Project: May1601

Project Title: ICS/SCADA Traffic Baseline and HoneyPot

Client:	Alliant Energy	Contact
Project Contact:	Wesley Daniels	Email: wesleydaniels@alliantenergy.com
ISU Staff Adviser:	Doug Jacobson	Email: dougj@iastate.edu

Student Designers:	Team Role	Contact
Jonathan Osborne	Team Leader	Email: osborj1@iastate.edu
Jonathan Hope	Webmaster	Email: jonhope3@iastate.edu
Korbin Stich	Key Concept Holder	Email: kdstich@iastate.edu
Daniel Borgerding	Communication Leader	Email: dborg92@iastate.edu
Nik Kinkel	Key Concept Holder	Email: nskinkel@iastate.edu

Weekly Meeting #4	Date: 9/29/15
Members:	Present:
Jonathon Hope:	☒
Korbin Stich:	☒
Daniel Borgerding:	☒
Jonathon Osborne:	☒
Nik Kinkel:	☒

Discussion Notes:

Goals:

- Research and develop better understanding of project parameters.
- Get in touch with our contact at Alliant Energy to clarify some design specifications.
- Research categories will be divided amongst team members and discussed further at next group meeting.

Achievements:

1. Designed and implemented fake HTTP/HTTPS login honeypot
2. Designed and implemented fake SSH server honeypot
3. Drafted initial firewall and network architecture specifications.
4. Researched build and deployment automation tools
    - Initial prototype will use Ansible and (possibly) Docker

Pending Issues:

- Verify hardware is adequate to run initial prototype Honeypot.
- Identify constraints of minimal IDS on present hardware.
- Client may provide the following information at a future date: Possible SCADA environment details.
- Identify possible means of testing/verification of prototype results.

Weekly Personal Contributions:	Hours:	Total Hours:
Jonathon Hope: Contributions: Began research on build deployment/automation. Began research on deployment tools (Ansible).	2	6
Korbin Stich: Contributions: Further researched hardware specifications for SCADA honepot system. Set up device firewall using IP tables in Debian OS.	4	10
Daniel Borgerding: Contributions: Researched possible project redefinement for greater EE implementation.	4	11
Jonathon Osborne: Contributions: Built initial website and updated it with a bit more style. Began Research on splunk.	3	7
Nik Kinkel: Contributions: prototyped network architecture and firewall setup. designed and implemented prototype HTTP/HTTPS server honeypot. designed and implemented prototype SSH server honeypot. prototyped initial build automation and deployment infrastructure.	10	14