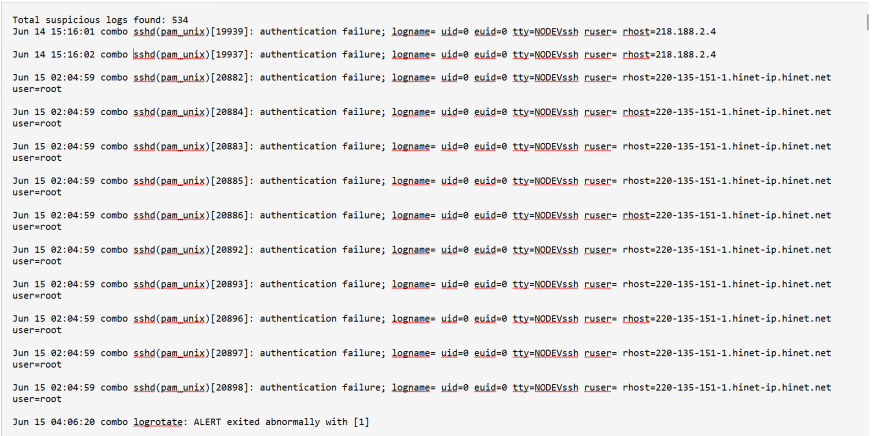
Group Automation Assignment Report

Process Behind the Code

1. Log File Analysis
    a. Reads and parses log Files
        i. Lines 3 and 4
    b. Filters for relevant data in the log files
        i. Line 7
    c. Generates a summary report text file on suspicious logs
        i. Lines 9 - 12
2. System Performance Monitoring
    a. Import the psutil library
        i. Line 18
    b. Collects system metrics
        i. Lines 21 - 26
    c. Logs the performance data
        i. Lines 29 and 30
    d. Generates alerts for high usage
        i. Lines 33 and 34
3. Alert Generation
    a. Defines the event to monitor
    b. Sends alerts via email
        i. a and b on lines 39 - 55
4. Automating Routine Security Checks
    a. Installs and uses nmap for vulnerability scanning
        i. Lines 65 - 71
    b. Monitors network traffic with scapy
        i. Lines 76 - 83

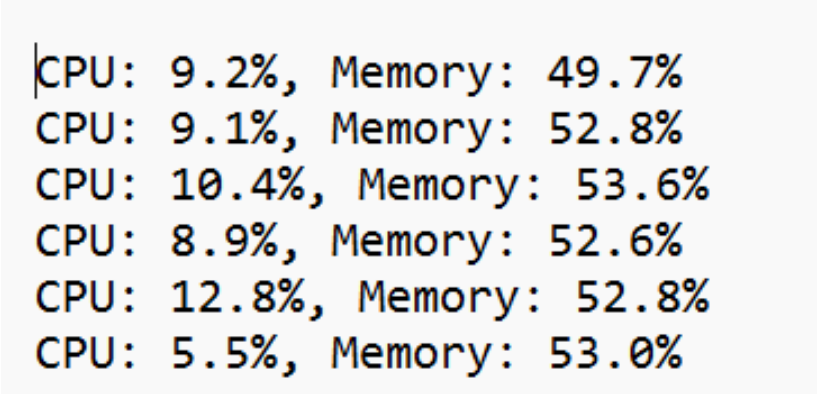
Screenshot of Outputs

- From Log File Analysis



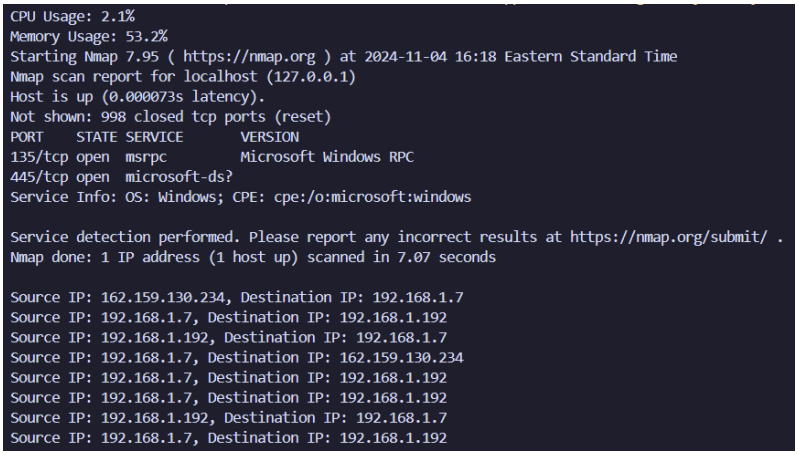
```
Total suspicious logs found: 534
Jun 14 15:16:01 combo sshd(pam_unix)[19939]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4

Jun 14 15:16:02 combo sshd(pam_unix)[19937]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4

Jun 15 02:04:59 combo sshd(pam_unix)[20882]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20884]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20883]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20885]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20886]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20892]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20893]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20896]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20897]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 02:04:59 combo sshd(pam_unix)[20898]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net
user=root

Jun 15 04:06:20 combo logrotate: ALERT exited abnormally with [1]
```

- From System Performance Monitoring



```
CPU: 9.2%, Memory: 49.7%
CPU: 9.1%, Memory: 52.8%
CPU: 10.4%, Memory: 53.6%
CPU: 8.9%, Memory: 52.6%
CPU: 12.8%, Memory: 52.8%
CPU: 5.5%, Memory: 53.0%
```

- Terminal Output



```
CPU Usage: 2.1%
Memory Usage: 53.2%
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-04 16:18 Eastern Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000073s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds

Source IP: 162.159.130.234, Destination IP: 192.168.1.7
Source IP: 192.168.1.7, Destination IP: 192.168.1.192
Source IP: 192.168.1.192, Destination IP: 192.168.1.7
Source IP: 192.168.1.7, Destination IP: 162.159.130.234
Source IP: 192.168.1.7, Destination IP: 192.168.1.192
Source IP: 192.168.1.7, Destination IP: 192.168.1.192
Source IP: 192.168.1.192, Destination IP: 192.168.1.7
Source IP: 192.168.1.7, Destination IP: 192.168.1.192
```