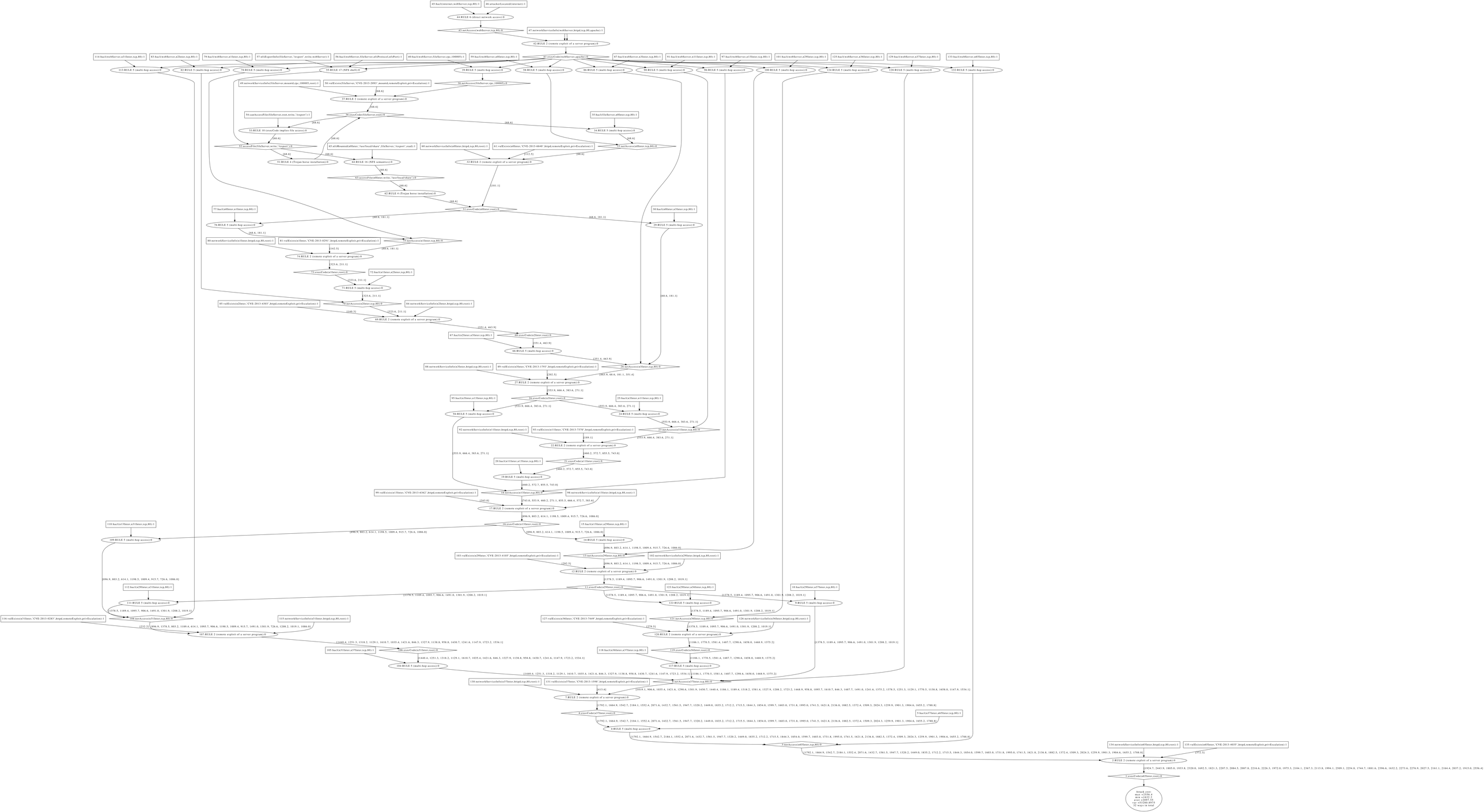
45:hacl1internet,webServer,tcp,80):1
46:attackerLocated(internet):1
44:RULE 6 (direct network access):0
43:netAccess(webServer,tcp,80):0
47:networkServiceInfo(webServer,httpd,tcp,80,apache):1
42:RULE 2 (remote exploit of a server program):0
114:hacl(webServer,a11host,tcp,80):1
83:hacl(webServer,a2host,tcp,80):1
79:hacl(webServer,a1host,tcp,80):1
57:vulExploit(vulFileServer,'export',write,webServer):1
56:hacl(webServer,fileServer,nfsProtocol,nfsPort):1
60:hacl(webServer,fileServer,rpc_100005):1
59:hacl(webServer,a0host,tcp,80):1
41:execCode(webServer,apache):0
87:hacl(webServer,a3host,tcp,80):1
91:hacl(webServer,a11host,tcp,80):1
97:hacl(webServer,a12host,tcp,80):1
101:hacl(webServer,a29host,tcp,80):1
125:hacl(webServer,a36host,tcp,80):1
129:hacl(webServer,a37host,tcp,80):1
133:hacl(webServer,a40host,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
10: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-2015-2093',mountdremoteExploit,privEscalation):1
52:netAccess(fileServer,rpc_100005):0
37:RULE 2 (remote exploit of a server program):0
54:canAccessFile(fileServer,root,write,'/export'):1
36:execCode(fileServer,root):0
55:hacl(fileServer,a0host,tcp,80):1
53:RULE 10 (execCode implies file access):0
54:RULE 5 (multi-hop access):0
63:vulMountedOnHost('/usr/local/share',fileServer,'/export',read):1
61:vulExists(a0host,'CVE-2013-6643',httpd,remoteExploit,privEscalation):1
60:networkServiceInfo(a0host,httpd,tcp,80,root):1
51:RULE 10 (execCode implies file access):0
57:accessFile(fileServer,write,'/export',):0
51:RULE 4 (Trojan horse installation):0
64:RULE 16 (NFS semantics):0
63:accessFile(a0host,write,'/usr/local/share',):0
62:RULE 4 (Trojan horse installation):0
52:netAccess(a0host,tcp,80):0
32:RULE 2 (remote exploit of a server program):0
77:hacl(a0host,a1host,tcp,80):1
76:RULE 5 (multi-hop access):0
31:execCode(a0host,root):0
30:hacl(a0host,a3host,tcp,80):1
29:RULE 5 (multi-hop access):0
80:networkServiceInfo(a1host,httpd,tcp,80,root):1
81:vulExists(a1host,'CVE-2013-6291',httpd,remoteExploit,privEscalation):1
75:netAccess(a1host,tcp,80):0
14:RULE 2 (remote exploit of a server program):0
72:hacl(a1host,a2host,tcp,80):1
73:execCode(a1host,root):0
71:RULE 5 (multi-hop access):0
85:vulExists(a2host,'CVE-2013-4503',httpd,remoteExploit,privEscalation):1
70:netAccess(a2host,tcp,80):0
84:networkServiceInfo(a2host,httpd,tcp,80,root):1
69:RULE 2 (remote exploit of a server program):0
67:hacl(a2host,a3host,tcp,80):1
68:execCode(a2host,root):0
66:RULE 5 (multi-hop access):0
88:networkServiceInfo(a3host,httpd,tcp,80,root):1
89:vulExists(a3host,'CVE-2013-1795',httpd,remoteExploit,privEscalation):1
26:netAccess(a3host,tcp,80):0
27:RULE 2 (remote exploit of a server program):0
65:hacl(a3host,a1host,tcp,80):1
94:RULE 5 (multi-hop access):0
25:hacl(a3host,a11host,tcp,80):1
24:RULE 5 (multi-hop access):0
92:networkServiceInfo(a11host,httpd,tcp,80,root):1
93:vulExists(a11host,'CVE-2013-7359',httpd,remoteExploit,privEscalation):1
23:netAccess(a11host,tcp,80):0
22:RULE 2 (remote exploit of a server program):0
20:hacl(a11host,a13host,tcp,80):1
21:execCode(a11host,root):0
19:RULE 5 (multi-hop access):0
99:vulExists(a13host,'CVE-2013-6362',httpd,remoteExploit,privEscalation):1
18:netAccess(a13host,tcp,80):0
98:networkServiceInfo(a13host,httpd,tcp,80,root):1
17:RULE 2 (remote exploit of a server program):0
110:hacl(a13host,a31host,tcp,80):1
16:execCode(a13host,root):0
15:hacl(a13host,a29host,tcp,80):1
109:RULE 5 (multi-hop access):0
14:RULE 5 (multi-hop access):0
103:vulExists(a29host,'CVE-2013-4105',httpd,remoteExploit,privEscalation):1
13:netAccess(a29host,tcp,80):0
102:networkServiceInfo(a29host,httpd,tcp,80,root):1
12:RULE 2 (remote exploit of a server program):0
112:hacl(a29host,a31host,tcp,80):1
11:execCode(a29host,root):0
123:hacl(a29host,a36host,tcp,80):1
10:hacl(a29host,a37host,tcp,80):1
111:RULE 5 (multi-hop access):0
122:RULE 5 (multi-hop access):0
9:RULE 5 (multi-hop access):0
116:vulExists(a31host,'CVE-2013-0263',httpd,remoteExploit,privEscalation):1
108:netAccess(a31host,tcp,80):0
115:networkServiceInfo(a31host,httpd,tcp,80,root):1
127:vulExists(a36host,'CVE-2013-7449',httpd,remoteExploit,privEscalation):1
121:netAccess(a36host,tcp,80):0
126:networkServiceInfo(a36host,httpd,tcp,80,root):1
107:RULE 2 (remote exploit of a server program):0
126:RULE 2 (remote exploit of a server program):0
105:hacl(a31host,a37host,tcp,80):1
106:execCode(a31host,root):0
118:hacl(a36host,a37host,tcp,80):1
119:execCode(a36host,root):0
104:RULE 5 (multi-hop access):0
117:RULE 5 (multi-hop access):0
130:networkServiceInfo(a37host,httpd,tcp,80,root):1
131:vulExists(a37host,'CVE-2013-3598',httpd,remoteExploit,privEscalation):1
8:netAccess(a37host,tcp,80):0
7:RULE 2 (remote exploit of a server program):0
5:hacl(a37host,a40host,tcp,80):1
6:execCode(a37host,root):0
4:RULE 5 (multi-hop access):0
3:netAccess(a40host,tcp,80):0
134:networkServiceInfo(a40host,httpd,tcp,80,root):1
135:vulExists(a40host,'CVE-2013-4035',httpd,remoteExploit,privEscalation):1
2:RULE 2 (remote exploit of a server program):0
1:execCode(a40host,root):0
Attack goal
mca =1.0e-4
mca =1522.2
scr =2097.35
mca =2097.35
32 ways in total