Assignment #4

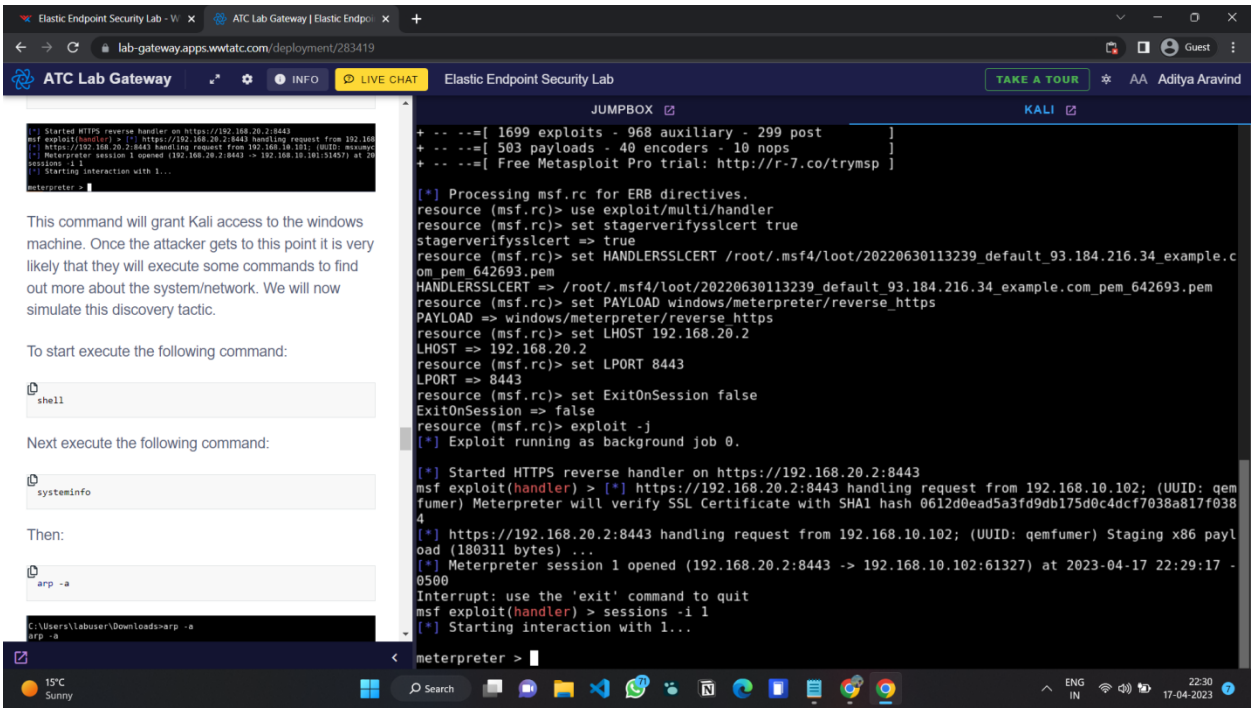
Aditya Aravind Medepalli

Intrusion Detection and Analysis

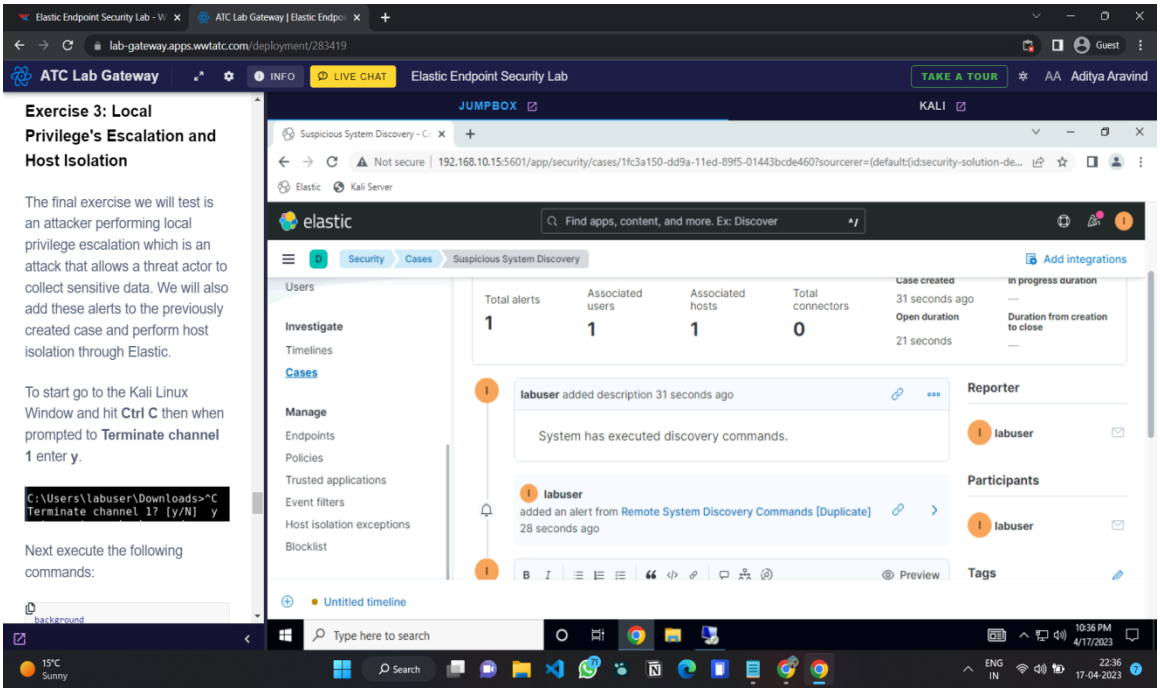
Saint Louis University

April 17th, 2023

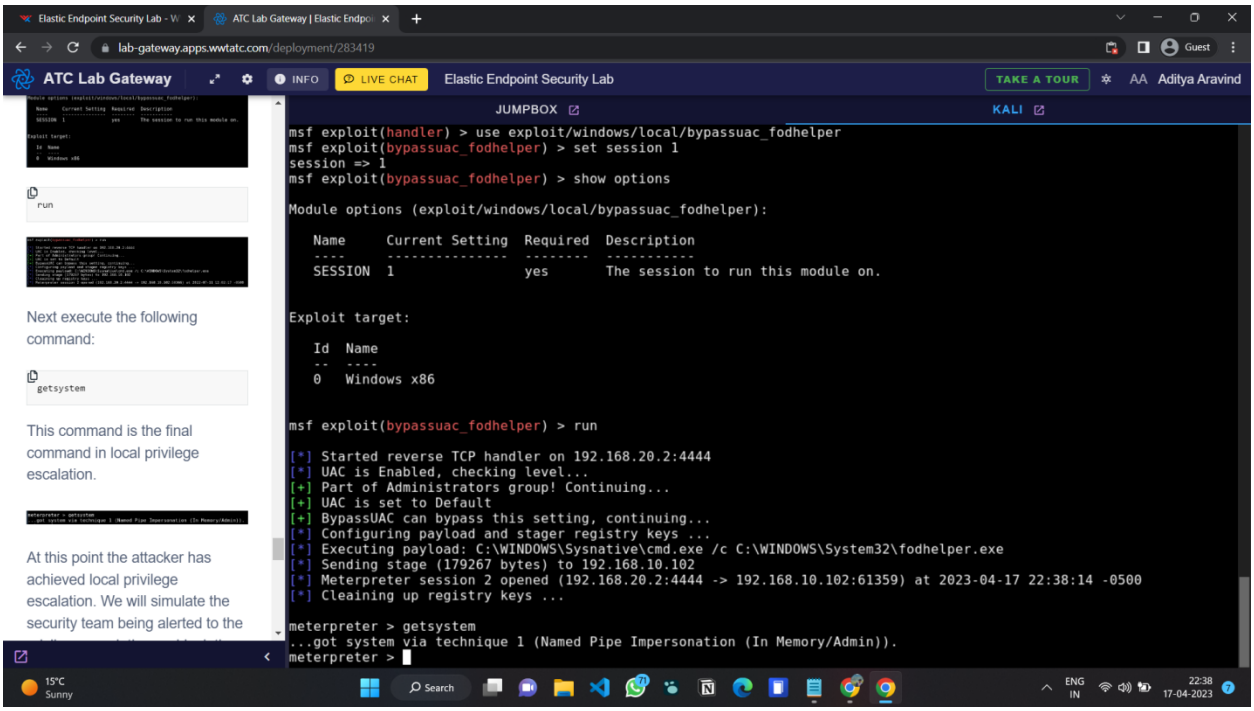
Exercise 1 - Phishing Link and Malware Download



Exercise 2: Execution, Discovery, and Create a Case



Exercise 3: Local Privilege's Escalation and Host Isolation



a. What was the most challenging step?

The intricacies of launching a Meterpreter session to connect with a remote host and making it operational in a Windows environment present a formidable challenge in the art of hacking. This is because the Windows system has robust security measures in place that are purposefully designed to thwart any unauthorized access attempts, and initiating a Meterpreter session requires expert-level circumvention of these measures. Furthermore, the task of configuring the session to function flawlessly in the Windows environment entails a complex set of commands and configurations that demand technical proficiency and Windows-specific knowledge using alerts and rules in kibana. The successful launch of a Meterpreter session in a Windows environment requires a hacker to possess a profound understanding of the intricacies of the Windows operating system, coupled with advanced hacking techniques and tools. It is worth

noting that even seasoned hackers may encounter significant difficulties during this phase due to the meticulous planning, precise execution, and thorough troubleshooting needed to guarantee a smooth and undetected session operation.

b. The goal of this lab is to introduce users to XDR technology through the use of an Endpoint Security solution. In your perspective, what do you think about security detection rules and navigating alerts, monitoring, and response capabilities of this Endpoint Security?

Security detection rules hold paramount importance in the realm of identifying potential security threats and breaches within an organization's network. These rules can be adjusted to trigger alerts when specific events or patterns are detected, such as unusual network traffic, unauthorized access attempts, or suspicious user activity. The arduous task of navigating alerts and monitoring, is a formidable challenge for security analysts, as they must adeptly distinguish between legitimate alerts and false positives, whilst simultaneously investigating and responding to security incidents.

In tandem with detection rules, effective response capabilities are equally important for the mitigation of security threats and the minimization of their impact. Endpoint Security solutions are typically bestowed with a range of response capabilities, including the quarantine of infected devices, blocking of malicious traffic, and the provision of detailed forensic data to support incident investigation. It is noteworthy, however, that automated response actions may not always be suitable or effective, necessitating human intervention in certain scenarios.

In conclusion, a truly robust Endpoint Security solution ought to offer comprehensive security detection rules and monitoring capabilities, coupled with a diverse array of effective response actions. Moreover, such a solution must be agile, and scalable to dynamically adapt to the evolving needs and shifting threat landscape of the organization.