Reflections Made Throughout Module 2 - Networking and Information Management

Seminar 1 Reflection: May 15th - STRIDE and DREAD Applications to Mannequin Case:

In preparation for this seminar we applied STRIDE and DREAD analysis to the Mannequin case study. This seminar provided less discussion and more presentation from the assigned groups. Most groups followed a similar approach in the DREAD analysis with most threats falling between a medium and high risk. One outcome of this exercise wasn't so much what the various groups found or decided on as a threat level; it was the fact that a relatively tech savvy person with the motivation to learn basic network exploitation could achieve very real and moderate to high risk exploits on a hospital network. Cracking the WPS pin for the mannequin presents a relatively low risk and would be unlikely to be achievable on today's networks. Furthermore, if the hospital was using WPA-Personal and WPS for their internal wireless then they are asking to be hacked. The DoS attack has the potential to be the most impactful. By finding the MAC address of the mannequin and putting a block on that address they were able to effectively kill connection to the device. Extend this risk to an individual who's managed to get onto the internal network (through ethernet or other means) and they'd have the ability to put deny rules on a range of MAC addresses on the network. Operating room printers or even MRI machines (if they're network attached) could cause far reaching and potential life-impacting repercussions. Ultimately, what the student's targeted isn't the risk, it's what else they could apply similar exploits to that is particularly noteworthy.

Seminar 3 Reflection: May 29th - OSI vs TCP/IP:

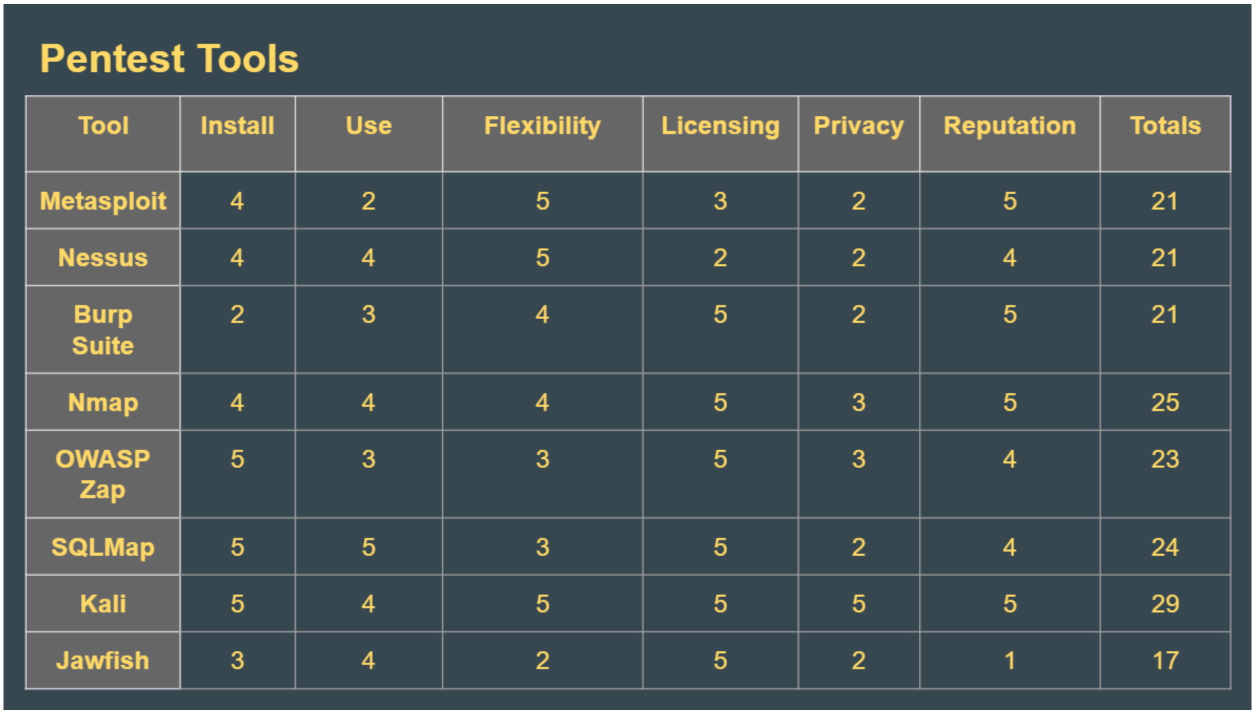
While the brunt of this seminar session was to review the AWS Educate/Elastic Beanstalk issues a number of users have been experiencing, some time was dedicated to discussing work to be carried out on the e-portfolio segment.I find myself and a number of other students confused by the relevance of the e-portfolio, especially as a tool to be used after completion of this program. Perhaps it would be better realized if we weren’t bound to using Github; a clunky mechanism for managing content and reflective pieces.

It wasn’t until the end of the seminar that we covered some discussable content relating to the OSI model and the TCP/IP standard used today. Since originally covering these platforms in my IT Professional college program, I was often confused by the OSI vs TCP/IP and how they fit together. Umar’s point on “Framework vs Protocol” was somewhat of an “aha” moment. The idea that TCP/IP are the protocols to be applied up and down the OSI **framework** was very helpful as I’ve always seen the two applied this way. Following the seminar I dove into a few of the proposed OSI protocols and can say that I don’t recognize any of them because they’re not used! Perhaps the most contentious discussion point at the end of the seminar was the opinion of whether the framework for OSI (7 layers) should be used or the melded TCP/IP framework where only 4 layers are used. While the consensus was that the simplicity of the TCP/IP framework is better for developers and makes for simpler application design than the OSI model, I have to disagree. I believe an awareness of both is a necessity and which framework you choose should be dependent on the nature of the application you’re developing. If you’re creating a largely web based program then perhaps the OSI model’s granularity is superfluous and unnecessary, but if the program is suitably complex, I believe the OSI model can help clarify where and how processes and functions take place. Furthermore, troubleshooting or setting security policy or general networking can be made easier with an understanding of what layer a service or feature relies on. Perhaps the granularity of OSI isn’t always necessary, but neither are verbose logs; there can be information overload, but sometimes having access to all available information is what is needed.

Seminar 4 Reflection: June 12th

This seminar, as with the previous two, spent a solid chunk of time reviewing administrative elements throughout the module, as well as expectations and e-portfolio progress. Some time was spent reviewing another risk modeling framework called the Cyber Kill Chain, by Lockheed Martin. This has been reviewed in the launch module and loosely compared to other threat analysis frameworks. While much of my threat analysis applied throughout the courses have been based around the STRIDE model (which stands for, Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege), I may switch to an emphasis on the Cyber Kill Chain model as it aligns closer to the defense space that I currently work. My personal observation of this model is that it seems more reactionary as it tracks the path an attacker might take from the recon stage to the ation and objective phase. It's a lot of analysis to make for one vulnerability, where something like the STRIDE model allows you to bundle threats under one of the five categories and analyze risks and impacts categorically. The advantage of this, in my mind, is that you can potentially find secure solutions more efficiently by seeing related risks next to each other/broadly categorized allowing for blanket solutions to be provided.

This seminar also focused on the various pentest tools and their uses. I don't have much to reflect on here as the task seemed to be to arbitrarily rank various features of differing tools in a table. How this will help me in the future is uncertain, but I suppose I have a better idea of some of the drawbacks and benefits of these tools. For instance, I learned that most every tool used in reconnaissance is relatively noisy, especially ones focused on rapid results like Nikto or Nessus. The table below outlines what I felt each pentest should be rated in terms of a one to five scale.



Pentest Tools

Tool	Install	Use	Flexibility	Licensing	Privacy	Reputation	Totals
Metasploit	4	2	5	3	2	5	21
Nessus	4	4	5	2	2	4	21
Burp Suite	2	3	4	5	2	5	21
Nmap	4	4	4	5	3	5	25
OWASP Zap	5	3	3	5	3	4	23
SQLMap	5	5	3	5	2	4	24
Kali	5	4	5	5	5	5	29
Jawfish	3	4	2	5	2	1	17

Having never used most of these tools, I'm sure my opinion will change as I gain more experience. Metasploit ended up being rated lower, but I know it's one of the industry standards in pentesting, so perhaps with more experience my opinion will change.

Seminar 5 Reflection: June 26th

Seminar five reviewed the various policy standards applicable to both different industries as well regions. For example, we covered the application of HIPAA; a standard taken quite seriously for health related data in the USA and Canada. I find some of the policy and regulatory aspects of data and industry one of my preferred areas of the field and hope to find myself in a compliance or audit role some day. Basically my entire immediate family (minus myself) is in the healthcare industry so topics surrounding HIPAA are fairly routine. Professionally I've dealt with this field by trying to get small municipalities to gain HIPAA compliance because their offices routinely store local clinic data.

This seminar outlined how some of these policies and procedures can overlap to embody similar requirements in different regions or industries. For example, while HIPAA isn't practiced in Europe/United Kingdom there are overlapping policies on areas such as pseudo-anonymization of patient details. This is observed under HIPAA by using initials in all communications regarding health information. General Data Protection Regulation (GDPR) has a bit more flexibility by using first name only.

PCI largely targets financial systems and ecommerce presences, but in many cases adheres to similar general standards, focusing on secure infrastructure requirements. My general takeaway is that, while you should be compliant to the industry standard that best fits your region and industry, any of these compliance standards would bring an infrastructure to at least a minimum level of cybersecurity. There will no doubt be specific requirements to each, but focuses on encryption, anonymization and data security will create some effective overlap in any of these standards.