**Justin Goncalves**
12/4/2024

# AIG Security Engineering Program

## Table of Contents



## Program Overview:

Welcome to AIG's Shields Up: Cybersecurity Job Simulation!

In this simulation, you will learn skills - both non-technical and technical - that are used in the world of cybersecurity. Specifically, notify internal stakeholders that may be at risk from a ransomware attack and then help recover some hacked files. You will learn how to analyze alerts from the Cybersecurity & Infrastructure Security Agency (CISA), in collaboration with the FBI and the NSA - and then apply the intel to reduce the risk of an attack on AIG.

We hope this program provides a great resource for you to up-skill and strengthen your resume as you explore career options and a potential career in cybersecurity!

Skills you will learn and practice: Cybersecurity, Vulnerability Triage, Security Advisory, Problem Solving, Research, Communication, Data Analysis, Strategy, Software Development, Python, Security Engineering, Solution Architecture, Design Thinking

**Task One:** Responding to a zero-day vulnerability
CISA has just released an alert on a new zero-day vulnerability for Apache Log4j. Research the vulnerability and publish an advisory to affected teams to alert and prevent exploitation.

What you'll learn

- How to address a vulnerability that may affect internal infrastructure

What you'll do

- Review some recent publications from the Cybersecurity & Infrastructure Security Agency (CISA)
- Research the reported vulnerability
- Draft an email to affected teams to alert them of the vulnerability, and explain how to remediate

**Task Two:** (Technical) Bypassing Ransomware
One of our servers has been exploited by the Log4j vulnerability, and the attacker just tried to load some ransomware! Write a bruteforcer to break into the ransomware-encrypted files, so we don't have to pay the ransom

What you'll learn

- What 'bruteforcing' involves
- How to respond to a ransomware virus using Python

What you'll do

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

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

*Review the scenario below. Then complete the tasks and activities.*

### Scenario

"Hi there, my name is Justine, and I am part of our information security team. We just received an alert from the Cybersecurity and Infrastructure Agency (CISA) that was released in collaboration with the FBI and the NSA. It published a joint urgent advisory about an emerging vulnerability regarding the popular open-source logging software Apache Log4j. I've attached the advisory in the resource section below. We often subscribe to vulnerability feeds such as these to stay on top of vulnerabilities disclosed to the public, so we can fix them before an attacker can exploit them.

As an information security analyst, I'll need you to respond to the zero-day vulnerability. Please do so by researching the vulnerability, analyzing our infrastructure list, and drafting an advisory email to the affected teams which contains a remediation program, and assurances to prevent exploitation. Our Chief Information Security Officer (CISO) is concerned about the recent increase in ransomware attacks, and combined with the recent Log4j vulnerability, it can be the perfect recipe for an attacker to strike. Ransomware viruses often encrypt all files on a device, asking for payment in order to access the decrypted file. Make sure to check out all of the resources. You'll need to identify which teams and infrastructure may have been affected by the vulnerability."

### Here is the background information for your task

You are an Information Security Analyst in the Cyber & Information Security Team.

A common task and responsibility of information security analysts is to stay on top of emerging vulnerabilities to make sure that the company can remediate them before an attacker can exploit them.

In this task, you will be asked to review some recent publications from the Cybersecurity & Infrastructure Security Agency (CISA). The Cybersecurity & Infrastructure Security Agency (CISA) is an Agency that has the goal of reducing the nation's exposure to cybersecurity threats and risks.

After reviewing the publications, you will then need to draft an email to inform the relevant infrastructure owner at AIG of the seriousness of the vulnerability that has been reported.

### Here is your task

The CISA has recently published the following two advisories:

The first advisory (Log4j), outlines a serious vulnerability in one of the world's most popular logging software.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a

The second advisory explores how ransomware has been increasing and is becoming professionalized - a concern for a large company like AIG.
https://www.cisa.gov/news-events/news/cisa-fbi-nsa-and-international-partners-issue-advisory-ransomware-trends-2021

Your task is to respond to the Apache Log4j zero-day vulnerability that was released to the public by advising affected teams of the vulnerability.

**First**, conduct your research on the vulnerability using the “CISA Advisory" resources provided above as a starting point.

**Next**, analyze the “Infrastructure List” below to find out which infrastructure may be affected by the vulnerability, and which team has ownership.

| Product Team | Product Name | Team Lead | Services Installed |
|---|---|---|---|
| IT | Workstation Management System | Jane Doe (tech@email.com) | ● OpenSSH<br>● dnsmasq<br>● lighttpd |
| Product Development | Product Development Staging Environment | John Doe (product@email.com) | ● Dovecot pop3d<br>● Apache httpd<br>● Log4j<br>● Dovecot imapd<br>● MiniServ |
| Marketing | Marketing Analytics Server | Joe Schmoe (marketing@email.com) | ● Microsoft ftpd<br>● Indy httpd<br>● Microsoft Windows RPC<br>● Microsoft Windows netbios-ssn<br>● Microsoft Windows Server 2008 R2 - 2012 microsoft ds |
| HR | Human Resource Information System | Joe Bloggs (hr@email.com) | ● OpenSSH<br>● Apache httpd<br>● rpcbind2-4 |

**Resources to help you with the task**

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a
2. https://www.cisa.gov/news-events/news/cisa-fbi-nsa-and-international-partners-issue-advisory-ransomware-trends-2021

## Research Conducted on the Log4j Vulnerability

To effectively address the Log4j vulnerability, I began by thoroughly reviewing the advisory issued by CISA, the FBI, and the NSA. This advisory detailed the critical nature of the vulnerability, known as Log4Shell, which affects Log4j versions 2.0-beta9 through 2.15.0. The advisory highlighted the vulnerability's ability to enable unauthenticated remote code execution by exploiting the Java Naming and Directory Interface (JNDI), leading to severe consequences such as full system compromise. Additionally, I noted that active exploitation of this vulnerability had already been observed globally, underscoring its urgency.

After understanding the technical details, I analyzed our internal infrastructure list to identify potentially impacted systems. By cross-referencing the advisory with the services installed across various teams, I determined that the Product Development Staging Environment was particularly at risk due to its use of Log4j. This environment's critical role in development processes made it a priority for immediate remediation, ensuring the vulnerability was addressed before exploitation could occur.

## Log4j Vulnerability Security Advisory Email

After identifying the impacted system, I drafted an advisory email to notify the infrastructure owner. The email detailed the risk, explained how the vulnerability could be exploited, and provided remediation steps such as upgrading Log4j and isolating vulnerable assets.

Zero-Day Vulnerability Advisory Email

**From**: AIG Cyber & Information Security Team
**To**: John Doe (product@email.com)
**Subject**: Security Advisory: Log4j Vulnerability Impacting Product Development Staging Environment

Hello John,

The AIG Cyber & Information Security Team would like to notify you of a critical Log4j vulnerability **(CVE-2021-44228)** recently disclosed in the security community. This vulnerability directly impacts the Product Development Staging Environment infrastructure due to its use of Log4j.

**Vulnerability Overview:**
Log4j is an open-source logging library commonly used in applications and enterprise systems. The disclosed vulnerability, known as Log4Shell, affects versions Log4j2 2.0-beta9 through 2.15.0. It allows unauthenticated attackers to exploit the Java Naming and Directory Interface (JNDI) to perform remote code execution (RCE), which can lead to full system compromise. This vulnerability is critical, with exploitation already being observed by threat actors globally.

**Risk/Impact:**
The vulnerability is classified as critical due to the potential for remote code execution. An attacker could exploit this vulnerability to gain unauthorized access to the Product Development Staging Environment, exfiltrate sensitive data, deploy ransomware, or perform other malicious actions.

**Affected Versions:**
Log4j2 2.0-beta9 through 2.15.0

**Remediation Steps:**
To address this vulnerability, we recommend the following immediate actions:

- **Identify vulnerable systems**: Audit all assets and applications in the Product Development Staging Environment to identify instances of Log4j running affected versions.
- **Apply patches**: Upgrade to Log4j version 2.16.0 (Java 8) or 2.12.2 (Java 7) as recommended by Apache.
- **Isolate vulnerable systems**: Treat all identified vulnerable assets as compromised and isolate them from the network until remediation is complete.
- **Monitor for exploitation**: Review system logs and monitor for indicators of compromise or abnormal activity.

We strongly urge you to implement the above measures immediately to safeguard your environment. Please confirm with the security team once remediation steps have been applied and the issue has been resolved. If you encounter any challenges or identify signs of exploitation, report them immediately.

For any further questions or concerns, don’t hesitate to reach out to us.

Kind regards,
Justin Goncalves
*AIG Cyber & Information Security Team*

## Task 2: (Technical) Bypassing Ransomware

*Review the scenario below. Then complete the tasks and activities.*

### Scenario

Your advisory email in the last task was great. It provided context to the affected teams on what the vulnerability was, and how to remediate it.

Unfortunately, an attacker was able to exploit the vulnerability on the affected server and began installing a ransomware virus. Luckily, the Incident Detection & Response team was able to prevent the ransomware virus from completely installing, so it only managed to encrypt one zip file.

Internally, the Chief Information Security Officer does not want to pay the ransom, because there isn't any guarantee that the decryption key will be provided or that the attackers won't strike again in the future.

Instead, we would like you to bruteforce the decryption key. Based on the attacker's sloppiness, we don't expect this to be a complicated encryption key, because they used copy-pasted payloads and immediately tried to use ransomware instead of moving around laterally on the network.

### Here is the background information for your task

In this task, you will write a Python script to bruteforce the decryption key of the encrypted file.

Bruteforcing is the act of repeatedly trying different combinations to break the password encryption (based on either randomly generated passwords, or from a list of passwords to try). In the resource below, we've provided a small subset of passwords from Rockyou - a widely know password wordlist that contains thousands of common passwords in one wordlist.

Ransomware will often encrypt all files on a device, and sometimes give the decryption key after the ransom has been paid (but this is not always the case!). In this task, we would like you to break the encryption without paying the ransom.

Download the `enc.zip` and **rockyou.txt** files and create a Python script to attempt to bruteforce the password on the encrypted file. Once you have gained access to the encrypted file, past your python script under the super sensitive confidential information, and upload it!

## Security Engineering to Bypass Ransomware

In this task, I wrote and executed a Python script to brute-force the password of an encrypted zip file affected by a ransomware attack. The script used the zipfile library to iterate through each password in the rockyou.txt wordlist, systematically attempting to decrypt the file. I created a function, attempt_extract, which attempted to unlock the file with each password and exited the loop once the correct key was found.

Once executed, the script successfully identified "SPONGEBOB" as the decryption key, unlocking the encrypted file. This process required precise handling of the wordlist and careful debugging to ensure the script iterated through the passwords efficiently while correctly handling exceptions for failed attempts. This approach allowed me to unlock the file and demonstrate the practicality of automated brute-forcing techniques.

This is the super sensitive, confidential document that was affected by the ransomware.
Congratulations on the bruteforce!

You can paste your bruteforce script in the box below:

```
'''
AIG Security Engineering Program
Justin Goncalves
Bruteforce Python Script
'''

from zipfile import ZipFile

# Use a method to attempt to extract the zip file with a given
password
def attempt_extract(zf_handle, password):
    try:
        zf_handle.extractall(pwd=password)
        print(f"[+] Password found: {password.decode('utf-8')}")
        return True
    except:
        return False

def main():
    print("[+] Beginning bruteforce ")
    with ZipFile('enc.zip') as zf:
        with open('rockyou.txt', 'rb') as f:
            for line in f:
                # Iterate through password entries in rockyou.txt
                password = line.strip()
                # Attempt to extract the zip file using each
password
                if attempt_extract(zf, password):
                    # Exit the loop if the password is found
                    break
            else:
                # This block executes if no password in the list
works
                print("[-] Password not found in list")

if __name__ == "__main__":
    main()
```

## Personal Reflection

This task was an excellent opportunity to deepen my understanding of brute-force techniques and how they can be applied in real-world scenarios to mitigate cybersecurity incidents. By writing a Python script to decrypt an encrypted file, I gained valuable experience with automation, problem-solving, and handling large datasets like the `rockyou.txt` wordlist. This process helped me see how essential programming and scripting skills are for quickly responding to ransomware attacks and similar threats in a cybersecurity environment.

Developing the script required a methodical approach to implementing error handling, iterative logic, and leveraging built-in Python libraries such as `zipfile`. I also learned the importance of efficiency in coding, as each iteration over a wordlist needs to be optimized for time-sensitive scenarios. Successfully unlocking the file reinforced my confidence in applying technical skills to address challenges that arise in a Security Operations Center (SOC) setting.

Looking ahead, the knowledge gained from this task will be invaluable as I prepare for a career in cybersecurity. This experience not only improved my ability to write effective scripts but also highlighted the importance of resilience and persistence when tackling complex problems. I feel more prepared to handle similar real-world incidents in the future and contribute meaningfully to the security of organizational systems.

Certificate of Completion

AIG NEW YORK JOBS CEO COUNCIL

Forage

Inspiring and empowering future professionals

# JUSTIN GONCALVES

## Shields Up: Cybersecurity Job Simulation

Certificate of Completion

December 4th, 2024

Over the period of December 2024, JUSTIN GONCALVES has completed practical tasks in:

Responding to a zero-day vulnerability
(Technical) Bypassing ransomware

**Tom Brunskill**
CEO, Co-Founder of Forage

Enrolment Verification Code 3BDo9FBY86A2MFatk | User Verification Code rCsmcFfq94jiPnW64 | Issued by **Forage**