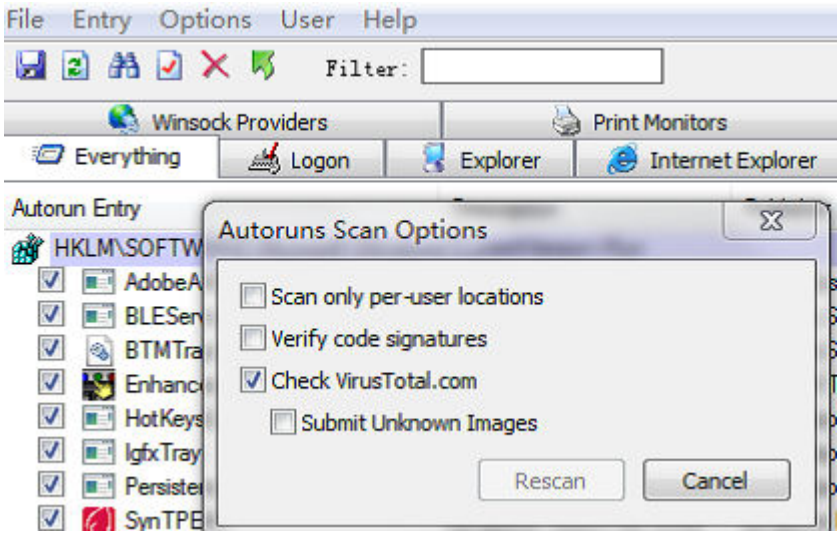


步骤2 在弹出的对话框中，单击“Agree”。

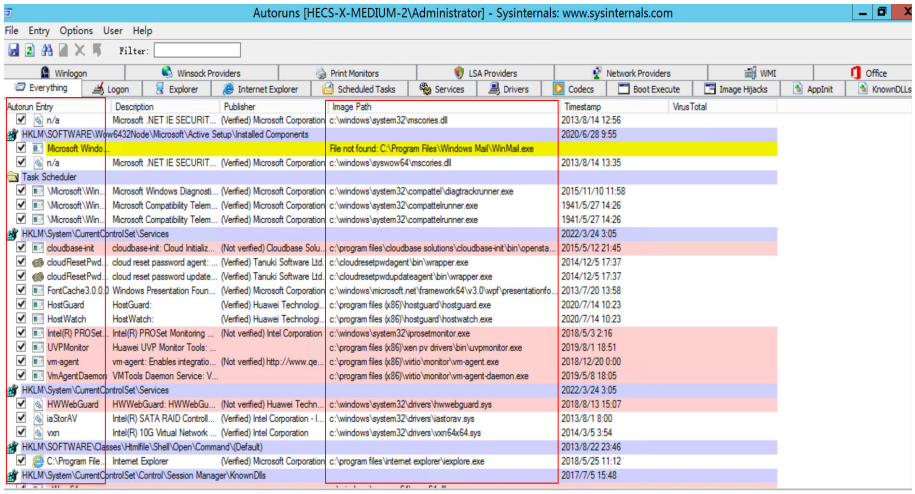
图 5-9 AutoRuns



步骤3 在上方的菜单栏中，选择“Options > Scan Options”，勾选“CheckVirusTotal.com”，打开在线检测进程功能。

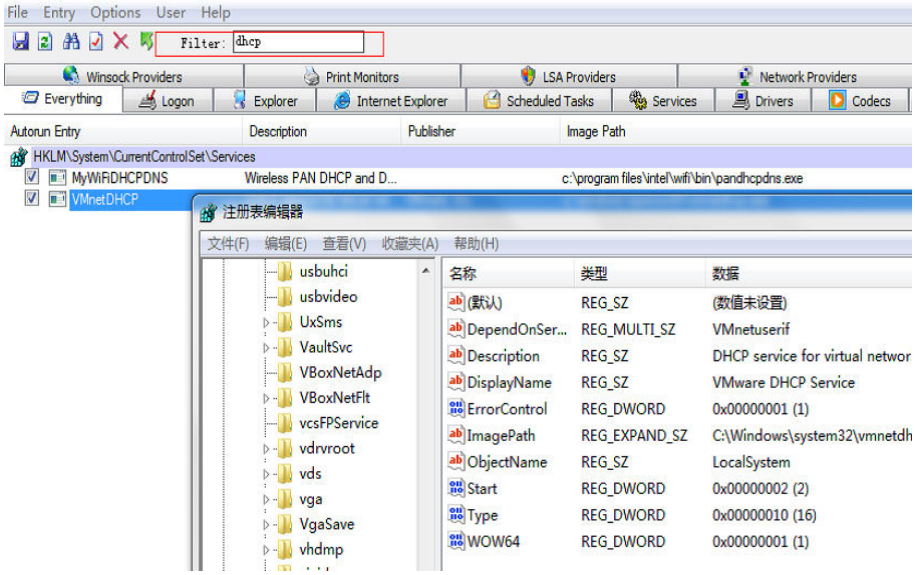


步骤4 检查“Autorun”列和“Images Path”列是否存在异常文件（非系统和正常业务部署创建文件）。



步骤5 如果发现可疑进程，双击该进程名，可直接定位到注册表位置。可以在“Filter”中过滤可疑进程的名字。

图 5-10 打开注册表编辑器



----结束

5.2.2.1.3 步骤 3：网络分析

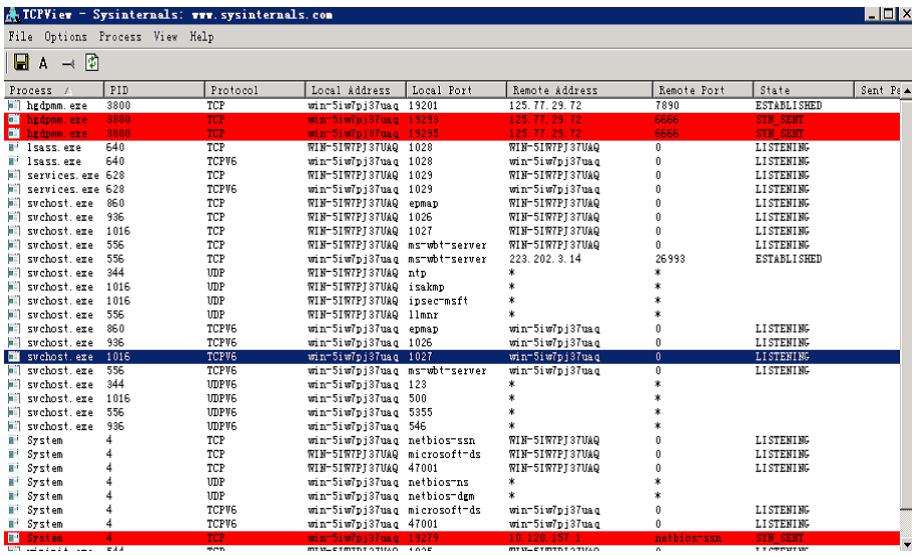
该章节为您介绍如何通过TCPView工具查看当前TCP连接状态，排查可疑进程，可疑进程一般用红色标记。

前提条件

推荐下载“TCPView”工具。

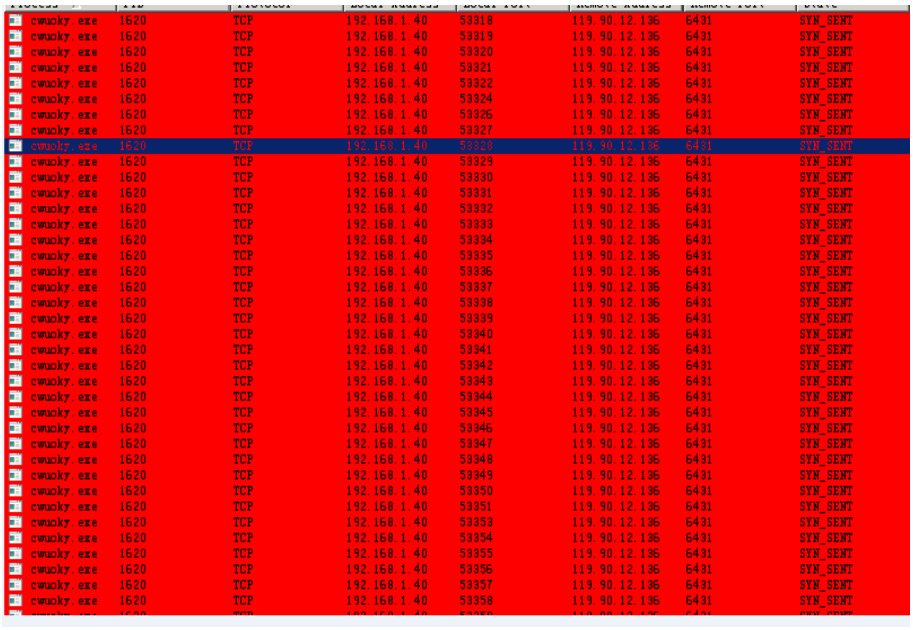
操作步骤

步骤1 打开“TCPView”文件夹，双击“Tcpview.exe”文件，在弹出的对话框中，单击“Agree”。



步骤2 查看当前TCP连接状态，判断该进程是否为木马程序。

- 如果发现存在不知名进程，并且存在大量的SYN_SENT状态的连接，该进程疑似为木马程序。
- 如果某个进程的连接的端口非常有规律（如6666，2333等），或者在RemoteAddress这一栏自动解析的host中包含mine，pool，xmr等关键字，该进程疑似被感染病毒。



步骤3 （仅供参考）您可以通过安全检测网站，检测外网远程地址或者URL进行在线查询判断。

- 检测地址：**https://x.threatbook.cn/**
- 微步检测IP：需要检测的网站IP。

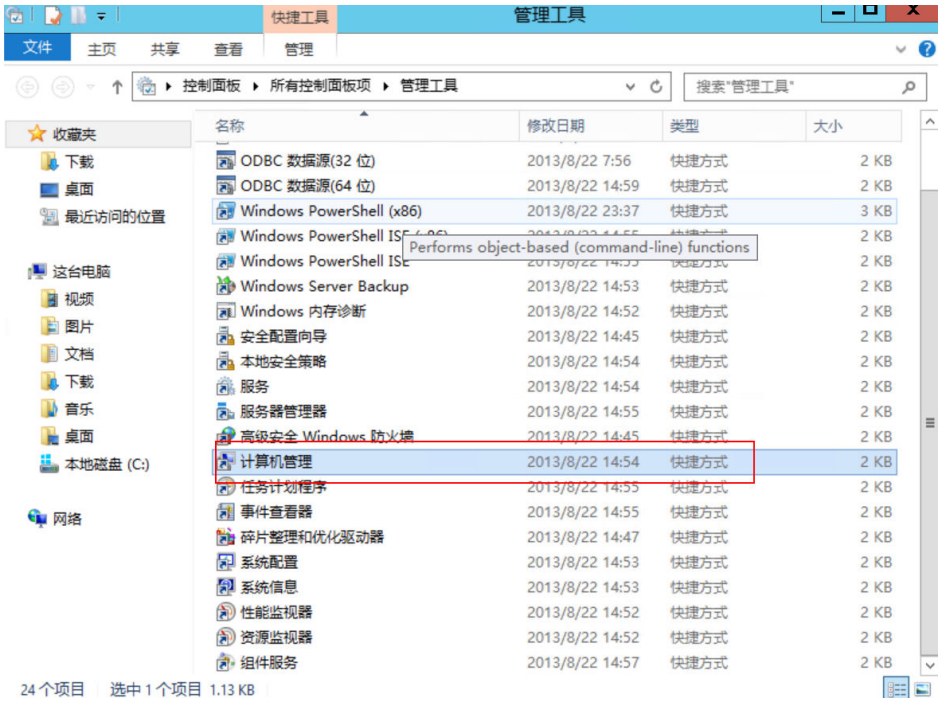
----结束

5.2.2.1.4 步骤 4：异常用户分析

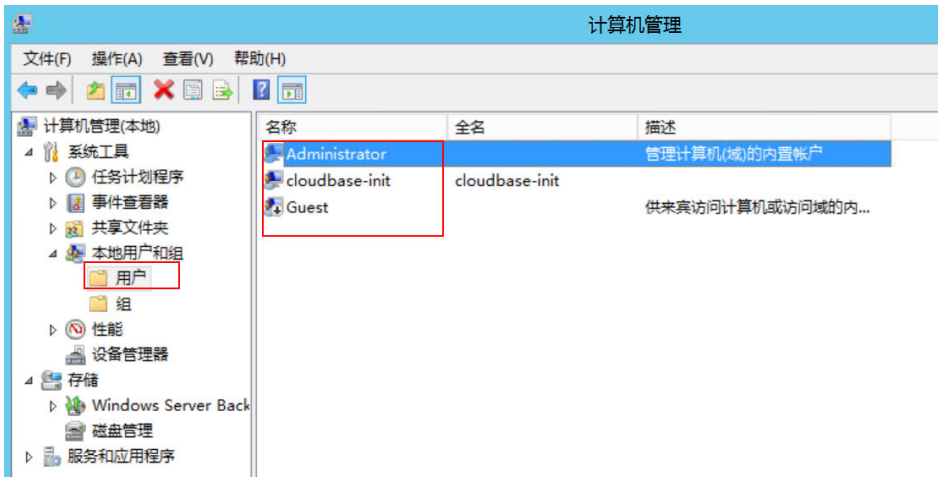
该章节为您介绍如何分析异常用户。

操作步骤

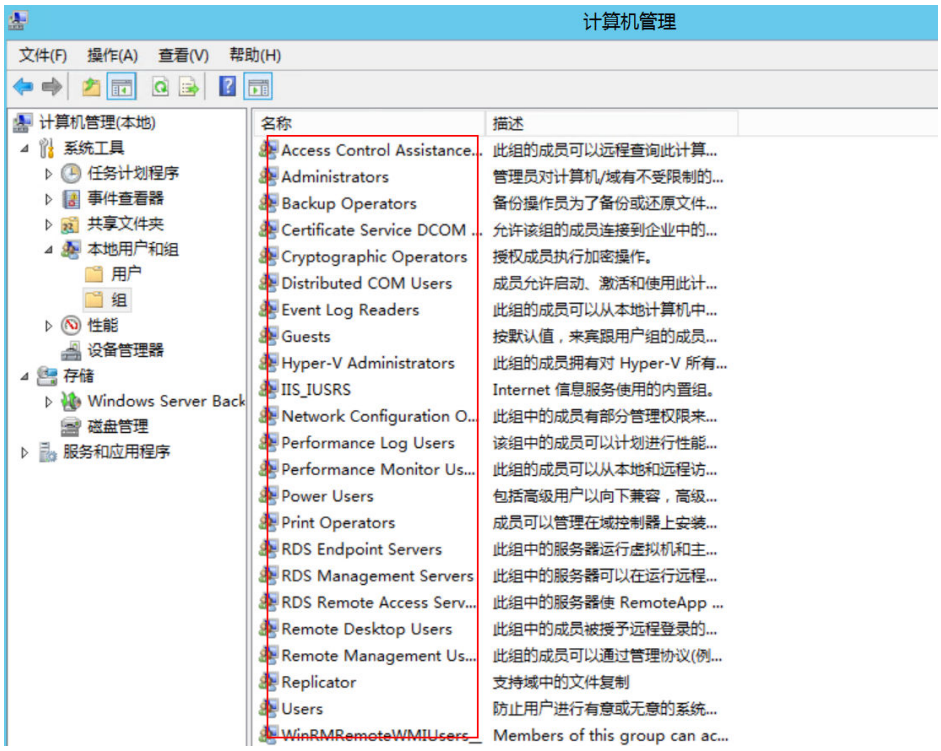
步骤1 打开“控制面板 > 管理工具 > 计算机管理”。



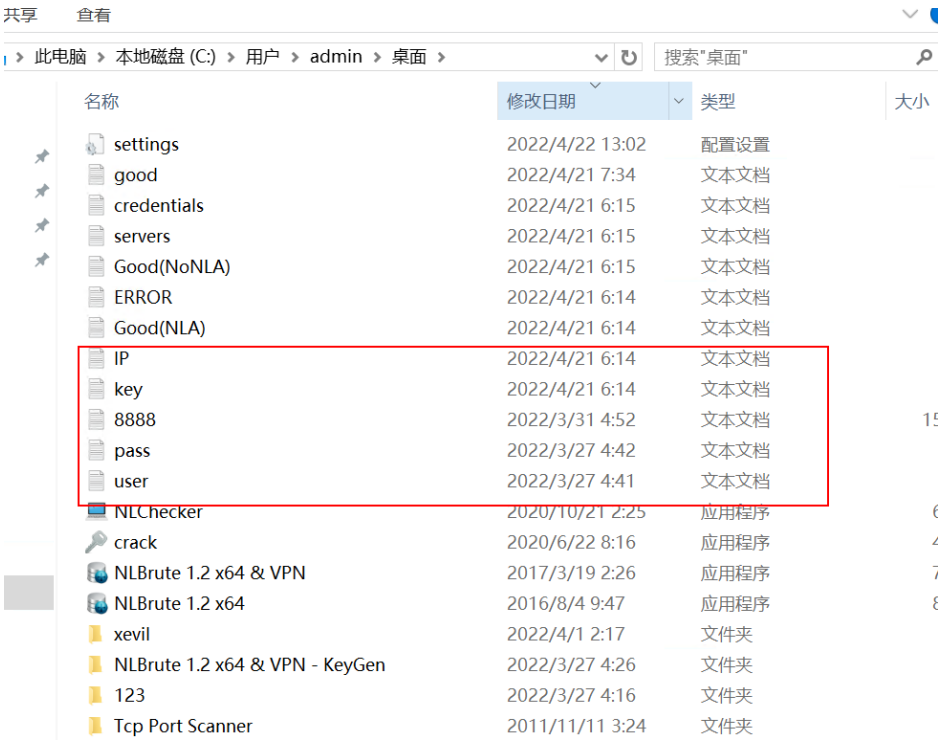
步骤2 在左侧导航树中，选择“本地用户和组 > 用户”，查看主机是否存在异常用户。



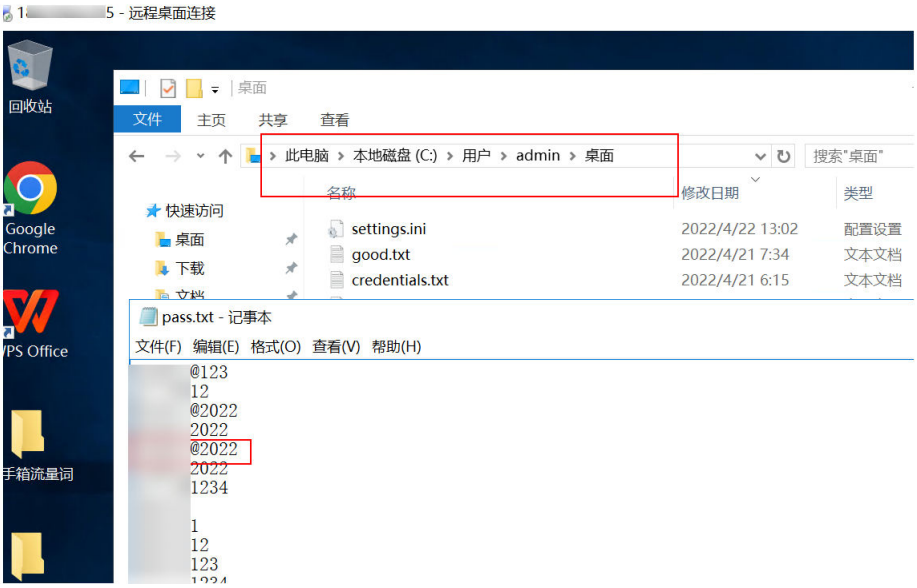
步骤3 在左侧导航树中，选择“本地用户和组 > 组”，检测组是否存在异常。



步骤4 检测主机内的异常用户目录下是否存在异常文件（非系统和业务部署创建的文件）。



步骤5 对异常文件分析，是否为正常业务部署创建的文件，或者通过杀毒软件对文件进行安全检测。



----结束

5.2.2.2 方案二：DOS 系统命令排查

本章节介绍如何通过DOS系统命令进程排查。

常用命令

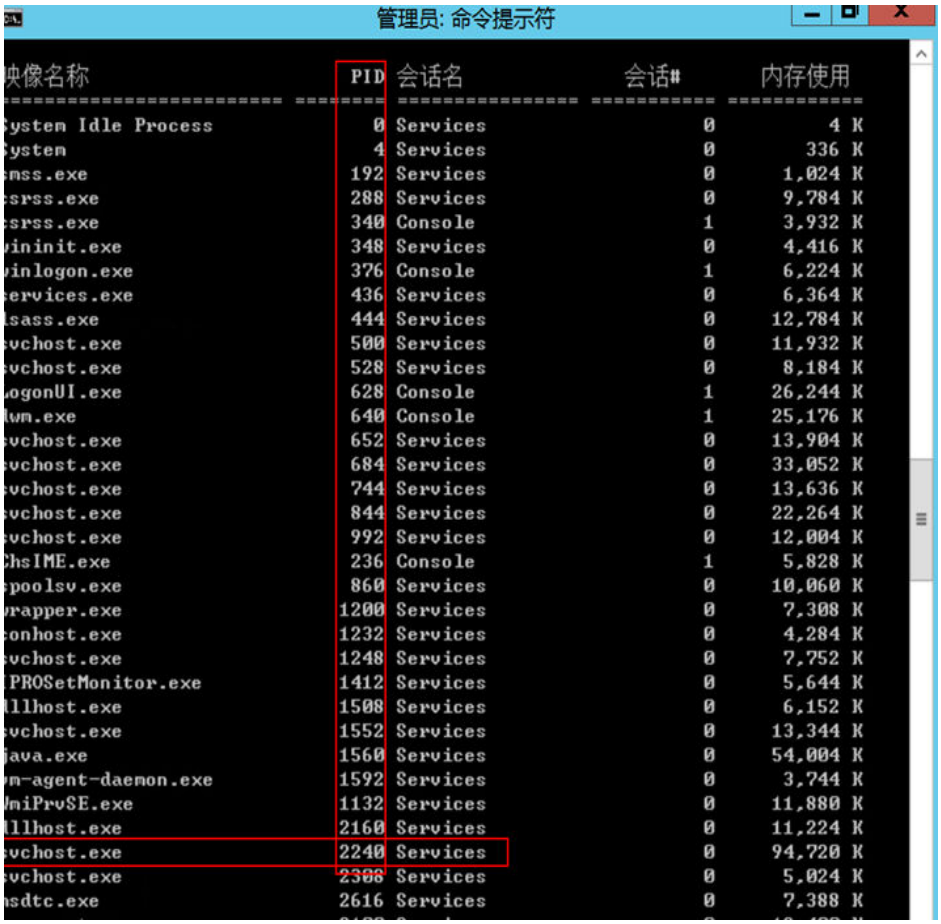
命令	作用
cd	切换目录。 • 当前目录：【./】(同级目录)可省略 • 上一级目录：【../】 • 上上一级目录：【../../】
dir /a:（磁盘）	缺省包含所有文件（系统文件.隐含文件）
more	分屏显示文件内容
tasklist	查看进程
netstat -ano	查看链接
wmic startup list full	查看自启
net user	查看用户
示例： • 查找D:\Apps\下，包含“DR”的文件： **dir /a-d /s "D:\Apps\IDE" | findstr "DR"** • 查找C盘下，包含“exe”的文件和目录：dir /s C: | findstr "exe"	

操作步骤

步骤1 查看是否存在异常进程。

查询命令：**tasklist**

根据查询结果排除系统进程或业务应用进程，锁定异常进程。



步骤2 查看网络分析，是否存在异常的IP链接主机。

查询命令：**netstat –ano**

1. 根据查询结果排除业务连接端口或业务外部地址连接，锁定可疑地址。
2. 使用**微步在线**确认可疑地址是否属于恶意或非正常业务的海外地址。
3. 通过异常连接的“PID”,通过值（如2240）在**步骤1**的查询结果找到进程（如vchost.exe）。

步骤3 检查是否存在异常用户。

1. 命令：**net user**，查询用户信息。

```
C:\Users\Administrator>net user

User accounts for \\HECS-T

-------------------------------------------------------------------------------
Administrator            cloudbase-init           DefaultAccount
Guest                    WDAGUtilityAccount
The command completed successfully.
```

2. 查询命令：**net user** +用户名（如administrator），查询用户更改主机密码的时间。

```
C:\Users\Administrator>net user  Administrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/11/2024 9:08:32 AM
Password expires             Never
Password changeable          9/11/2024 9:08:32 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   9/11/2024 9:37:07 AM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.
```

3. 查询命令：**systeminfo**，查询是否存在重启。

   主机重启会自动清理数据，无法分析用户数据，需查询重要文件目录，请参见**步骤4**。


```
C:\Users\Administrator>systeminfo

Host Name:                 HECS-T
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                [redacted]
Original Install Date:     1/2/2022, 11:39:46 AM
System Boot Time:          9/11/2024, 9:35:54 AM
System Manufacturer:       OpenStack Foundation
System Model:              OpenStack Nova
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2450 Mhz
BIOS Version:              SeaBIOS rel-1.12.1-0-ga5cab58-20230305_150410-szxrtosci10000, 4/1/2014
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,690 MB
Virtual Memory: Max Size:  4,111 MB
Virtual Memory: Available: 2,882 MB
```

步骤4 检查文件分析，是否存异常文件。

查询命令：**dir /s** + 文件目录（如C:）+ **| findstr "exe"**

查询磁盘中（如C盘)下，"exe"的文件和目录，根据查询结果排除系统文件或应用创建文件，锁定异常文件。

```
c:\Users>dir /s C: | findstr "exe"
01/02/2022  11:43 AM    <DIR>          ServerManager.exe_StrongName_m3xk0k0ucj0oj3ai2hibnhnv4xobnimj
 Directory of c:\Users\Administrator\AppData\Local\Microsoft_Corporation\ServerManager.exe_StrongName_m3xk0k0ucj0oj3ai2h
ibnhnv4xobnimj
 Directory of c:\Users\Administrator\AppData\Local\Microsoft_Corporation\ServerManager.exe_StrongName_m3xk0k0ucj0oj3ai2h
ibnhnv4xobnimj\10.0.0.0
06/17/2024  01:12 PM    <DIR>          Indexed DB
 Directory of c:\Users\Administrator\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB
09/11/2024  09:39 AM         2,097,152 IndexedDB.edb
09/11/2024  09:39 AM            16,384 IndexedDB.jfm
09/11/2024  09:18 AM            37,014 {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}_charmap_exe
```

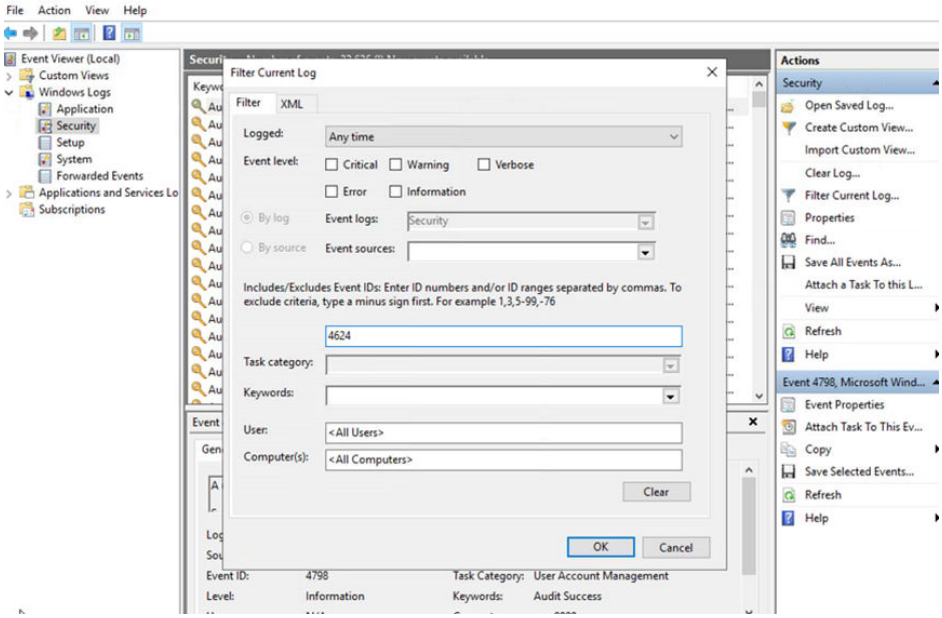
说明

建议重点排查以下目录：“windows”、“windows\system32”、“windows/system32\drivers”、“c:\program files\internet explorer/”、“c:\program files\internet explorer\plugin”、“c:\program files\common files\miscrosoft shared”-临时文件夹。

步骤5 查看windows主机登录日志（登录成功事件ID：4624），排查主机是否存在异常登录情况。

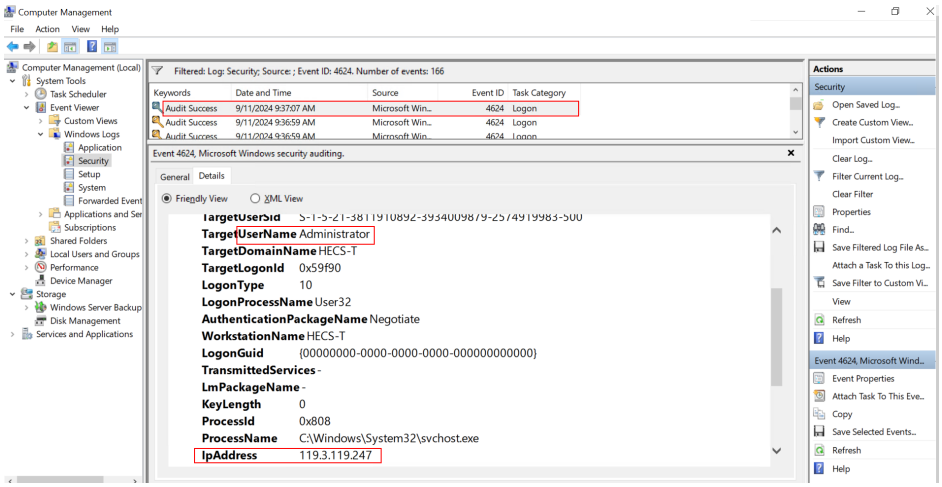
1. 打开“计算机管理”，选择“系统工具 > 事件查看器 > Windows 日志 > 安全”，单击右侧“筛选当前日志”。
2. 填写“包括/排除事件 ID”：4624。

图 5-11 筛选当前日志



3. 查询结果如图 **查询结果**所示

图 5-12 查询结果



步骤6 如果上述方法均不能解决您的疑问，请“提交工单”寻求更多帮助。

----结束

5.2.2.3 Windows 主机安全加固建议

- 设置安全组，仅向公网开放必要端口，业务WEB控制台端口、局域网内部通信端口避免暴露在公网。关闭高危端口（135，139，445），或限制允许访问端口的源IP。
- 应用程序不要以管理员权限账号运行，应用程序（如Web）不使用数据库管理员权限账号与数据库交互。
- 业务数据定期异地备份，避免黑客入侵主机造成数据丢失。
- 定期检测系统和软件中的安全漏洞，及时更新系统安全补丁，将软件版本升级到官方最新版本。

- 建议从官方渠道下载安装软件，对非官方渠道下载的软件，建议使用杀毒软件扫描后再运行。
- 不随意点开不明邮件链接或者网页链接。
- 请勿使用默认账户默认密码或弱密码。
- 设置所有OS系统口令（包括管理员和普通用户）、数据库账号口令、WEB应用系统管理账号口令为强口令 ，密码12位以上。
- 提升安全性的方法：
  - 不使用空口令或系统缺省的口令，因为这些口令很容易被攻击者进入甚至不需要任何成本，为典型的弱口令。
  - 设置高长度&高复杂度字符口令。
  - 口令不要设置连续的某个字符（例如：AAAAAAAA）或重复某些字符的组合（123123）。
  - 口令使用复杂组合，如大写字母(A-Z)、小写字母(a-z)、数字(0-9)和特殊字符。每类字符至少包含一个。
  - 口令中尽量不要包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail地址等与本人有关的信息，以及字典中的单词。
  - 口令不应该为用数字或符号代替某些字母的单词，例如，passwd。
  - 定期更换口令。
  - 口令中不建议出现huawei字样或者带有键盘特征（例如：123qwe!@#，passwd）的密码。

5.3 主机安全排查（Linux 操作系统）

5.3.1 排查思路

Linux主机排查主要分为用户和应用两部分。

- **用户**：通过进程、网络进行分析，查看运行进程的用户。对用户家目录下的用户名目录进行排查是否存在异常文件，是否存在异常登录或暴力破解。
- **应用**：查看进程所属应用，应用的目录下是否有异常文件。

5.3.2 排查过程

本章节介绍Linux操作系统中主机安全排查的具体过程。

操作步骤

步骤1 查看主机是否存在异常进程。

查询命令：**top**

根据CPU占用率、进程名称等判断是否存在异常进程，如下可疑进程CPU占用率超过100%。

```
top - 15:26:55 up 5 days, 21:08,  3 users,  load average: 3.54, 3.36, 3.29
Tasks: 115 total,   1 running, 114 sleeping,   0 stopped,   0 zombie
%Cpu(s):100.0 us,  0.0 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3879812 total,   528792 free,  1769656 used,  1581364 buff/cache
KiB Swap:   524284 total,   208680 free,   315604 used.  1124856 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
25267 oracle    20   0  824248 270772   3480 S 149.2  7.0   4540:04 logind
13493 oracle    20   0  315280 266712   1384 S  50.2  6.9   3728:28 [kthreaddi]
 2107 oracle    -2   0 1790412   1364   1168 S   0.3  0.0   9:19.83 oracle
 2120 oracle    20   0 1795020  27780  23392 S   0.3  0.7  13:02.99 oracle
```

步骤2 根据异常进程PID值，查看文件位置。

查询命令：**lsof -p**+进程PID值（如25267）

```
[root@h          ~]# lsof -p25267
COMMAND   PID   USER   FD      TYPE   DEVICE SIZE/OFF     NODE NAME
logind  25267 oracle  cwd       DIR    253,1     4096  2496248 /home/oracle/.config
logind  25267 oracle  rtd       DIR    253,1     4096        2 /
logind  25267 oracle  txt       REG    253,1  7805520  2496251 /home/oracle/.config/logind
logind  25267 oracle  mem       REG    253,1   109976  1836518 /usr/lib64/libresolv-2.17.so
logind  25267 oracle  mem       REG    253,1    31344  1836506 /usr/lib64/libnss_dns-2.17.so
logind  25267 oracle  mem       REG    253,1    61560  1836508 /usr/lib64/libnss_files-2.17.so
logind  25267 oracle  mem       REG    253,1  2156344  1836490 /usr/lib64/libc-2.17.so
logind  25267 oracle  mem       REG    253,1  1136944  1836498 /usr/lib64/libm-2.17.so
logind  25267 oracle  mem       REG    253,1    19248  1836496 /usr/lib64/libdl-2.17.so
logind  25267 oracle  mem       REG    253,1    43712  1836520 /usr/lib64/librt-2.17.so
logind  25267 oracle  mem       REG    253,1   142144  1836516 /usr/lib64/libpthread-2.17.so
logind  25267 oracle  mem       REG    253,1   163312  1844706 /usr/lib64/ld-2.17.so
logind  25267 oracle    0r      CHR      1,3      0t0     1031 /dev/null
logind  25267 oracle    1w      CHR      1,3      0t0     1031 /dev/null
logind  25267 oracle    2w      CHR      1,3      0t0     1031 /dev/null
logind  25267 oracle    3u  a_inode     0,10        0     6394 [eventpoll]
```

步骤3 发现目录下的异常文件（带有xmr或mine的标识）。

1. 查看文件命令：**ll -art**

```
[root@          ' .config]# ll -art
total 13676
-rwxrwxrwx 1 oracle oinstall      54 Jan  9  2002 start
-rwxrwxrwx 1 oracle oinstall  838583 Jun 15  2018 h64
-rwxr-xr-x 1 oracle oinstall     337 Feb 14  2020 go
-rwx--x--x 1 oracle oinstall  215960 Dec 19  2020 arm
-rwx--x--x 1 oracle oinstall 5092504 Dec 19  2020 xmrigMiner
-rwxr-xr-x 1 oracle oinstall 7805520 Apr 28 13:30 logind
-rwxrwxrwx 1 oracle oinstall     243 Apr 28 13:31 update
drwxr-xr-x 2 oracle oinstall    4096 Jun 25 00:25 .
-rwxrwxrwx 1 oracle oinstall     392 Jun 25 00:31 libs
-rw-r--r-- 1 oracle oinstall      21 Jun 27 11:59 dir.dir
-rw-r--r-- 1 oracle oinstall      51 Jun 27 11:59 cron.d
-rwxr--r-- 1 oracle oinstall     212 Jun 27 11:59 upd
-rwxr-xr-x 1 oracle oinstall       6 Jun 27 11:59 bash.pid
-rw-r--r-- 1 oracle oinstall    2771 Jun 27 11:59 config.json
drwx------ 5 oracle oinstall    4096 Jun 28 16:44 ..
[root@h          7 .config]# pwd
/home/oracle/.config
[root@h          ' .config]#
```

2. 查询木马路径：**pwd**

   查询文件中是否存在异常地址：**strings** +文件名（如config.json）+ **|grep xmr**

```
[root@          7 .config]# pwd
/home/oracle/.config
[root@h          .config]# strings config.json |grep xmr
            "url": "xmr.flooder.org:80",
[root@h          7 .config]# pwd
/home/oracle/.config
```

说明

建议重点排查以下目录：/etc为配置文件、/tmp为临时文件、/bin为可执行文件。

- 用户命令；用到的库文件可能在/lib，配置文件可能在/etc，/sbin为可执行文件。
- 管理命令；用到的库文件可能在/lib，配置文件可能在/etc，/usr/为只读文件，shared read-only，/usr/local为第三方软件）
- Linux命令大全请参见**Linux命令大全**。

3. 发现疑似矿池信息，将URL（xmr.flooder.org:80）放到**微步**上检测，结果为矿池。

步骤4 查看主机用户权限。

查询命令：**cat /etc/passwd|grep** +用户名（如bash）

```
dr-xr-xr-x.  2 root root       16384 Feb 26 12:38 .
[root@hecs-144007 sbin]# cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
csp:x:1000:1000::/home/csp:/bin/bash
oracle:x:1001:1001::/home/oracle:/bin/bash
```

说明

nologin的用户没有登录权限，此处需重点查看存在登录权限的用户。

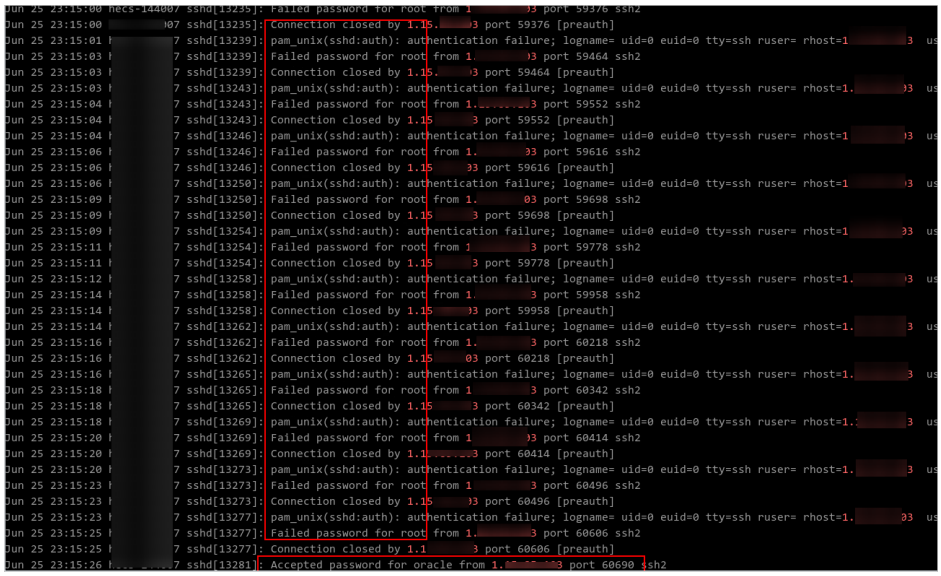
步骤5 根据主机登录日志文件，查看异常登录记录。

查询命令：**cat** +文件名（如 secure）**|grep Acc|grep** +用户名（如oracle）

根据成功日志寻找登录主机的习惯时间，需关注与木马植入相近的时间。

```
[root@r      log]# cat secure*|grep Acc|grep oracle
Jun 27 11:44:52 l          sshd[24188]: Accepted password for oracle from 1          13 port 34288 ssh2
Jun 27 11:59:06            sshd[25220]: Accepted password for oracle from 1          port 42032 ssh2
Jun 28 16:43:53 h          sshd[348]: Accepted password for oracle from 5:          44 port 37048 ssh2
Jun 25 23:15:26 h          sshd[13281]: Accepted password for oracle from 1          3 port 60690 ssh2
```

根据登录的时间关注是否有异常IP登录及登录的频次（包括成功或失败的次数），若异常IP登录次数多则疑似为爆破行为。



步骤6 如果上述方法均不能解决您的疑问，请“提交工单”寻求更多帮助。

----结束

5.3.3 Linux 主机安全加固建议

- 设置所有OS系统口令（包括管理员和普通用户）、数据库账号口令、应用（WEB）系统管理账号口令为强口令，密码12位以上。
- 将主机登录方式设置为密钥登录。
- 应用程序不以管理员权限账号运行，应用程序（如Web）不使用数据库管理员权限账号与数据库交互设置安全组，仅向公网开放必要端口，业务WEB控制台端口、局域网内部通信端口避免暴露在公网。关闭高危端口（如SSH端口），或采取限制允许访问端口的源IP、使用VPN/堡垒机建立的运维通道等措施消减风险。
- 业务数据定期异地备份，避免黑客入侵主机造成数据丢失。
- 定期检测系统和软件中的安全漏洞，及时更新系统安全补丁，将软件版本升级到官方最新版本。
- 建议从官方渠道下载安装软件，对非官方渠道下载的软件，建议使用杀毒软件扫描后再运行。
- 为彻查主机和应用方面潜在的安全风险，建议使用主机安全服务深度防御：

  企业主机安全服务请参见：**https://www.huaweicloud.com/intl/zh-cn/product/hss.html**。