CSCI 420 SOFTWARE SECURITY

MIA WEBER

04/03/2023

NUARI Tabletop Exercise

During the Exercise

For the NUARI tabletop exercise I had the assigned role of Cyber Incident Response or Cyber IR. In this role I was primarily focused on the practical aspects of the response to the incident as well as the continuous monitoring of the situation as it developed. Putting together an incident response report was just the beginning, and by working with the SOC managers the other Cyber Defense IR we were able to identify the cause of the alerts and attacks, take action to prevent similar attacks from happening, and isolated systems so that we could clean up systems and get tools back online for customers and shareholders.

As Cyber Defense Incident Responder, my official responsibilities described by NUARI included providing tech support to enterprise, monitoring external data sources, maintaining currency of cyber defense threat condition, determine which issues impact the enterprise, and receive and analyze network alerts from within the enterprise and determine the cause of the alerts. As far as discussing methods of monitoring external data sources goes, this included asking questions like where to look for the latest threat information, where to look for the latest patch releases, and what is the order of the incident response actions.

Some of the interesting things that happened during the exercise included the injects that were released during turn 1 and turn 2. Some of the information that was provided to me as the cyber defense IR included the announcement of US sanctions that angered foreign powers, an FBI alert for a phishing campaign that is targeting manufacturing including the space industry using PDFs that act as a downloader for malware. The FBI report provided no specific details on the email or malware used but cited injections called “kitsune” as potentially involved. There was also a joint advisory with the FBI and CISA that cited beliefs that hacking groups were receiving material support from foreign groups that were targeting government networks, energy companies, and components of critical infrastructure. The joint advisory also highlighted the tactics, techniques, and procedures (TTPs) used by cyber actors such as phishing, email spoofing, multi-factor authentication and more. It also describes preventative

measures such as training, attention to details, and authenticating applications among others. I also received a SNORT alert that told me that I was currently under attack and that the perpetrators were targeting web applications. In addition, I also received an email about the postponement of the underwater basket weaving tournament which was clearly a spam email although it's important to note that there didn't appear to be any downloadable files or links included in the email.

Some of the questions that were asked during this first round were about what types of impacts are tolerable to the organization? Is it worth preventing attachments to emails if it means that the business operations will be impacted? On one hand it is important to take action to prevent things from getting worse, but it is also important to ask ourselves if we can detect malicious people on the system currently, and since we most likely will be able to (given the services that have been impacted and brought offline) will blocking attachments too little too late?

At this point our group determined that it was important to notify the FBI about the attacks that we have seen as it could pose a threat to national security due to the existing suspicions of foreign powers being behind similar attacks. The cyber defense IRs also discussed how we should be using Wireshark and SNORT to look for suspicious activity and continue to monitor and analyze network traffic. In addition, we discussed how SNORT can be used as a warning system to block suspicious web traffic based on their IP addresses, signatures, and behaviors. The facilitators had interesting input at this point with discussing the capabilities of next-gen firewalls that allow for this kind of customization and modification. We also discussed as a group how to handle the company response and when to tell employees and shareholders.

During turn 2 the priority shifted to getting rid of the malware, verifying the authenticity of backups, and determining what all is vulnerable. Since at this point both payroll and the outlook Calander went down it was reasonable to assume that confidential employee and company data was compromised and potentially tampered with. Many other Microsoft services are now vulnerable as well as any other services that are running alongside the payroll service or share vulnerable dependencies. Our team also decided that it was important to halt all non-vital functions and regain control of the systems. Most of this turn was focused on things that fell out of the jurisdiction of the cyber defense IR because we talked a lot about the moral implications of telling or not telling employees about payroll being down and the implications on business operations that this outage will have. Beyond just "yes, we need to get the systems back online and retore from secure backups" there wasn't too much more input from any of the cyber defense IRs during this turn.

Conclusion and Takeaways

The most challenging part of this exercise for me was staying within my role as a Cyber Defense IR. Most of my responsibilities were small and detailed oriented that were challenging to express and act on since we didn't have any tools like Wireshark or SNORT in front of us. It was a unique experience to not take action on anything but just identify the actions that should be taken. In addition, it felt like it was easier for the SOC and NOC managers to speak out and share what are good next steps and then most of the time it felt like I was just chiming in saying "yes! Great idea, that falls within my responsibility." and that was the end of it. That was frustrating at times because it felt like I didn't get to play a super active role, but I also think that was influenced by my unfamiliarity with the role and responsibilities as well. Despite reading the preparation materials I felt unprepared to play the role and definitely was learning as I went and figuring out where I fit best in the exercise best as I went. This was mentioned in the post exercise feedback discussion as well, so I think that was a general feeling of the exercise. It would have been helpful to have had a case study or sample situation with each role's broken-down responsibilities or potential actions spelled out.

Overall, I appreciated the lack of preparation that was required for this exercise, and I didn't feel like there was too much more that I wanted to have known going in. I learn best by doing hands on things, so I think that this opportunity enabled me to learn a lot in an engaging and interesting way. I also kind of wish that the facilitator had pointed us in more interesting directions. It felt like the people who had interesting and managerial roles had a lot to talk about and speak up about and I was getting lost in the weeds and had to make the choice between staying quiet and true to my role or speaking up but maybe in the process going beyond the scope of my responsibilities. I wish that the facilitators had pushed a little bit more to give people working in low-level positions more to say and contribute that was both helpful to the overall discussion and true to our role's responsibilities.