**DARPA INTRUSION DETECTION EVALUATION**

**Detections List File**

The following list documents the attacks occuring in the second week of 1999 training data.

The date, starting time, and destination(s) of each attack are provided. In addition, the name of the attack is provided as a source of identification.

Brief descriptions of each type of attack are provided following the list of detections. The attack names in the detection list provide hyperlinks to the brief descriptions that follow.

The names provided are those that were used during the evaluation and may not be the only names by which an attack is known.

**Detections List**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Date** | **Start\_Time** | **Destination** | **Score** | **Name** |
| 1 | 03/08/1999 | 08:01:01 | hume.eyrie.af.mil | 1 | NTinfoscan |
| 2 | 03/08/1999 | 08:50:15 | zeno.eyrie.af.mil | 1 | pod |
| 3 | 03/08/1999 | 09:39:16 | marx.eyrie.af.mil | 1 | back |
| 4 | 03/08/1999 | 12:09:18 | pascal.eyrie.af.mil | 1 | httptunnel |
| 5 | 03/08/1999 | 15:57:15 | pascal.eyrie.af.mil | 1 | land |
| 6 | 03/08/1999 | 17:27:13 | marx.eyrie.af.mil | 1 | secret |
| 7 | 03/08/1999 | 19:09:17 | pascal.eyrie.af.mil | 1 | ps attack |
|  |  |  |  |  |  |
| 8 | 03/09/1999 | 08:44:17 | marx.eyrie.af.mil | 1 | portsweep |
| 9 | 03/09/1999 | 09:43:51 | pascal.eyrie.af.mil | 1 | eject |
| 10 | 03/09/1999 | 10:06:43 | marx.eyrie.af.mil | 1 | back |
| 11 | 03/09/1999 | 10:54:19 | zeno.eyrie.af.mil | 1 | loadmodule |
| 12 | 03/09/1999 | 11:49:13 | pascal.eyrie.af.mil | 1 | secret |
| 13 | 03/09/1999 | 14:25:16 | pascal.eyrie.af.mil | 1 | mailbomb |
| 14 | 03/09/1999 | 13:05:10 | 172.016.112. 001-114.254 | 1 | ipsweep |
| 15 | 03/09/1999 | 16:11:15 | marx.eyrie.af.mil | 1 | phf |
| 16 | 03/09/1999 | 18:06:17 | pascal.eyrie.af.mil | 1 | httptunnel |
|  |  |  |  |  |  |
| 17 | 03/10/1999 | 12:02:13 | marx.eyrie.af.mil | 1 | satan |
| 18 | 03/10/1999 | 13:44:18 | pascal.eyrie.af.mil | 1 | mailbomb |
| 19 | 03/10/1999 | 15:25:18 | marx.eyrie.af.mil | 1 | perl (Failed) |
| 20 | 03/10/1999 | 20:17:10 | 172.016.112. 001-114.254 | 1 | ipsweep |
| 21 | 03/10/1999 | 23:23:00 | pascal.eyrie.af.mil | 1 | eject (console) |
| 22 | 03/10/1999 | 23:56:14 | hume.eyrie.af.mil | 1 | crashiis |
|  |  |  |  |  |  |
| 23 | 03/11/1999 | 08:04:17 | hume.eyrie.af.mil | 1 | crashiis |
| 24 | 03/11/1999 | 09:33:17 | marx.eyrie.af.mil | 1 | satan |
| 25 | 03/11/1999 | 10:50:11 | marx.eyrie.af.mil | 1 | portsweep |
| 26 | 03/11/1999 | 11:04:16 | pigeon.eyrie.af.mil | 1 | neptune |
| 27 | 03/11/1999 | 12:57:13 | marx.eyrie.af.mil | 1 | secret |
| 28 | 03/11/1999 | 14:25:17 | marx.eyrie.af.mil | 1 | perl |
| 29 | 03/11/1999 | 15:47:15 | pascal.eyrie.af.mil | 1 | land |
| 30 | 03/11/1999 | 16:36:10 | 172.016.112. 001-254 | 1 | ipsweep |
| 31 | 03/11/1999 | 19:16:18 | pascal.eyrie.af.mil | 1 | ftp-write |
|  |  |  |  |  |  |
| 32 | 03/12/1999 | 08:07:17 | marx.eyrie.af.mil | 1 | phf |
| 33 | 03/12/1999 | 08:10:40 | marx.eyrie.af.mil | 1 | perl (console) |
| 34 | 03/12/1999 | 08:16:46 | pascal.eyrie.af.mil | 1 | ps (console) |
| 35 | 03/12/1999 | 09:18:15 | duck.eyrie.af.mil | 1 | [pod](http://www.ll.mit.edu/ideval/docs/detections_1999.html#pod) |
| 36 | 03/12/1999 | 11:20:15 | marx.eyrie.af.mil | 1 | neptune |
| 37 | 03/12/1999 | 12:40:12 | hume.eyrie.af.mil | 1 | crashiis |
| 38 | 03/12/1999 | 13:12:17 | zeno.eyrie.af.mil | 1 | loadmodule |
| 39 | 03/12/1999 | 14:06:17 | marx.eyrie.af.mil | 1 | perl (Failed) |
| 40 | 03/12/1999 | 14:24:18 | pascal.eyrie.af.mil | 1 | ps |
| 41 | 03/12/1999 | 15:24:16 | pascal.eyrie.af.mil | 1 | eject |
| 42 | 03/12/1999 | 17:13:10 | pascal.eyrie.af.mil | 1 | portsweep |
| 43 | 03/12/1999 | 17:43:18 | pascal.eyrie.af.mil | 1 | ftp-write |

**Attack Descriptions**

|  |  |
| --- | --- |
| back | Denial of service attack against apache webserver where a client requests a URL containing many backslashes. |
| crashiis | A single, malformed http request causes the webserver to crash. |
| dict | Guess passwords for a valid user using simple variants of the account name over a telnet connection. |
| eject | Buffer overflow using eject program on Solaris. Leads to a user->root transition if successful. |
| ffb | Buffer overflow using the ffbconfig UNIX system command leads to root shell |
| format | Buffer overflow using the fdformat UNIX system command leads to root shell |
| ftp-write | Remote FTP user creates .rhost file in world writable anonymous FTP directory and obtains local login. |
| guest | Try to guess password via telnet for guest account. |
| httptunnel | There are two phases to this attack:  Setup — a  web "client" is setup on the machine being attacked, which is configured, perhaps via crontab, to periodically make requests of a "server" running on a non-privilaeged port on the attacking machine.  Action — When the periodic requests are recieved, the server encapsulates commands to be run by the "client" in a cookie.. things like "cat /etc/passwd".. etc.. |
| imap | Remote buffer overflow using imap port leads to root shell |
| ipsweep | Surveillance sweep performing either a port sweep or ping on multiple host addresses. |
| land | Denial of service where a remote host is sent a UDP packet with the same source and destination |
| loadmodule | Non-stealthy loadmodule attack which resets IFS for a normal user and creates a root shell |
| mailbomb | A Denial of Service attack where we send the mailserver many large messages for delivery in order to slow it down, perhaps effectively halting normal operation. |
| multihop | Multi-day scenario in which a user first breaks into one machine |
| neptune | Syn flood denial of service on one or more ports. |
| nmap | Network mapping using the nmap tool. Mode of exploring network will vary—options include SYN |
| ntinfoscan | A process by which the attacker scans an NT machine for information concerning its configuration, including ftp services, telnet services, web services,  system account information, file systems and permissions. |
| perlmagic | Perl attack which sets the user id to root in a perl script and creates a root shell |
| phf | Exploitable CGI script which allows a client to execute arbitrary commands on a machine with a misconfigured web server. |
| pod | Denial of service ping of death |
| portsweep | Surveillance sweep through many ports to determine which services are supported on a single host. |
| ps | Ps takes advantage of a racecondition in the ps command in Sol. 2.5, allowing a user to gain root access. |
| rootkit | Multi-day scenario where a user installs one or more components of a rootkit |
| satan | Network probing tool which looks for well-known weaknesses. Operates at three different levels. Level 0 is light |
| secret |  |
| smurf | Denial of service icmp echo reply flood. |
| spy | Multi-day scenario in which a user breaks into a machine with the purpose of finding important information where the user tries to avoid detection. Uses several different exploit methods to gain access. |
| syslog | Denial of service for the syslog service connects to port 514 with unresolvable source ip. |
| teardrop | Denial of service where mis-fragmented UDP packets cause some systems to reboot. |
| warez | User logs into anonymous FTP site and creates a hidden directory. |
| warezclient | Users downloading illegal software which was previously posted via anonymous FTP by the warezmaster. |
| warezmaster | Anonymous FTP upload of Warez (usually illegal copies of copywrited software) onto FTP server. |