Huanjie Guo ID:10655496

1.Test plan

Type of cyber security test	**The effectiveness of the risk treatments**
Vulnerability scanning	1.Check the version and setting of the App, back-end, and website to find the vulnerability. 2. Check if the server has updated the security patches. 3. Calculate the hash of the data of patients, and if it changes, notify the administrator. 4. Scan the network of the server to find if there are some ports that can be closed.
Penetrating test	1. Clear objective Collect the information like IP address and domain of the ROC. 2. Information Collection Try to get the sensitive URL of the backend. Scan each port to make sure which application runs on it. Try to get the version of the operating system of the server. Try to detect the defense device and software. Try to get the information of the person who registers the domain and the name of the administrator in ROC. 3. Scan vulnerability Check if the OS has updated the new patches. Scan if there is any vulnerability in the port of 21/9090/7001/22/3389. Try to get the request of the server to check that if the token is in the cookie without encryption. 4. Validate the vulnerability. Use automatic scanning tools to get the results. Guess the username and password of the server, or use the BF algorithm to break it. 5. Information analysis Analyze if there is a firewall and how to bypass it. Analyze if the server has detected mechanism, IP packet monitor. Analyze the code used to attack, such as XSS, DDoS, and SQL injection. 6. Report Report what vulnerabilities have been found in the system of ROC and give some feedback about how to fix them.
Blue Team	1. Train the employees to prevent them from leaking data of the ROC. 2. Set up the firewall. 3. Secure database with strong password and encryption algorithm.

	4. Backup all data of ROC.
Purple Team	1. Work with the blue team to review how the server, apps, and sensitive documents are being protected and how events are being detected. 2. Work with the red team to address how the blue team's detection capability can be subverted.
Privacy Testing	1. Check if the ROC system only collects and uses patience' data and O2 relevant data relevant to its purposes. 2. Check if the ROC system has a method of tracking the consent of doctors and administrators. 3. Check if the ROC system can maintain a flag indicating that the information of patience, doctor, and O2 is in dispute.

2.Technical and technique-al takeaways from the guest lecturers

Topic	Guest	Recorded material available	Question and answer session(live)	Compulsory
Malware Evolution	Jon Noel	Hackers will use malware to steal our money, information, use our resources, and destroy a brand. Signature-based tools (anti-virus, firewalls, and intrusion prevention) are only effective against 30-50% of current security threats. The biggest vulnerability today is people.	I realize that encrypted communication like WhatsApp comes up with the end to end encryption to can secure our communication, but some people would use it to do things that are not on the correct side of the law. So cybersecurity can be a double-edged sword.	YES
Att&ck!	Paul Vlissidis	1.The framework of cybersecurity is Identify, Protect, Detect, Respond, Recover. 2. The attack vectors for Red Team can be exploitation, physical breaches, voice, email, SMS, instant messaging, wireless, and target personal footprints of staff. 3. The task of the Red Team is to define, observe, attack, assess, review.	I learn that the root causes of cybersecurity are mainly because of people and it is a little bit difficult to do a background check for a foreign because you need to go back to the source country to get stuff like criminal records. Besides, states are using cyber to gain an advantage in some diplomatic and sometimes less than diplomatic activities. That is what the world is and always	YES

		4. We can use purple teaming to improve cyber resilience.	be.	
Forced Digital Transformation	Ian Thornton	1. The lesson learned in 2020 is that diversity is equal to resilience, dependency increases vulnerability, control leads to predictability, observation is information, vision without resources is a hallucination, complexity is the enemy of security, and 70 to 93 percent of all communication is nonverbal. 2.There are some progress in the past five years, including multifactor authentication, vulnerability management, firewall access control lists, Geo-IP restrictions, SIEM/Logging, Network Performance Monitoring, Server Performance Monitoring.	From this session, I realize that it is a terrible situation now and it is unlikely that we will go back to the office soon because of the Covid-19. But fortunately, we are resilient creatures, and we will be in a position to move into this work from home. In the future, what we will see is a decreased pressure within the center part of the city.	YES