# FreeBSD 試題(筆試與實作題)

姓名 :

簡答題:

今有一部伺服器,有 200G 的硬碟兩顆,網路卡一片,要提供本校 XXX 系使用者做為系所網站(web)及系所成員電子郵件(email)使用,使用的作業系統為 FreeBSD 11.0-RELEASE,試回答下列子問題:

A1. 簡述整個安裝的流程

A2. 如何規劃磁碟並簡述這樣劃分的理由.

A3. 簡述系統安裝完成後,要正式上線前需要向電算中心申請的事項

A4. 簡述如何提升系統安全性避免被駭客攻陷

A5. 簡述升級本機作業系統至 FreeBSD 11.0-RELEASE 的最新版本 FreeBSD 11.0-RELEASE-p15 的程序

A6. 假設使用的程式所使用的檔案皆為系統預設路徑且系統有開啓內建的 sshd,請詳細列出從紀錄中抓出從 1.2.3.4 來的嘗試登入紀錄並輸出到/tmp/XXX 這個檔案的的命令.

(僅選擇 email 伺服器管理的可以跳過 B 系列子題)

B1. 簡述 web 端的安裝與設定部份

B2. 簡述如被駭客攻擊本機端 web 服務的處置對應方式

B3. 簡述如何得知 web 系統程式應該升級及升級所使用的 web 系統程式的方式

B4. 假設使用的 web 端程式所使用的檔案皆為系統預設路徑,請詳細列出從紀錄中抓出從 1.2.3.4 來的網頁存取紀錄並輸出到/tmp/XXX 這個檔案的的命令.

B5. 今有本校某單位網站之網頁存取記錄如下, 請判斷哪些 ip 的存取可能是攻擊行為及理由.(本小題為筆試題)

```
1393203790.743      0 109.236.84.144 TCP_MISS/404 575 GET http://chekfast.zennolab.com/proxy.php - FIRSTUP_PARENT/127.0.0.1 text/html
1393203809.093      1 173.208.194.114 TCP_MISS/404 587 POST http://fdc.xchecker.net/proxy2013/http/engine7.php - FIRSTUP_PARENT/127.0.0.1 text/html
1393203818.275     20 159.226.199.209 TCP_MISS/200 120653 GET http://www.sci-hub.org/ - FIRSTUP_PARENT/127.0.0.1 text/html
1393203829.444     20 182.118.28.150 TCP_MISS/200 120653 GET http://moffice.ccu.edu.tw/index.php - FIRSTUP_PARENT/127.0.0.1 text/html
1393203971.108     17 66.249.77.86 TCP_MISS/200 79023 GET http://webmail.ccu.edu.tw/ - FIRSTUP_PARENT/127.0.0.1 text/html
1393204044.584      0 222.168.165.23 TCP_MISS/404 591 GET http://pubs.acs.org/doi/pdf/10.1021/jf049083j - FIRSTUP_PARENT/127.0.0.1 text/html
1393204052.946     22 66.249.77.86 TCP_MISS/200 80402 GET http://webmail.ccu.edu.tw/ - FIRSTUP_PARENT/127.0.0.1 text/html
1393204054.773      5 66.249.74.18 TCP_MISS/200 74630 GET http://moffice.ccu.edu.tw/ - FIRSTUP_PARENT/127.0.0.1 text/html
1393204064.482      0 111.243.249.187 TCP_MISS/404 572 GET http://www.google.com/search?tbo=d&source=hp&num=1&btnG=Search&q=niceman - FIRSTUP_PARENT/127.0.0.1 text/html
```

(僅選擇 web 伺服器管理的可以跳過 C 系列子題)

C1. 簡述 mail 端的安裝與設定部份

C2. 簡述如被駭客攻擊本機端 mail 服務的處置對應方式

C3. 簡述如何得知 email 系統程式應該升級及升級所使用的 email 系統程式的方式

C4. 假設使用的 email 端的程式所使用的檔案皆為系統預設路徑,請詳細列出從紀錄中抓出從 ip 8.8.8.8 來的紀錄並輸出到/tmp/XXX 這個檔案的命令.

C5. 今有某郵件的表頭, 請說明本郵件在郵件伺服器中的流向(於什麼時間點經過哪些郵件伺服器).(本小題為筆試題)

```
Return-Path: <dduu@bfz.amtbotanicals.com>
Received: from mail02.ccu.edu.tw (mail02.ccu.edu.tw [140.123.5.112])
          by incoming.ccu.edu.tw (8.14.4/8.14.3) with ESMTP id s1LKTJeP080345
          for <consults@incoming.ccu.edu.tw>; Sat, 22 Feb 2014 04:29:20 +0800 (CST)
          (envelope-from dduu@bfz.amtbotanicals.com)
Received: from localhost (localhost [127.0.0.1])
          by mail02.ccu.edu.tw (8.14.1/8.14.1) with ESMTP id s1LKTIpJ099513
```

for <consults@ccunix.ccu.edu.tw>; Sat, 22 Feb 2014 04:29:18 +0800 (CST)
(envelope-from dduu@bfz.amtbotanicals.com)
X-Spam-Score: 5.387
X-Spam-Level: *****
X-Spam-Status: No, score=5.387 tagged_above=2 required=6.31
tests=[BAYES_00=-2.599, FORGED_MUA_OUTLOOK=4.056, HTML_MESSAGE=0.001,
MIME_BASE64_NO_NAME=0.224, RCVD_IN_SORBS_DUL=2.046,
ROUND_THE_WORLD_LOCAL=1.659]
Received: from mail02.ccu.edu.tw ([127.0.0.1])
by localhost (mail02.ccu.edu.tw [127.0.0.1]) (amavisd-new, port 10026)
with LMTP id AquCYVMpbaMn for <consults@ccunix.ccu.edu.tw>;
Sat, 22 Feb 2014 04:29:11 +0800 (CST)
Received: from mail04.ccu.edu.tw (nopam.ccu.edu.tw [140.123.5.120])
by mail02.ccu.edu.tw (8.14.1/8.14.1) with ESMTP id s1LKTAqS099506
for <consults@ccunix.ccu.edu.tw>; Sat, 22 Feb 2014 04:29:11 +0800 (CST)
(envelope-from dduu@bfz.amtbotanicals.com)
Received: from mail04.ccu.edu.tw (nopam.ccu.edu.tw [140.123.5.120])
by nopam.ccu.edu.tw (NOPAM 20100526(G2)) with ESMTP id 147EB2C4
Sat Feb 22 04:29:08 2014
(envelope-from <dduu@bfz.amtbotanicals.com>)
Received: from bfz.amtbotanicals.com ([121.15.122.6])
by mail04.ccu.edu.tw (8.14.1/8.14.1) with ESMTP id s1LKT3oI032431
for <consults@ccunix.ccu.edu.tw>; Sat, 22 Feb 2014 04:29:04 +0800 (CST)
(envelope-from dduu@bfz.amtbotanicals.com)
Received: from xjrkwa (unknown [187.152.227.178])
by amtbotanicals.com with SMTP id wZw75XHYgP20F0So.1
for <consults@ccunix.ccu.edu.tw>; Sat, 22 Feb 2014 04:29:24 +0800
Message-ID: <C2DF753017474B8018776BAF7AC76FB1@xjrkwa>
From: =?utf-8?B?5YWx5a2Y5Lqh?= <dduu@bfz.amtbotanicals.com>
To: <consults@ccunix.ccu.edu.tw>
Subject: =?utf-8?B?5Y+Y6LW36JCn5aKZIA==?=
Date: Sat, 22 Feb 2014 04:29:18 +0800
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0E11_0164CB8D.1DB99040"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5512
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5512
X-NOPAM-Status: type=0; s=120, (GSD sync, gs=0, s=120, p=11)
X-NOPAM-DIAG: 121.15.122.6, 163.com, BL3, 120