Cybersecurity BILT Meeting – May 20, 2015

Meeting Minutes

Welcome and Introduction – John Sands

Meeting Link:
https://meetings.webex.com/collabs/#/meetings/detail?uuid=IC28JSKXI4FJKRYPU1HNNWETSJ-B2LB&context=meeting&email=QUhTUwAAAALCzBW8AV7aRhnUELiAC0G%2BrWChoEi1q1E7F55Ql41%2FqhPNvANBD47O4ZkJnqyFLuzizJVshSZwxHXUusI5kNxQyP%2F9QZGU1Fqonxb%2FNKhomA%3D%3D&inviter=U76QGT7U5WWJSQ67VFHF4F16IW-B2LB

Scripting for Security Professional lab Series (Powershell) introduction

John Sands –What I want to basically do is give you an update of what's happening with curriculum. Looks like we don't have a lot of partners on today, but I'll give you an update. Moraine Valley was the lead, so I thought I would show you quick things this morning regarding where we are with some of the Cyber curriculum. We have submitted all the courses and are working on the last two items I'm showing you this morning. We asked for your support and we went ahead and pursued some labs for teaching scripting within the Cyber courses. If you remember, the reasoning behind some of that is that the CAE's standards had changed; they renewed those standards a couple years ago. One of the things that will be required of community colleges that teach Cyber, if they want to pursue the CAE2Y, is that they are going to have to incorporate some scripting within the courses. So, I'm happy to report that we had our last labs turned in and we had a couple different authors working on them: Mike Macino, from Addison area Career Center and another person from University of Delaware. But, we now have those labs go through Q&A; I thought I would show you one of them to see that they follow the same format.

As you can see, all of our labs basically follow that exact format. The labs can be delivered the NetLab environment. This supplements our basic courses, so we have a series of twelve labs. Our approach is to use some of the more advanced scripting language that's out there, so we looked at PowerShell, and Python. An idea is that we would expose our students to the basics of using these scripting languages, and then ultimately use the capstone lab in each of these areas. They are going to create some type of tool that might scan ports or look at log files; they could actually write a script file that would do that. This is an example of one of the labs that might get turned in. The layout is exactly the same format we use on all our other labs. Same look and feel that we've had with all of our labs and they will be embedded into the lab environment, so when students are using the lab environment they can actually pull down these pdf's. Same layout, we have an introduction to the lab, we introduce some of the concepts and we have them walk through and do some specific task. I'll tell you we have a lot of schools that are extremely interested in using these. One thing that I

would like to point out because we are teaching some basic concepts of programming, is that we don't really need a comprehensive pod; you can see the pods are really simple. Typically, it's going to be a Microsoft Box, a client, and a Linux Box. We are teaching PowerScript and PowerShell from the Microsoft side and teaching Python from the Linux side, although you could do the Python from Windows, if you wanted to; it's the same kind of layout. I'm pretty happy because it goes through all the basics of scripting and it gives them three small projects, but from the three projects you can build some other projects. Just letting everyone know we were able to complete that; these are in the review process I would be able to disseminate them this summer.

The second thing is that we also completed the CASP Course and it's a little bit different than anything else we've done. Again, it aligns with whatever is happening with the CAE requirements, and I would say it's also from feedback from members of the BILT. What we're basically doing with this course is that we are exposing students to the basics of Information Security Management. We understand that Chief Information Security Officers and Professionals are going to come out of four-year institutions, but we did hear that our practitioners are going to play a role in the overall management of Information Security Systems. We wanted to expose them to frameworks and to some other processes and tools that are used in managing an environment. I have a list here of all the labs that are part of this, but I'll just show you a couple of these and leave it at that. Basically, as part of this course and as part of the capstone, each pair of students has to pick a company that they're going to work with in doing an Information Security Management evaluation. It's going to start with the whole concept of how strategic planning works, so we actually have them go in and do things like an Environmental Scan, we have them do a SWOT Analysis, a Risk Analysis and so on. Let me show you a couple of the worksheets and what they look like. To start off … they are picking their company and then gathering information about the organization itself: everything from the website to assets, how the organization is structured and so on. Then we do a simple checklist of the kind of things that they are going to have to be concerned with in the security management plan. From there, we go into a cryptographic tool because it's part of the CAST and SAP Certification. So, I don't know how many of you have used CRYPTOOL, but it's a really great way to teach Cryptography. So, you can see the task they are going to do. They're going to download and install the tool open the file that has Cleartext in it. They are going to learn how to use a modern symmetrical encryption system to encrypt the contents of the file. They will also then decrypt the file to change algorithms, so they can compare 3DES to AES. Then we will have them create a digital certificate and review the process of how PKI works and we'll use that certificate in an asymmetrical encryption algorithm. Now they will encrypt the same file, using a digital certificate, in this case, an RSA. Then we have then do a hybrid process so they are going to learn how symmetrical and asymmetrical encryption works together to form a fully secure encryption system, by encrypting and exchanging keys. If you have used CRYPTOOL, you know it shows a great step-by-step process with each stage, and what happens. Finally, we get into having them do things by using Password Hash Tools and HMAC, to do a password. So, they get some overview of all the basic components of Cryptography.

Let me show you a couple on the management side... We have a couple different components associated with RISK. By the way, the course also includes three case studies. One of the case

studies uses the Target Case Study. We basically have four different research articles on the Target Data Breach, so they have to go through those and do some additional research, and then they have to complete a case study. They are going to give some details about the attacks and the effects of the attacks, and so on. Based on what they learned, what are some recommendations they would make and a conclusion about the impact of this data breach and what we can learn from it. We give them thee different case studies of different modern data breaches and we try to take something within the last year that was in the news; it will seem a little more practical to them. Again, we have three case studies embedded through put the course, and then, the rest of this is are going to be based on ISO framework, so we have them do the environmental scan.

One of the things that we've heard, especially from our people of NSA, is that they would like to see us use more data in the class where students have to do some data analytics. That is what some of these are about. We are having students become familiar with some of the website that are out there, by using the CVE Database and the CVE Details website, created by MITRE. Then, we have them collect data based on their organization, have them plug this information into an Excel spread sheet, and have them manipulate the data to generate different types of charts, in different ways. This is to represent risk that is opposed by the organization and impact on each of the assets. It's somewhat scripted and we are going to give them the specific types of charts that we want them to use, but we will want them to take that and launch that into other things. We will leverage these in some of the later exercises, so once they fill their data in, the charts starts to build and they can see some comparative analysis; they can calculate risk score, and things like that. From there, we want them to summarize the data that they have collected, so they can actually present this in a meaningful way.

Then, we have them see how to use tools that do full blown quantitative and qualitative risk assessment. We introduce them to all these different concepts in the course itself and then we expect them to go in and be able to do some calculations. So, they're going to be able to calculate risk scores take it to risk assessment. They are going to look at things like single loss expectancy, annualized rate of occurrence, and so on. I'm going to have them pick five different assets that they are going to do a quantitate risk assessment. In the second part we will be showing how to do a risk inventory. This whole chart here abides by the 2700 series standards for doing a risk inventory, and then we get into to doing qualitative risk assessment. Similar to how DHS does the warning systems for the level of threat to the US, we want them to be able to do something similar with the internal risk of their assets. The way these work is by changing the two variables; they can use a representative color representing the level of risk. If I change the impact of probability, you can see the color changes immediately based on those issues. We want you to see how we can use tools, like Excel, to represent symbols ways of representing the risk. It doesn't necessarily have to be quantitative; you can use qualitative means of representing the risk, as well. These are examples of what we are doing and what we are doing in that class. I hope that we have captured what we heard from your feedback.

Matt Glover – Some of the challenges in the industry that I'm seeing are having well-rounded knowledge; by focusing on getting them the basics of Network Engineering and Server Application or Systems Engineering that they can figure out exactly where the threat is and does it sit far away. Can you paint that picture for me?

John Sands – Yes, I am always leery of the term engineering because I don't know if we are at that level, however, I know do throw it around a little at our level. So basically, the first things that students are exposed to in the stackable certificates are the hardware and software familiarity and understanding. Everything from building a machine on the hardware side of it, with the A+ curriculum, installing software and troubleshooting software, to doing patches and turning on security features. The networking Asset would be the next certificate, so once they've mastered basic hardware and software, they go into the network side. We use the Cisco curriculum, as well as, the Aligned CompTIA and that's what most of the partner's curriculum look like. They're learning everything from basic switching and routing to each of the different network services from ARP to DHCP DMs. All of the different services that form the backbone of our network time services, and so on. We have over 200 labs where they set this stuff up on real equipment in the virtual environment, so they are hopefully getting a lot of that lab before they get to this class. We have on both desktop and server level Microsoft and a couple different courses that we have developed as a group in Linux, and also some basic database orientation. I wouldn't say that they are database experts, but enough at least to provide support for the database.

It's exactly what you said; they sort of pull it all together. If they don't understand those things then they can't possibly do a risk assessment or internal, or external scan, or even attempt to do strategic planning. What we're really trying to teach students are that security is really about strategic planning, not reactive planning, necessarily. Too often students think that the only job is to react to things that happened. We want to make sure that they understand that organizations do not want to take that posture; they want to plan and try to prevent things from happening. That's the whole thing behind this. The idea of looking to the future and monitoring things on the web, so as to know what the latest threats and zero-day attacks are; I try to take as many inputs as possible. I know we've had some off-line discussions with some of the people on the team and that's how we have identified some of those activities. There are twelve exercises to do from a Physical Security Audit, Operational Security, and Instance Response. So, it's really basic stuff, it's not going to be Cical level. These are tasks to be performed by our practitioners, or they can be involved in performing them.

Ann Beheler - Where are you going to use that, what course?

John Sands - I think it makes most sense to put them in the Certified Ethical Hacking. You and I have talked about this and one of the things that we're hearing from people in our Certified Hacking class is that some of the stuff is old, because we still use XP in some of the labs. I try to explain to people that the challenge is that in the past we did not have scripting or programming components in the program. If you look at the modern day ethical hacking set of labs, you have to incorporate some of them and that's how you can reveal the vulnerabilities nowadays. The newer operating systems were not as wide open as XP was. By enabling those labs we're going to actually represent more

relevant and up-to-date types of Pentest and testaments of our systems within the Certified Ethical Hacking class; I think that's where they will fit.

Ann Beheler – That's great. We are teaching Python this summer per instructions from the Networking BILT and our Working Connections, and I'm wondering if I can make these labs available. I don't know how generic they are, but maybe I can make them available to the person who is teaching. Paul somebody…

John Sands – We can definitely make him available. They look really good. My first run through, I did some of the labs and tried them; they were really pretty good. The thing about these is that they are real simple. The virtual environment is only three machines and it scales well and these should rapidly available. I would like to have more people contribute to a library with this where we can take it to the next step.

Ann Beheler– Sure, and another thing is having a group of professors test it out this summer. That's one quick way to QC use.

John Sands- I agree. We're a lead in Cyber, so I don't think there is a lot going on at this point in the grant. We're really coming to the end here…

Ann Beheler – We're getting the third party reviews done and trying to track who is using what…. We're in the wrap up phase, of the DOL Grant. John and I are talking about trying how we are going to support the curriculum on a go forward basis. I know that the CTC (Convergence Technology Center) is going to disseminate the Cyber, Networking, and Programming Curricula for the foreseeable future, but John and I are talking about going after some money from NSF to keep some of this updated. What do you guys think? You think that is a good idea?

John Sands– We all know it's a short shelf life for this type of material.

Ann Beheler – Business people, would you like to see some of this curriculum updated? Kept updated?

Matt Glover– Absolutely.

Ann Beheler – Okay, we'll be coming to you for letters, for sure.

We're nearing the end. We have done the curriculum we needed to do, we're getting final reviews we need to get and we're putting it in the repository for DOL. It's going to take a lot of time get all the I's dotted and t's crossed, but were doing fine on that.

John Sands- That's all I have on curriculum in labs, so we're pretty much on time with that. I thought the other things we would talk about are some of the student things that are happening on the Cyber side. I asked Dave if he had a minute or two just to share some of the things that he is doing. We're really going to miss some of these supplemental services that the grant has provided. The school is going to try to implement some of these things, but we can't possibly do it at the level that we are

doing now, especially when you hear some of the supplemental things that we are proving for our students. Dave, do you want to talk a little about the event you have coming up?

Dave- The first week of June, we basically put together what we call a "Test Fest". This is working with three different departments: everything from the CompTIA Cisco Exams, AutoCAD, Graphic Design and the Microsoft certification. This is a way for students to 'brain dump' at the end of the semester into their certification exam, so rather than take the summer off and have a break, we're promoting the exam for students to come in, eat some free pizza, go to review workshops, have some discount vouchers and try to get their certification. One other thing were going to be doing is helping with student resumes that week we haven't spoken with yet. In regards to resumes, it's a great way for students to get excited about taking the certification exams because we know employers are looking for these exams on their resume. We have a lot of students changing careers, coming back to school without that solid three to five, ten years of experience in IT, so this is a great way to supplement that experience on their resume. So far, we have been promoting this for about 3 weeks now. We have 88 people signed up for Test Fest, which is fantastic, for all different workshops and sessions; we have a couple quests speakers coming in. I think those numbers are unbelievable for only a few weeks of promoting. That's on top of the many things we have been able to do with the DOL Grant here. There was feedback from employers saying we need some students that are well rounded with both SecurityPlus and Linux Plus, a little bit of Microsoft Server. After listening to this call, I 100% agree that having students that are well rounded and have those foundational skills for IT is very important. That's why we have been trying to work on different things and put together the Test Fest.. That's what we have been doing at Moraine, the last few weeks.

Ann Beheler – Dave, you might also comment just on what you do in general as a Career Coach.

Dave – Basically, our goal as Career Coaches is to navigate with our students that are transitioning careers through the program, by helping pick out classes, prepare the their resumes, and participate mock interviews. Over the last view years, we've brought employers: everyone from Microsoft, Dell and SecureWorks to small companies and school districts, who are looking for IT students. We try to prep our students for the resume prep and interviews with employer feedback. I always like to say… we have a little bit of hand holding for our students to get them from Point A to Point B, from college to career. In the last few years with this DOL Grant, we have been able to do that…it's fantastic. We have a whole team of people here; student specialists who help students on a daily basis reach their IT career goals. That's pretty much a recap of what we do.

Student's Success

John Sands– I have to admit, I'm a little nervous because we had our graduation last week and we had the largest class of graduates from our program ever. I have been at that school for 28 years, so I have to say that Dave and his team have done an incredible job. Part of what they are doing is

tracking every single student through the entire program and making sure that they complete their certificates, their degrees, and whatever supplemental services are necessary. I'm very nervous what's going to happen next year because I have a feeling we are going to recognize a decrease in our numbers without the additional support we had. It has been phenomenal, like I said, it's been phenomenal! The largest class we have ever had the eight years I've been here.

Ann Beheler – John, here at Collin, we have gotten institutional research involved and we have proven that the fall / spring retention rate of the students that have used Career Coach services versus those that have not used Career Coach services, is almost double. Based on that information gotten funding for retaining three Career Coaches, and it looks like at this point, it's going to be supported by supplemental money, with hard money from the college. I don't know, the data is speaking here.

John Sands – I agree. I'm hoping our institution sees the value and makes the same commitment.

Ann Beheler – Did you get hard data? You may have to get institutional research…

John Sands - That's the beauty of this grant, that it provides that highest quality data, I think we've had in years. Our administration knows about it, so it's really going to be a matter of how we can do something about improving the types of services we have to something similar to what was in the DOL Grant. It still comes down to dollars without the DOL money; it's tough to have even just a good ratio of student coaches to students. Our students have come to expect this assistance, so it's going to be interesting to see where we go from here.

Ann Beheler – Our 3 Career Coaches are not just going to be just for IT, they're going to have to be for all technical programs. It will be diluted quite a bit, but it's a least better than what we've had prior to the DOL Grant, at least.

John Sands – We have taken some of the best practices from the team and this college is actually going to have a specific place on campus for students… the Student Success Center. I still don't think it totally replicates what we've done in the grant. Like you said, I hope the data speak loud and clear and they make a similar type of commitment to our groups. I've been involved in a lot of different grants, but with this one in particular, the student success component of it been unbelievable, with what they have been able to achieve. It felt good sitting at graduation the other night seeing a huge line of our graduates.

Ann Beheler – We had a similar experience Friday night and it was great fun, I have to say.

SCADA Components

John Sands – I already covered the scripting, but the SCADA, that's actually where I'm at today. Same kind of thing, were not building a full blown SCADA class, but as part of our SecurityPlus and part of our forensic class, we want to have a couple labs that introduce students to the whole idea of

automotive processes control. I'm actually at a Siemens class this week; it's sort of an interesting program. Siemens has stepped up and provided a free class that teaches how the Siemens PLC's and SCADA systems work. They have allowed us to send 3instructors free of charge, and each is getting their own PLC, HMI and System Interrogation kit, which includes all the software, and so on. This is really a great opportunity. Ideally, what I'd like to do is set up something like a Small City Simulator to see how automation impacts our modern life and what vulnerabilities are out there as a result of that. We started this with the DOL Grant; we've got a couple labs that we've generated that will be appended to the SecurityPlus Curriculum, but I think it's going to launch us to exposing students to the whole SCADA Process Control aspect. Our challenge now is how to virtualize it and do it effectively so we can engage students, so they are not just looking at a simulator. They can see lights turning on and off, the whole distribution system and components that we take for granted every day that are all totally automated with our information systems today. That's where we are at with it… We received a small grant to build a small lab, like I mentioned earlier, but now our challenge is to integrate everything.

Danielle- Are you familiar at all with National Collegiate Cyber Defense Competition?

John Sands – Yes, we host the mid-west regional and actually use our virtual environments before the other regionals. We have been doing it from the very beginning and I know they are talking about incorporating more and more of the SCADA stuff into the CCDC.

Danielle – Right, at the Nationals this year they just had San Antonio – the whole competition was built around that and they actually had boards with xxxx on them with little LED lights in a city that would turn red and green on whether or not systems were good or not. I'm sure if you talk to xxx, maybe an introduction in xxxx San Antonio that set that up…

John Sands – I didn't go this year, but I usually work with Greg. We have also been working with Allan Pollard and David Brown's group at Sims, because they got that little Simulation City. That's the direction we want to go, is to make it really where you're simulating basic systems, the critical systems for a city. I think we want to look at both models and see where they can take this.

Danielle – So, you're not looking at mirroring one specific one.

John Sands – The things that happened at Nationals, I'm sure those we can put in our competition next year. I want to try to put some of this into the SecurityPlus Curriculum. If you look at the objectives, they at least touch on it, so they need to know a little bit about it.

At this point we are a little ahead of schedule today, but any other types of trends, things you want us to hear about, just remember we're late in the cycle now, so this is our last six months. We'll have one more of these meetings in August.

Ann Beheler – John, yours and our program are going to continue, so I'd like to invite these folks to continue working with us.

John Sands – Definitely, we're still waiting on hearing about funding. Either way, it will still run in some form or another, but we're still waiting to hear about our funding approval.

John Sands – Anything else we should be incorporating into our curriculum? Things you'd like to see that you're not seeing at this point?

Ann Beheler – Matt, can you talk to the whole group about how you thought security should be included in everything that we teach and networking?

Matt Glover- Absolutely, it's a cornerstone. It's kind of like teaching an Engineering class on how to build a bridge. You're not going to teach them how to make the bridge fall down. You're going to teach them how to build a stable bridge that includes the foundation, how to put guard rails on the bridge so that people don't fall off of it. Same framework needs to be understood for all the security layers that go with networking, so it needs to be embedded in everything. It's like building a bridge that can be easily broken; it is like building a bridge on sand. Does that make sense? Having security embedded in anything that we are creating within IT, whether it's Application Development, Systems Engineering, Networking Engineering, all of it has to have security, as an enabler.

John Sands– When I try to look at what the world is going to look like in the future, you hear about these Google cars now, etc. Can you imagine some of the technologies being deployed if security isn't at the highest level in what they are designing?

Matt Glover– I just spoke at a Cyber Security Event this morning. One of the Cyber Security guys said that his daughter has Type I Diabetes and he won't let her have the wireless version of the insulin pump because the coder who put it together didn't use Cyber Security Protocols. It's easily hacked and somebody could give her a lethal injection of her insulin, so she's totally non-wireless. These are the challenges of the future, these are the challenges of the internet of things, and these are the challenges of everything that is a cornerstone. Aside from the fact that I need a Network Engineer to be a Cyber Security person at their very core, we also need somebody who has a Cyber Security mindset. They need to be looking holistically at the entire environment and is not taking one thing from the other, but looking at it as a group because there will be persistent threats coming from different angles, so there's always going to be a need for a specialist in delivering Cyber Security.

John Sands – I couldn't agree more.

Matt Glover– Is that what you were looking for, Ann?

Ann - Yes, and I think there's been more of a separation between Networking and Cyber Security, than perhaps there should have been. I recognize that you can't teach all of security and all of networking all together, but the Cyber Security rests on networking or on programming, depending on which piece you're working on. In my opinion, there's no need to not be incorporating principles of Cyber Security all the way from the beginning. There's always going to be one more threat that you will have to worry about and one more thing that you have to include in the Cyber Security

specific courses, anyway. This spring is the first time that I heard you guys be really strong about that.

Matt Glover- Yes, it's becoming more of a challenge in the industry around us; I think we like to turn a blind eye to it. As I've seen our Engineers that I've spent $100,000year on chasing ghosts, I need to get more people who we can bring in at the $40/50,000 mark, so that they can confirm that there is a threat. We can use the higher dollar resources to secure the threat. It's a different model… For the people that are going to be getting degrees, we will be helping them get into an entry level position within a few years. They can go from making $40/$50,000 a year to $75,000 an year, in a span of 2 or 3 years. Once they get more and more experience, the sky's the limit from there.

John Sands – I can't agree more. It's one of the reasons we thought this CASP Course was so important. Even the first case study, where we talk about the Target Case Study, a lot of what happened in the data breach could easily been avoided if the steps to secure work stations and devices were taken as seriously as other components of basic networking. It's the practitioners, the people supporting the systems every day, who need to play a more important role in making sure that those devises are secured.

Matt Glover – The Target Breach was a little bit different. Those guys ignored the information that was provided by the practitioners saying …"we got a problem, this is what we're seeing" and it was consistently ignored, which is why seven of the eleven C-Suite members in-target were all canned.

John Sands - If you don't have rules and responsibilities at that level, specific roles in who's ultimately responsible, it will funnel down to the lower level in operations people.

Matt Glover – That's right. I just think that the great news now is because the CEO's, board members and the higher echelon of leadership is understands that they will be fired in the event of a security breach. It has specially invigorated the amount of dollars that's going into Cybersecurity. I'll give you a quick example; one of the panelists in my interview today was from Texas Instruments and started at TI a few years ago. They only had 5 Security Analysts that were on the team; they had 900 IT staff. Today he has 44 Security Analysts on the team and still 900 staff. So, that gives a clear indication of what the importance of Cybersecurity is; that's TI.

John Sands – I was informed at Siemens that one of the most recent devices that we could purchase, failed in many ways with security. They just announced a brand new family for PLC's, specifically around a power unit and making the devises more secure, especially because we're seeing more distribution of automation, making each of those boxes secure. It was never a design feature in the early days, even when we bought the latest thing out there. Just in that period of time, they've come to recognize they actually need a whole other line to build their feature on.

Matt Glover – I agree. I'm pretty excited about it.

Ann Beheler – We have one more meeting out of the office of DOL, but I sure hope the group continues and I want to stay involved. I'm serious about going after funding to keep this curriculum updated.

Matt Glover – You guys need me to write a letter or anything like that, just let me know.

Ann Beheler – Of course, we will. Thank you so much Matt and I bet others on the call will too.

John Sands – Our next meeting will be in August. Again, thanks everyone for your time again today and we'll get a date out here in the next couple of weeks when the next meeting will be; that will be our last meeting under the DOL operations.

Tina Sawa- John, it's tentative for August 5th right now.

Adjournment at 10:45am