主机安全

故障排除

产品文档

腾讯云

文档目录

故障排除
Linux 入侵类问题排查思路

最近更新时间：2020-06-17 11:54:54

深入分析，查找入侵原因

一、检查隐藏帐户及弱口令

1. 检查服务器系统及应用帐户是否存在 **弱口令**：
   - 检查说明：检查管理员帐户、数据库帐户、MySQL 帐户、tomcat 帐户、网站后台管理员帐户等密码设置是否较为简单，简单的密码很容易被黑客破解。
   - 解决方法：以管理员权限登录系统或应用程序后台，修改为复杂的密码。
   - 风险性：高。
2. 使用 `last` 命令查看下服务器近期登录的帐户记录，确认是否有可疑 IP 登录过机器：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统帐户实施提权或其他破坏性的攻击。
   - 解决方法：检查发现有可疑用户时，可使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
   - 风险性：高。
3. 通过 `less /var/log/secure|grep 'Accepted'` 命令，查看是否有可疑 IP 成功登录机器：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统帐户实施提权或其他破坏性的攻击。
   - 解决方法： 使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
   - 风险性：高。
4. 检查系统是否采用 **默认管理端口**：
   - 检查系统所用的管理端口（SSH、FTP、MySQL、Redis 等）是否为默认端口，这些默认端口往往被容易自动化的工具进行爆破成功。
   - 解决方法：
     a. 在服务器内编辑 `/etc/ssh/sshd_config` 文件中的 Port 22，将22修改为非默认端口，修改之后需要重启 ssh 服务。

        注意：
        当对端口进行修改时，需同时在 云服务器控制台 上修改对应主机的安全组配置，在其入站规则中，放行对应端口，详情请参见 添加安全组规则。

     b. 运行 `/etc/init.d/sshd restart`（CentOS）或 `/etc/init.d/ssh restart`（Debian / Ubuntu） 命令重启是配置生效。

c. 修改 FTP、MySQL、Redis 等的程序配置文件的默认监听端口21、3306、6379为其他端口。
d. 限制远程登录的 IP，编辑 /etc/hosts.deny 、 /etc/hosts.allow 两个文件来限制 IP。

- 风险性：高。

5. 检查 /etc/passwd 文件，看是否有非授权帐户登录：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统帐户实施提权或其他破坏性的攻击。
   - 解决方法： 使用命令 usermod -L 用户名 禁用用户或者使用命令 userdel -r 用户名 删除用户。
   - 风险性：中。

二、检查恶意进程及非法端口

1. 运行 netstat –antp 查看下服务器是否有未被授权的端口被监听，查看下对应的 pid。
   - 检查服务器是否存在恶意进程,恶意进程往往会开启监听端口，与外部控制机器进行连接。
   - 解决方法：
     a. 若发现有非授权进程，运行 ls -l /proc/$PID/exe 或 file /proc/$PID/exe （ $PID 为对应的 pid 号），查看下 pid 所对应的进程文件路径。
     b. 如果为恶意进程，删除下对应的文件即可。
   - 风险性：高。
2. 使用 ps -ef 和 top 命令查看是否有异常进程
   - 检查说明：运行以上命令，当发现有名称不断变化的非授权进程占用大量系统 CPU 或内存资源时，则可能为恶意程序。
   - 解决方法：确认该进程为恶意进程后，可以使用 kill -9 进程名 命令结束进程，或使用防火墙限制进程外联。
   - 风险性：高。

三、检查恶意程序和可疑启动项

1. 使用 chkconfig --list 和 cat /etc/rc.local 命令查看下开机启动项中是否有异常的启动服务。
   - 检查说明：恶意程序往往会添加在系统的启动项，在用户关机重启后再次运行。
   - 解决方法：如发现有恶意进程，可使用 chkconfig 服务名 off 命令关闭，同时检查 /etc/rc.local 中是否有异常项目，如有请注释掉。
   - 风险性：高。
2. 进入 cron 文件目录，查看是否存在非法定时任务脚本。
   - 检查说明：查看 /etc/crontab ， /etc/cron.d ， /etc/cron.daily ， cron.hourly/ ， cron.monthly ， cron.weekly/ 是否存在可疑脚本或程序。
   - 解决方法：如发现有不认识的计划任务，可定位脚本确认是否正常业务脚本，如果非正常业务脚本，可直接注释掉任务内容或删除脚本。
   - 风险性：高。

四、检查第三方软件漏洞

1. 如果您服务器内有运行 Web、数据库等应用服务，请您限制应用程序帐户对文件系统的写权限，同时尽量使用非 root 帐户运行。
   - 检查说明：使用非 root 帐户运行可以保障在应用程序被攻陷后攻击者无法立即远程控制服务器，减少攻击损失
   - 解决方法：
     a. 进入 web 服务根目录或数据库配置目录；
     b. 运行 `chown -R apache:apache /var/www/xxxx` 、 `chmod -R 750 file1.txt` 命令配置网站访问权限。
   - 风险性：中。
   - 参考示例
2. 升级修复应用程序漏洞
   - 检查说明：机器被入侵，部分原因是系统使用的应用程序软件版本较老，存在较多的漏洞而没有修复，导致可以被入侵利用。
   - 解决方法：比较典型的漏洞例如 ImageMagick、openssl、glibc 等，用户可以根据腾讯云已发布安全通告指导通过 apt-get/yum 等方式进行直接升级修复。
   - 风险性：高。

网站目录文件权限的参考示例如下：

场景：

我们假设 HTTP 服务器运行的用户和用户组是 www，网站用户为 centos，网站根目录是 `/home/centos/web` 。

方法/步骤：

1. 我们首先设定网站目录和文件的所有者和所有组为 centos，www，如下命令：

```
chown -R centos:www /home/centos/web
```

2. 设置网站目录权限为750，750是 centos 用户对目录拥有读写执行的权限，设置后，centos 用户可以在任何目录下创建文件，用户组有有读执行权限，这样才能进入目录，其它用户没有任何权限。

```
find -type d -exec chmod 750 {} \;
```

3. 设置网站文件权限为640，640指只有 centos 用户对网站文件有更改的权限，HTTP 服务器只有读取文件的权限，无法更改文件，其它用户无任何权限。

```
find -not -type d -exec chmod 640 {} \;
```

4. 针对个别目录设置可写权限。例如，网站的一些缓存目录就需要给 HTTP 服务有写入权限、discuz x2 的 `/data/` 目录就必须要写入权限。

```
find data -type d -exec chmod 770 {} \;
```

被入侵后的安全优化建议

1. 尽量使用 SSH 密钥进行登录，减少暴力破解的风险。
2. 在服务器内编辑 `/etc/ssh/sshd_config` 文件中的 Port 22，将 22 修改为其他非默认端口，修改之后重启 SSH 服务。可使用命令重启

   ```
   /etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian/Ubuntu）
   ```

   > 注意：
   > 当修改端口时，需同时在 云服务器控制台 上修改对应主机安全组配置，在其入站规则中放行对应端口，详情请参见 添加安全组规则。

3. 如果必须使用 SSH 密码进行管理，选择一个好密码。
   - 无论应用程序管理后台（网站、中间件、tomcat 等）、远程 SSH、远程桌面、数据库，都建议设置复杂且不一样的密码。
   - 下面是一些好密码的实例（可以使用空格）：
     `1qtwo-threeMiles3c45jia`
     `caser, lanqiu streets`
   - 下面是一些弱口令的示例，可能是您在公开的工作中常用的词或者是您生活中常用的词：
     公司名+日期（coca-cola2016xxxx）
     常用口语（Iamagoodboy）
4. 使用以下命令检查主机有哪些端口开放，关闭非业务端口。

   ```
   netstat -antp
   ```

5. 通过**腾讯云-安全组防火墙**限制仅允许制定 IP 访问管理或通过编辑 `/etc/hosts.deny` 、 `/etc/hosts.allow` 两个文件来限制 IP。
6. 应用程序尽量不使用 **root** 权限。
   例如 Apache、Redis、MySQL、Nginx 等程序，尽量不要以 root 权限的方式运行。
7. 修复系统提权漏洞与运行在 root 权限下的**程序漏洞**，以免恶意软件通过漏洞提权获得 root 权限传播后门。
   - 及时更新系统或所用应用程序的版本，如 Struts2、Nginx，ImageMagick、Java 等。
   - 关闭应用程序的远程管理功能，如 Redis、NTP 等，如果无远程管理需要，可关闭对外监听端口或配置。
8. 定期**备份**云服务器业务数据。
   - 对重要的业务数据进行异地备份或云备份，避免主机被入侵后无法恢复。
   - 除了您的 home，root 目录外，您还应当备份 /etc 和可用于取证的 /var/log 目录。
9. 安装腾讯云**主机安全 Agent**，在发生攻击后，可以了解自身风险情况。

Windows 入侵类问题排查思路

最近更新时间：2020-03-18 18:25:42

深入分析，查找入侵原因

一. 检查帐户和弱口令

1. 查看服务器已有系统或应用帐户是否存在弱口令。
   - 检查说明：主要检查系统管理员帐户、网站后台帐户、数据库帐户以及其他应用程序（FTP、Tomcat、phpMyAdmin 等）帐户是否存在弱口令。
   - 检查方法：根据实际情况自行确认。
   - 风险性：高。
2. 查看下服务器内是否有非系统和用户本身创建的账户。
   - 检查说明：一般黑客创建的异常账户账户名会在本地用户组显示出来。
   - 检查方法：打开 cmd 窗口，输入 `lusrmgr.msc` 命令，查看是否有新增的账号，如有管理员群组的（Administrators）里的新增账户，如有，请立即禁用或删除掉。
   - 风险性：高。
3. 检查是否存在隐藏账户名。
   - 检查说明：黑客为了逃避检查，往往会在您服务器内创建隐藏用户，隐藏账户在本地用户内是查看不到的。
   - 检查方法（您也可以通过下载 LP_Check 安全工具检查是否有隐藏账户）：
     a. 在桌面打开运行（可使用快捷键 Win + R），输入 regedit，即可打开注册表编辑器。
     b. 选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认无法查看该选项内容，右键菜单选择权限，打开权限管理窗口。
     c. 选择当前用户（一般为 administrator），将权限勾选为完全控制，然后确定，关闭注册表编辑器。
     d. 再次打开注册表编辑器，即可选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users。
     e. 在 Names 项下可以看到实例所有用户名，如出现本地账户中没有的账户，即为隐藏账户，在确认为非系统用户的前提下，可删除此用户。
   - 风险性：高。

二. 检查恶意进程和端口

1. 检查是否存在恶意进程在系统后台运行。
   - 检查说明：攻击者在入侵系统后，往往会运行恶意进程与外部进行通信，通过分析外联的进程，即可以找出入侵的控制进程。
   - 检查方法：
     a. 登录服务器，选择【开始】>【运行】。
     b. 输入 cmd，然后输入 netstat –nao 查看下服务器是否有未被授权的端口被监听。

c. 打开任务管理器，检查对应的 PID 进程号所对应的进程是否为正常进程，例如通过 PID 号查看下运行文件的路径，删除对应路径文件，您也可以通过微软官方提供的 Process Explorer 工具进行排查。

- 风险性：高。

三. 检查恶意程序及启动项

1. 检查服务器内部是否有异常的启动项。

- 检查说明：攻击者在入侵系统后，往往会把恶意程序放到启动项中开机执行。
- 检查方法：

a. 登录服务器，选择【开始】>【所有程序】>【启动】。

b. 默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

c. 选择【开始】 >【运行】，输入 msconfig，查看是否存在命名异常的启动项目，若存在则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

d. 选择【开始】>【运行】，输入 regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：
HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
检查右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

- 风险性：高。

2. 查看正在连接的会话。

- 检查说明：检查计算机与网络上的其它计算机之间的会话或计划任务。
- 检查方法：

a. 登录服务器，选择【开始】>【运行】。

b. 输入 cmd，然后输入 netstat -ano，检查计算机与网络上的其它计算机之间的会话，并确认是否为正常连接。输入 schtasks，检查计算机中的计划任务，并确认是否为正常的计划任务。

- 风险性：中。

四. 检查第三方软件漏洞

1. 如果您服务器内有运行对外应用软件（WWW、FTP 等），请您对软件进行配置，**限制应用程序的权限，禁止目录浏览或文件写权限。**
2. **开通腾讯云 Web 应用防火墙防护**，查看 Web 应用防护攻击日志。

如何恢复网站或系统

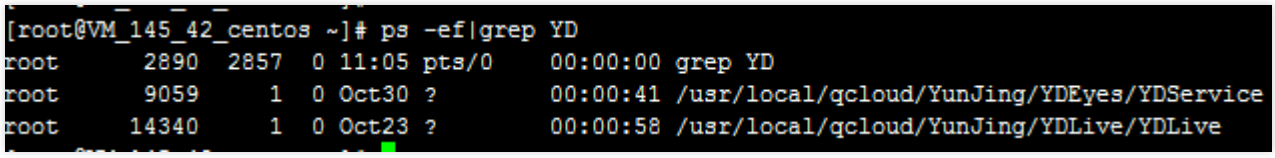
1. **系统确认被入侵后，往往系统文件会被更改和替换，此时系统已经变得不可信，最好的方法就是重新安装系统，同时给新系统安装所有补丁。**
2. 改变所有系统账号的密码为 **复杂密码**（至少与入侵前不一致）。
3. **修改默认远程桌面端口**，操作如下：
   i. 选择【开始】>【运行】，然后输入 regedit。
   ii. 打开注册表，进入如下路径： HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
   iii. KEY_LOCAL_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp
   iv. 修改下右侧的 PortNamber 值。
4. 配置腾讯云安全组防火墙只允许 **指定 IP 才能访问远程桌面端口。**
5. **定期备份重要业务数据和文件。**
6. **定期更新操作系统及应用程序组件版本（如 FTP、Struts2 等）**，防止被漏洞利用。
7. 安装**腾讯云主机安全 Agent** 和防病毒软件进行定期体检和扫描。

Linux 客户端离线排查

最近更新时间：2020-08-24 15:12:46

客户端进程未启动排查

1. 请查询主机安全进程是否存在。输入： `ps -ef|grep YD` 。
2. 正常状态下，主机安全存在两个进程，如下图所示：



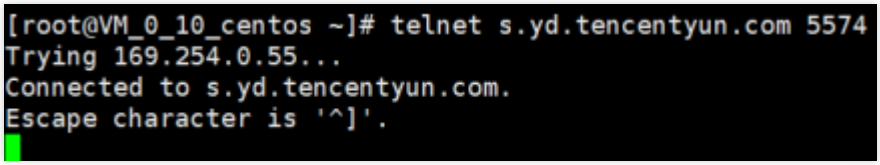
3. 如果进程不存在，可能存在以下情况：
   - 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
   - 客户端可能出现异常冲突或者崩溃，导致进程没有启动。
4. 排查方法：
   - 可查看客户端日志，存放路径： `/usr/local/qcloud/YunJing/log` 。
   - 可执行命令： `sh /usr/local/qcloud/YunJing/startYD.sh` 启动主机安全服务。

网络故障排查

如果进程存在，但主机安全不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 检查 DNS 是否被修改，可以通过执行如下命令行进行排查：
   - VPC 网络和黑石服务器环境： `telnet s.yd.tencentyun.com 5574` 。

     正常情况下：返回如下图所示结果。



     如果无法访问：

     a. 可以尝试修改 `dns nameserver` 字段： `vim /etc/resolv.conf`

     `nameserver 183.60.83.19`

     `nameserver 183.60.82.98`

b. 修改完成后，重新执行 `telnet s.yd.tencentyun.com 5574` 检测能否连通。

```
[root@VM_0_7_centos ~]# cat /etc/resolv.conf
options timeout:1 rotate
; generated by /usr/sbin/dhclient-script
nameserver 183.60.83.19
nameserver 183.60.82.98
```

c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

- 基础网络环境（非 VPC 服务器）：`telnet s.yd.qcloud.com 5574`。

  正常情况下：返回如下图所示结果。

```
[root@VM-28-45-centos ~]# telnet s.yd.qcloud.com 5574
Trying 10.53.78.111...
Connected to s.yd.qcloud.com.
Escape character is '^]'.
```

  如果无法访问：

  a. 可以尝试修改 `dns nameserver` 字段：`vim /etc/resolv.conf`，先把原有的 `nameserver` 字段注释，再新增 `nameserver` 字段，具体的 nameserver ip 相关内容，请参见 内网服务。

  b. 修改完成后，重新执行 `telnet s.yd.qcloud.com 5574` 检测能否可以连通。

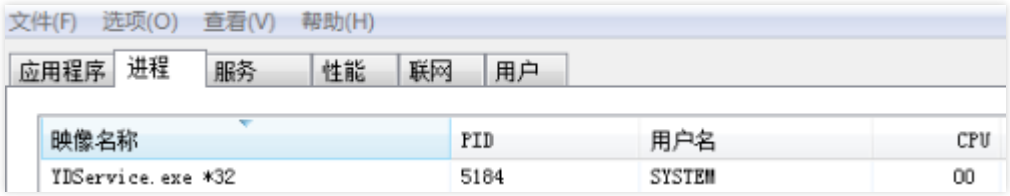
2. 防火墙策略限制，需要开放 TCP 端口：5574、8080、80、9080。
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径：`/usr/local/qcloud/YunJing/log`）提交工单 进行反馈。

Windows 客户端离线排查

最近更新时间：2020-08-24 15:12:52

客户端进程未启动排查

1. 请查询主机安全进程是否存在。
   打开 Windows 任务管理器，查找名为 YDService.exe 的进程是否存在。



2. 如果进程不存在，可能存在以下情况：
   - 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
   - 客户端可能出现异常冲突或者崩溃，导致进程没有启动。
3. 排查方法：
   - 可查看客户端日志，存放路径： C:\Program Files\QCloud\YunJing\log 。
   - 可执行命令： sc start ydservice 手动运行客户端。

网络故障排查

如果进程存在，但 CVM 不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 检查 DNS 是否被修改，可以通过执行如下命令行进行排查，只要其中一个返回正常结果，则表示 DNS 无问题：
   - 基础网络下载地址（非 VPC 服务器）： telnet s.yd.qcloud.com 5574 。
   - VPC 和黑石服务器下载： telnet s.yd.tencentyun.com 5574 。
2. 防火墙阻拦导致故障，需要开放5574、8080、80、9080端口。
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径： C:\Program Files\QCloud\YunJing\log ）提交工单 进行反馈。