Universidade Federal do Rio Grande do Norte
Instituto Metrópole Digital

MANUAL DO USUÁRIO- INSIDER THREAT

Este manual foi elaborado por:
Sara Paloma de Souza
Thais Fernandes Lins

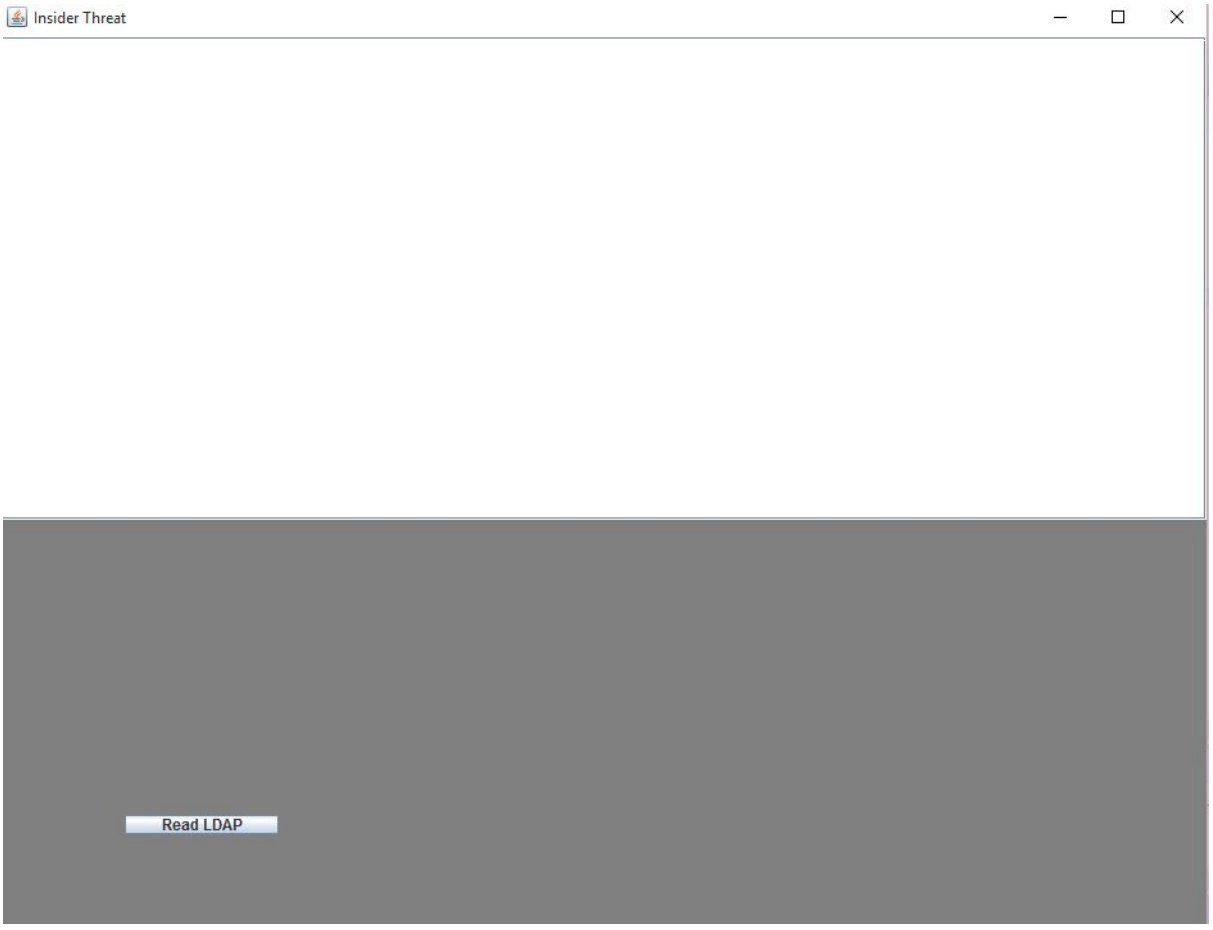
Índice Geral:

1- Acessando o sistema

Para acessar o sistema deve-se seguir as orientações colocadas no arquivo READ.txt.

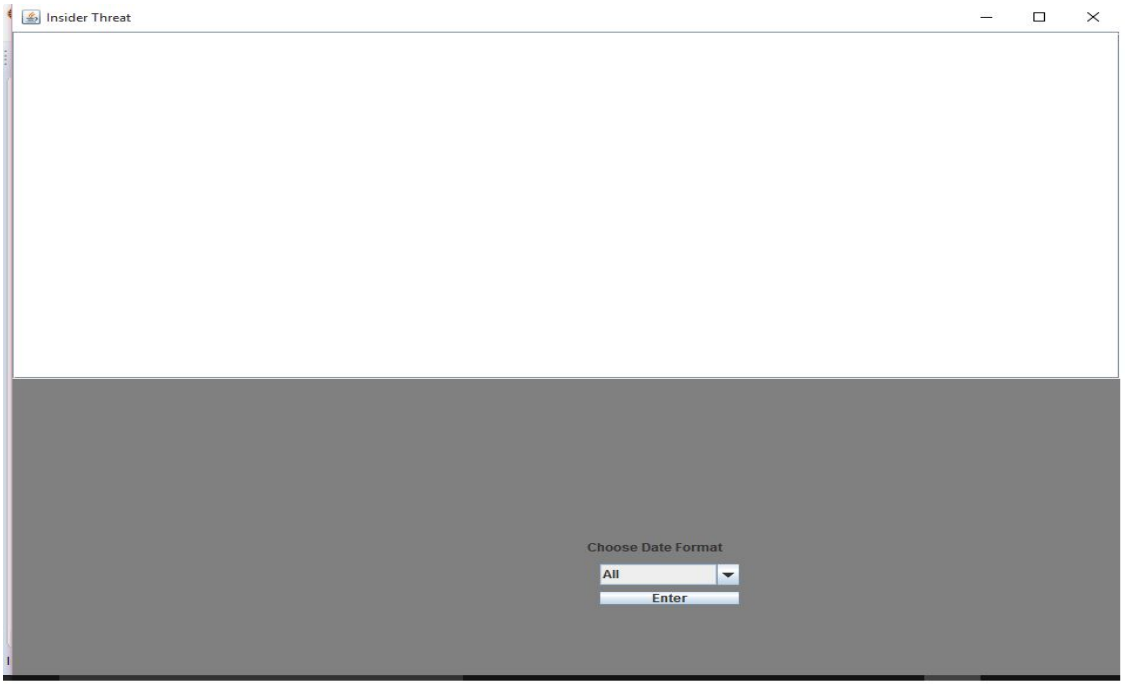
2- Tela inicial

Após seguir as recomendações e o programa estiver devidamente inicializado, aparecerá essa tela:

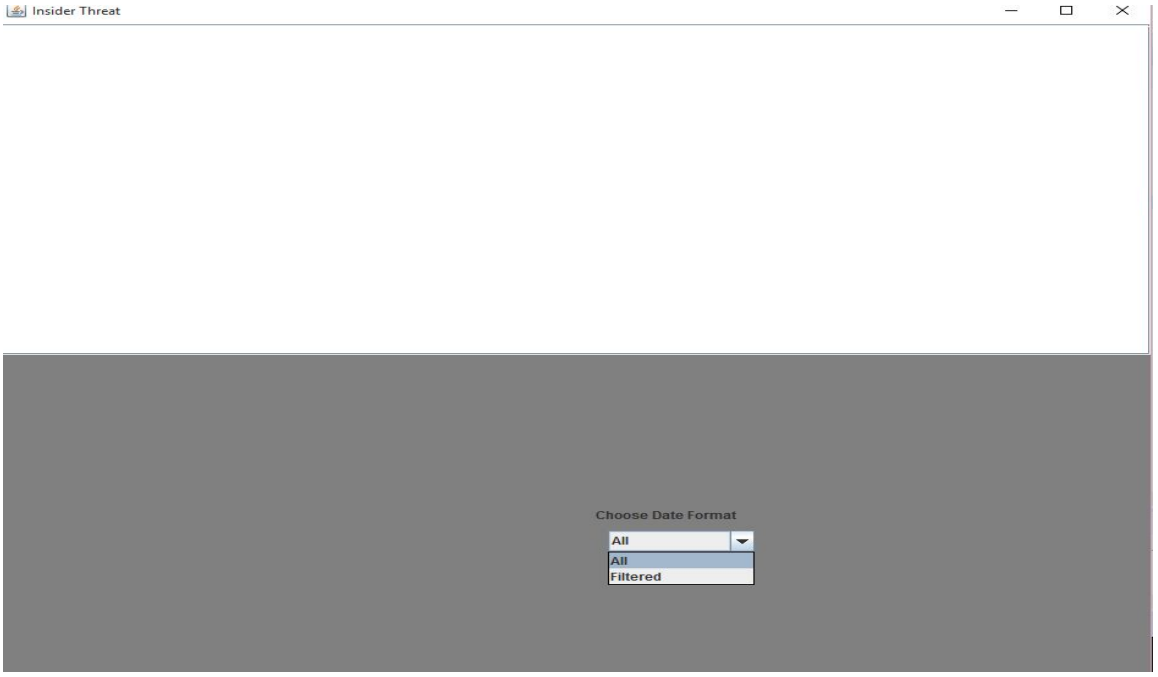


3- Leitura dos arquivos

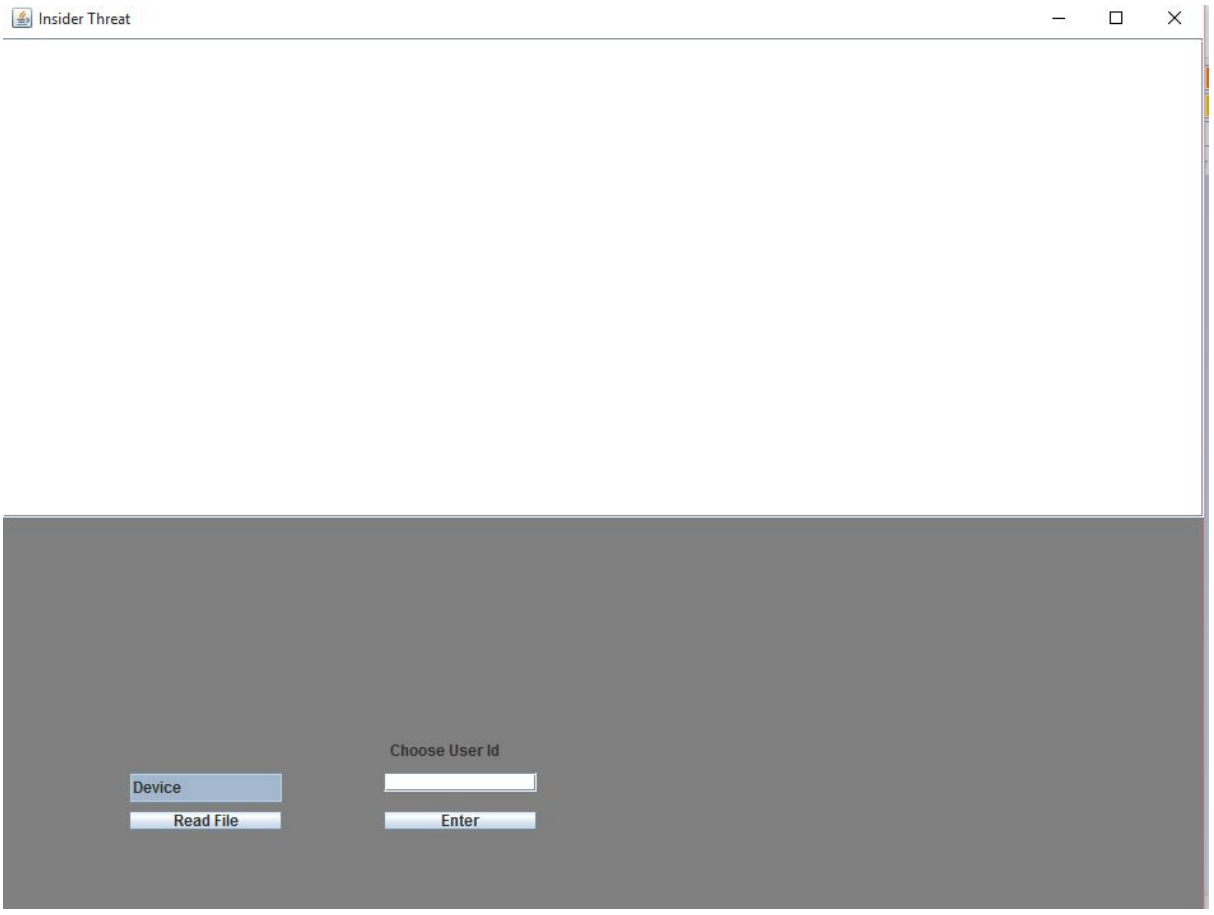
O botão **Read LDAP** é para a leitura do arquivo que contém as informações dos usuários, a qual é o primeiro passo para o funcionamento do programa, ao clicar nele irá aparecer a seguinte tela:



O campo “Choose Date Format” é para escolher o modo como a árvore será mostrada para o usuário, a qual pode ser de 2 formas, a primeira mostra todas as datas passadas em que o usuário realizou uma atividade e nesse caso pode-se ler cada arquivo de uma vez, essa opção é a **All**, que está sendo mostrada acima, a segunda opção é mostrar a árvore com os dados filtrados por um período de tempo definido, tal opção se chama **Filtered** , como mostra a imagem abaixo:

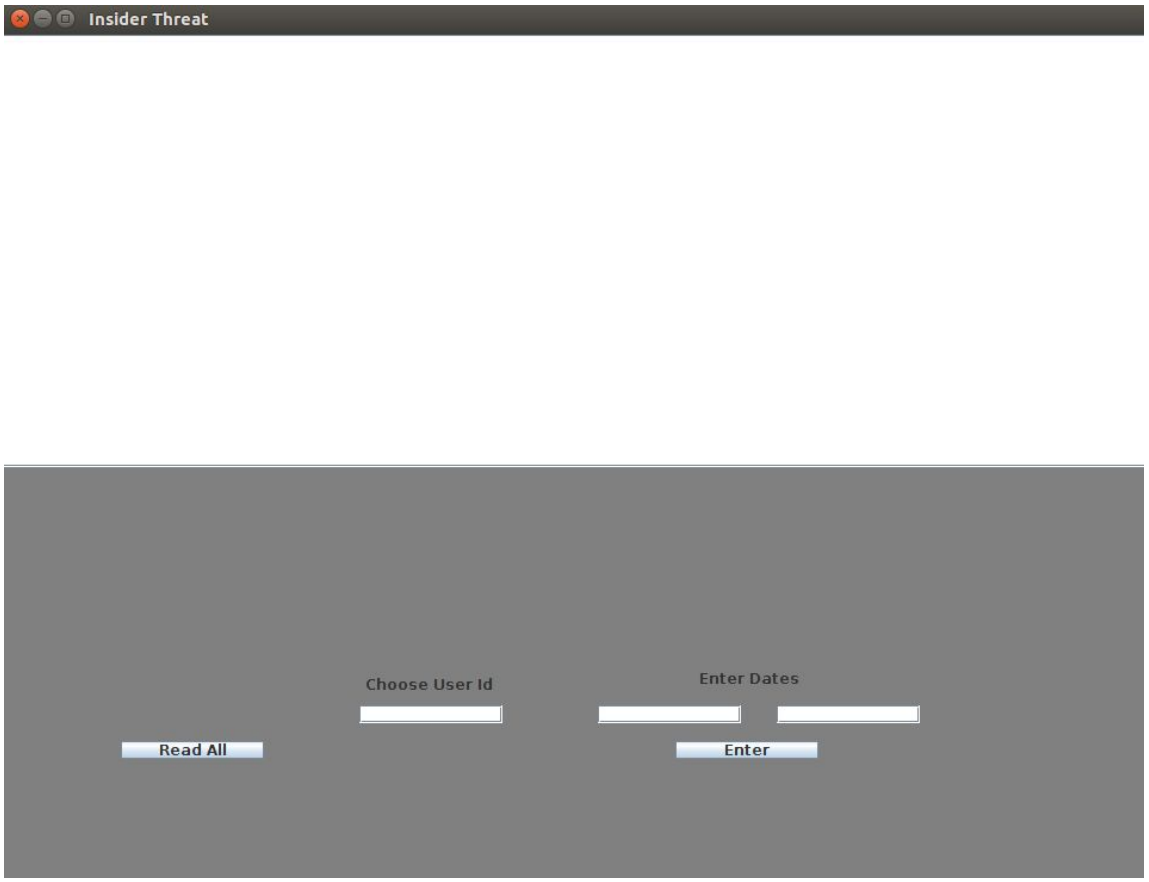


3.1- Ao escolher a opção **All** e clicar no botão **Enter** o usuário será redirecionado para está tela:



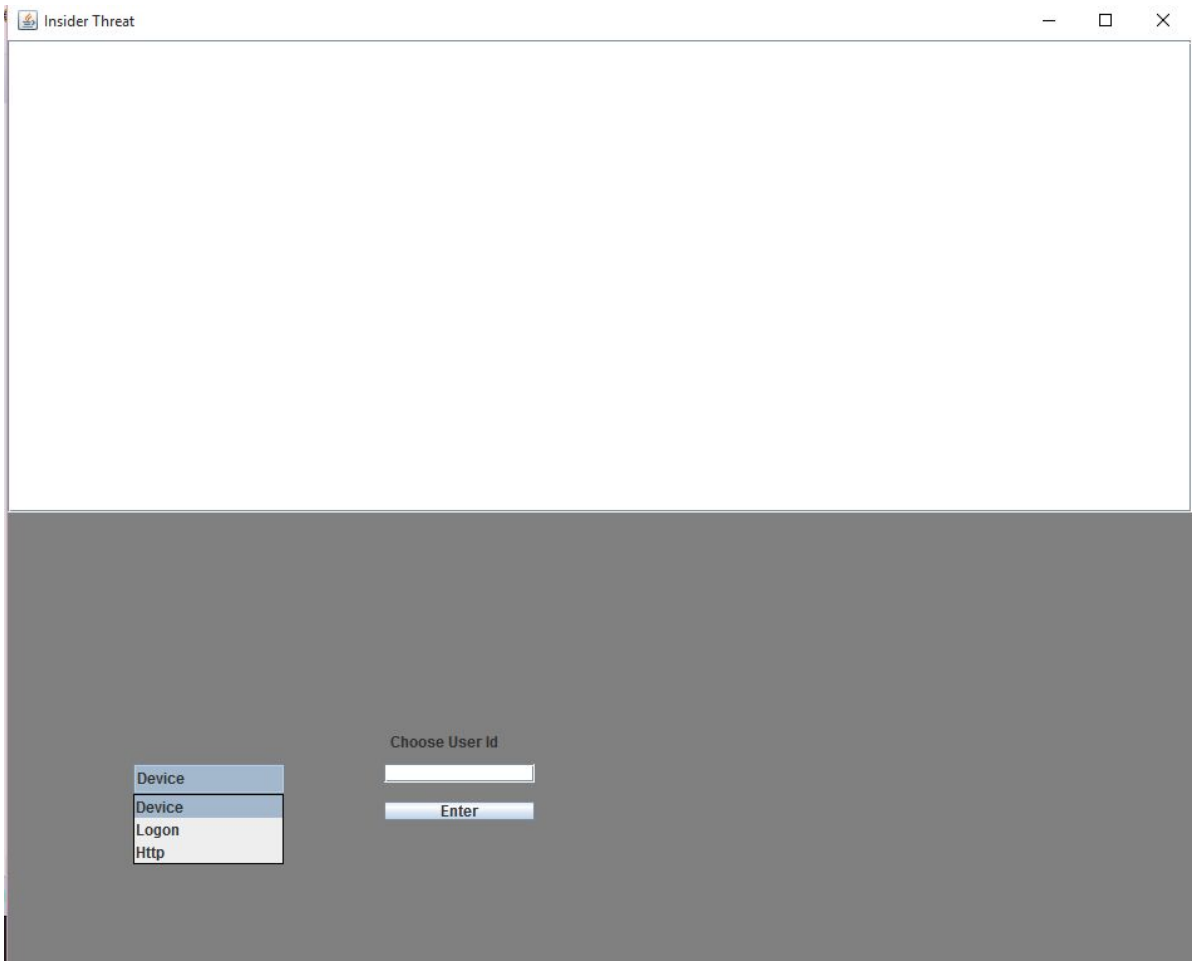
Na tela acima aparece um combobox azul no lado esquerdo para escolher o tipo de arquivo que será lido, neste campo deve-se clicar em cima do campo azul, escolher o tipo de arquivo que se deseja ler, clicar no nome, e após isso clicar no botão **Read File** e o arquivo desejado será lido**.**

3.2 - Ao escolher a opção **Filtered** o usuário será redirecionado para a seguinte tela:



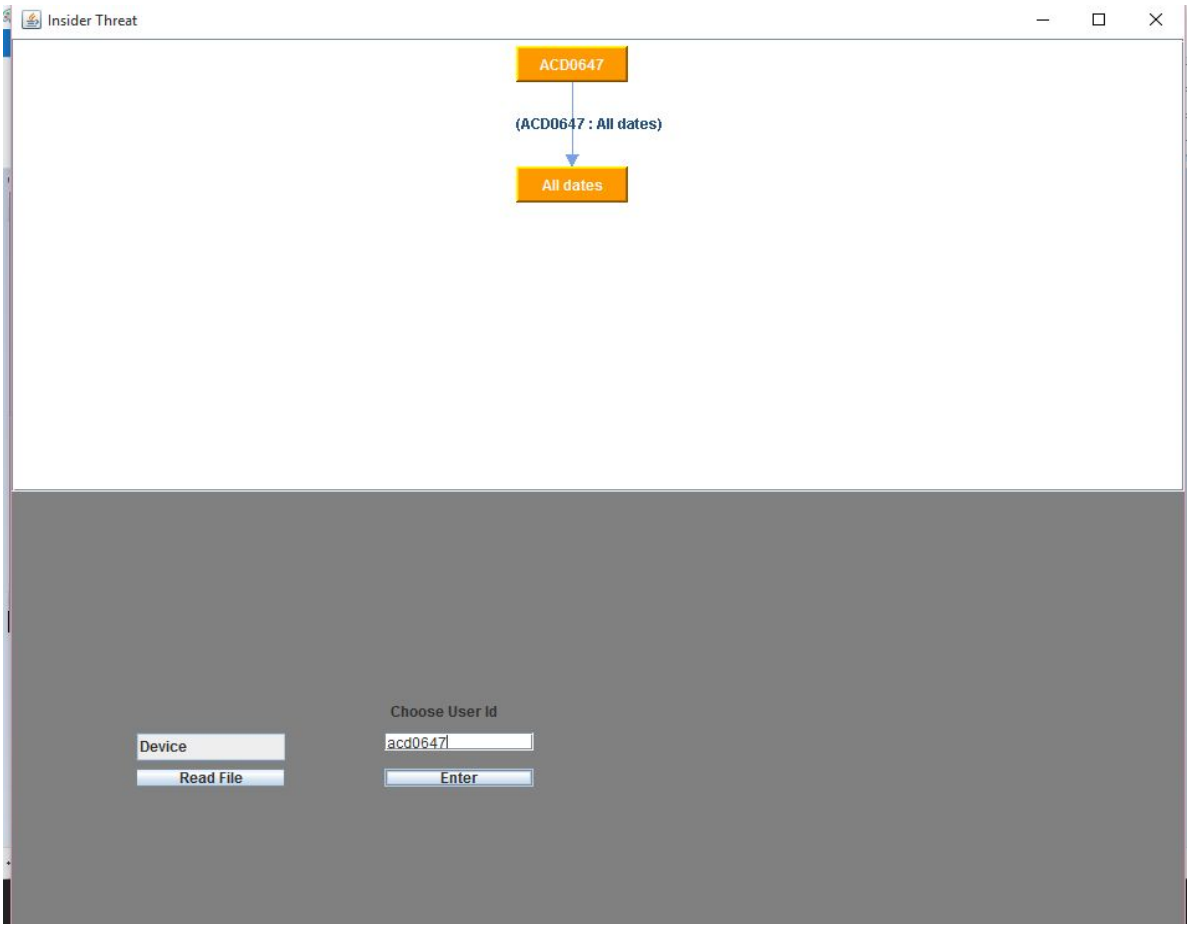
Na tela acima deve-se primeiramente clicar no botão **Read All** para ler todos os arquivos restantes, pois a árvore só será gerada com a filtragem de dados de acordo com um período de tempo específico, se as leituras de todos os arquivos tiverem sido realizadas. Segundamente, insere-se um id de usuário no campo de texto abaixo de “Choose User Id” e insere-se uma data inicial no primeiro campo abaixo de “Enter Dates” e uma data final no segundo campo abaixo de “Enter Dates”, a partir disso ao clicar no **Enter** abaixo dos campos das datas, gera-se uma árvore em que as datas das atividades realizadas pelo usuário são filtradas de acordo com o período de tempo escolhido.

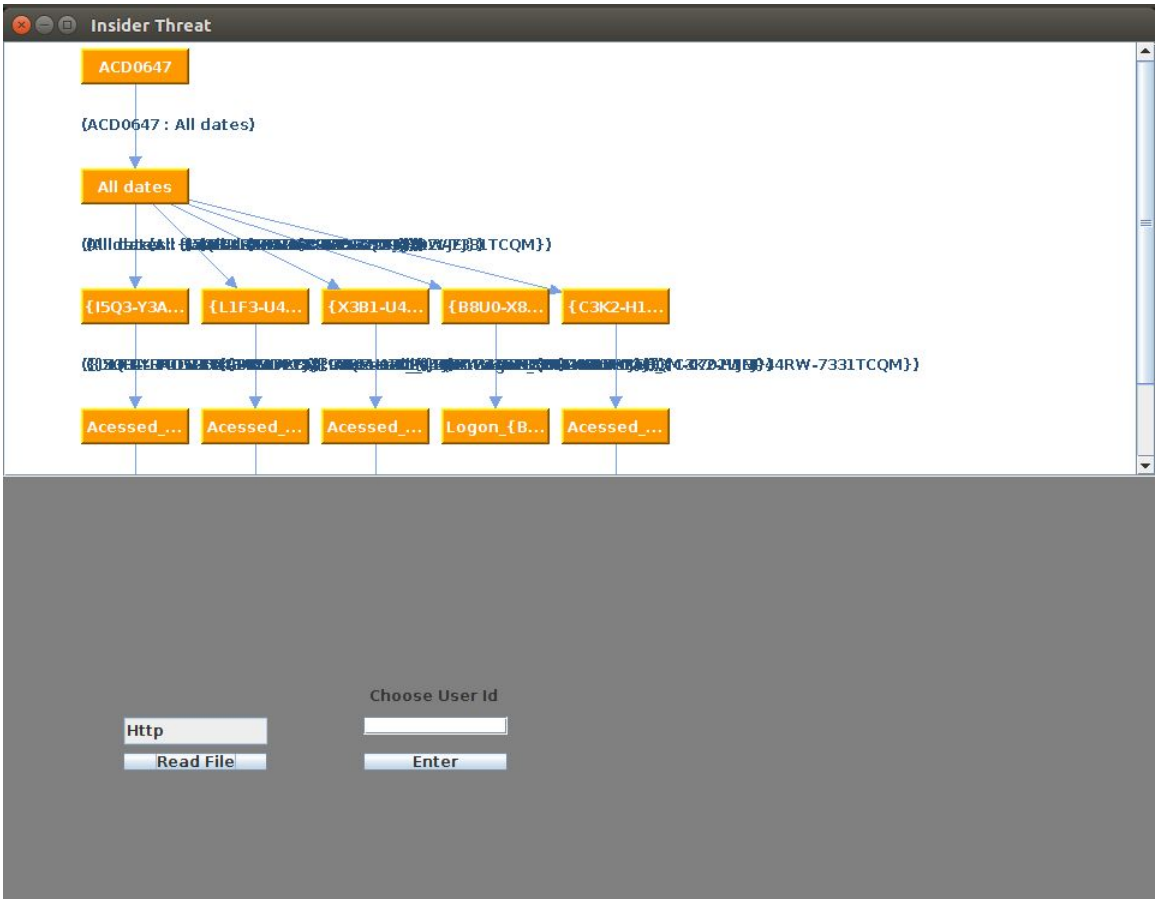
4- Visualizar perfil de um determinado usuário



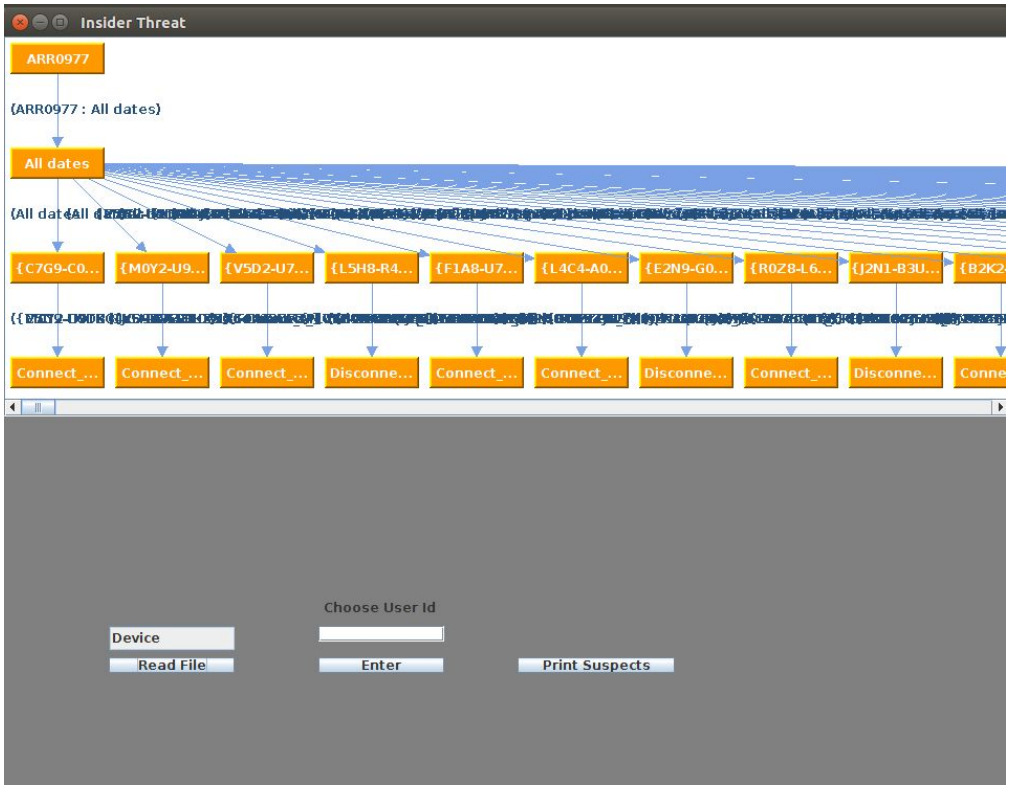
Ao explicar a leitura dos arquivos no programa previamente, já se explicou uma maneira de gerar e visualizar a árvore de perfil de usuário .

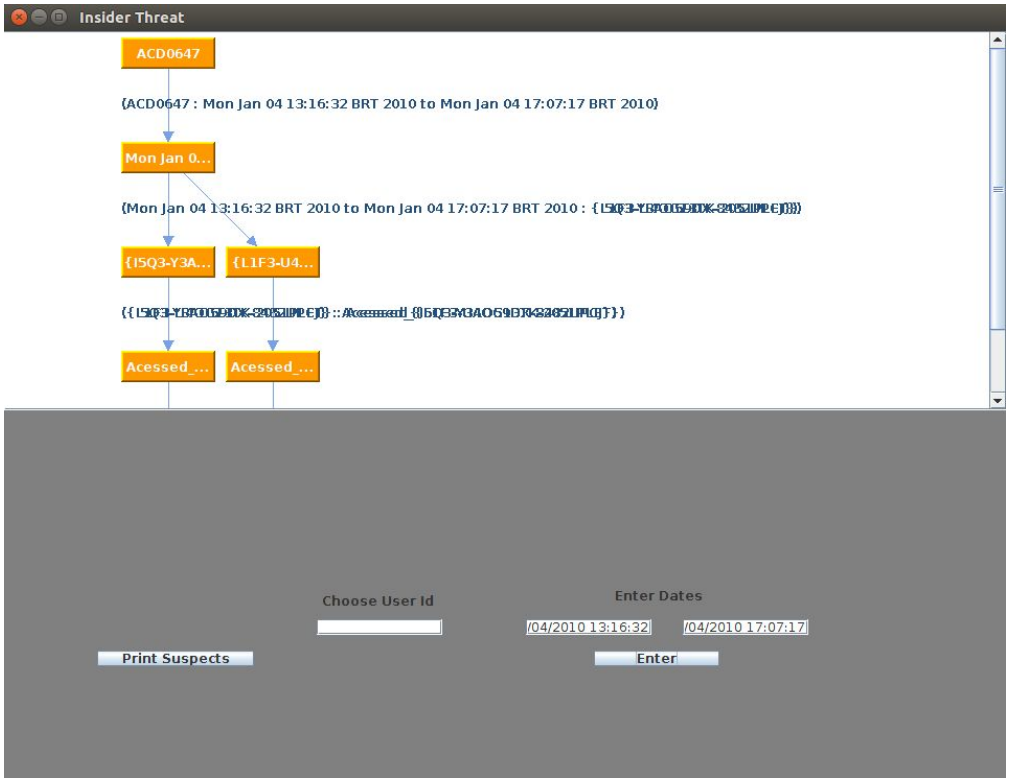
Outro modo que pode-se gerar uma árvore é após escolher a opção **All** no campo “Choose Date Format”. Ao ler-se o arquivo LDAP, já é possível gerar uma árvore contendo somente as informações do perfil de usuário selecionado sem que hajam atividades relacionadas a esse perfil. Para fazer a busca de um usuário pelo id, deve-se usar o campo “Choose User Id”, no campo de texto deve-se escrever o id do usuário desejado, e clicar no botão **Enter** após isso os dados do usuário serão mostrados, em forma de uma árvore. Caso o perfil procurado não exista, aparece uma mensagem no console do Eclipse avisando que o usuário não foi encontrado (“User Not Found”). A cada nova leitura de arquivo (caso todos não tenham sido lidos antes de se inserir o id do usuário) a árvore será atualizada com novas informações.


Insider Threat
ACD0647
(ACD0647 : All dates)
All dates
Choose User Id
Device
acd0647
Read File
Enter


Insider Threat
ACD0647
(ACD0647 : All dates)
All dates
{I5Q3-Y3A...
{L1F3-U4...
{X3B1-U4...
{B8U0-X8...
{C3K2-H1...
Acessed_...
Acessed_...
Acessed_...
Logon_{B...
Acessed_...
Choose User Id
Http
Read File
Enter

5- Detecção de usuários anômalos





Qualquer que seja a escolha de data, após a leitura dos arquivos “Device”,”Logon” e “Http”, pode-se imprimir os usuários que são considerados ameaças internas pelo sistema para um arquivo “threats.txt” que ficará localizado na pasta “logs”, para fazer isso é preciso clicar o botão “**Print Suspects”,**.

6- Salvar o resultado do processamento em arquivo

O resultado do processamento do perfil é salvo automaticamente em um arquivo na pasta “users” no momento em que o usuário insere o id para gerar a árvore de um determinado perfil, o arquivo resultante terá como nome id do usuário escolhido.