
45:hacl(internet,webServer,tcp,80):1
46:attackerLocated(internet):1
44:RULE 6 (direct network access):0
43:netAccess(webServer,tcp,80):0
47:networkServiceInfo(webServer,httpd,tcp,80,apache):1
42:RULE 2 (remote exploit of a server program):0
114:hacl(webServer,n31Inter,tcp,80):1
83:hacl(webServer,n2Inter,tcp,80):1
79:hacl(webServer,n1Inter,tcp,80):1
57:nfsExportInfo(fileServer,'/export',write,webServer):1
56:hacl(webServer,fileServer,nfsProtocol,nfsPort):1
40:hacl(webServer,fileServer,rpc,100005):1
59:hacl(webServer,n0Inter,tcp,80):1
41:execCode(webServer,apache):0
87:hacl(webServer,n3Inter,tcp,80):1
91:hacl(webServer,n11Inter,tcp,80):1
97:hacl(webServer,n13Inter,tcp,80):1
101:hacl(webServer,n29Inter,tcp,80):1
125:hacl(webServer,n36Inter,tcp,80):1
129:hacl(webServer,n37Inter,tcp,80):1
133:hacl(webServer,n65Inter,tcp,80):1
113:RULE 5 (multi-hop access):0
82:RULE 5 (multi-hop access):0
78:RULE 5 (multi-hop access):0
55:RULE 17 (NFS shell):0
39:RULE 5 (multi-hop access):0
58:RULE 5 (multi-hop access):0
86:RULE 5 (multi-hop access):0
90:RULE 5 (multi-hop access):0
96:RULE 5 (multi-hop access):0
100:RULE 5 (multi-hop access):0
124:RULE 5 (multi-hop access):0
128:RULE 5 (multi-hop access):0
132:RULE 5 (multi-hop access):0
49:networkServiceInfo(fileServer,mountd,rpc,100005,root):1
50:vulExists(fileServer,'CVE-2013-4857',mountd,remoteExploit,privEscalation):1
38:netAccess(fileServer,rpc,100005):0
[68.6]
37:RULE 2 (remote exploit of a server program):0
[68.6]
54:canAccessFile(fileServer,root,write,'/export'):1
36:execCode(fileServer,root):0
35:hacl(fileServer,n0Inter,tcp,80):1
[68.6]
[68.6]
53:RULE 10 (execCode implies file access):0
34:RULE 5 (multi-hop access):0
[68.6]
[68.6]
[68.6]
52:accessFile(fileServer,write,'/export'):0
65:nfsMounted(n0Inter,'/usr/local/share',fileServer,'/export',read):1
60:networkServiceInfo(n0Inter,httpd,tcp,80,root):1
61:vulExists(n0Inter,'CVE-2013-0180',httpd,remoteExploit,privEscalation):1
33:netAccess(n0Inter,tcp,80):0
[68.6]
[68.6]
[82.5]
[68.6]
51:RULE 4 (Trojan horse installation):0
64:RULE 16 (NFS semantics):0
32:RULE 2 (remote exploit of a server program):0
[68.6]
63:accessFile(n0Inter,write,'/usr/local/share'):0
[68.6]
[151.1]
62:RULE 4 (Trojan horse installation):0
[68.6]
77:hacl(n0Inter,n1Inter,tcp,80):1
31:execCode(n0Inter,root):0
30:hacl(n0Inter,n3Inter,tcp,80):1
[68.6, 151.1]
[68.6, 151.1]
76:RULE 5 (multi-hop access):0
29:RULE 5 (multi-hop access):0
[68.6, 151.1]
80:networkServiceInfo(n1Inter,httpd,tcp,80,root):1
81:vulExists(n1Inter,'CVE-2013-2255',httpd,remoteExploit,privEscalation):1
75:netAccess(n1Inter,tcp,80):0
[112.1]
[68.6, 151.1]
74:RULE 2 (remote exploit of a server program):0
[180.7, 263.2]
73:execCode(n1Inter,root):0
72:hacl(n1Inter,n2Inter,tcp,80):1
[180.7, 263.2]
71:RULE 5 (multi-hop access):0
[180.7, 263.2]
85:vulExists(n2Inter,'CVE-2013-3023',httpd,remoteExploit,privEscalation):1
70:netAccess(n2Inter,tcp,80):0
84:networkServiceInfo(n2Inter,httpd,tcp,80,root):1
[186.3]
[180.7, 263.2]
69:RULE 2 (remote exploit of a server program):0
[68.6, 151.1]
[449.5, 367.0]
67:hacl(n2Inter,n3Inter,tcp,80):1
68:execCode(n2Inter,root):0
[449.5, 367.0]
66:RULE 5 (multi-hop access):0
[449.5, 367.0]
88:networkServiceInfo(n3Inter,httpd,tcp,80,root):1
89:vulExists(n3Inter,'CVE-2013-4275',httpd,remoteExploit,privEscalation):1
28:netAccess(n3Inter,tcp,80):0
[145.8]
[449.5, 68.6, 367.0, 151.1]
27:RULE 2 (remote exploit of a server program):0
[512.8, 296.9, 595.3, 214.4]
95:hacl(n3Inter,n13Inter,tcp,80):1
26:execCode(n3Inter,root):0
25:hacl(n3Inter,n11Inter,tcp,80):1
[512.8, 296.9, 595.3, 214.4]
[512.8, 296.9, 595.3, 214.4]
94:RULE 5 (multi-hop access):0
24:RULE 5 (multi-hop access):0
[512.8, 296.9, 595.3, 214.4]
92:networkServiceInfo(n11Inter,httpd,tcp,80,root):1
93:vulExists(n11Inter,'CVE-2013-3214',httpd,remoteExploit,privEscalation):1
23:netAccess(n11Inter,tcp,80):0
[303.8]
[512.8, 296.9, 595.3, 214.4]
22:RULE 2 (remote exploit of a server program):0
[512.8, 296.9, 595.3, 214.4]
[816.6, 600.7, 899.1, 518.2]
20:hacl(n11Inter,n13Inter,tcp,80):1
21:execCode(n11Inter,root):0
[816.6, 600.7, 899.1, 518.2]
19:RULE 5 (multi-hop access):0
[816.6, 600.7, 899.1, 518.2]
99:vulExists(n13Inter,'CVE-2013-6878',httpd,remoteExploit,privEscalation):1
18:netAccess(n13Inter,tcp,80):0
98:networkServiceInfo(n13Inter,httpd,tcp,80,root):1
[213.5]
[512.8, 899.1, 518.2, 296.9, 816.6, 595.3, 214.4, 600.7]
17:RULE 2 (remote exploit of a server program):0
[1030.1, 808.8, 427.9, 814.2, 726.3, 1112.6, 731.7, 510.4]
110:hacl(n13Inter,n31Inter,tcp,80):1
16:execCode(n13Inter,root):0
15:hacl(n13Inter,n29Inter,tcp,80):1
[1030.1, 808.8, 427.9, 814.2, 726.3, 1112.6, 731.7, 510.4]
[1030.1, 808.8, 427.9, 814.2, 726.3, 1112.6, 731.7, 510.4]
109:RULE 5 (multi-hop access):0
14:RULE 5 (multi-hop access):0
[1030.1, 808.8, 427.9, 814.2, 726.3, 1112.6, 731.7, 510.4]
103:vulExists(n29Inter,'CVE-2013-1607',httpd,remoteExploit,privEscalation):1
13:netAccess(n29Inter,tcp,80):0
102:networkServiceInfo(n29Inter,httpd,tcp,80,root):1
[382.2]
[1030.1, 808.8, 427.9, 814.2, 726.3, 1112.6, 731.7, 510.4]
[1030.1, 808.8, 427.9, 814.2, 726.3, 1112.6, 731.7, 510.4]
12:RULE 2 (remote exploit of a server program):0
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
112:hacl(n29Inter,n31Inter,tcp,80):1
11:execCode(n29Inter,root):0
123:hacl(n29Inter,n36Inter,tcp,80):1
10:hacl(n29Inter,n37Inter,tcp,80):1
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
111:RULE 5 (multi-hop access):0
122:RULE 5 (multi-hop access):0
9:RULE 5 (multi-hop access):0
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
116:vulExists(n31Inter,'CVE-2013-4101',httpd,remoteExploit,privEscalation):1
108:netAccess(n31Inter,tcp,80):0
115:networkServiceInfo(n31Inter,httpd,tcp,80,root):1
127:vulExists(n36Inter,'CVE-2013-3023',httpd,remoteExploit,privEscalation):1
121:netAccess(n36Inter,tcp,80):0
126:networkServiceInfo(n36Inter,httpd,tcp,80,root):1
[227.9]
[1412.3, 1030.1, 1191.0, 808.8, 810.1, 427.9, 1196.4, 814.2, 1108.5, 726.3, 1494.8, 1112.6, 1113.9, 731.7, 892.6, 510.4]
[348.3]
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
107:RULE 2 (remote exploit of a server program):0
120:RULE 2 (remote exploit of a server program):0
[1412.3, 1191.0, 810.1, 1196.4, 1108.5, 1494.8, 1113.9, 892.6]
[1120.5, 738.3, 1640.2, 1258.0, 1418.9, 1036.7, 1038.0, 655.8, 1424.3, 1042.1, 1722.7, 1336.4, 954.2, 1340.5, 1341.8, 959.6]
[1760.6, 1539.3, 1158.4, 1544.7, 1456.8, 1843.1, 1462.2, 1240.9]
105:hacl(n31Inter,n37Inter,tcp,80):1
106:execCode(n31Inter,root):0
118:hacl(n36Inter,n37Inter,tcp,80):1
119:execCode(n36Inter,root):0
[1120.5, 738.3, 1640.2, 1258.0, 1418.9, 1036.7, 1038.0, 655.8, 1424.3, 1042.1, 1722.7, 1336.4, 954.2, 1340.5, 1341.8, 959.6]
[1760.6, 1539.3, 1158.4, 1544.7, 1456.8, 1843.1, 1462.2, 1240.9]
104:RULE 5 (multi-hop access):0
117:RULE 5 (multi-hop access):0
[1120.5, 738.3, 1640.2, 1258.0, 1418.9, 1036.7, 1038.0, 655.8, 1424.3, 1042.1, 1722.7, 1336.4, 954.2, 1340.5, 1341.8, 959.6]
[1760.6, 1539.3, 1158.4, 1544.7, 1456.8, 1843.1, 1462.2, 1240.9]
130:networkServiceInfo(n37Inter,httpd,tcp,80,root):1
131:vulExists(n37Inter,'CVE-2013-1866',httpd,remoteExploit,privEscalation):1
8:netAccess(n37Inter,tcp,80):0
[286.7]
[1539.3, 1412.3, 1158.4, 1544.7, 1418.9, 1036.7, 1038.0, 655.8, 1424.3, 1042.1, 1191.0, 810.1, 1196.4, 1456.8, 1843.1, 1462.2, 1336.4, 954.2, 1722.7, 1340.5, 1341.8, 959.6, 1108.5, 1494.8, 1240.9, 1113.9, 1120.5, 1760.6, 738.3, 1640.2, 1258.0, 892.6]
7:RULE 2 (remote exploit of a server program):0
[1025.0, 1926.9, 1544.7, 1179.3, 1826.0, 1699.0, 1445.1, 1831.4, 1705.6, 1323.4, 1324.7, 942.5, 1711.0, 1328.8, 2047.3, 1477.7, 1096.8, 1483.1, 1743.5, 2129.8, 1748.9, 1623.1, 1240.9, 2009.4, 1627.2, 1628.5, 1246.3, 1395.2, 1781.5, 1527.6, 1400.6, 1407.2]
6:execCode(n37Inter,root):0
5:hacl(n37Inter,n65Inter,tcp,80):1
[1025.0, 1926.9, 1544.7, 1179.3, 1826.0, 1699.0, 1445.1, 1831.4, 1705.6, 1323.4, 1324.7, 942.5, 1711.0, 1328.8, 2047.3, 1477.7, 1096.8, 1483.1, 1743.5, 2129.8, 1748.9, 1623.1, 1240.9, 2009.4, 1627.2, 1628.5, 1246.3, 1395.2, 1781.5, 1527.6, 1400.6, 1407.2]
4:RULE 5 (multi-hop access):0
[1025.0, 1926.9, 1544.7, 1179.3, 1826.0, 1699.0, 1445.1, 1831.4, 1705.6, 1323.4, 1324.7, 942.5, 1711.0, 1328.8, 2047.3, 1477.7, 1096.8, 1483.1, 1743.5, 2129.8, 1748.9, 1623.1, 1240.9, 2009.4, 1627.2, 1628.5, 1246.3, 1395.2, 1781.5, 1527.6, 1400.6, 1407.2]
134:networkServiceInfo(n65Inter,httpd,tcp,80,root):1
135:vulExists(n65Inter,'CVE-2013-6811',httpd,remoteExploit,privEscalation):1
3:netAccess(n65Inter,tcp,80):0
[448.8]
[1025.0, 1926.9, 1544.7, 1179.3, 1826.0, 1699.0, 1445.1, 1831.4, 1705.6, 1323.4, 1324.7, 942.5, 1711.0, 1328.8, 2047.3, 1477.7, 1096.8, 1483.1, 1743.5, 2129.8, 1748.9, 1623.1, 1240.9, 2009.4, 1627.2, 1628.5, 1246.3, 1395.2, 1781.5, 1527.6, 1400.6, 1407.2]
2:RULE 2 (remote exploit of a server program):0
[1926.5, 1545.6, 1931.9, 2192.3, 2578.6, 2197.7, 2071.9, 1689.7, 2458.2, 2076.0, 2077.3, 1695.1, 1844.0, 2230.3, 1976.4, 1849.4, 2496.1, 1473.8, 1856.0, 2375.7, 1993.5, 1628.1, 2274.8, 2147.8, 1893.9, 2280.2, 2154.4, 1772.2, 1773.5, 1391.3, 2159.8, 1777.6]
1:execCode(n65Inter,root):0
Attack cost:
max =2578.6
min =1391.3
aver =1993.425
var =85175.7844
32 ways in total