

The Top 10 Log Entries that Show You've Been Hacked

Dr. Tina Bird

<http://www.loganalysis.org>

tbird@precision-guesswork.com

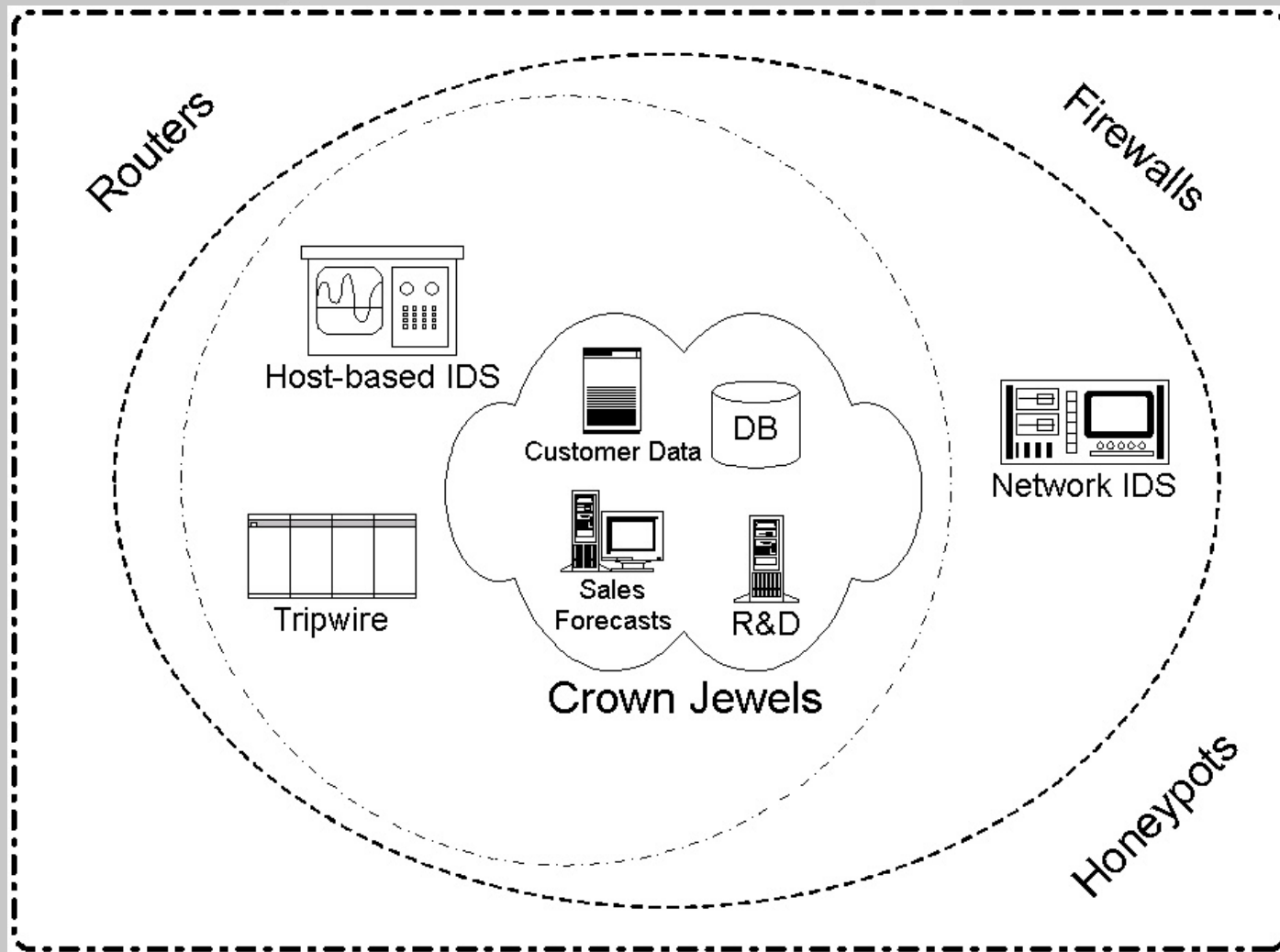
Last modified: 20 December 2002

In search of the unusual

The common item to look for when reviewing log files is anything that appears out of the ordinary.

*CERT Coordination Center
Intrusion Detection Checklist*

A Network Ecosystem



Why NIDS isn't Enough

```
Jan 2 16:19:23 yyy.yyy.yyy.yyy  
snort [1260]: RPC Info Query:  
216.216.74.2:963 ->  
xxx.xxx.xxx.xxx:111
```

```
Jan 2 16:19:31 yyy.yyy.yyy.yyy  
snort [1260]: spp_portscan:  
portscan status from 216.216.74.2:  
2 connections across 1 hosts:  
TCP (2), UDP (0)
```

Buffer Overflows

```
Jan 02 16:19:45 xxx.xxx.xxx.xxx rpc.statd[351]:  
gethostbyname error for  
^X÷ÿ¿^X÷ÿ¿^Y÷ÿ¿^Y÷ÿ¿^Z÷ÿ¿^Z÷ÿ¿^ [÷ÿ¿^ [÷ÿ¿bffff75  
0  
804971090909090687465676274736f6d616e7972652065  
20726f7220726f66  
bffff718  
bffff719   bffff71a  
bffff71b
```

!

!

Buffer Overflown?

```
Jan 02 16:20:25 xxx.xxx.xxx.xxx  
  adduser[12152]: new user:  
  name=cgi, uid=0, gid=0,  
  home=/home/cgi, shell=/bin/bash  
Jan 02 16:22:02 xxx.xxx.xxx.xxx  
  PAM_pwdb[12154]: password for  
  (cgi/0) changed by ((null)/0)
```

Hacked via FTP

```
Sep 23 17:31:55 www inetd[1638]: pid 28592: exit  
status 1
```

```
Sep 23 17:33:20 www ftpd[28594]: FTP LOGIN  
REFUSED (ftp in /etc/ftpusers) FROM  
203.55.23.150 [203.55.23.150], ftp
```

```
Sep 23 17:33:47 www ftpd[28595]: FTP LOGIN  
REFUSED (ftp in /etc/ftpusers) FROM  
203.55.23.150 [203.55.23.150], ftp
```

```
Sep 23 17:33:58 www inetd[1638]: pid 28596: exit  
status 1
```

```
Sep 23 17:52:38 www useradd[28609]: new user:  
name=jogja, uid=506, gid=10, home=/etc/jogja,  
shell=/bin/bash
```

Hacked via FTP cont.

```
Sep 23 17:55:34 www PAM_pwdb[28610]: password for  
(jogja/506) changed by ((null)/0)
```

```
Sep 23 17:58:03 www PAM_pwdb[28612]: check pass;  
user unknown
```

```
Sep 23 17:58:04 www login[28612]: FAILED LOGIN 1  
FROM 202.155.35.132 FOR ku ^H^H^H^H, User not  
known to the underlying authentication module
```

```
Sep 23 17:58:11 www PAM_pwdb[28612]:  
authentication failure; (uid=0) -> jogja for  
login service
```

```
Sep 23 17:58:12 www login[28612]: FAILED LOGIN 2  
FROM 202.155.35.132 FOR jogja, Authentication  
failure
```

Attacks on IIS

- ◇ Inappropriate access to server info:

```
http://host/index.asp?something=..\  
..\..\..\WINNT\system32\cmd.exe?/c  
+DIR+e:\WINNT\*.txt
```

- ◇ SQL injection attack on MS-SQL:

```
http://host/cgi-  
bin/lame.asp?name=john`;EXEC  
master.dbo.xp_cmdshell'cmd.exe dir  
c:'--
```

Configuration Change on Cisco IOS

```
%SYS-5-CONFIG: Configured from  
host1-config by rcp from  
172.16.101.101
```

Interface in Promiscuous Mode

```
Nov 30 23:56:13 172.16.6.110
```

```
kernel[-1]: device eth1 left  
promiscuous mode
```

```
Nov 30 23:56:13 172.16.6.110
```

```
kernel[-1]: device eth1  
entered promiscuous mode
```

Slapper: Linux/SSL worm

- ◇ Apache/mod-SSL worm discovered 13 Sept 2002; exploits buffer overflow in SSL v2

```
[error] SSL handshake failed: HTTP  
spoken on HTTPS port; trying to  
send HTML error page
```

```
[error] OpenSSL: error:1407609C:SSL  
routines:SSL23_GET_CLIENT_HELLO:
```

```
http request [Hint: speaking HTTP to  
HTTPS port!?!]
```

Apache Chunked Encoding Vuln

- ◇ FreeBSD worm detected in the wild 28 June 2002:

```
[Sat Jun 29 15:06:40 2002] [notice]  
child pid 21452 exit signal  
Segmentation Fault (11)
```

```
[Sat Jun 29 15:06:41 2002] [error]  
[client 172.16.159.57] client sent  
HTTP/1.1 request without hostname  
(see RFC2616 section 14.23): /
```

Nimda: Worm Sign

```
204.120.69.195 - - [18/Sep/2001:09:35:12 -0500] "GET
  /MSADC/root.exe?/c+dir HTTP/1.0" 404 - "-" "-"
204.120.69.195 - - [18/Sep/2001:09:35:12 -0500] "GET
  /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 -
  "-" "-"
204.120.69.195 - - [18/Sep/2001:09:35:12 -0500] "GET
  /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 -
  "-" "-"
204.120.69.195 - - [18/Sep/2001:09:35:12 -0500] "GET
  /scripts/..%255c../winnt/system32/cmd.exe? /c+dir
  HTTP/1.0" 404 - "-" "-"
```

Nimda: Worm Sign cont.

```
204.120.69.195 - - [18/Sep/2001:09:35:19 -0500]
  "GET /scripts/..%35%63../winnt/system32
  /cmd.exe?/c+dir HTTP/1.0" 400 215 "-" "-"
204.120.69.195 - - [18/Sep/2001:09:35:22 -0500]
  "GET /scripts/..%35c../winnt/system32
  /cmd.exe?/c+dir HTTP/1.0" 400 215 "-" "-"
204.120.69.195 - - [18/Sep/2001:09:35:23 -0500]
  "GET /scripts/..%25%35%63../winnt/system3/
  cmd.exe?/c+dir HTTP/1.0" 404 - "-" "-"
204.120.69.195 - - [18/Sep/2001:09:35:23 -0500]
  "GET /scripts/..%25%35%63../winnt/system32
  /cmd.exe?/c+dir HTTP/1.0" 404 - "-" "-"
```

SSH CRC-32 Attack

```
sshd[6169]: fatal: Local:  
Corrupted check bytes on  
input.
```

```
sshd[6253]: fatal: Local: crc32  
compensation attack: network  
attack detected
```

Code Red

```
128.101.47.28 - - [28/Sep/2001:00:43:43 -  
0400] "GET  
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XXX%u9090%u6858%ucbd3%u7801%u9090%u6858  
%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9  
090%u9090%u8190%u00c3%u0003%u8b00%u531b  
%u53ff%u0078%u0000%u00=a HTTP/1.0" 404  
284 "-" "-"
```

What to look for

- ◇ Passwords changed by someone other than the user – especially VID 0 users with null logins
- ◇ Processes dying with error code 1
- ◇ Long messages full of random characters
- ◇ Unexpected configuration changes

What to look for cont.

- ◇ The least-frequent messages generated on your network
- ◇ Messages containing the words *fatal*, *panic* or *password/passwd*
- ◇ Sudden increase or decrease in the number of messages received from a host or application
- ◇ Events recorded by multiple devices