43:fileAttr(victimHost,'/home/victimAccount/3aka3.doc',-,r,w,x,-,-,-,-,-,-):1
42:RULE 91 (BB - owner file access):0
41:ownerAccessible(victimHost,exec,'/home/victimAccount/3aka3.doc'):0
44:fileOwner(victimHost,victimAccount,'/home/victimAccount/3aka3.doc'):1
40:RULE 82 (BB - owner file access):0
47:hasAccount(victimUser,victimHost,victimAccount):1
39:localFileProtection(victimHost,victimAccount,exec,'/home/victimAccount/3aka3.doc'):0
46:RULE 80 (BB - A User can execute code using his account on a specific host):0
38:RULE 81 (BB - A legitimate account can access file):0
45:execCode(victimUser,victimHost,victimAccount):0
37:canAccessFile(victimHost,victimAccount,exec,'/home/victimAccount/3aka3.doc'):0
50:isNetScript(victimHost,pupyC2Server,reversePupy,http,1234,pupyPayload):1
51:dataBind(victimHost,'/home/victimAccount/3aka3.doc',pupyPayload):1
52:aclNW(victimHost,pupyC2Server,http,1234):1
36:RULE 79 (BB - execCode implies file access):0
49:RULE 73 (BB - Direct script network access - Existing Script):0
34:networkServiceInfo(pupyC2Server,root,pupyd,http,1234):1
35:accessFile(victimUser,victimHost,exec,'/home/victimAccount/3aka3.doc'):0
48:scriptNetAccess(victimHost,pupyC2Server,'/home/victimAccount/3aka3.doc',reversePupy,http,1234):0
33:RULE 72 (BB - Script access an exposed service):0
32:canScriptAccessHost(victimHost,pupyC2Server,'/home/victimAccount/3aka3.doc',reversePupy,http,1234):0
31:RULE 70 (BB - Flow associated port and protocol):0
54:RULE 71 (BB - Data flow initiated by script):0
15:fileAttr(victimHost,'/bin',d,r,w,x,r,-,x,r,-,x):1
14:RULE 88 (BB - owner file access):0
24:RULE 91 (BB - owner file access):0
13:ownerAccessible(victimHost,write,'/bin'):0
16:fileOwner(victimHost,root,'/bin'):1
23:ownerAccessible(victimHost,exec,'/bin'):0
12:RULE 82 (BB - owner file access):0
22:RULE 82 (BB - owner file access):0
21:localFileProtection(victimHost,root,exec,'/bin'):0
11:localFileProtection(victimHost,root,write,'/bin'):0
20:RULE 81 (BB - A legitimate account can access file):0
19:canAccessFile(victimHost,root,exec,'/bin'):0
10:RULE 81 (BB - A legitimate account can access file):0
9:canAccessFile(victimHost,root,write,'/bin'):0
101:fileAttr(victimHost,'/bin/ps',-,r,w,x,-,-,-,r,w,x):1
100:RULE 91 (BB - owner file access):0
102:fileOwner(victimHost,root,'/bin/ps'):1
99:ownerAccessible(victimHost,exec,'/bin/ps'):0
98:RULE 82 (BB - owner file access):0
97:localFileProtection(victimHost,root,exec,'/bin/ps'):0
96:RULE 81 (BB - A legitimate account can access file):0
95:canAccessFile(victimHost,root,exec,'/bin/ps'):0
74:fileAttr(victimHost,'/bin/certutil',-,r,w,x,-,-,-,r,w,x):1
73:RULE 91 (BB - owner file access):0
75:fileOwner(victimHost,root,'/bin/certutil'):1
72:ownerAccessible(victimHost,exec,'/bin/certutil'):0
71:RULE 82 (BB - owner file access):0
70:localFileProtection(victimHost,root,exec,'/bin/certutil'):0
69:RULE 81 (BB - A legitimate account can access file):0
68:canAccessFile(victimHost,root,exec,'/bin/certutil'):0
65:fileAttr(victimHost,'/bin/cat',-,r,w,x,-,-,-,r,w,x):1
64:RULE 91 (BB - owner file access):0
66:fileOwner(victimHost,root,'/bin/cat'):1
63:ownerAccessible(victimHost,exec,'/bin/cat'):0
62:RULE 82 (BB - owner file access):0
61:localFileProtection(victimHost,root,exec,'/bin/cat'):0
60:RULE 81 (BB - A legitimate account can access file):0
59:canAccessFile(victimHost,root,exec,'/bin/cat'):0
30:flowBind(reversePupy,http,1234):0
29:isReverseShell(victimHost,pupyC2Server,'/home/victimAccount/3aka3.doc'):1
53:dataFlow(victimHost,pupyC2Server,reversePupy,_):0
28:RULE 67 (BB - Reverse shell data flow):0
27:dataFlowReverseShell(reversePupy):0
26:RULE 66 (BB - The remote root user has write access to the dataFlow):0
25:accessDataFlow(attacker,write,reversePupy):0
57:located(attacker,pupyC2Server):1
56:RULE 99 (BB - An user who is located in a host has root access to that host):0
55:localAccess(attacker,pupyC2Server,root):0
128:fileAttr(victimHost,'/bin/zip',-,r,w,x,-,-,-,r,w,x):1
127:RULE 91 (BB - owner file access):0
129:fileOwner(victimHost,root,'/bin/zip'):1
126:ownerAccessible(victimHost,exec,'/bin/zip'):0
125:RULE 82 (BB - owner file access):0
124:localFileProtection(victimHost,root,exec,'/bin/zip'):0
123:RULE 81 (BB - A legitimate account can access file):0
122:canAccessFile(victimHost,root,exec,'/bin/zip'):0
110:fileAttr(victimHost,'/bin/rm',-,r,w,x,-,-,-,r,w,x):1
109:RULE 91 (BB - owner file access):0
111:fileOwner(victimHost,root,'/bin/rm'):1
108:ownerAccessible(victimHost,exec,'/bin/rm'):0
107:RULE 82 (BB - owner file access):0
106:localFileProtection(victimHost,root,exec,'/bin/rm'):0
105:RULE 81 (BB - A legitimate account can access file):0
104:canAccessFile(victimHost,root,exec,'/bin/rm'):0
119:fileAttr(victimHost,'/bin/tcpdump',-,r,w,x,-,-,-,r,w,x):1
118:RULE 91 (BB - owner file access):0
120:fileOwner(victimHost,root,'/bin/tcpdump'):1
117:ownerAccessible(victimHost,exec,'/bin/tcpdump'):0
116:RULE 82 (BB - owner file access):0
115:localFileProtection(victimHost,root,exec,'/bin/tcpdump'):0
114:RULE 81 (BB - A legitimate account can access file):0
113:canAccessFile(victimHost,root,exec,'/bin/tcpdump'):0
92:fileAttr(victimHost,'/bin/ls',-,r,w,x,-,-,-,r,w,x):1
91:RULE 91 (BB - owner file access):0
90:ownerAccessible(victimHost,exec,'/bin/ls'):0
93:fileOwner(victimHost,root,'/bin/ls'):1
89:RULE 82 (BB - owner file access):0
88:localFileProtection(victimHost,root,exec,'/bin/ls'):0
87:RULE 81 (BB - A legitimate account can access file):0
86:canAccessFile(victimHost,root,exec,'/bin/ls'):0
83:fileAttr(victimHost,'/bin/find',-,r,w,x,-,-,-,r,w,x):1
82:RULE 91 (BB - owner file access):0
84:fileOwner(victimHost,root,'/bin/find'):1
81:ownerAccessible(victimHost,exec,'/bin/find'):0
80:RULE 82 (BB - owner file access):0
79:localFileProtection(victimHost,root,exec,'/bin/find'):0
78:RULE 81 (BB - A legitimate account can access file):0
77:canAccessFile(victimHost,root,exec,'/bin/find'):0
18:RULE 65 (BB - User is able to use a reverse shell):0
94:RULE 65 (BB - User is able to use a reverse shell):0
67:RULE 65 (BB - User is able to use a reverse shell):0
58:RULE 65 (BB - User is able to use a reverse shell):0
121:RULE 65 (BB - User is able to use a reverse shell):0
103:RULE 65 (BB - User is able to use a reverse shell):0
112:RULE 65 (BB - User is able to use a reverse shell):0
85:RULE 65 (BB - User is able to use a reverse shell):0
76:RULE 65 (BB - User is able to use a reverse shell):0
17:execCode(attacker,victimHost,root):0
8:RULE 79 (BB - execCode implies file access):0
7:accessFile(attacker,victimHost,write,'/bin'):0
130:dataBindDir(victimHost,'/bin',deletionUtil):1
131:dataBind(victimHost,'/bin/rm',deletionUtil):1
132:isDeletionUtil(rm):1
133:malicious(attacker):1
6:RULE 2 (T1070.004 - Indicator Removal on Host - File Deletion):0
5:indicatorRemovalOnHostFileDeletion(attacker,victimHost,deletionUtil):0
4:RULE 1 (T1070 - Indicator Removal on Host):0
3:indicatorRemovalOnHost(attacker,victimHost,deletionUtil):0
2:RULE 7 (Asset - Able to remove generated artifacts on host):0
1:canRemoveArtifacts(attacker,victimHost,deletionUtil):0