

# 目錄

## 第 1 篇 網路伺服器主機安全防護入門

### Ch1 安全架站規劃與防護基礎導論

1.1 建立你的安全性觀念 .....	1-2
1.1.1 了解基本安全性概念 .....	1-3
1.1.2 執行通訊分析 .....	1-5
1.1.3 學習分析保護需求 .....	1-7
1.2 常見的攻擊類型 .....	1-8
1.2.1 存取式的攻擊 .....	1-9
1.2.2 竄改式的攻擊 .....	1-12
1.2.3 阻斷服務式的攻擊 .....	1-13
1.3 常見的安全威脅與駭客入侵手法 .....	1-15
1.3.1 網路安全的威脅來源 .....	1-16
1.3.2 常見的駭客技術 .....	1-17
1.3.3 共享與密碼問題 .....	1-19
1.3.4 社交工程 .....	1-25
1.3.5 程式設計的缺失與緩衝區溢位 .....	1-25
1.3.6 病毒、蠕蟲與木馬程式 .....	1-25
1.3.7 怪客偵測與基本防衛技巧 .....	1-26
1.4 架設伺服器前的基礎規劃 .....	1-29
1.4.1 伺服器主機的類型挑選 .....	1-29
1.4.2 Linux 發行套件的選擇 .....	1-31
1.4.3 災難復原的方案設計 .....	1-32

## Ch2 你的主機安全嗎

<b>2.1</b> 主機實體存取的安全配置.....	2-2
<b>2.1.1</b> 你的主機存放的地點安全嗎？.....	2-2
<b>2.1.2</b> BIOS 的基本防護.....	2-5
<b>2.1.3</b> 啟動載入器的安全配置.....	2-8
<b>2.2</b> 檔案系統的安全性配置.....	2-14
<b>2.2.1</b> 磁碟分割區的重要性.....	2-14
<b>2.2.2</b> 磁碟分割區的掛載.....	2-17
<b>2.2.3</b> 使用者的存取權限控制 - 1.....	2-20
<b>2.2.4</b> 使用者的存取權限控制 - 2.....	2-24
<b>2.3</b> 套件與服務的安全性配置.....	2-34
<b>2.3.1</b> 關閉不需要使用的服務與移除套件.....	2-34
<b>2.3.2</b> 訂閱安全性更新與定期修補漏洞.....	2-38
<b>2.4</b> 善用記錄檔案與分析潛在性問題.....	2-43
<b>2.4.1</b> 記錄檔的使用.....	2-43
<b>2.4.2</b> 統計系統執行狀態.....	2-46
<b>2.4.3</b> 自動監測程式的使用.....	2-51

## Ch3 認識加密演算法與憑證的使用

<b>3.1</b> 加密與解密.....	3-2
<b>3.1.1</b> 常見加解密機制.....	3-3
<b>3.1.2</b> 雜湊演算法與數位簽章.....	3-8
<b>3.1.3</b> 使用者密碼的基本防護.....	3-11
<b>3.2</b> 憑證的使用.....	3-15
<b>3.2.1</b> 建立一個最高層的憑證管理中心 (Root CA).....	3-18
<b>3.2.2</b> 透過憑證管理中心來簽發證書.....	3-22
<b>3.2.3</b> 建立一個憑證廢止清單 (Certificate Revocation List).....	3-26
<b>3.3</b> 保護 Linux 作業系統中的檔案與分割區.....	3-26
<b>3.3.1</b> 分割區的加密操作.....	3-27
<b>3.3.2</b> 磁碟容器檔案的加密操作.....	3-31
<b>3.4</b> 於 Linux 間的安全性連線與資料傳輸防護.....	3-37
<b>3.4.1</b> 透過 SSH 傳輸協定來進行遠端連線與資料的傳遞.....	3-39
<b>3.4.2</b> 透過金鑰來建立主從伺服器間的永久信任關係.....	3-42

## Ch4 網路服務的基本安全配置

4.1 認識 Linux 服務.....	4-2
4.1.1 獨立式服務的管理 .....	4-3
4.1.2 短暫式服務的管理 .....	4-7
4.1.3 查詢目前系統中所執行的服務.....	4-11
4.2 防護你的短暫式服務.....	4-16
4.2.1 控制短暫式服務的資源.....	4-19
4.2.2 蜂蜜罐（Honey Pots）的使用.....	4-21
4.3 TCP Wrappers 機制的使用 .....	4-22
4.3.1 透過 TCP Wrappers 機制建置一個安全服務.....	4-23
4.3.2 TCP Wrappers 的其他應用 .....	4-27
4.4 Stunnel 的使用.....	4-28
4.4.1 透過 Stunnel 的網路服務應用 .....	4-30

## 第 2 篇 實戰 IPTABLES 防火牆建置工程

### Ch5 Netfilter 架構與 IPTABLES 防火牆管理工具介紹

5.1 防火牆基本概念與功能 .....	5-2
5.1.1 如何辨別允許與不允許的存取.....	5-3
5.2 常見防火牆組態架構 .....	5-12
5.2.1 封包過濾 .....	5-13
5.2.2 應用程式等級閘道器（Application Level Gateway, ALG） .....	5-14
5.2.3 電路層閘道式防火牆（Circuit-Level Gateway） .....	5-15
5.2.4 DMZ .....	5-17
5.3 Netfilter 與 IPTABLES 基本概念 .....	5-19
5.3.1 表與鏈的使用 .....	5-21
5.3.2 IPTABLES 工具基本語法介紹 .....	5-30
5.3.3 規則的使用.....	5-35

### Ch6 實戰防火牆建置與安裝

6.1 防火牆建置前的初始化作業 .....	6-2
6.1.1 相關核心監控模組的啟用 .....	6-3
6.1.2 IPTABLES 腳本程式的初始步驟 .....	6-14
6.1.3 清除任何已經存在的規則 .....	6-16

<b>6.1.4</b> 重新定義預設規則.....	6-17
<b>6.2</b> 基本 TCP 封包過濾實戰.....	6-19
<b>6.2.1</b> 避免隱匿掃描的最佳方式：TCP 旗標的過濾.....	6-20
<b>6.2.2</b> 阻絕惡意的 Spoofing 的動作.....	6-26
<b>6.3</b> 保護本機所提供的服務.....	6-30
<b>6.3.1</b> 常見的本機服務使用的無特權埠號的防護.....	6-31
<b>6.3.2</b> 針對基本網路服務的防護.....	6-33
<b>6.3.3</b> 常見 TCP/UDP 網路服務的防護.....	6-35
<b>6.3.4</b> ICMP 封包的控管.....	6-48
<b>6.4</b> 封包的處理，應該將封包往那裡放？.....	6-52
<b>6.5</b> 安裝設計好的防火牆腳本程式.....	6-53

## Ch7 實戰 NAT 技術

<b>7.1</b> NAT 概論.....	7-2
<b>7.1.1</b> IP 網段的區分與虛擬 IP (Private IP) 位址.....	7-3
<b>7.1.2</b> NAT 的分類.....	7-7
<b>7.2</b> IPTABLES 中的 NAT 語法.....	7-9
<b>7.2.1</b> IPTABLES 中的 NAT 相關語法 - SNAT.....	7-10
<b>7.2.2</b> IPTABLES 中的 NAT 相關語法 - DNAT/NAPT.....	7-16
<b>7.3</b> 於 IPTABLES 中實踐 NAT 技術範例.....	7-17
<b>7.3.1</b> 私人區域網路建置範例.....	7-18

## Ch8 實戰應用程式等級閘道器的應用

<b>8.1</b> 應用程式等級閘道器概論.....	8-2
<b>8.2</b> 何謂 Proxy 伺服器.....	8-3
<b>8.2.1</b> 常見的 Proxy 伺服器分類.....	8-4
<b>8.2.2</b> Squid 的安裝與配置.....	8-6
<b>8.3</b> Squid 的組態實戰.....	8-8
<b>8.3.1</b> 針對網頁瀏覽器的存取控制.....	8-20
<b>8.3.2</b> PAC 檔案的使用.....	8-25
<b>8.4</b> Squid 進階組態與應用.....	8-30
<b>8.4.1</b> Proxy 驗證的使用.....	8-30
<b>8.4.2</b> Squid 日誌分析.....	8-35

## 第 3 篇 網路安全攻防實戰

### Ch9 入侵偵測與回應

<b>9.1</b> 何謂入侵偵測 .....	9-2
<b>9.1.1</b> 入侵偵測系統的種類 .....	9-3
<b>9.1.2</b> 蜂蜜罐入侵偵測防護系統架構.....	9-7
<b>9.2</b> 入侵偵測的執行時機? .....	9-10
<b>9.2.1</b> 當你的主機已經遭受到危害時，會有甚麼徵狀呢? .....	9-11
<b>9.2.2</b> 主機被入侵了，你能做什麼呢? .....	9-15
<b>9.3</b> Tripwire 實戰.....	9-17
<b>9.3.1</b> 取得、編譯與安裝新版的 Tripwire.....	9-19
<b>9.3.2</b> Tripwire 基本組態方式與組態檔說明 .....	9-25
<b>9.3.3</b> 學習原則的管理與編輯.....	9-28
<b>9.3.4</b> 安裝建立好的原則檔案與執行配置好的 Tripwire .....	9-33
<b>9.3.5</b> 更改/更新原則檔案與自動化執行 Tripwire .....	9-37
<b>9.4</b> 監控主機與相關服務的狀態 – Nagios 實戰 .....	9-39
<b>9.4.1</b> 於 Linux 主機中安裝 Nagios .....	9-40
<b>9.4.2</b> Nagios 的基本運行架構 .....	9-48
<b>9.4.3</b> Nagios 的組態檔案架構 .....	9-52
<b>9.4.4</b> 進階認識 Nagios 的主要組態檔案架構.....	9-59
<b>9.4.5</b> Nagios 服務所提供的 CGI 程式應用 .....	9-79
<b>9.4.6</b> 撰寫 Nagios 監控主機與服務的定義檔案 .....	9-90

### Ch10 常見網路監控與攻擊偵測工具介紹

<b>10.1</b> 防護入門：從網路監控開始著手.....	10-2
<b>10.1.1</b> NTOP 工具的使用.....	10-2
<b>10.1.2</b> TCPDump 嗅探與分析你網路中的封包.....	10-11
<b>10.1.3</b> 監聽網路上的 ARP 紀錄 – 使用 ARPwatch.....	10-17
<b>10.2</b> Snort 超強網路入侵偵測與防禦軟體 (Part I) .....	10-24
<b>10.3</b> Snort 超強網路入侵偵測與防禦軟體 (Part II) .....	10-32
<b>10.4</b> Snort 超強網路入侵偵測與防禦軟體 (Part III) .....	10-44
《範例一：透過 reference 規則選項來引入其他外部攻擊識別系統》 .....	10-50
《範例二：透過 classtype 規則選項來定義類型項目》 .....	10-53

《範例三：透過 fragbits 規則選項來判斷 IP 封包表頭欄位資訊》 .....	10-62
《範例四：透過 react 規則選項來進行惡意存取的阻擋》 .....	10-65
<b>10.5 Snort 超強網路入侵偵測與防禦軟體 (Part IV)</b> .....	10-66
<b>10.5.1 BASE 的安裝與設定</b> .....	10-66
<b>10.5.2 透過網頁來檢視相關警報訊息</b> .....	10-70

## Ch11 實戰 Apparmor

<b>11.1 何謂 AppArmor?</b> .....	11-2
<b>11.1.1 取得與安裝 AppArmor 程式</b> .....	11-3
<b>11.1.2 參與獲得更多 AppArmor 的支援</b> .....	11-6
<b>11.2 第一次接觸 AppArmor</b> .....	11-7
<b>11.2.1 瞭解 AppArmor 運作模式</b> .....	11-8
<b>11.2.2 瞭解 AppArmor 組態檔案架構與語法</b> .....	11-11
<b>11.3 建立與管理 AppArmor 組態檔案</b> .....	11-18
<b>11.3.1 透過 YaST2 控制中心來建立 AppArmor 組態檔案</b> .....	11-18
<b>11.3.2 透過指令來建立 AppArmor 組態檔案</b> .....	11-27
<b>11.3.3 管理 AppArmor 組態檔案</b> .....	11-35
<b>11.3.4 AppArmor 運作監控與事件回報</b> .....	11-40

## Ch12 虛擬私有網路 VPN 的運用

<b>12.1 虛擬私有網路概論</b> .....	12-2
<b>12.1.1 虛擬私有網路組成元件</b> .....	12-3
<b>12.1.2 用戶型與站台型虛擬私有網路</b> .....	12-5
<b>12.2 虛擬私有網路標準技術</b> .....	12-7
<b>12.2.1 IPSec</b> .....	12-7
<b>12.2.2 PPTP</b> .....	12-11
<b>12.2.3 SSL VPN</b> .....	12-12
<b>12.2.4 L2F 與 L2TP</b> .....	12-13
<b>12.2.5 MPLS</b> .....	12-13
<b>12.3 透過 OpenVPN 來建置企業用 VPN 環境</b> .....	12-14
<b>12.3.1 安裝與部屬 OpenVPN 基本環境</b> .....	12-14
<b>12.3.2 建立 OpenVPN 伺服器與用戶端所需憑證</b> .....	12-17
<b>12.3.3 組態 OpenVPN 環境設定</b> .....	12-22
<b>12.3.4 啟動與測試 OpenVPN 服務</b> .....	12-35

## 第 4 篇 Linux 基礎伺服器建置與安全防護

### Ch13 網域名稱伺服器規劃與建置

<b>13.1</b> 網域名稱系統基本概論.....	13-2
<b>13.1.1</b> 何謂網域？.....	13-4
<b>13.1.2</b> 網域名稱伺服器運作方式.....	13-7
<b>13.1.3</b> 常見網域名稱伺服器類型.....	13-10
<b>13.2</b> 快取型網域名稱伺服器組態.....	13-10
<b>13.2.1</b> 組態快取型網域名稱伺服器的方式.....	13-12
<b>13.3</b> 主從關係架構的網域名稱伺服器組態.....	13-14
<b>13.3.1</b> 基本架構與所需套件.....	13-14
<b>13.3.2</b> 主要網域名稱伺服器組態.....	13-15
<b>13.3.3</b> 驗證主要網域名稱伺服器組態.....	13-19
<b>13.3.4</b> 從屬網域名稱伺服器組態.....	13-20
<b>13.3.5</b> 驗證從屬網域名稱伺服器組態.....	13-21
<b>13.4</b> 網域名稱伺服器安全配置.....	13-25

### Ch14 郵件伺服器規劃與建置

<b>14.1</b> 何謂電子郵件.....	14-2
<b>14.1.1</b> 電子郵件的運作方式.....	14-2
<b>14.1.2</b> 常見電子郵件通訊協定介紹.....	14-4
<b>14.2</b> 透過 Postfix 來組態郵件伺服器.....	14-6
<b>14.2.1</b> 組態前的基本作業.....	14-6
<b>14.2.2</b> Postfix 郵件伺服器組態檔案 master.cf 解析.....	14-8
<b>14.2.3</b> SuSEConfig 中的 Postfix 組態檔案解析.....	14-9
<b>14.2.4</b> Postfix 郵件伺服器組態檔案 main.cf 解析.....	14-15
<b>14.2.5</b> 組態一個基本 Postfix 郵件伺服器範例.....	14-22
<b>14.2.6</b> 驗證基本 Postfix 郵件伺服器的運作.....	14-24
<b>14.2.7</b> 組態具備 SMTP-AUTH 功能的 Postfix 郵件伺服器範例.....	14-28
<b>14.2.8</b> 驗證具備 SMTP 驗證功能的 Postfix 郵件伺服器運作.....	14-30
<b>14.3</b> Postfix 郵件伺服器安全防護配置.....	14-31
<b>14.3.1</b> Postfix 郵件伺服器查詢表單的使用.....	14-31
<b>14.3.2</b> 透過過濾條件讓 Postfix 郵件伺服器更加安全.....	14-35

<b>14.3.3</b> 搭配防毒軟體建構具有防毒功能的 Postfix 郵件伺服器.....	14-39
<b>14.4</b> POP3 伺服器組態.....	14-44
<b>14.5</b> 郵件伺服器的防火牆規則配置.....	14-46

## Ch15 網頁伺服器規劃與建置

<b>15.1</b> 全球資訊網概論.....	15-2
<b>15.1.1</b> URI 與 URL.....	15-2
<b>15.1.2</b> WWW 通訊協定.....	15-3
<b>15.2</b> APACHE 網頁伺服器的組態.....	15-4
<b>15.2.1</b> 所需要的套件.....	15-5
<b>15.2.2</b> 完成你的第一部網頁伺服器.....	15-9
<b>15.2.3</b> APACHE 網頁伺服器與 PHP 的第一次親密接觸.....	15-13
<b>15.3</b> APACHE 虛擬網頁伺服器.....	15-15
<b>15.3.1</b> Name-Based 虛擬網頁伺服器.....	15-16
<b>15.3.2</b> IP-Based 虛擬網頁伺服器.....	15-19
<b>15.4</b> APACHE 網頁伺服器安全存取組態.....	15-21
<b>15.5</b> APACHE 網頁伺服器防火牆規則配置.....	15-26

## Ch16 檔案傳輸伺服器 FTP 規劃與建置

<b>16.1</b> 規劃與架設 FTP 伺服器.....	16-2
<b>16.1.1</b> PureFTP 伺服器套件安裝.....	16-3
<b>16.1.2</b> Pure-FTPd 基本環境配置.....	16-5
<b>16.2</b> Pure-FTPd 伺服器配置範例.....	16-10
<b>16.2.1</b> 設定一個匿名者登入的 PureFTP 伺服器.....	16-10
<b>16.2.2</b> 設定一個具備登入驗證的 Pure-FTPd 伺服器.....	16-12
<b>16.2.3</b> 設定一個使用虛擬使用者登入驗證的 PureFTP 伺服器.....	16-14
<b>16.2.4</b> 設定虛擬 Pure-FTPd 伺服器.....	16-16
<b>16.3</b> Pure-FTPd 伺服器的安全配置.....	16-18

## 附錄 A 建置與規畫 ulogd 服務