**Name: Muhammad Usman Ali Sadiq**

# Cyber Security

Company: Digital Empowerment Network

# Task 03

# Developing Incident Response Plans

## ➢ Identify Potential Security Incidents and Scenarios

### Conduct a Threat Assessment:

**Example Scenarios**:

- **Malware Infection**: A user inadvertently downloads malware, compromising their workstation.
- **Phishing Attack**: An employee falls victim to a phishing email, disclosing their credentials.
- **Insider Threat**: A disgruntled employee accesses sensitive data without authorization.
- **Data Breach**: An attacker exploits a vulnerability in a web application to access customer data.

### Categorize Incidents by Severity:

- **Low Severity**: Minor malware detected; no sensitive data affected.
- **Medium Severity**: Phishing incident with potential credential theft.
- **High Severity**: Data breach affecting sensitive customer information.

## Define Roles and Responsibilities for the Response Team

**Incident Response Team Structure**:

- **Incident Commander**: Oversees incident management.
  - **Name**: [Insert Name]
  - **Contact Info**: [Insert Contact Info]
- **Technical Lead**: Coordinates technical response.
  - **Name**: [Insert Name]
  - **Contact Info**: [Insert Contact Info]
- **Communications Officer**: Handles all communications and press releases.
  - **Name**: [Insert Name]
  - **Contact Info**: [Insert Contact Info]
- **Legal Advisor**: Ensures compliance with laws and regulations.
  - **Name**: [Insert Name]
  - **Contact Info**: [Insert Contact Info]
- **Forensic Analyst**: Conducts investigations and analyzes incidents.
  - **Name**: [Insert Name]
  - **Contact Info**: [Insert Contact Info]

- **Responsibilities**:
  - Each member's responsibilities should be documented in the IRP to clarify expectations during an incident.

## Develop Step-by-Step Response Procedures

**Preparation**:

- **Maintain Security Controls**: Ensure firewalls, antivirus, and intrusion detection systems (IDS) are updated.

**Identification**:

- **Incident Reporting Mechanism**: Create an internal email or ticketing system for reporting incidents.

**Containment**:

- **Short-term Containment**: Isolate the affected system from the network.
- **Long-term Containment**: Implement temporary fixes to allow business operations while addressing the incident.

**Eradication**:

- **Remove Malware**: Use antivirus tools to clean infected systems.
- **Review and Patch Vulnerabilities**: Ensure that any exploited vulnerabilities are patched.

**Recovery**:

- **System Restoration**: Restore affected systems from clean backups.
- **Monitoring**: Implement enhanced monitoring to detect any signs of recurrence.

**Post-Incident Analysis**:

- **Conduct a Debriefing**: Document lessons learned and recommendations for improvement.

## ➢ Conduct Training and Simulation Exercises

**Training Schedule**:

- **Quarterly Training Sessions**: Focus on different incident types each quarter.

**Simulation Exercises**:

- **Tabletop Exercises**: Conduct discussions around hypothetical scenarios.
- **Live Simulations**: Execute a mock incident response to test readiness and coordination

## ➢ Review and Update the Plan Regularly

**Schedule Reviews**:

**Biannual Review of the IRP**: Set specific dates .

**Feedback Mechanism**:

**Post-Incident Surveys**: Collect feedback from team members involved in incident response to enhance the IRP.

# Implementation Steps

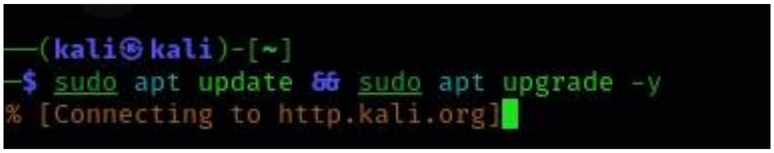
1. **Draft the IRP**: Fill in the template with specific details relevant to your organization.
2. **Distribute the Plan**: Share the IRP with all relevant stakeholders and team members.
3. **Conduct Initial Training**: Schedule a kick-off training session to familiarize everyone with the plan.

4. **Implement Monitoring Tools**: Ensure necessary tools for detecting incidents are in place.
5. **Plan the First Simulation**: Organize an initial tabletop exercise to test the response procedures.

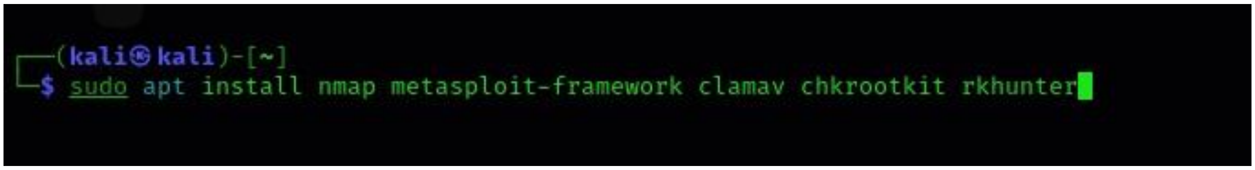
# Practical

## Setting Up Your Environment:

Before you begin, ensure you have the necessary tools installed. Kali Linux comes pre-installed with many security tools, but you may want to ensure some essential ones are ready to use:



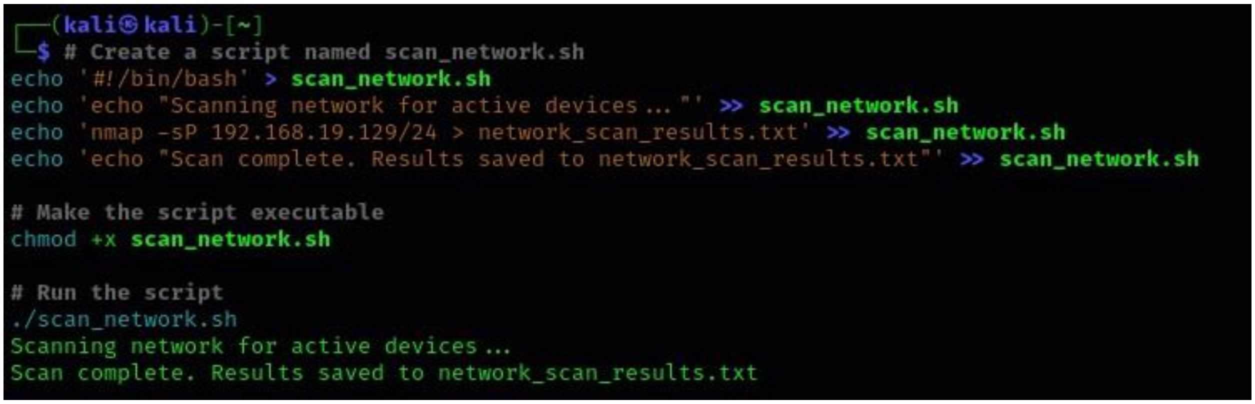
```
──(kali㉿kali)-[~]
─$ sudo apt update && sudo apt upgrade -y
% [Connecting to http.kali.org]
```



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install nmap metasploit-framework clamav chkrootkit rkhunter
```

## ➢ Identifying Potential Security Incidents

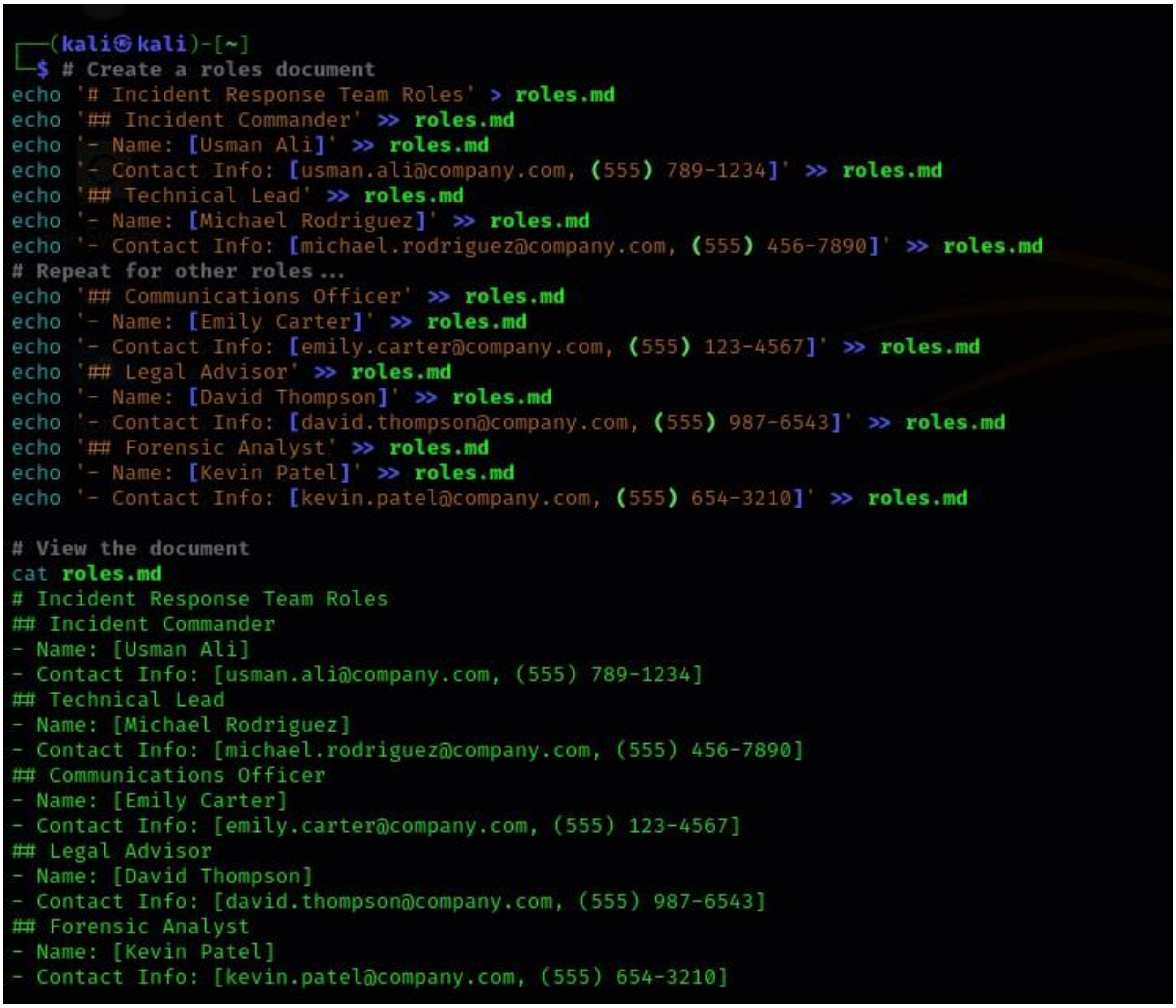
You can write a script to scan the network for active devices and services using Nmap. This helps identify potential entry points for security incidents.



```
┌──(kali㉿kali)-[~]
└─$ # Create a script named scan_network.sh
echo '#!/bin/bash' > scan_network.sh
echo 'echo "Scanning network for active devices..."' >> scan_network.sh
echo 'nmap -sP 192.168.19.129/24 > network_scan_results.txt' >> scan_network.sh
echo 'echo "Scan complete. Results saved to network_scan_results.txt"' >> scan_network.sh

# Make the script executable
chmod +x scan_network.sh

# Run the script
./scan_network.sh
Scanning network for active devices...
Scan complete. Results saved to network_scan_results.txt
```

## ➢ Defining Roles and Responsibilities

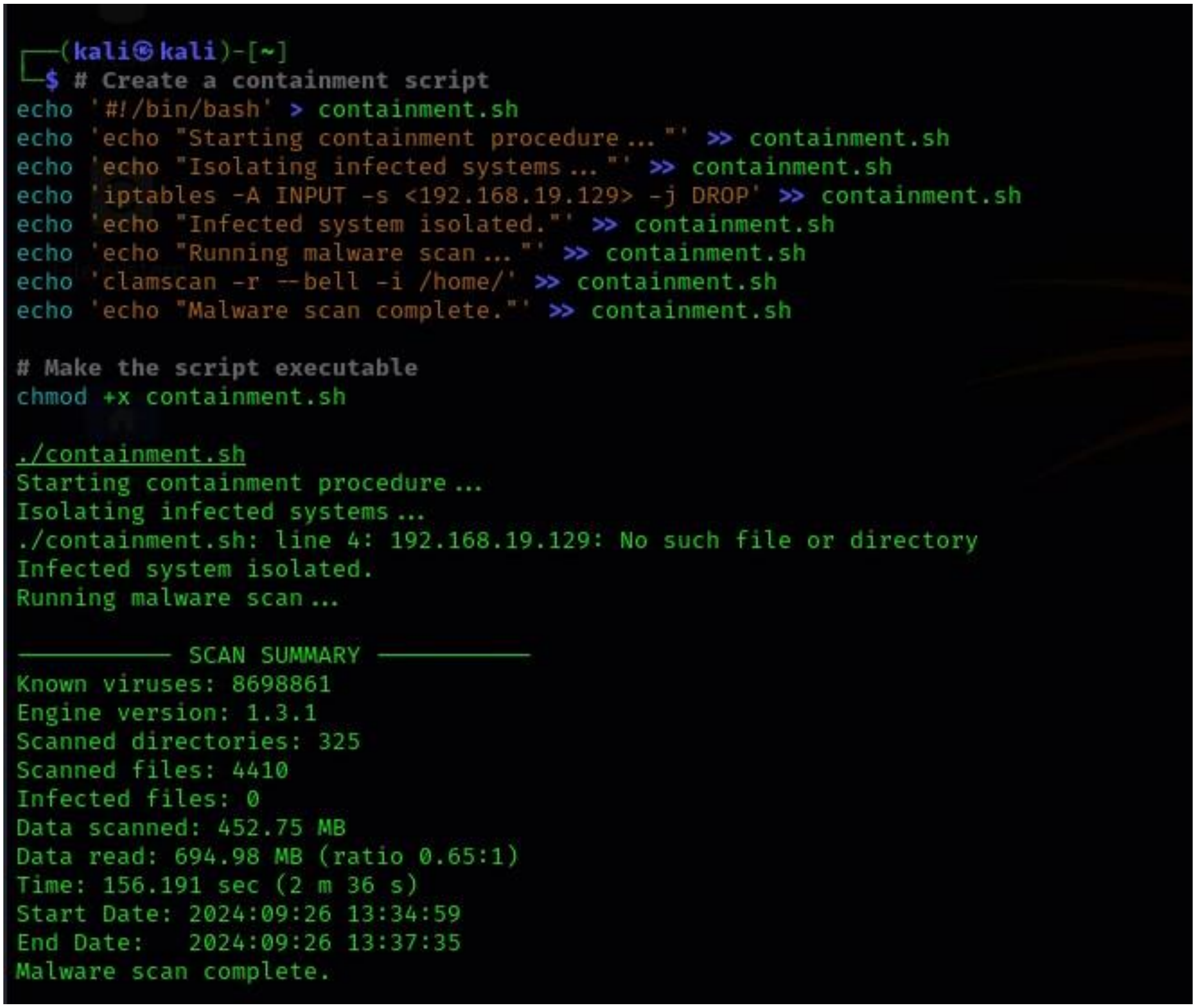
This can be documented in a markdown file or text file. Here’s how you can create a simple document for roles.



```
┌──(kali㉿kali)-[~]
└─$ # Create a roles document
echo '# Incident Response Team Roles' > roles.md
echo '## Incident Commander' >> roles.md
echo '- Name: [Usman Ali]' >> roles.md
echo '- Contact Info: [usman.ali@company.com, (555) 789-1234]' >> roles.md
echo '## Technical Lead' >> roles.md
echo '- Name: [Michael Rodriguez]' >> roles.md
echo '- Contact Info: [michael.rodriguez@company.com, (555) 456-7890]' >> roles.md
# Repeat for other roles...
echo '## Communications Officer' >> roles.md
echo '- Name: [Emily Carter]' >> roles.md
echo '- Contact Info: [emily.carter@company.com, (555) 123-4567]' >> roles.md
echo '## Legal Advisor' >> roles.md
echo '- Name: [David Thompson]' >> roles.md
echo '- Contact Info: [david.thompson@company.com, (555) 987-6543]' >> roles.md
echo '## Forensic Analyst' >> roles.md
echo '- Name: [Kevin Patel]' >> roles.md
echo '- Contact Info: [kevin.patel@company.com, (555) 654-3210]' >> roles.md

# View the document
cat roles.md
# Incident Response Team Roles
## Incident Commander
- Name: [Usman Ali]
- Contact Info: [usman.ali@company.com, (555) 789-1234]
## Technical Lead
- Name: [Michael Rodriguez]
- Contact Info: [michael.rodriguez@company.com, (555) 456-7890]
## Communications Officer
- Name: [Emily Carter]
- Contact Info: [emily.carter@company.com, (555) 123-4567]
## Legal Advisor
- Name: [David Thompson]
- Contact Info: [david.thompson@company.com, (555) 987-6543]
## Forensic Analyst
- Name: [Kevin Patel]
- Contact Info: [kevin.patel@company.com, (555) 654-3210]
```

## ➢ Developing Step-by-Step Response Procedures

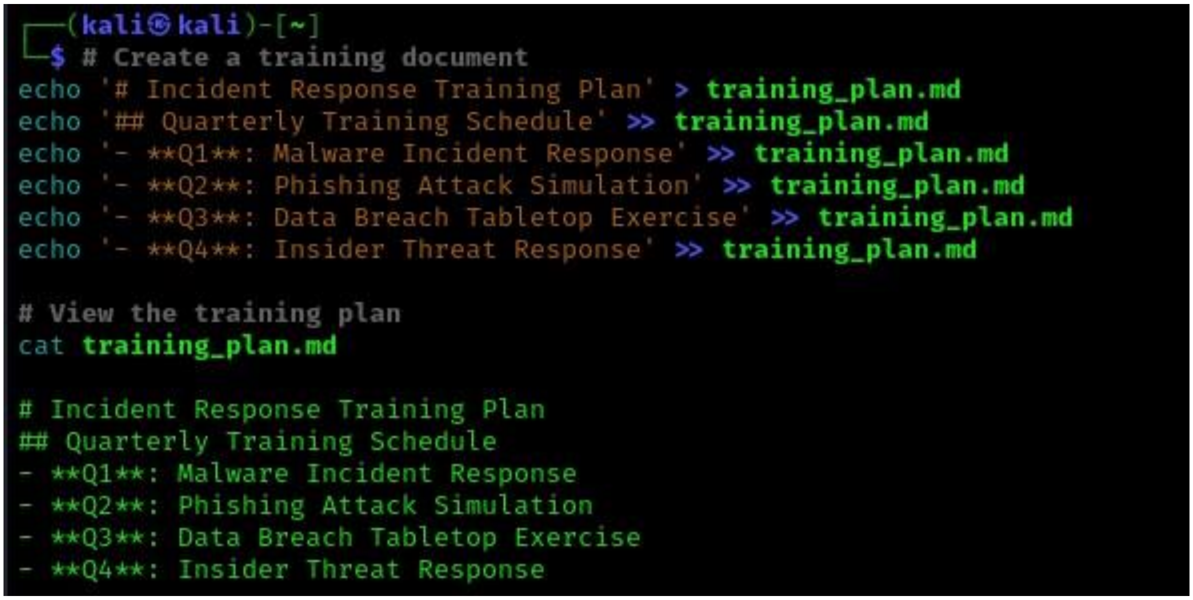
You can create scripts for various procedures. Below is an example of a script for containment and eradication of malware.



```
┌──(kali㉿kali)-[~]
└─$ # Create a containment script
echo '#!/bin/bash' > containment.sh
echo 'echo "Starting containment procedure..."' >> containment.sh
echo 'echo "Isolating infected systems..."' >> containment.sh
echo 'iptables -A INPUT -s <192.168.19.129> -j DROP' >> containment.sh
echo 'echo "Infected system isolated."' >> containment.sh
echo 'echo "Running malware scan..."' >> containment.sh
echo 'clamscan -r --bell -i /home/' >> containment.sh
echo 'echo "Malware scan complete."' >> containment.sh

# Make the script executable
chmod +x containment.sh

./containment.sh
Starting containment procedure...
Isolating infected systems...
./containment.sh: line 4: 192.168.19.129: No such file or directory
Infected system isolated.
Running malware scan...

----------- SCAN SUMMARY -----------
Known viruses: 8698861
Engine version: 1.3.1
Scanned directories: 325
Scanned files: 4410
Infected files: 0
Data scanned: 452.75 MB
Data read: 694.98 MB (ratio 0.65:1)
Time: 156.191 sec (2 m 36 s)
Start Date: 2024:09:26 13:34:59
End Date:   2024:09:26 13:37:35
Malware scan complete.
```

## ➢ Conducting Training and Simulation Exercises

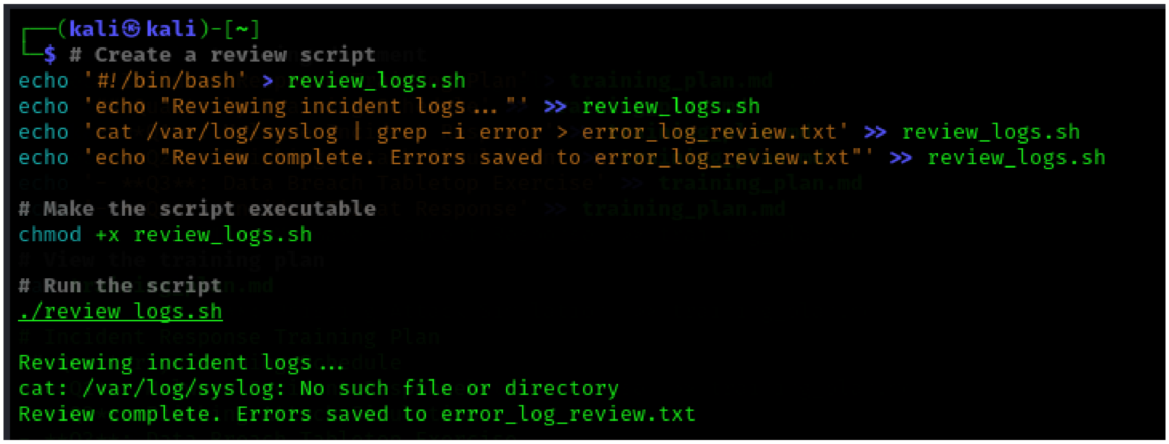
You can create a simple exercise document using a text file.



```
┌──(kali㉿kali)-[~]
└─$ # Create a training document
echo '# Incident Response Training Plan' > training_plan.md
echo '## Quarterly Training Schedule' >> training_plan.md
echo '- **Q1**: Malware Incident Response' >> training_plan.md
echo '- **Q2**: Phishing Attack Simulation' >> training_plan.md
echo '- **Q3**: Data Breach Tabletop Exercise' >> training_plan.md
echo '- **Q4**: Insider Threat Response' >> training_plan.md

# View the training plan
cat training_plan.md

# Incident Response Training Plan
## Quarterly Training Schedule
- **Q1**: Malware Incident Response
- **Q2**: Phishing Attack Simulation
- **Q3**: Data Breach Tabletop Exercise
- **Q4**: Insider Threat Response
```

## ➢ Reviewing and Updating the Plan Regularly

Create a script to automate the review of logs or incident reports. This can include checking for changes in the file system.



```
┌──(kali㉿kali)-[~]
└─$ # Create a review script
echo '#!/bin/bash' > review_logs.sh
echo 'echo "Reviewing incident logs..."' >> review_logs.sh
echo 'cat /var/log/syslog | grep -i error > error_log_review.txt' >> review_logs.sh
echo 'echo "Review complete. Errors saved to error_log_review.txt"' >> review_logs.sh

# Make the script executable
chmod +x review_logs.sh

# Run the script
./review_logs.sh

Reviewing incident logs...
cat: /var/log/syslog: No such file or directory
Review complete. Errors saved to error_log_review.txt
```