Manual do operador: Representando comportamento de usuários para detecção de ameaças internas

Felipe Tiberio Maciel Barbosa[1], Matheus Allan de Oliveira[1]

[1]Instituto Metrópole Digital – Universidade Federal do Rio Grande do Norte (UFRN)
Natal – RN – Brasil

felipetiberio@yahoo.com.br, matheusrpd@ufrn.edu.br

Este é um manual de operador para o sistema desenvolvida no projeto de disciplina Representando comportamento de usuários para detecção de ameaças internas(Inside Threat Project), na disciplina IMD0040 - Linguagem de Programação II. Visando a melhor utilização possível do sistema, pedimos que siga todas as instruções corretamente. Utilizamos para o desenvolvimento a IDE Eclipse, seria recomendado que fosse utilizada a mesma para a sua execução.

1. Abrir projeto no Eclipse

Ao abrir o Eclipse, clique na opção 'File' do menu e clique em 'Open Projects from file System…' , após abrir uma nova tela encontre a na aba 'Import source' o botão 'Directory'. Com isso você terá acesso aos diretórios do seu computador, vá até a pasta do projeto e selecione a pasta **InsideThreat.** Com isso voltará para tela anterior, basta clicar em 'Finish" e você terá o sistema aberto como projeto no Eclipse.

2. Adicionar os arquivos de logs

O sistema está feito para executar alguns arquivos do formato .csv, que armazenam os dados necessários para o tratamento de informações. Como são arquivos grandes, os sistemas de armazenamento do projeto, GitHub, e o sistema da UFRN, Sigaa, para envio do projeto não conseguem fazer uploads desses arquivos. Com isso, pedimos que baixem os arquivos, seguindo o link logo abaixo, e os coloquem na pasta **Data** dentro da pasta **InsiderThreat.**

Obs.: os arquivos necessários são os LDAP.csv, logon.csv, device.csv e http.csv

Link dos arquivos:
https://www.dropbox.com/sh/vaxjhh5w7qkj477/AAAnpwW7yH9qSa4XmChQnmBfa?dl=0&lst=

Atenção: os arquivos não pode ter seus nomes alterados, como também não estarem em outra pasta além da que foi instruída acima.

3. Execução do sistema

Após a realização dos passos anteriores, basta clicar sobre o projeto que está sendo representado pelo nome **InsideThreat [InsideThreat-Project master]** na aba 'Package Explorer' do Eclipse. Tendo clicado sobre o projeto como descrito acima, clique no botão do submenu acima do Eclipse verde com um símbolo de player com o nome de 'Run Debug'. Com isso, abrirá a aba 'Console' do Eclipse e você verá a mensagem de que está lendo o

arquivo LDAP.csv que trata-se dos usuários, logo após verá uma mensagem com a quantidade de usuários cadastrados e um menu com as opções disponíveis no sistema. Com as seguintes funcionalidades:

1. **Criar atividades de logon:** Essa opção fará a criação das atividades de logon de acordo com o arquivo logon.csv, essa opção irá criar todas as atividades disponibilizadas no arquivo;
2. **Criar atividades de devices:** Essa opção fará a criação das atividades de device de acordo com o arquivo device.csv, essa opção irá criar todas as atividades disponibilizadas no arquivo;
3. **Criar atividades de http:** Essa opção fará a criação das atividades de http de acordo com o arquivo http.csv, essa opção irá criar todas as atividades disponibilizadas no arquivo;
4. **Criar atividades de logon em um período específico:** Essa opção fará a criação das atividades de logon de acordo com o arquivo logon.csv, essa opção irá criar as atividades que esteja dentro do prazo determinado pelo o operador, para isso quando aparecer "Digite a data inicial:" coloque a data no formato mm/dd/aaaa e quando aparecer "Digite a data final:" faça o mesmo;

   Obs.: a data é no formato mm/dd/aaaa, por exemplo, a data 01/10/2010 é dia 10 de Janeiro de 2010;

5. **Criar atividades de device em um período específico:** Essa opção fará a criação das atividades de device de acordo com o arquivo device.csv, essa opção irá criar as atividades que esteja dentro do prazo determinado pelo o operador, para isso quando aparecer "Digite a data inicial:" coloque a data no formato mm/dd/aaaa e quando aparecer "Digite a data final:" faça o mesmo;

   Obs.: a data é no formato mm/dd/aaaa, por exemplo, a data 01/10/2010 é dia 10 de Janeiro de 2010;

6. **Criar atividades de http em um período específico:** Essa opção fará a criação das atividades de http de acordo com o arquivo http.csv, essa opção irá criar as atividades que esteja dentro do prazo determinado pelo o operador, para isso quando aparecer "Digite a data inicial:" coloque a data no formato mm/dd/aaaa e quando aparecer "Digite a data final:" faça o mesmo;

   Obs.: a data é no formato mm/dd/aaaa, por exemplo, a data 01/10/2010 é dia 10 de Janeiro de 2010;

7. **Visualizar árvore de um usuário:** Essa opção imprime na tela a árvore de um determinado usuário. Para isso, pedirá o nome do usuário, coloque-o e verá a árvore ser impressa;
8. **Comparar histogramas de dois usuários:** Essa opção fará a comparação de dois usuários, com isso será impresso o histograma de cada um dos dois. Para que isso ocorra, você terá que colocar o nome dos dois usuários quando for solicitado;
9. **Salvar árvore de todos usuários em arquivos:** Essa opção irá salvar em arquivos as árvores de cada um usuário no sistema, os arquivos irão para pasta **DB** dentro de **InsideThreat.** O nome de cada arquivo será o id dos usuários;

10. **Salvar árvore de um usuário em arquivo:** Essa opção irá salvar a árvore de um usuário em um arquivo, o arquivo irá para pasta **DB** dentro de **InsideThreat.** O nome do arquivo será o id do usuário. Para isso, você terá que colocar o nome do usuário que deseja salvar quando for solicitado;
11. **Verificar se o usuário é uma anomalia:** Essa opção verifica se um determinado usuário é anomalia no sistema, em comparação com o perfil médio do seu papel. Para isso, você terá que colocar o nome do usuário que deseja salvar quando for solicitado. E terá uma mensagem com a resposta;
12. **Visualizar histogramas do perfis médios:** Essa opção fará a impressão de todos os histogramas de cada papel presente no sistema. Não é necessário mais nenhuma ação;
13. **Visualizar ranking dos usuários de um papel:** Essa opção irá mostrar o ranking de usuários com os valores de distância Euclidiana para o perfil médio de um determinado papel. Para isso, você terá que dizer qual o papel que deseja ver o ranking quando for solicitado;
14. **Sair:** Essa opção irá sair sair do sistema e você receberá uma mensagem "Até a próxima!".