Cấu trúc của knowledge base

<knowledgeBase>

<Predicates>

<Predicate Name="DoSServUFTP">

<Arg id="895" Pos="1" Attr="varchar(15)"></Arg>

<Arg id="896" Pos="2" Attr="int"></Arg>

</Predicate>

</Predicates>

------------------------------------------------------------------------------

<Implications>

<Implication>

<ImplyingName>RootAccess</ImplyingName>

<ImpliedName>Access</ImpliedName>

<ArgMap>

<ImplyingArg id="6"></ImplyingArg>

<ImpliedArg id="15"></ImpliedArg>

</ArgMap>

</Implication>

</Implications>

--------------------------------------------------------------------------------

<HyperAlertTypes>

<HyperAlertType Name="BLEEDING-EDGE SCAN NMAP -sA">

<Fact FactName="SrcIPAddress" FactType="varchar(15)"></Fact>

<Fact FactName="SrcPort" FactType="int"></Fact>

<Fact FactName="DestIPAddress" FactType="varchar(15)"></Fact>

<Fact FactName="DestPort" FactType="int"></Fact>

<Protocol ProtocolName="TCP"></Protocol>

<Consequence>

<Predicate Name="FixedService">

<Arg id="102" ArgName="DestIPAddress"></Arg>

<Arg id="103" ArgName="DestPort"></Arg>

</Predicate>

</Consequence>

</HyperAlertType>

</HyperAlertTypes>

</knowledgeBase>

Hyper-alert type bao gồm fact, prerequisite, consequence. Các hyper alert được dùng làm input cho các analysis utility. Các utility bao gồm 2 loại: hyper-alert generating utility (aggregation/disaggregation, clustering analysis, focused analysis, missed attack hypotheses) và feature extraction utility (frequency analysis, link analysis, association analysis, attack strategy extraction)

Focused Analysis: dùng để lọc alert dựa vào các constraint qui định sẵn (knowledge base). ????

Clustering analysis: dùng để lựa chọn các hyper-alert thành các group, các group này có những đặc điểm giống nhau.

Aggregation/disaggregation: dựa vào time interval constraint để gộp các hyper-alert lại, người ta cũng có thể tách các hyper-alert đã được gộp lại để thu thập thêm thông tin.

Link analysis: phân tích sự liên hệ 2 chiều giữa các giá trị trong thuộc tính của các hyper alert.

Association analysis: tìm kiếm tần số xuất hiện của các giá trị trong attribute của alert.

Attack strategy extraction: tìm kiếm tấn công từ correlation graph (directed graph), trong đó mỗi node là một hyper-alert type.

Miss attack hypotheses.

