APENDICE B.

DATOS DE ENTRENAMIENTO.

En este apéndice se presentan los datos de entrenamiento y pruebas que se utilizaron en el diseño y evaluación del sistema de detección de intrusos presentado en esta tesis. Los datos fueron tomados del proyecto de Detección de Intrusos desarrollado por el departamento de sistemas de la Pontificia Universidad Javeriana de Bogotá Colombia realizado en el 2003 [TOR03].

DATOS DE COMPORTAMIENTO NORMAL: 285 DATOS.

DESCRIPCION: Datos que representan requerimientos http de comportamiento común y no intrusivo. Son necesarios para que la red tenga una perspectiva de lo que es normal para poder definir lo que no es.

&@_@=@&@_@	&@_@=@.txt	&@=/@/&@=@
&@=/@/@&@_	&@=@&@_@=@	&@=@&@=/@/
&@=@_@&@=/	&@=@_@&@=@	./@&@=@&@=
./@/@&@=@&	./@/@.ini	./@/@/@.ex
.@/@/@.cgi	.@/@/@/@.	.\@\@.ini&
.cgi?@_@=@	.cgi?@=&@=	.exe/@_@.e
.php&@_@=@	.php?@=@/@	.txt&@=/@/
/&@=@.php&	/@&@=@&@=@	/@&@=@@@&@
/@.@ @/	/@.@.@.@.@	/@.@.@.php
/@.@.@.php	/@.@/@@@@@@	/@.@@@@@@@@
/@.asa@@@@	/@.asp.@@@	/@.asp@@@@
/@.bat@@@@	/@.cfm?@=@	/@.cfm@@@@
/@.cgi?@=@	/@.cgi@@@@	/@.dbm@@@@
/@.dll/_@_	/@.exe/@@@	/@.exe/@_@
/@.exe/_@_	/@.exe?@=@	/@/&@=@.ph
/@/@&@_@=	/@/@&@=@&@	/@/@&@=@@
/@/@&@=@@@	/@/@.@.@.@	/@/@.@.@.p
/@/@.@@@@@	/@/@.cfm?@	/@/@.ini@@
/@/@.mdb@@	/@/@.nsf@@	/@/@.php@@
/@/@.php@@	/@/@.txt@@	/@/@/@.@.@
/@/@/@.@.@	/@/@/@.@/@	/@/@/@.@@@
/@/@-@@@@@	/@/@@@@@@@@	/@/@_@.@@@
/@/@_@.@_@	/@/@_@.asp	/@/@_@.cgi

/@/@_@.htm
/@/@_@.php
/@/@_@_@.p
/@-@.@-@.h
/@-@/@.@@@
/@-@/@.cfm
/@-@/@.inc
/@-@/@.txt
/@-@/@_@.p
/@-@/@_@_@
/@-@@@@@@@
/@@@@@@@@@
@&@=/@/@&@
@&@=@&@=@-
@&@=@.@&@_
@.@?@=@&@=
@.cgi?@=&@
@.exe/@_@.
@.php&@_@=
@/&@=@.php
-@/@/@.txt
@/@/@/@.@/
@/@/@/@.ex
@/@@&@_@=
@/@-@.inc.
@/@-@/@/@.
@/@_@.@_@_
-@/@_@/@.p
-@/@_@_@_@
@?@=@&@=@&
@-@.@-@.ht
@-@/@.@/@=
@@@@@@@@@@
@\@.ini&@=
@_@&@=/@/@
@_@.@?@=@
@_@/@.dll/
@_@/@/@.ph
@_@_@.@.cg
@_@=@&@_@=
@_@=@.txt&
@_@=@@@@@@
@=/@.asp@@
@=/@/@@@@
@=@&@[@][@
@=@&@=@&@=
@=@&@=@://
@=@&@=@_@&
@=@.@&@=/@
@=@.txt&@=
@=@-@-@&@=
@=@@@@@@@@
@=@_@&@=@&
[@][@]=@&@
\@.ini&@=@
_@&@=@&@_@
/@/@_@.log
/@/@_@/@.p
/@/@_@_@_@
/@-@/.@/@/
/@-@/@.asp
/@-@/@.cgi
/@-@/@.php
/@-@/@_@.@
/@-@/@_@/@
/@-@-@.@@@
/@@@@@@@@@
@&@[@][@]=
@&@=@&@_@=
@&@=@&@=@&
@&@=@.php&
@.@?@=@/@/
@.cgi?@=@&
@.exe/_@_@
@.php?@=@/
-@/.@/@/@.
-@/@/@.xml
@/@/@/@.as
-@/@/@/@/@
-@/@-@.@/@
-@/@-@/@.p
@/@-@/@-@.
-@/@_@.cgi
@/@_@/@.ph
@/@_@_@_@.
@?@=@&@=@/
@-@.cgi?@=
@-@/@.cgi/
@-@=@@@@@@
@][@]=@&@=
@_@&@=@&@=
@_@.cgi?@=
@_@/@.exe/
@_@/@/@_@_
@_@_@_@.@.
@_@=@&@=@&
@_@=@://@/
@=*&@=@&@=
@=/@/&@=@.
@=/@/@@@@@
@=@&@_@=@&
@=@&@=@.@&
@=@&@=@-@-
@=@&@=@_@&
@=@.@.org
@=@://@/@@
@=@-@@@@@@
@=@_@&@=/.
@=@_@&@=@_
[@]=@&@=@&
\@\@.ini&@
_@&@=@&@=@
/@/@_@.nsf
/@/@_@@@@@
/@/@=@.@&@
/@-@/@.@/@
/@-@/@.bat
/@-@/@.exe
/@-@/@.plx
/@-@/@_@.c
/@-@/@_@@@
/@-@-@.jsp
/@-@@@@@@@
@&@_@=@&@_
@&@=@&@=/@
@&@=@&@=@_
@.@.@/@.js
@.cgi?@_@=
@.dll/_@_@
@.exe?@=@&
@.txt&@=/@
-@/@/@.php
-@/@/@/@.@
@/@/@/@.e
@/@?@=@&@=
-@/@-@.cgi
@/@-@/@.ph
-@/@@@@@@@@
-@/@_@.php
@/@_@_@.ph
@/@=@.@&@=
@-@&@=@@@@
@-@/.@/@/@
-@@@@@@@@@@
@[@][@]=@&
@]=@&@=@&@
@_@&@=@_@&
@_@.exe?@=
@_@/@/@.cg
@_@/_@_@/@
@_@=/@/@@
@_@=@&@=@.
@_@=@://@@
@=*&@=@@@@
@=/@/@&@_@
@=;@=@&@=@
@=@&@=/@/@
@=@&@=@.ph
@=@&@=@@@@
@=@.@&@_@_
@=@.php&@_
@=@://@@@@
@=@@@@@@@@
@=@_@&@=/@
@=@_@@@@@@
\@.ini&@=.
_@&@=/@/@&
_@&@=@_@&@

@/@.dll/
_@/@/@.cgi
_@/_@_@/@.
_@_@/@.exe
_@_@\@.cnf
_@=@&@=@.@
=/@/&@=@.p
=@&@=@.@&@
=@&@=@-@-@
=@.@&@=/@/
=@-@-@&@="
=@_@&@=@_@
exe?@=@&@=
p &@=@&@=@
php?@=@&@=
t&@=/@/&@=
_@/@.exe/@
_@/@/@.php
_@_@.@.cgi
_@_@/@.pwd
_@_@_@.@.c
_@=@.txt&@
=/@/@&@_@=
=@&@=@.php
=@&@=@_@&@
=@.php&@_@
=@_@&@=/@/
asp &@=@&@
hp&@_@=@.t
p&@_@=@.tx
php?@=@/@.
txt&@=/@/&
@/@.exe/
_@/@/@_@_@
_@_@/@.dll
_@_@/_@_@/
_@=@&@=@&@
=*&@=@&@=.
=@&@_@=@&@
=@&@=@://@
=@.@&@_@_@
=@.txt&@=/
=@_@&@=@&@
cgi?@=@&@=
jsp?@=@&@=
php&@_@=@.
sp &@=@&@=
xt&@=/@/&@

INYECCION DE COMANDOS: 143 DATOS.

DESCRIPCION: Datos anómalos, que representan ejecución directa de comandos de internet a través de shells o código de maquina.

&@='';@ '';
.@/@=;@ @.
.EXE? -@ @
/@.@/@=;@
/@/@.@/@=;
/@/@|&@_@=
'; @ `@ `;
;@ /@/@|&@
;@|@
?@_@=@&@=|
?@=@&@=;@
@ /@/@|?@=
@&@=;@ /@/
@&@=|/@/@|
@'(@ @
@.bat?&@
@.bat?|@ .
@.cgi?@=%0a@
@.exe|@
@/@&@_@= ;
@/@;@ /@/@
@;@|@
@?@=&@=;@
@?|@
-@-@&@='';@
@@@ @ /@/@
@|&@_@=@&@
@+@+@:\+/@
@='';@ '';
&@=;@ /@/@
.bat?&@
.exe|@
/@.bat|@ @
/@/@.bat|@
/@;@ /@/@|
;&@=/@/@ /
;@ /@/@|?@
? -n @:\PATH;//@
?@=%0a@&@=@
?|@
@ @:\@.ini
@&@=;@ /@|
@&@=|@ /@/
@.@.org |
@.bat?&@
@.bat|@ @:
@.cgi?@=;&
@.exe|@ @:
@/@.@/@=;@
@/@|&@_@=@
@?/c+@
@?@=;@ /@
@?|=@
@-@&@='';@
@-@-@&@='';
@|@
@= @ /@/@@
@='';@ '';
'(@
.bat|@ @:\
/@&@_@= ;@
/@/@ /@/@|
/@/@|&@_@
''; @ `@ `
;@ /@/@
;@ @|@
?%0a@
?@=;&@=/@/
@ /@/@@@@@@
@&@_@= ;@;
@&@=@&@=|/
@&@=+'@'=
@.@/@=;@ @
@.bat?&@+@
@.cgi?'%0a/@
@.EXE? -@
@/@ /@/@|
@/@.bat|@
@/@=;@ @.@
@?@%0a@
@?@=@&@=;@
@@ @ /@/@&
@-@&@=;@ /
@_@=@';@@@
@|@ " @" @
@=" -@|@ "
@=%0a@

@=/@/@&@=;
@=;@ /@/@|
@=;@|@
@=@";@
@=@&@=|@ /
@=@;@|@
@='@@@@@@@@
@=@|@
@=`@ @` @
@=|@ /@/@|
@=+'@"='+
|@ " @" @
=" -@|@ "
=%0a@
=;&@=/@/@
=;@"@
=@|&@
at|@ @:\@\
cgi?@=&@=;
@=;&@
@=;@"@
@=@ @ @ @_
@=@%0a@
@=@&@=|@ @
@=@-@&@=;@
@=@_@&@=;@
@=@+@:@.@.
@=|/@/@/@|
@=|@|@@@@@
_@=@&@_@=<
|@ /@/@|&@
=";@
=&@=;@ /@/
=;@ /@/@|&
=;@|"@
=`@` @
bat|@ @:\@
t|@ @:\@\@
@=;@ /@/@@
@=;@|"@
@=@ @@@@@@@
@=@&@=;@ /
@=@&@=+'@'
@=@@@ @ /@
@=@|&@
@=`/@/@`@@
@=|@
@"='+&@=@
|&@_@=@&@=
|@ @:\@\@.
=";@ "; @
=;&@
=;@ @|@
=@;@|@
=|@
cgi?@=%0a/

MODIFICACION DE PATH: 260 DATOS.

DESCRIPCION: Datos que representan la modificación de privilegios de un servidor por parte de un atacante por medio de vulnerabilidades en el sistema.

"./."./@/@
%@..%@..%@
%@..%@/@/@
%@/@/@/@.e
&@=../../.
&@=@&@=../
*//../../.
.%@..%@..%
.%00@
...nsf/../
../../..//
../../@/@/
../@
../@/@ /@/
..@/../../
..\..\..\.
..\..\@
..\@
..€Ç¯../@/
..box//../
./."./@/@.
./../..//@
./../../@/
./.|./.|./
.//@
.@../@/@/
"./@/@.ini
%@..%@../@
%@../@/@/@
%00/@
&@=..\..\.
*&@=@&@=..
."./."./@/
.%@..%@..%
..%@..%@..
...nsf//..
../../../@
..//.../.
../@%00@
../@/@&@=.
..@//../..
..\..\..\.
..\..\@.in
..\@\@.ini
..€Ç¯..€Ç¯
..nsf/../.
./../../..
./../../@&
./../../@/
.//.../..
./@/@ /@/@
.@..@..
%@..%@..%@
%@..%@../@
%@../@/@/@
%00html
&@=/../../
*.@//@.jsp
."./@/@.in
.%@..%@../
...box//..
../../../.
../../@/@/
..//.../@
../@&@=@&@
../@/@&@=@
..@/@/@/@
..\..\..\@
..\..\@\@.
..\\@
..Â../@/
..nsf//../
./../../..
./../../@.
./../@&@=@
.//.../@.
./@/@&@=..
.@..@../

```
.@..@/@/
.@=../../.
.Â_..Â_../
/..%@..%@.
/...//@.ba
/...@//../
/...nsf//.
/../@/@/@_
/..\\@
/..Â..Â.
/..Á/../@/
//.../...
//../../..
/@/../@/@/
/@-@/..%@.
/@-@//.%@/
@..%@..%@/
@..%@/@/@/
@.../@
@..@/@/@
@..\@
@.@=../../
@.ntf+++++
@/*//../..
@/.%@/@/@.
@/..%@..%@
@/../../..
@/..@..@
@/..Â£..Â£
-@//.%@/.%
@//////@
-@//@/@/@.
@-@//.%@/.
@-@=../../
@[@]=../..
@_/@/..%@.
@=.|./.|./
@=/../../.
@=@&@=..\.
\..\..\..\
\..\@\@.in
_/@/..%@.@
_@_@=.|./.
_@=@&@=../
|./.|./.|.
¯../@/@/@.
¯..Á¯../@/
++++++++++
=@:\@\@.in
Â..ÂÂ..ÂÂ.
Á/..Á/..Á/
Á¯..Á¯..Á¯
Â£..Â£..Â£
ÂÂ..ÂÂ..ÂÂ
Ç¯..€Ç¯../
f/../../..
.@/../../.
.\..\..\..
.Â_..Â_../
/..%@..%@.
/...//@.in
/...box//.
/../../../
/../<@>@('
/..€Ç¯..€Ç
/..Â_..Â_.
/..Á/..Á/.
//.../@.b
//////@
/@/..@..
/@-@/.../
/@-@//@/@/
@..%@../@.
@..%2f@
@..@../@
@..@/@/@/
@..\\@
@.|./@
@.php @
@/.%@/.%@/
@/.%@/@/@/
-@/.../..
@/../@/@/@
@/..\\@
@/..ÂÂ..ÂÂ
@//.%@/.%@
@///@
@-@/.../.
@-@-@=..\.
-@-@=..\..
@]=../../.
-@=..\..\.
@=/&@=../.
@=/../@
@=@:\&@=@&
\..\..\@.i
]/..%@..%@
_@&@=/../.
_@=../../.
_@=@&@=..\
|./.|./@/@
¯..€Ç¯../@
¯..Á¯..Á¯.
=@&@=..\..
=@_@&@=/..
Á/../@/@/@
Á¯../@/@/@
Â£../@/@/@
ÂÂ../@/@/@
box//../..
Ç¯..€Ç¯..€
f//../../.
.@//../../
.\..\..\@.
.Á..Á..Á
/.../.../
/...@/../.
/...nsf/..
/../@/@/@.
/..@..@.
/..Á..Á.
/..Â_..Â_.
//.%@/.%@/
//.../@.i
/@/../../.
/@/\..\..\
/@-@/..@.
@..%@..%@/
@..%@../@/
@..%5c@
@..@..@/
@..\..\@
@.//@
@.ini&@=..
@/%00@
@/.%@/./@/
-@/..%@..%
@/.../...
-@/..@..
@/..€Ç¯..€
@/./@/@/@.
@//../../.
@//@
@-@/..@..
-@-@=../..
@-@=..\..\
@_/@/..%@.
@=..\..\..
@=/../../.
@=@&@=../.
[@]=../../
\..\..\@\@
_/@/..%@.@
_@/..%@..%
_@=.|./.|.
|.%2F.|@
|@..\\@
¯..€Ç¯..€Ç
++++++.nsf
=@:\&@=@&@
£../@/@/@.
Á/..Á/../@
Á¯..Á¯../@
Â£..Â£../@
ÂÂ..ÂÂ../@
Ç¯../@/@/@
exe/@_@.ex
f+++++++++
```

i&@=..\..\
ni&@=..\..
ntf+++++++
php?@=@://@
x//../../.
ini&@=..\.
nsf/../../
ox//../../
sf/../../.
xe/@_@.exe
ini.@.txt
nsf//../..
php&@=../.
sf//../../

INYECCION DE COMANDOS SQL: 11 DATOS.

DESCRIPCION: Inyección de comandos para acceder a bases de datos *SQL*.

' --@
' group @
' UNION @
'; SELECT @
' @ @
' having @
'; @ @
'union @ select
' @ 1==1--@
' OR 1==1--@
'; insert @

XSS (CROSS SITE SCRIPT): 74 DATOS.

DESCRIPCION: Inyección de comandos por medio de lenguajes de programación como java, java script, .y html.

")</@>.jsp
"@:"> <@:@
"><@>@(@)<
&@=<@>@=@;
('@');&@;/
(@)</@><!-
/&@;@&@;@(
/@/<@>@(@.
/<@>@("@")
;@&@;@('@'
;</@>&@=<@
@ @="@.@"?
@&@;@('@')
@&@=@&@=<@
@&@=<@>@</
@(\"@\")</
'@;@
~/<@>@(@.@
</@>&@=@&@
<@:@> <@:
=@&@="><@>
=@&@=<@>@<
=@;</@>&@=
=<@>@.@(@.
p/<@>@('@'
")</@>/@.@
"@:"><@:@>
&@;@&@;@('
("@")</@>/
('@');</@>
.@)</@>&@=
/@.jsp/<@>
/@:@></@:@
/<@>@('@')
;@('@');&@
@ @()</@:
@" @ @()</
@&@_@=<@>@
@&@=@:<@>@
@&@=<@>@=@
@.@);</@>&
`@ `;@();@
</@:@></@
</@>&@=<@>
<@:@>@ "@:
=@&@=@:<@>
=@&@=<@>@=
=<@>@(@)</
=<@>@.@</@
sp/<@>@('@
"@")</@>/@
"@\")</@>.
&@=<@>@</@
()</@:@></
('@')</@>.
.jsp/<@>@(
/@/@/<@>@(
/</@><@>@(
:<@>@('@')
;</@>&@=@&
@ @()</@:@
@")</@>/@.
@&@="><@>@
@&@=<@>@.@
@(@.@)</@>
@.@)</@>&@
|@||/@|
</@:@></@:
<@:@> <@
<@>@('@')<
=@&@=<@>@.
=@:<@>@('@
=<@>@(@.@)
=<@>@=@;</