**Minutes for the Fall 2018 Cybersecurity Club Meeting**

**October 24th, 2018 at 5:30 PM in Stright 107A**

**Presenters:** Dan Richmond, Dr. Waleed Farag, Paul Grieggs, James Lutz, and Matthew Scott.

1. Dan introduced the upcoming Cyber Security Day on Tuesday October 30th and asked for any attendees who are willing to volunteer. Volunteers will be responsible for handing out attendance slips and a survey form at the end of the event.
2. Dr. Farag expanded on Cyber Security Day and displayed the presenters for the day. He also showed the news posting for the hackathon which can be found at <https://www.iup.edu/news-item.aspx?id=259108&blogid=6543>.
3. Paul Grieggs introduced himself and what he is interested in doing with the Cyber Security Club. He is willing to put together presentations along with his coworkers to bring relevant information to the club. Students can contact him at pmgriegg@iup.edu to suggest topics for future presentations.
4. James started his presentation on our CNY Hackathon experience. In his presentation, he went over the competition’s architecture, threats, goals, and more.
5. The key components of the presentation expanded on the biggest issues which the hackathon had to offer. Some of which are expanded below.
6. SSH Key threats. How adding SSH keys allowed the red team to connect to our machines.
7. MYSQL Server was one of the services which had to be running in order to gain points from the scoring engine. This included user accounts that could possibly be threats. User passwords had to be managed.
8. SSH & FTP Server was another service. A specific user needed FTP access and had to be able to log in and get files from their home directory via FTP. Security had to be taken into account when setting up FTP to prevent the red team from using it as a vector of attack.
9. Removing persistence via SSH Keys and killing a user’s session with the kill command proved to be effective during the competition.
10. CRONTAB scheduled process had to be examined.
11. The chattr command was useful for attacks on certain file’s permissions.
12. Red team dropped a database table and deleted the database backup which introduced a major issue. This showed the importance of redundant backups.
13. Aliasing commands such as iptables. Blocked our access to critical system utilities. Had to find ways to recover those utilities.
14. James concluded his presentation and introduced Matt who mentioned a few things about the CTF challenges which he completed.
15. Matt showed an example of a steganography CTF challenge which he completed.
16. David mentioned a few things about the red team and how they were nice at first but then ramped up their game and started taking our services down since we were in first place.

 The meeting concluded at 6:45 PM.