陳奕嘉 E94115011 資訊115

**Advanced Cybersecurity Tactics & AI for Cybersecurity   
(12/23演講報告心得)**

**Table of Contents**

1. Cybersecurity Threat Landscape
2. Attack Kill Chain & Frameworks
3. AI for Cybersecurity and Cybersecurity for AI
4. Summary

**Session 1: Cybersecurity Threat Landscape**

For the first session, I was struck by how dynamic and ever-changing the cybersecurity threat landscape is. We delved into the concept of supply chain attacks and discussed why attackers often succeed—an unsettling reminder that our defenses need to be as agile and adaptive as the threats themselves. The conversation around Zero Trust Architecture (ZTA) resonated with me the most. The idea of continuously verifying identities, never taking any user or system for granted, felt incredibly relevant both in a corporate setting and in daily life.

It reminded me of my own habits, like using multi-factor authentication (MFA) for personal email or banking accounts. Hearing how companies implement MFA to guard against compromised credentials underscored for me that simple, regular security practices can make a significant difference.

Another highlight was revisiting the CIA Triad (Confidentiality, Integrity, and Availability). It’s interesting to realize how these principles—ones I’ve heard about before in various contexts—apply seamlessly to everyday tasks. Whether it’s using strong passwords on social media accounts, keeping regular backups of important files, or ensuring software is updated, these are steps I already practice to keep my personal digital footprint secure.

Finally, I appreciated learning about Red and Blue Team exercises. The proactive nature of running simulated attacks to uncover vulnerabilities is a strategy that, on reflection, I already apply in a smaller way—like staying vigilant for phishing attempts in my personal inbox. It’s reassuring to see how much overlap there is between corporate cybersecurity measures and everyday digital hygiene.

Overall, this session drove home the point that cybersecurity is not a distant, technical field; it’s a routine part of modern life. Our personal habits, whether it’s something as simple as safeguarding passwords, do contribute to a more secure digital environment.

**Session 2: Attack Kill Chain & Frameworks**

In the second session, I discovered how essential it is to understand the structure of a cyberattack through the concept of the Attack Kill Chain. Seeing the lifecycle laid out step by step—reconnaissance, exploitation, data exfiltration, and more—helped me grasp how attackers progress and, more importantly, how we can disrupt them at various points.

It was eye-opening to learn that the Kill Chain model has evolved since its introduction in 2011. Attackers now skip or blend stages to avoid detection, which parallels the way we see criminals attempting to trick online banking systems or social engineering their way around safeguards. This made me think of my own online banking habits—like verifying suspicious transactions or being cautious with emails requesting financial information—reminding me to remain vigilant because threats adapt rapidly.

The session also introduced the MITRE ATT&CK frameworks, which offer a detailed view of common attack techniques. This part underscored how important it is to be aware of tactics like phishing, credential dumping, and lateral movement. On a personal level, I realized it’s the same vigilance I use when I get strange links or login alerts—if something seems off, it probably is.

Threat Lifecycle Management (TLM) tied everything together, reminding me of how we respond to incidents in real life: collecting evidence, investigating thoroughly, and neutralizing threats. If I notice odd transactions on a credit card, my immediate response is to call the bank and freeze the account. The same logic applies to cybersecurity incidents—act quickly, gather information, and mitigate damage.

Reflecting on this session, I see the value of anticipating attacker moves. Whether in an organization or for personal devices, understanding the Kill Chain framework helps me feel more prepared, like I can spot risks sooner and respond more effectively.

**Session 3: AI for Cybersecurity and Cybersecurity for AI**

The final session explored a fascinating intersection: how AI both strengthens and challenges cybersecurity. As someone who relies heavily on AI-powered apps—like virtual assistants, recommended playlists, and even spam filters—learning about AI’s role in threat detection made me think about just how pervasive this technology is in my daily routines.

The shift from signature-based to behavior-based detection was particularly intriguing. Traditional antivirus solutions rely on known malware signatures, but AI models can spot unusual patterns and detect threats without an obvious signature. This reminded me of how streaming services seem to ‘know’ my preferences; they spot trends in my behavior. Similarly, AI-driven security tools pick up on irregular traffic patterns or anomalies in user behavior, potentially catching attacks before they spread.

Yet, this session also addressed AI’s vulnerabilities, like poisoning attacks, where malicious data skews the model’s training. It’s daunting to realize that as AI becomes more powerful, criminals can exploit it in new ways. I connected this to how misinformation online can manipulate trending topics or distort recommendations. The same principle applies in a cybersecurity context: if the AI model is fed the wrong data, it can be led astray.

Hearing about adversarial training and ensemble learning showed me how experts are tackling these challenges, and it made me reflect on how we train ourselves in everyday life: repeated exercises, simulations, and learning from mistakes all strengthen our defenses. The example of ML-based intrusion detection further emphasized AI’s potential—monitoring network traffic in real-time is like having a security guard who never sleeps.

From this session, I walked away with a mixed sense of both optimism and caution. AI’s ability to improve our defenses is immense, but it also introduces new attack surfaces. As AI becomes more embedded in daily life, ensuring these systems are protected is a responsibility we all share.

**Summary**

After listening to this seminar, I’m more convinced than ever that cybersecurity isn’t just for IT professionals—it’s a shared responsibility. We rely on digital platforms for so much, from socializing to banking, and even for critical infrastructure. Concepts like Zero Trust remind me to never let my guard down with unsolicited emails or risky downloads. The Kill Chain framework challenges me to think one step ahead of potential attackers. And the discussions around AI highlight that our tools are getting smarter, but so are the threats.

Ultimately, these seminars underscored the importance of developing strong cybersecurity habits. Whether it’s using MFA, staying updated on current threats, or understanding how AI-driven services operate, these behaviors add up to a healthier digital ecosystem. For me, the biggest takeaway is that small, consistent practices—both at home and at work—contribute significantly to overall security. By integrating these lessons into daily routines, we collectively build a more resilient and safe online world.