**AIG internship**

**Task 1: Responding to a zero-day vulnerability**

* Review some recent publications from the Cybersecurity & Infrastructure Security Agency (CISA)
  + apache Log4j
  + vulnerability [CVE-2021-44228](https://nvd.nist.gov/vuln/detail/CVE-2021-44228)
  + java based library containing flaw, that can be exploited
  + 3 billion devices run java
  + apache software foundation creator of log4j released emergency patch which fixed the vulnerarbility
* Research the reported vulnerability
  + **Researched**
* Draft an email to affected teams to alert them of the vulnerability, and explain how to remediate
* **From:**AIG Cyber & Information Security Team  
  **To:** Product Development Team (product@email.com)  
  **Subject:**Security Advisory concerning Product Development Staging Environment | Log4j  
  —  
  **Body:**  
  Hello John Doe,  
    
  AIG Cyber & Information Security Team would like to inform you that a recent Log4j vulnerability has been discovered in the security community that may affect the Product Development Staging Environment infrastructure.  
    
  Vulnerability Overview  
  Log4j is a common open-source tool used for application logging and monitoring across the web. Recently, a vulnerability has been identified in versions Log4j2 2.0-beta9 through 2.15.0 that would allow an unauthenticated attacker to perform remote code execution on affected infrastructure, making this a critical vulnerability. You can learn more in the NIST disclosures: [NVD - CVE-2021-44228](https://nvd.nist.gov/vuln/detail/CVE-2021-44228) and [NVD - CVE-2021-45046](https://nvd.nist.gov/vuln/detail/CVE-2021-45046).  
    
  Affected products  
  Log4j2 2.0-beta9 through 2.15.0  
    
  Risk & Impact  
  Critical - remote code execution (RCE). An attacker will be able to remotely access the Product Development Staging Environment infrastructure to exfiltrate data or execute malicious actions.  
    
  Remediation  
  ● Identify any assets or infrastructure running the affected Log4j version  
  ● Update to the following versions: Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7)  
  ● Be on the lookout for any signs of exploitation  
    
  If you identified any signs of exploitation, please immediately reach out. After you have remediated this vulnerability, please confirm with the security team by replying to this email.  
    
  For any questions or issues, don’t hesitate to reach out to us.  
    
  Kind regards,  
  AIG Cyber & Information Security Team
* analyze the “Infrastructure List” below to find out which infrastructure may be affected by the vulnerability, and which team has ownership.
  + Product Development Staging Environment may be affected by vulnerability, and Product Development has ownership

**Task 2 -** Write a Python script to bruteforce the decryption key of the encrypted file, to avoid paying a ransom

* from zipfile import ZipFile
* def attempt\_extract(zf\_handle, password):
* try:
* zf\_handle.extractall(pwd=password)
* return True
* except:
* return False
* def main():
* print("[+] Beginning bruteforce ")
* with ZipFile('enc.zip') as zf:
* with open('rockyou.txt', 'rb') as f:
* for p in f:
* password = p.strip()
* if attempt\_extract(zf, password):
* print("[+] Correct password: %s" % password)
* exit(0)
* else:
* print("[-] Incorrect password: %s" % password)
* print("[+] Password not found in list")
* if \_\_name\_\_ == "\_\_main\_\_":
* main()