

運用: 毎日、管理者アカウントに意味不明なメールがきます。

サーバシステムでは、管理用ツールとして毎日自動実行されるジョブが初期設定されており、実行結果を管理者(root)宛てに送信します。

一通目

From: root@ns.お客様ドメイン (Cron Daemon)
Date: Tue, 14 Dec 2004 04:04:24 +0900
To: root@ns.お客様ドメイン名
Subject: Cron run-parts /etc/cron.daily

本文先頭行が /etc/cron.daily/00webalizer: となっているメールは、Cron により毎日実行される cron.daily に登録された Webalizer によるログ解析プロセスの出力結果となります。

/etc/cron.daily/00webalizer:

```
Error: Skipping oversized log record
Error: Skipping oversized log record
Error: Skipping oversized log record
Error: Skipping oversized log record
Error: Skipping oversized log record
Error: Skipping oversized log record
Error: Skipping oversized log record
Warning: Truncating oversized referrer field [8375]
Warning: Truncating oversized referrer field [11595]
Error: Skipping oversized log record
Error: Skipping oversized log record
Warning: Truncating oversized referrer field [20348]
```

上記、Skipping oversized log record や、oversized referrer field は、アクセスログ情報レコードが下記のようなレコードとなっている場合に発生いたします。

```
210.143.96.70 - - [14/Dec/2004:10:44:59 +0900] "SEARCH /¥¥x90¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x
02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥x
b1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x
02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥x
b1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x
02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥x
b1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x
02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x02¥¥x
b1¥¥x02¥¥xb1¥¥x02¥¥xb1¥¥x
--- (省略) ---
```

このようなアクセスログは、Windows 系OS の WebDAV の脆弱性を付いたワームによるアクセスとなります。

運用: 毎日、管理者アカウントに意味不明なメールがきます。

----- httpd End -----

上記、httpd Begin ~ httpd End までは、httpd セクションとなり、Apache Webサーバによるアクセスログ情報より、不正なアクセスログの情報のみピックアップしております。

前述の Webalizer アクセス解析でも不正とされた Windows 系OS の WebDAV の脆弱性を付いたワームによるアクセスが抜粋されております。

----- pam_unix Begin -----

dovecot:

Unknown Entries:

authentication failure; logname= uid=0 euid=0 tty= ruser= rhost=
user=mizuno-katumi: 25 Time(s)

authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= : 7
Time(s)

check pass; user unknown: 7 Time(s)

su:

Sessions Opened:

(uid=0) - cyrus: 1 Time(s)

(uid=0) - news: 1 Time(s)

----- pam_unix End -----

pam_unix セクションでは、認証に関連する 1日分のログ情報のサマリーを記録しております。

各アカウント名、パスワードによる認証と結果を確認可能です。

----- Connections (secure-log) Begin

Connections:

Service ftp:

210.143.106.4: 2 Time(s)

210.143.96.70: 1 Time(s)

Unmatched Entries

dovecot-auth: pam_succeed_if: requirement "uid 100" not met by user
"test"

dovecot-auth: pam_succeed_if: requirement "uid 100" not met by user
"test3"

運用: 毎日、管理者アカウントに意味不明なメールがきます。

(省略)

```
----- Connections (secure-log) End
-----
```

Connections セクションでは、外部からサーバへの接続に関するログ情報を表示します。

接続したプロトコル(ftp等)と、接続元IPアドレス情報等の 1日分の情報がこちらで確認可能となります。

****Unmatched Entries**** では、LogWatch により用意されたエラー情報のパターンにマッチしなかった情報が出力されます。

メール受信用サーバ dovecot では、認証毎に requirement "uid 100" のログ情報が記録される現象があり、****Unmatched Entries**** へと分類されておりますが、特に問題が発生している訳ではございません。

```
----- sendmail Begin -----
```

Bytes Transferred: 96428995

Messages Sent: 187

Total recipients: 208

Unknown local users:

Total: 91

sendmail セクションは複数のブロックに分かれており、上記は記録された 1日分のサマリー情報となります。

上記の例では、メール配送による転送量が 96428995 byte あり、送られたメールが 187 通、受信したメールが 208 通となっております。

また、ローカルユーザーへの Unknown users が 91 件発生しております。

Top relays (recipients/connections - min 10 rcpts, max 50 lines):

35/35: ghost.prox.ne.jp [210.143.96.70]

34/25: www.ixent.ne.jp [210.143.106.5]

上記の例では、メールをリレー(送信)した元クライアントのIPアドレスを、受信者数/接続数の表示で多い順に一部抜粋してます。

運用: 毎日、管理者アカウントに意味不明なメールがきます。

Relaying denied:

From ns.prox.ne.jp [210.143.96.65] to sunhaorong@nbip.net.cn: 2 Time(s)
From [211.158.33.193] to doreen@cta.cq.cn: 1 Time(s)
From [221.140.55.94] to smtphunter77@daum.net: 1 Time(s)
From [61.80.47.78] to talent311@daum.net: 1 Time(s)
From p3009-ipad03sasajima.aichi.ocn.ne.jp [61.199.117.9] to sunhaorong@nbip.net.cn: 1 Time(s)

Total: 5

Relaying denied: はリレー(送信)を拒否したログの抜粋となり、5件発生しております。

E-server サービスでは、POP before SMTP のチェックが初期設定で行われており、受信認証に成功していない不正リレーは拒否されます。

Client quit before communicating:

210.143.96.66: 2 Time(s)
210.143.96.70 : 3 Time(s)

Client quit before communicating: は、コネクションを接続するも何もなくそのまま切断した時の、接続元IPアドレスの情報となります。

Authentication warnings:

[210.143.96.70] didn't use HELO protocol: 1 Time(s)

Authentication warnings: は、認証警告情報となります。

上記の例では、IPアドレスが 210.143.96.70 からの接続時に HELO コマンドが無かった事を示しております。

Unknown hosts:

prox.cp.jp: 1 Time(s)
prox.so.jp: 1 Time(s)

Total: 2

Unknown hosts: は、ホスト名不明による配送エラーの発生となります。
上記の例では 2件発生しており、ドメイン名間違いのようです。

****Unmatched Entries****

Fixed MIME Content-type header field (possible attack): 1 Time(s)

運用: 毎日、管理者アカウントに意味不明なメールがきます。

****Unmatched Entries**** では、LogWatch により用意されたエラー情報のパターンにマッチしなかった情報が出力されます。

Summary:

Total Mail Rejected: 103

----- sendmail End -----

最後はサマリー情報となり、上記例では、メールを拒否した件数が 103 件となります。

----- SSHD Begin -----

Illegal users from these:

andrew/none from ::ffff:210.143.96.70 1 Time(s)

angel/none from ::ffff:210.143.96.65 1 Time(s)

ben/none from ::ffff:210.143.96.65 1 Time(s)

betty/none from ::ffff:210.143.96.65: 1 Time(s)

(省略)

----- SSHD End -----

SSHD セクションは、sshd によるログ情報からの抜粋となります。

sshd へのログインを試行した不正ユーザー情報が記録されております。

これらは、ありがちなアカウント名とパスワードを使用してログイン可能なサーバを探しているスクリプトの仕業となります。

E-server では、sshd へのログインに RSA 認証モードを初期設定しておりますので、SSH 秘密鍵のないユーザーはログイン不可能となっており、特に気にする必要はないかと思われます。

----- Disk Space -----

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda2	36G	9.0G	25G	27%	/
/dev/hda1	99M	12M	82M	13%	/boot
none	125M	0	125M	0%	/dev/shm

LogWatch End

運用: 毎日、管理者アカウントに意味不明なメールがきます。

Disk Space セクションは、ディスク使用量の情報となります。
上記の例では利用料は 27% (余り 73%) となっている事がわかります。

一意的回答 ID: #1164

作成者: IXENT テクニカルサポート

最終更新: 2004-12-14 14:46