Group number: Dec1703

Project title: HackTrack

Client & Advisor: Dr. Tom Daniels

Team Members & Roles:

Davis Batten – Team Key Concept Holder
Vitalie Cernetchi – Team Communications Leader
Nicholas Lewis – Team Communications Leader
Daniel Doyle – Team Leader
Anh Nguyen –Team Webmaster

o **Bi-Weekly Summary**

These last two weeks the team has been discussing a lot of the more in-depth questions of the actual design of the web application. We have reached a point where we need to answer vital questions about the behavior of our attack graph before we can continue. We have been meeting three times per week and continue to make progress hashing out the details in our project. We were able to complete the majority of the forms that will be involved in the front-end of the project, and we are close to being able to implement pathfinding and hypothesis generation on the back-end.

o **Past bi-week accomplishments**
   ● Davis Batten: Integrated forms for node reporting; extended the services for hosts, networks, and privileges, added a page component for flags and reporting flag captures
   ● Vitalie Cernetchi: Worked on new transitions form and began work on transitions API
   ● Nicholas Lewis: Found a neo4j query to discover paths of various lengths and specifications. This solved the BFS problem.
   ● Dan Doyle: Created team graphs based on the scenario graph with relationships
   ● Anh Nguyen: Created Form for reporting new nodes: host, privilege, network

o   **Pending issues**

- We still have not been able to configure GraphAware's UUID plugin. So for now we have been handling UUIDs manually, but this is not scalable.
- We still need some helper methods for selecting very specific portions of team graphs (subgraphs under a host, graphs with only valid transitions, etc.).
- Will our naive task priority system suffice, or will we need to develop our own formula or algorithm for calculating task priority?

o   **Individual contributions**

NAME	Individual Contributions	Hours this bi-week	HOURS cumulative
Davis Batten	Services for node creation, integrated forms, flag capture pages	16	84
Vitalie Cernetchi	Transitions form	8	48
Nicholas Lewis	Found neo4j pathing method	8	55
Daniel Doyle	Team graphs in DB, graph traversal clarifications	8	59
Anh Nguyen	Form reporting for new nodes	6	51

o   **Plan for coming bi-week**
- Davis Batten:
- Vitalie Cernetchi: Finish up the transitions api
- Nicholas Lewis: Use the "Derived From" property to create hypothesis' on other team graphs
- Daniel Doyle: Configure GraphAware UUID or similar for database
- Anh Nguyen: Claiming a captured flag.

o   **Summary of weekly advisor meeting**

In our advisor meetings with Professor Daniels in the last two weeks, we discussed security flaws that arise from assuming the condition of the database. We also notified Daniels that Neo4j has a flaw for our particular use case as the internal ID's of objects are not static, and can't be relied upon for selection. Now that portions of pathfinding logic have been

defined, we have been discussing the different kinds of pathfinding that will need to be done. We came up with two major kinds, hypothesis generation (being started by the successful addition of a new transition), and task priority (which prioritizes suggested hypothesis confirmation tasks based on how few hypothesis confirmations are required to reach the flag). However Daniels is looking into additional research to determine if this will suffice or we need to write our task rank formula or algorithm.