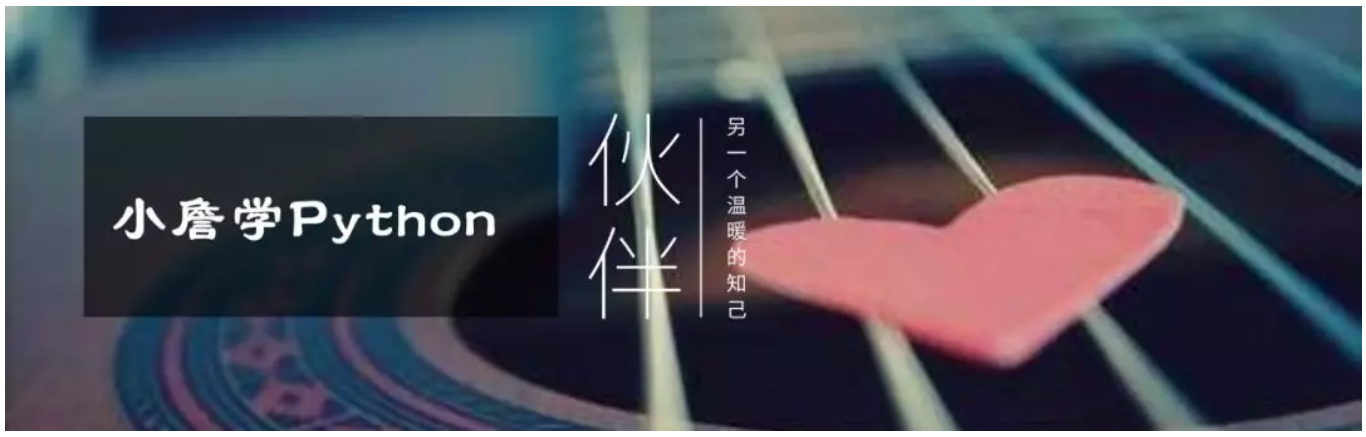
黑客入侵你Linux服務器的一萬種玩法...

高俊峰 小詹學Python 今天



編輯：陶家龍、孫淑娟

出處：https://www.cnblogs.com/MYSQLZOUQI/p/5317916.html

> 安全是IT 行業一個老生常談的話題了，從之前的“棱鏡門”事件中折射出了很多安全問題，處理好信息安全問題已變得刻不容緩。

因此做為運維人員，就必須了解一些安全運維準則，同時，要保護自己所負責的業務，首先要站在攻擊者的角度思考問題，修補任何潛在的威脅和漏洞。

本文主要分為如下五部分展開：

- **賬戶和登錄安全**
- **遠程訪問和認證安全**
- **文件系統安全**
- **Linux 後門入侵檢測工具**
- **服務器遭受攻擊後的處理過程**

賬戶和登錄安全

賬戶安全是系統安全的第一道屏障，也是系統安全的核心，保障登錄賬戶的安全，在一定程度上可以提高服務器的安全級別，下面重點介紹下Linux 系統登錄賬戶的安全設置方法。

①刪除特殊的賬戶和賬戶組

Linux 提供了各種不同角色的系統賬號，在系統安裝完成後，默認會安裝很多不必要的用戶和用戶組。

如果不需要某些用戶或者組，就要立即刪除它，因為賬戶越多，系統就越不安全，很可能被黑客利用，進而威脅到服務器的安全。

Linux系統中可以刪除的默認用戶和組大致有如下這些：

> ***可刪除的用戶，****如adm，lp，sync，shutdown，halt，news，uucp，operator，games，gopher等。*
>
> ***可刪除的組，****如adm，lp，news，uucp，games，dip，pppusers，popusers，slipusers等。*

②關閉系統不需要的服務

Linux 在安裝完成後，綁定了很多沒用的服務，這些服務默認都是自動啟動的。

對於服務器來說，運行的服務越多，系統就越不安全，越少服務在運行，安全性就越好，因此關閉一些不需要的服務，對系統安全有很大的幫助。

具體哪些服務可以關閉，要根據服務器的用途而定，一般情況下，只要係統本身用不到的服務都認為是不必要的服務。

例如：某台Linux 服務器用於www 應用，那麼除了httpd 服務和系統運行是必須的服務外，其他服務都可以關閉。

下面這些服務一般情況下是不需要的，可以選擇關閉：

> *anacron、auditd、autofs、avahi-daemon、avahi-dnsconfd、bluetooth、cpuspeed、firstboot、gpm、haldaemon、hidd、ip6tables、ipsec、isdn、lpd、mcstrans、messagebus、netfs、nfs、nfslock、nscd、pcscd portmap、readahead_early 、restorecond、rpcgssd、rpcidmapd、rstatd、sendmail、setroubleshoot、yppasswdd ypserv*

③密碼安全策略

在Linux 下，遠程登錄系統有兩種認證方式：

- **密碼認證**
- **密鑰認證**

密碼認證方式是傳統的安全策略，對於密碼的設置，比較普遍的說法是：至少6 個字符以上，密碼要包含數字、字母、下劃線、特殊符號等。

設置一個相對複雜的密碼，對系統安全能起到一定的防護作用，但是也面臨一些其他問題，例如密碼暴力破解、密碼洩露、密碼丟失等，同時過於復雜的密碼對運維工作也會造成一定的負擔。

密鑰認證是一種新型的認證方式，公用密鑰存儲在遠程服務器上，專用密鑰保存在本地，當需要登錄系統時，通過本地專用密鑰和遠程服務器的公用密鑰進行配對認證，如果認證成功，就成功登錄系統。

這種認證方式避免了被暴力破解的危險，同時只要保存在本地的專用密鑰不被黑客盜用，攻擊者一般無法通過密鑰認證的方式進入系統。

因此，在Linux 下推薦用密鑰認證方式登錄系統，這樣就可以拋棄密碼認證登錄系統的弊端。

Linux 服務器一般通過SecureCRT、Putty、Xshell 之類的工具進行遠程維護和管理，密鑰認證方式的實現就是藉助於SecureCRT 軟件和Linux 系統中的SSH 服務實現的。

④合理使用 su、sudo 命令

su命令：是一個切換用戶的工具，經常用於將普通用戶切換到超級用戶下，當然也可以從超級用戶切換到普通用戶。

為了保證服務器的安全，幾乎所有服務器都禁止了超級用戶直接登錄系統，而是通過普通用戶登錄系統，然後再通過su 命令切換到超級用戶下，執行一些需要超級權限的工作。

通過su命令能夠給系統管理帶來一定的方便，但是也存在不安全的因素，例如：系統有10個普通用戶，每個用戶都需要執行一些有超級權限的操作，就必須把超級用戶的密碼交給這10個普通用戶。

如果這10 個用戶都有超級權限，通過超級權限可以做任何事，那麼會在一定程度上對系統的安全造成了威協。

因此su 命令在很多人都需要參與的系統管理中，並不是最好的選擇，超級用戶密碼應該掌握在少數人手中，此時sudo 命令就派上用場了。

sudo命令：允許系統管理員分配給普通用戶一些合理的“權利”，並且不需要普通用戶知道超級用戶密碼，就能讓他們執行一些只有超級用戶或其他特許用戶才能完成的任務。

比如：系統服務重啟、編輯系統配置文件等，通過這種方式不但能減少超級用戶登錄次數和管理時間，也提高了系統安全性。

因此，sudo 命令相對於權限無限制性的su 來說，還是比較安全的，所以sudo 也被稱為受限制的su，另外sudo 也是需要事先進行授權認證的，所以也被稱為授權認證的su 。

sudo執行命令的流程是：將當前用戶切換到超級用戶下，或切換到指定的用戶下，然後以超級用戶或其指定切換到的用戶身份執行命令。

執行完成後，直接退回到當前用戶，而這一切的完成要通過sudo 的配置文件 /etc/sudoers 來進行授權。

sudo設計的宗旨是：賦予用戶盡可能少的權限但仍允許它們完成自己的工作，這種設計兼顧了安全性和易用性。

因此，強烈推薦通過sudo 來管理系統賬號的安全，只允許普通用戶登錄系統，如果這些用戶需要特殊的權限，就通過配置/etc/sudoers 來完成，這也是多用戶系統下賬號安全管理的基本方式。

⑤刪減系統登錄歡迎信息

系統的一些歡迎信息或版本信息，雖然能給系統管理者帶來一定的方便，但是這些信息有時候可能被黑客利用，成為攻擊服務器的幫兇。

為了保證系統的安全，可以修改或刪除某些系統文件，需要修改或刪除的文件有四個，分別是：

- **/etc/issue**
- **/etc/issue.net**
- **/etc/redhat-release**
- **/etc/motd**

/etc/issue 和 /etc/issue.net 文件都記錄了操作系統的名稱和版本號，當用戶通過本地終端或本地虛擬控制台等登錄系統時，/etc/issue 的文件內容就會顯示。

當用戶通過ssh 或telnet 等遠程登錄系統時，/etc/issue.net 文件內容就會在登錄後顯示。

在默認情況下/etc/issue.net文件的內容是不會在ssh登錄後顯示的，要顯示這個信息可以修改/etc/ssh/sshd_config文件，在此文件中添加如下內容即可：Banner /etc /issue.net。

其實這些登錄提示很明顯洩漏了系統信息，為了安全起見，建議將此文件中的內容刪除或修改。

/etc/redhat-release 文件也記錄了操作系統的名稱和版本號，為了安全起見，可以將此文件中的內容刪除。

/etc/motd 文件是系統的公告信息。每次用戶登錄後，/etc/motd 文件的內容就會顯示在用戶的終端。

通過這個文件系統，管理員可以發布一些軟件或硬件的升級、系統維護等通告信息，但是此文件的最大作用就是可以發布一些警告信息，當黑客登錄系統後，會發現這些警告信息，進而產生一些震懾作用。

看過國外的一個報導，黑客入侵了一個服務器，而這個服務器卻給出了歡迎登錄的信息，因此法院不做任何裁決。

遠程訪問和認證安全

①遠程登錄取消 telnet 而採用SSH 方式

telnet 是一種古老的遠程登錄認證服務，它在網絡上用明文傳送口令和數據，因此別有用心的人就會非常容易截獲這些口令和數據。

而且，telnet 服務程序的安全驗證方式也極其脆弱，攻擊者可以輕鬆將虛假信息傳送給服務器。

現在遠程登錄基本拋棄了telnet 這種方式，而取而代之的是通過SSH 服務遠程登錄服務器。

②合理使用 Shell 歷史命令記錄功能

在Linux 下可通過history 命令查看用戶所有的歷史操作記錄，同時shell 命令操作記錄默認保存在用戶目錄下的.bash_history 文件中。

通過這個文件可以查詢shell 命令的執行歷史，有助於運維人員進行系統審計和問題排查。

同時，在服務器遭受黑客攻擊後，也可以通過這個命令或文件查詢黑客登錄服務器所執行的歷史命令操作。

但是有時候黑客在入侵服務器後為了毀滅痕跡，可能會刪除.bash_history 文件，這就需要合理的保護或備份.bash_history 文件。

③啟用 Tcp_Wrappers防火牆

Tcp_Wrappers 是一個用來分析TCP/IP 封包的軟件，類似的IP 封包軟件還有iptables。

Linux 默認都安裝了Tcp_Wrappers。作為一個安全的系統，Linux 本身有兩層安全防火牆，通過IP 過濾機制的iptables 實現第一層防護。

iptables 防火牆通過直觀地監視系統的運行狀況，阻擋網絡中的一些惡意攻擊，保護整個系統正常運行，免遭攻擊和破壞。

如果通過了第一層防護，那麼下一層防護就是Tcp_Wrappers了。通過Tcp_Wrappers可以實現對系統中提供的某些服務的開放與關閉、允許和禁止，從而更有效地保證系統安全運行。

文件系統安全

①鎖定係統重要文件

系統運維人員有時候可能會遇到通過Root 用戶都不能修改或者刪除某個文件的情況，產生這種情況的大部分原因可能是這個文件被鎖定了。

在Linux 下鎖定文件的命令是Chattr，通過這個命令可以修改ext2、ext3、ext4 文件系統下文件屬性，但是這個命令必須有超級用戶Root來執行。和這個命令對應的命令是lsattr，這個命令用來查詢文件屬性。

對重要的文件進行加鎖，雖然能夠提高服務器的安全性，但是也會帶來一些不便。

例如：在軟件的安裝、升級時可能需要去掉有關目錄和文件的immutable屬性和append-only屬性，同時，對日誌文件設置了append-only屬性，可能會使日誌輪換（logrotate ）無法進行。

因此，在使用Chattr 命令前，需要結合服務器的應用環境來權衡是否需要設置immutable 屬性和append-only 屬性。

另外，雖然通過Chattr 命令修改文件屬性能夠提高文件系統的安全性，但是它並不適合所有的目錄。Chattr 命令不能保護/、/dev、/tmp、/var 等目錄。

根目錄不能有不可修改屬性，因為如果根目錄具有不可修改屬性，那麼系統根本無法工作：

- /dev 在啟動時，syslog 需要刪除並重新建立 /dev/log 套接字設備，如果設置了不可修改屬性，那麼可能出問題。
- /tmp 目錄會有很多應用程序和系統程序需要在這個目錄下建立臨時文件，也不能設置不可修改屬性。
- /var 是系統和程序的日誌目錄，如果設置為不可修改屬性，那麼系統寫日誌將無法進行，所以也不能通過Chattr 命令保護。

②文件權限檢查和修改

不正確的權限設置直接威脅著系統的安全，因此運維人員應該能及時發現這些不正確的權限設置，並立刻修正，防患於未然。下面列舉幾種查找系統不安全權限的方法。

查找系統中任何用戶都有寫權限的文件或目錄：

```
查找文件：find / -type f -perm -2 -o -perm -20 |xargs ls -al
查找目录：find / -type d -perm -2 -o -perm -20 |xargs ls -ld
```

查找系統中所有含“s”位的程序：

```
find / -type f -perm -4000 -o -perm -2000 -print | xargs ls -al
```

含有“s”位權限的程序對系統安全威脅很大，通過查找系統中所有具有“s”位權限的程序，可以把某些不必要的“s”位程序去掉，這樣可以防止用戶濫用權限或提升權限的可能性。

檢查系統中所有suid 及sgid 文件：

```
find / -user root -perm -2000 -print -exec md5sum {} ;
find / -user root -perm -4000 -print -exec md5sum {} ;
```

將檢查的結果保存到文件中，可在以後的系統檢查中作為參考。

檢查系統中沒有屬主的文件：

```
find / -nouser -o –nogroup
```

沒有屬主的孤兒文件比較危險，往往成為黑客利用的工具，因此找到這些文件後，要么刪除掉，要么修改文件的屬主，使其處於安全狀態。

③/tmp、/var/tmp、/dev/shm 安全設定

在Linux 系統中，主要有兩個目錄或分區用來存放臨時文件，分別是 /tmp 和 /var/tmp。

存儲臨時文件的目錄或分區有個共同點就是所有用戶可讀寫、可執行，這就為系統留下了安全隱患。

攻擊者可以將病毒或者木馬腳本放到臨時文件的目錄下進行信息收集或偽裝，嚴重影響服務器的安全。

此時，如果修改臨時目錄的讀寫執行權限，還有可能影響系統上應用程序的正常運行，因此，如果要兼顧兩者，就需要對這兩個目錄或分區進行特殊的設置。

/dev/shm 是Linux 下的一個共享內存設備，在Linux 啟動的時候系統默認會加載/dev/shm，被加載的/dev/shm 使用的是tmpfs 文件系統，而tmpfs 是一個內存文件系統，存儲到tmpfs 文件系統的數據會完全駐留在RAM 中。

這樣通過/dev/shm 就可以直接操控系統內存，這將非常危險，因此如何保證/dev/shm 安全也至關重要。

對於/tmp 的安全設置，需要看 /tmp 是一個獨立磁盤分區，還是一個根分區下的文件夾。

如果/tmp 是一個獨立的磁盤分區，那麼設置非常簡單，修改/etc/fstab 文件中 /tmp 分區對應的掛載屬性，加上nosuid、noexec、nodev 三個選項即可。

修改後的/tmp 分區掛載屬性類似如下：

```
LABEL=/tmp  /tmp ext3 rw,nosuid,noexec,nodev 0 0
```

其中，nosuid、noexec、nodev 選項，表示不允許任何suid 程序，並且在這個分區不能執行任何腳本等程序，並且不存在設備文件。

在掛載屬性設置完成後，重新掛載/tmp 分區，保證設置生效。

對於/var/tmp，如果是獨立分區，安裝 /tmp 的設置方法是修改/etc/fstab 文件即可。

如果是/var 分區下的一個目錄，那麼可以將 /var/tmp 目錄下所有數據移動到/tmp 分區下，然後在 /var 下做一個指向 /tmp 的軟連接即可。

也就是執行如下操作：

```
[root@server ~]# mv /var/tmp/* /tmp
[root@server ~]# ln -s  /tmp /var/tmp
```

如果/tmp 是根目錄下的一個目錄，那麼設置稍微複雜，可以通過創建一個loopback 文件系統來利用Linux 內核的loopback 特性將文件系統掛載到/tmp 下，然後在掛載時指定限制加載選項即可。

一個簡單的操作示例如下：

```
[root@server ~]# dd if=/dev/zero of=/dev/tmpfs bs=1M count=10000
[root@server ~]# mke2fs -j /dev/tmpfs
[root@server ~]# cp -av /tmp /tmp.old
[root@server ~]# mount -o loop,noexec,nosuid,rw /dev/tmpfs /tmp
[root@server ~]# chmod 1777 /tmp
[root@server ~]# mv -f /tmp.old/* /tmp/
[root@server ~]# rm -rf /tmp.old
```

最後，編輯/etc/fstab，添加如下內容，以便系統在啟動時自動加載loopback 文件系統：

```
/dev/tmpfs /tmp ext3 loop,nosuid,noexec,rw 0 0
```

Linux 後門入侵檢測工具

Rootkit 是Linux 平台下最常見的一種木馬後門工具，它主要通過替換系統文件來達到入侵和和隱蔽的目的，這種木馬比普通木馬後門更加危險和隱蔽，普通的檢測工具和檢查手段很難發現這種木馬。

Rootkit 攻擊能力極強，對系統的危害很大，它通過一套工具來建立後門和隱藏行跡，從而讓攻擊者保住權限，以使它在任何時候都可以使用Root 權限登錄到系統。

Rootkit 主要有兩種類型：文件級別和內核級別，下面分別進行簡單介紹。

文件級別的Rootkit 一般是通過程序漏洞或者係統漏洞進入系統後，通過修改系統的重要文件來達到隱藏自己的目的。

在系統遭受Rootkit 攻擊後，合法的文件被木馬程序替代，變成了外殼程序，而其內部是隱藏著的後門程序。

通常容易被Rootkit 替換的系統程序有login、ls、ps、ifconfig、du、find、netstat 等，其中login 程序是最經常被替換的。

因為當訪問Linux 時，無論是通過本地登錄還是遠程登錄，/bin/login 程序都會運行，系統將通過/bin/login 來收集並核對用戶的賬號和密碼。

而Rootkit 就是利用這個程序的特點，使用一個帶有根權限後門密碼的/bin/login 來替換系統的 /bin/login，這樣攻擊者通過輸入設定好的密碼就能輕鬆進入系統。

此時，即使系統管理員修改Root 密碼或者清除Root 密碼，攻擊者還是一樣能通過Root 用戶登錄系統。

攻擊者通常在進入Linux 系統後，會進行一系列的攻擊動作，最常見的是安裝嗅探器收集本機或者網絡中其他服務器的重要數據。

在默認情況下，Linux 中也有一些系統文件會監控這些工具動作，例如ifconfig 命令。

所以，攻擊者為了避免被發現，會想方設法替換其他系統文件，常見的就是ls、ps、ifconfig、du、find、netstat 等。

如果這些文件都被替換，那麼在系統層面就很難發現Rootkit 已經在系統中運行了。

這就是文件級別的Rootkit，對系統維護很大，目前最有效的防禦方法是定期對系統重要文件的完整性進行檢查。

如果發現文件被修改或者被替換，那麼很可能係統已經遭受了Rootkit 入侵。

檢查文件完整性的工具很多，常見的有Tripwire、 aide 等，可以通過這些工具定期檢查文件系統的完整性，以檢測系統是否被Rootkit 入侵。

內核級Rootkit 是比文件級Rootkit 更高級的一種入侵方式，它可以使攻擊者獲得對系統底層的完全控制權。

此時攻擊者可以修改系統內核，進而截獲運行程序向內核提交的命令，並將其重定向到入侵者所選擇的程序並運行此程序。

也就是說，當用戶要運行程序A 時，被入侵者修改過的內核會假裝執行A 程序，而實際上卻執行了程序B。

內核級Rootkit 主要依附在內核上，它並不對系統文件做任何修改，因此一般的檢測工具很難檢測到它的存在，這樣一旦系統內核被植入Rootkit，攻擊者就可以對系統為所欲為而不被發現。

目前對於內核級的Rootkit 還沒有很好的防禦工具，因此，做好系統安全防範就非常重要，將系統維持在最小權限內工作，只要攻擊者不能獲取Root 權限，就無法在內核中植入Rootkit 。

①Rootkit 後門檢測工具Chkrootkit

Chkrootkit 是一個Linux 系統下查找並檢測Rootkit 後門的工具，它的官方地址：

```
http://www.chkrootkit.org/
```

Chkrootkit 沒有包含在官方的CentOS 源中，因此要採取手動編譯的方法來安裝，不過這種安裝方法也更加安全。

Chkrootkit 的使用比較簡單，直接執行Chkrootkit 命令即可自動開始檢測系統。

下面是某個系統的檢測結果：

```
[root@server chkrootkit]# /usr/local/chkrootkit/chkrootkit
Checking `ifconfig'... INFECTED
Checking `ls'... INFECTED
Checking `login'... INFECTED
Checking `netstat'... INFECTED
Checking `ps'... INFECTED
Checking `top'... INFECTED
Checking `sshd'... not infected
Checking `syslogd'... not tested
```

從輸出可以看出，此系統的ifconfig、ls、login、netstat、ps 和top 命令已經被感染。

針對被感染Rootkit 的系統，最安全而有效的方法就是備份數據重新安裝系統。

Chkrootkit 在檢查Rootkit 的過程中使用了部分系統命令，因此，如果服務器被黑客入侵，那麼依賴的系統命令可能也已經被入侵者替換，此時Chkrootkit 的檢測結果將變得完全不可信。

為了避免Chkrootkit 的這個問題，可以在服務器對外開放前，事先將Chkrootkit 使用的系統命令進行備份，在需要的時候使用備份的原始系統命令讓Chkrootkit 對Rootkit 進行檢測。

②Rootkit 後門檢測工具 RKHunter

RKHunter 是一款專業的檢測系統是否感染Rootkit 的工具，它通過執行一系列的腳本來確認服務器是否已經感染Rootkit。

在官方的資料中，RKHunter 可以做的事情有：

MD5校验测试，检测文件是否有改动，比较系统命令的md5，从而判断系统命令是否被篡改
检测rootkit使用的二进制和系统工具文件
检测特洛伊木马程序的特征码
检测常用程序的文件属性是否异常
检测系统相关的测试
检测隐藏文件
检测可疑的核心模块LKM
检测系统已启动的监听端口

在Linux 終端使用RKHunter 來檢測，最大的好處在於每項的檢測結果都有不同的顏色顯示，如果是綠色的表示沒有問題，如果是紅色的，那就要引起關注了。

另外，在執行檢測的過程中，在每個部分檢測完成後，需要以Enter 鍵來繼續。

如果要讓程序自動運行，可以執行如下命令：

```
[root@server ~]# /usr/local/bin/rkhunter --check --skip-keypress
```

同時，如果想讓檢測程序每天定時運行，那麼可以在/etc/crontab 中加入如下內容：

```
30 09 * * * root /usr/local/bin/rkhunter --check --cronjob
```

這樣，RKHunter 檢測程序就會在每天的9:30 分運行一次。

服務器遭受攻擊後的處理過程

安全總是相對的，再安全的服務器也有可能遭受到攻擊。

作為一個安全運維人員，要把握的原則是：盡量做好系統安全防護，修復所有已知的危險行為，同時，在系統遭受攻擊後能夠迅速有效地處理攻擊行為，最大限度地降低攻擊對系統產生的影響。

①處理服務器遭受攻擊的一般思路

系統遭受攻擊並不可怕，可怕的是面對攻擊束手無策，下面就詳細介紹下在服務器遭受攻擊後的一般處理思路。

切斷網絡：所有的攻擊都來自於網絡，因此，在得知系統正遭受黑客的攻擊後，首先要做的就是斷開服務器的網絡連接，這樣除了能切斷攻擊源之外，也能保護服務器所在網絡的其他主機。

查找攻擊源：可以通過分析系統日誌或登錄日誌文件，查看可疑信息，同時也要查看系統都打開了哪些端口，運行哪些進程，並通過這些進程分析哪些是可疑的程序。

這個過程要根據經驗和綜合判斷能力進行追查和分析。下面會詳細介紹這個過程的處理思路。

分析入侵原因和途徑：既然系統遭到入侵，那麼原因是多方面的，可能是系統漏洞，也可能是程序漏洞。

一定要查清楚是哪個原因導致的，並且還要查清楚遭到攻擊的途徑，找到攻擊源，因為只有知道了遭受攻擊的原因和途徑，才能刪除攻擊源同時進行漏洞的修復。

備份用戶數據：在服務器遭受攻擊後，需要立刻備份服務器上的用戶數據，同時也要查看這些數據中是否隱藏著攻擊源。

如果攻擊源在用戶數據中，一定要徹底刪除，然後將用戶數據備份到一個安全的地方。

重新安裝系統：永遠不要認為自己能徹底清除攻擊源，因為沒有人能比黑客更了解攻擊程序。

在服務器遭到攻擊後，最安全也最簡單的方法就是重新安裝系統，因為大部分攻擊程序都會依附在系統文件或者內核中，所以重新安裝系統才能徹底清除攻擊源。

修復程序或系統漏洞：在發現系統漏洞或者應用程序漏洞後，首先要做的就是修復系統漏洞或者更改程序Bug，因為只有將程序的漏洞修復完畢才能正式在服務器上運行。

恢復數據和連接網絡：將備份的數據重新復製到新安裝的服務器上，然後開啟服務，最後將服務器開啟網絡連接，對外提供服務。

②檢查並鎖定可疑用戶

當發現服務器遭受攻擊後，首先要切斷網絡連接，但是在有些情況下，比如無法馬上切斷網絡連接時，就必須登錄系統查看是否有可疑用戶。

如果有可疑用戶登錄了系統，那麼需要馬上將這個用戶鎖定，然後中斷此用戶的遠程連接。

③查看系統日誌

查看系統日誌是查找攻擊源最好的方法，可查的系統日誌有 /var/log/messages、/var/log/secure 等。

這兩個日誌文件可以記錄軟件的運行狀態以及遠程用戶的登錄狀態，還可以查看每個用戶目錄下的.bash_history 文件。

特別是 /root 目錄下的.bash_history 文件，這個文件中記錄著用戶執行的所有歷史命令。

④檢查並關閉系統可疑進程

檢查可疑進程的命令很多，例如ps、top 等，但是有時候只知道進程的名稱無法得知路徑，此時可以通過如下命令查看。

首先通過pidof 命令可以查找正在運行的進程PID，例如要查找sshd 進程的PID。

執行如下命令：

```
[root@server ~]# pidof sshd
13276 12942 4284
```

然後進入內存目錄，查看對應PID 目錄下exe 文件的信息：

```
[root@server ~]# ls -al /proc/13276/exe
lrwxrwxrwx 1 root root 0 Oct  4 22:09 /proc/13276/exe -> /usr/sbin/sshd
```

這樣就找到了進程對應的完整執行路徑。如果還要查看文件的句柄，可以查看如下目錄：

```
[root@server ~]# ls -al /proc/13276/fd
```

通過這種方式基本可以找到任何進程的完整執行信息。

⑤檢查文件系統的完好性

檢查文件屬性是否發生變化是驗證文件系統完好性最簡單、最直接的方法，例如可以檢查被入侵服務器上/bin/ls 文件的大小是否與正常系統上此文件的大小相同，以驗證文件是否被替換，但是這種方法比較低級。

此時可以藉助於Linux 下rpm 這個工具來完成驗證，操作如下：

```
[root@server ~]# rpm -Va
....L...   c /etc/pam.d/system-auth
S.5.....   c /etc/security/limits.conf
S.5....T   c /etc/sysctl.conf
S.5....T     /etc/sgml/docbook-simple.cat
S.5....T   c /etc/login.defs
S.5.....   c /etc/openldap/ldap.conf
S.5....T   c /etc/sudoers
```

⑥重新安裝系統恢復數據

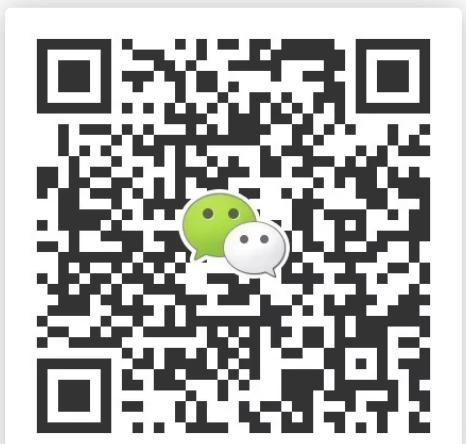
很多情況下，被攻擊過的系統已經不再可信任，因此，最好的方法是將服務器上面數據進行備份，然後重新安裝系統，最後再恢復數據即可。

數據恢復完成，馬上對系統做上面介紹的安全加固策略，保證系統安全。

END

來和小伙伴們一起向上生長呀！

掃描下方二維碼，添加小詹微信，可領取千元大禮包併申請加入Python學習交流群，群內僅供學術交流，日常互動，如果是想發推文、廣告、砍價小程序的敬請繞道！一定記得備註「交流學習」，我會盡快通過好友申請哦！



長按識別，添加微信

（添加人數較多，請耐心等待）

長按識別，關注小詹

（掃碼回复1024 領取程序員大禮包）

閱讀原文