Project Name:	Log4j/log4Shell
Project Team Members:	Pasha Khan, Derek Lin
Start of class	End of Day

Project Milestone	Due	Details	Notes from Standup with Instructor	
Proposal + Team Contract	Wednesday 4/6	Propose your idea to two (2) separate instructors for approval		Project Proposal - 4/6 end of class
Proof of Concept	Sunday 4/10	Can this idea turn into a reality? What do you need to do to prove it? The point is to identify any technical issues you may have. Determine if your project *can* be done.		PoC - 4/10 end of class
Minimum Viable Product	Friday 4/15	You have achieved the absolute minimum as far as necessary features show in PoC phase. This may look like you have solved your problem/challenge for at least one case.		Most Viable Product (MVP) - 4/15 end of class
Complete Project	Sunday 4/17	Iron out the kinks, receive feedback from peers and instructors, iterate over the MVP		Project Deadline 4/17 beginning of class
First Draft Script and Demo	4/20	Script must be complete and demo'd to instructors/		Script Deadline 4/20 first draft beginning of class
Recording	4/22	Recording complete		Presentation 4/22 end of class
Complete Presentation	4/22	Any final touches / editing - Share with friends, family, and social media.		
Present Project	4/23	Present Projects during graduation/friends & family		

Project Name:	Log4j/log4Shell Exploit
Project Team Members:	Pasha Khan, Derek Lin
	Specifics For Your Project
Overview	The log4j/log4Shell exploit (CVE-2021-44228) was a very critical vulnerability that affected a multitude of webservers around the world. On November 24th, 2021 the apache log4j opensource software, version 2.15.0 or prior vulnerability was reported. This software allows lookups to appear in log messages. When a malicious client inputs a request that contains malicious Java Naming Directory Interface (JNDI) query, the application server will receive the request but also malicious javacode can be downloaded and executed that can contain remote code execution. Due to this, in this project we will be exploring the vulnerability and looking into the given scripts and apply this to try to exploit a VM machine to show how the exploit operates.
PoC - Proof of Concept	Analyze and explain poc.py located at https://github.com/kozmer/log4j-shell-poc line for line and demonstrate how poc.py is able to expose the log4j vulnerability for version 2.15 and prove we are able to gain remote shell access.
MVP	We will be analyzing and explaining poc.py line for line.
Complete Project	Demonstrate how the exploit operates on a vulnerable target.
Stretch Goals	Create/code our own exploit and demonstrate its operation on a vulnerable target.

	Link	Notes:
Ex. Github		https://github.com/dereklin15/Fullstack-Capstone-Final-Project.git
Working Doc		https://drive.google.com/drive/folders/1eivoOHvLUBzfcB3B0lHXk_P5C9R1pJq3