## Attack Graph for small\_enterprise model 17:hacl(internet,webServer,tcp,80):1 18:attackerLocated(internet):1 16:RULE 6 (direct network access):0 15:netAccess(webServer,tcp,80):0 19:networkServiceInfo(webServer,httpd,tcp,80,apache):1 20:vulExists(webServer,'CAN-2002-0392',httpd,remoteExploit,privEscalation):1 14:RULE 2 (remote exploit of a server program):0 12:hacl(webServer,fileServer,rpc,100005):1 13:execCode(webServer,apache):0 24:hacl(webServer,fileServer,nfsProtocol,nfsPort):1 25:nfsExportInfo(fileServer,'/export',write,webServer):1 23:RULE 17 (NFS shell):0 11:RULE 5 (multi-hop access):0 10:netAccess(fileServer,rpc,100005):0 21:networkServiceInfo(fileServer,mountd,rpc,100005,root):1 22:vulExists(fileServer,vulID,mountd,remoteExploit,privEscalation):1 9:RULE 2 (remote exploit of a server program):0 7:canAccessFile(fileServer,root,write,'/export'):1 8:execCode(fileServer,root):0 6:RULE 10 (execCode implies file access):0 26:nfsMounted(workStation,'/usr/local/share',fileServer,'/export',read):1 5:accessFile(fileServer,write,'/export'):0 4:RULE 16 (NFS semantics):0 3:accessFile(workStation,write,'/usr/local/share'):0 2:RULE 4 (Trojan horse installation):0

1:execCode(workStation,root):0