ISM FINAL PRODUCT
PRODUCT PROGRESS ASSESSMENT

MANAV SOOD, AKASH BASKARAN

Thus far in our ISM Final Product, we have made substantial progress towards completion while also gaining significant understanding of the Cybersecurity field and penetration testing. In addition to making some modifications after gaining further knowledge of the intricacies of penetration testing with a drone, we have also completed research, acquisition of hardware, as well as initial setup in order to further progress towards our goal.

One of the significant challenges we encountered during the process of initially planning the Danger Drone was not only the financial burden but also the limited payload and flight time, as well as potential noise issues. Therefore, we have made the decision, with the guidance of our mentors, to switch to a Remote-Controlled land based deployment of the Raspberry Pi and all other equipment we will need to perform wireless penetration testing. Throughout the process of configuring the Pi, we have gained practice with industry-related skills when designing and installing the Raspberry Pi core, Kali Linux operating system, and IoT Village upon which we intend to deploy the remote-controlled vehicle. Additionally, experimentation in this project has also allowed us to deepen our understanding and skills with the large number of tools and programs catalogued in the Kali Linux distribution, which is an industry standard in the field of cybersecurity. Furthermore, another endeavor we have added to this Final Product is decrypting passwords grabbed from WPA2 networks with the assistance of a cloud-based compute server provided by Amazon Web Services.

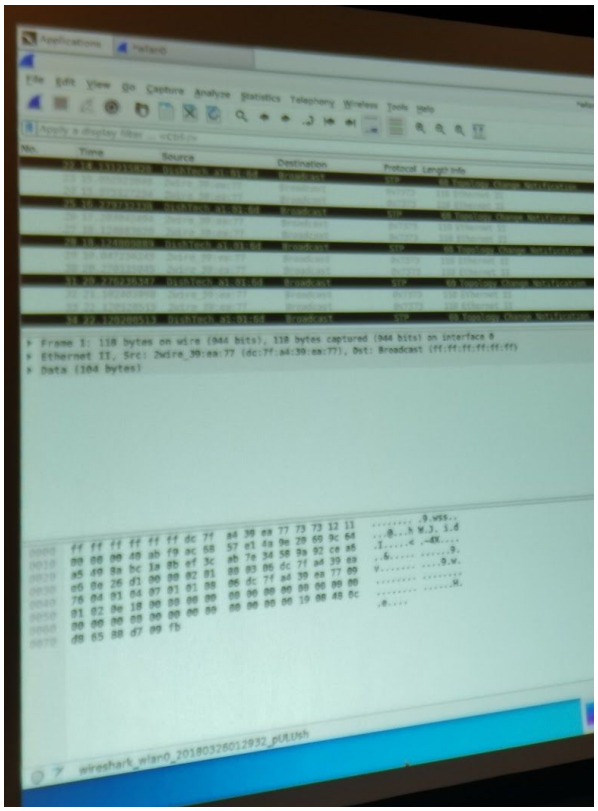
Although we have experienced great success thus far, one of the setbacks we have encountered is the set up of a test environment. However, since our main goal is to test aspects of a wireless network with Internet of Things devices connected, our home networks are suitable for the initial tests. Additionally, we have already been able to capture packets from the Kali-Pi with success, indicating that with the correct tools we would already be able to begin penetration testing. Additionally, since our calendar has outlined

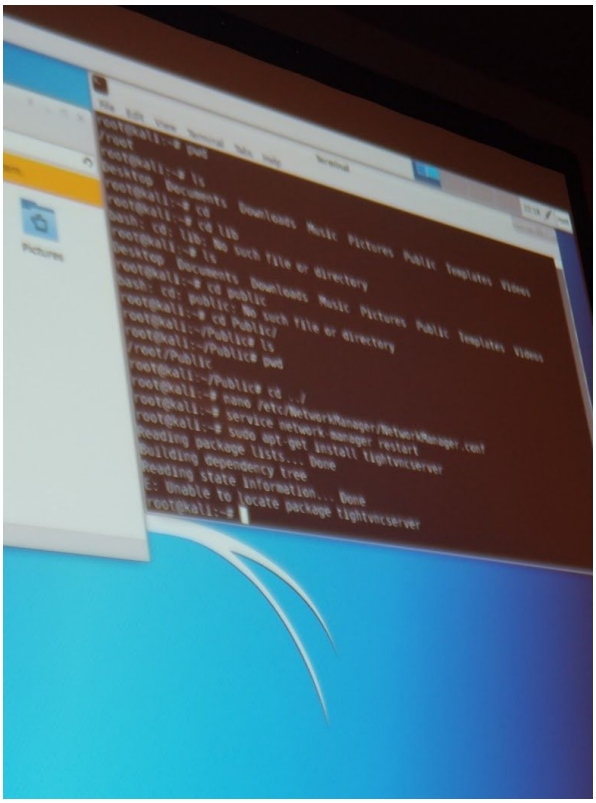
until 5/1/2018 for penetration testing to be complete, we are on schedule. As for the remaining tasks, we need to complete penetration testing on the RC-unit itself and document our findings as well as analyze the results.

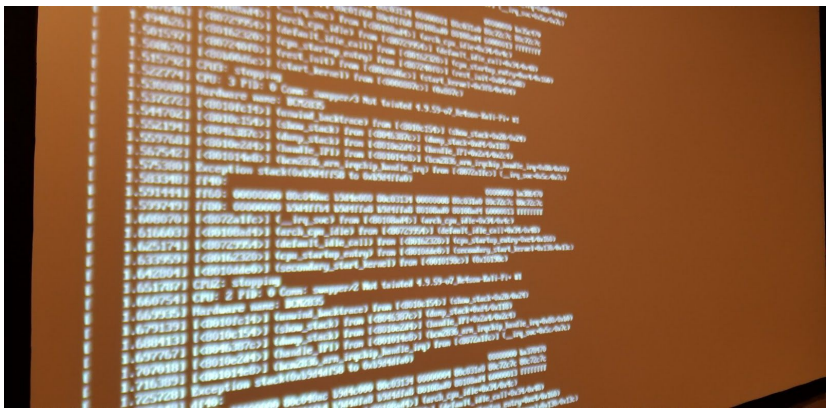
The Final Product is intended to be an individual project. Surely, working with someone else on such a time- and labor-intensive assignment requiring technical expertise and understanding and careful planning and deliberation would result in the butting of heads - at the very least. However, Manav and I have experienced none of the burdens of teamwork, while enjoying all of its benefits. We learn that we play very heavily into each other's strengths and also support each other's weaknesses. This successful pairing helps us remain steadfast in times of trouble so far during this project, such as when we needed to take over three hours simply setting up the Raspberry Pi core component because the initial installation and boot from the Kali OS kept failing due to fluctuations in power supply to the computing unit, forcing us to complete the 20-minute process of remounting the OS image to our microSD card every time the boot process failed. However, in such situations, our collective experience and affinity for technology and technological solutions aided in overcoming the obstacle. By the time we wrapped up with the Pi for the day, we were able to successfully boot the unit, interface with the device through a projector, and capture wireless network packets via Wireshark, a popular packet-sniffing tool.

Delving further into our project, it is incredibly evident that our mentors have and will continue to play critical roles in the development of our penetration testing tool. As previously mentioned, Manav's mentor has graciously provided us with dedicated cloud space with which we can quickly crack WPA2 encryptions to steal passwords and other information. My mentors of General Datatech, Dallas, have offered space at their campus as well as the physical components necessary to create our attack surface - the IoT village. Even still, the sheer expertise provided by our mentors has proven invaluable, which attests to how important they are to the progress of our Final Product.

Photos/Documentation:







Product Log - Manav Sood

Date	Hours	Description
1/25/2018	1	Brainstormed product ideas with Akash Baskaran, goal of creating a more hands-on final product, decided on creating a Danger Drone and penetration testing with war flying to illustrate vulnerabilities in wireless networks and potentially IoT devices
1/26/2018	1	Met with mentor to discuss viability of Danger Drone final product, revisions and additions
1/29/2018	1.5	Wrote and developed product proposal and calendar
2/2/2018	1	Researched penetration testing with drones
2/9/2018	1	Researched war driving and its applications with contrast to war flying and the danger drone concept
2/12/2018	.5	Revised timeline and materials for Product Proposal, opting to dedicate more time to penetration testing and modification of a consumer drone
2/16/2018	1.5	Met with mentor to talk about penetration testing of wireless networks, heat-mapping network traffic, cracking encryption, and other methods of penetration testing with the danger drone product
3/19/2018	2	Met with mentor to discuss best hardware for penetration testing and industry practices, discussed RC Car vs Drone implementation
3/25/2018	5	Met with Akash Baskaran to configure and test with Raspberry Pi with Kali Linux
3/26/2018	1	Product Progress Assessment
TOTAL	**15.5**	

Product Log - Akash Baskaran

Date	Hours	Description
1/25/2018	1	Brainstormed product ideas with Manav Sood, goal of creating a more hands-on final product, decided on creating a Danger Drone and penetration testing with war flying to illustrate vulnerabilities in wireless networks and potentially IoT devices
1/19/2018	2.5	Met with Eric Ballantyne, discussed Danger Drone idea, as well as repercussions on broader cyber security community
1/29/2018	1.5	Wrote and developed product proposal and calendar
2/2/2018	1	Conducted research into original Danger Drone by Bishop Fox
2/7/2018	2.5	Met with Moez Janmohammad to continue discussing Danger Drone idea. Presented Product Proposal and Calendar, revised calendar to accommodate for much for pen testing time.
2/9/2018	1	Conducted research into drones that could be used in our product design, took suggestions from Manav Sood to begin catalogue of drones and capabilities to present to Eric and Moe.
2/16/2018	.5	Began Product Log for submission, continued research into wireless connections that the device can hijack. Developed plan and research into drones for purchase with Manav Sood.
3/6/2018	2	Mentor visit with Moe to learn more about the IoT village, how DNS works, how the tool will operate. Discussed physical components needed to enhance operations of pen testing tool.
3/8/2018	2	Mentor visit with Moe and Eric to define objectives of pen testing tool. Learned about various aspects of the attack (Recon, Heat Mapping, Expected outcome, Payload delivery, device logistics). Delved deeper into idea of land-based delivery tool (RC Truck).
3/25/2018	5	Met with Manav Sood for Raspberry Pi configuration. Deliberated on war driving, potential alternatives to drone concept. Set up Raspberry Pi with Kali Linux distro, troubleshoot boot operations, configured network connections, captured packets through Wireshark.
3/26/2018	1	Worked on Product Progress Assessment, updated Product Log, set up future mentor visits for development of Final Product.
TOTAL	**20**	

Development of Product Calendar/Timeline

Date	Task
1/31	Share product proposal with mentors, receive feedback and revise
2/1 to 2/9	Research acquisition of drone, schematics, penetration testing, internet of things devices, construction of testing environment
2/25	FInalize drone plan, obtain pre-built drone. Begin experimentation/learning with Kali
3/1	Continue experimentation with Kali Linux penetration testing tools, complete gathering all materials needed and begin installation of software/hardware components needed to complete Danger Drone rendition
3/1	Complete installation, design and begin implementation of testing environment
3/7	Complete creation of testing environment, begin testing, develop drone capabilities as needed
3/15	Continue penetration testing, tweak drone as needed. Report changes/progress to penetration testing via written documentation
5/1	Complete penetration testing on network, document results and begin analysis. Report results and any changes after 3/15 via written documentation
5/5	Complete extensive analysis of penetration testing with Drones on IoT networks and popular routers