**Assignments**

**Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age**

Team Members:

1. Balaji Patil
2. Dhanraj Pawar
3. Kaushal Chougule
4. Atharv Pawar

# Assignment Distribution Table

|  |  |  |  |
| --- | --- | --- | --- |
| Assignment | Tasks | Assigned To | Deliverables |
| Vulnerability Assessment | Perform a vulnerability scan using Nessus and analyze the results. | Aditya Dange | Scan report with prioritized vulnerabilities. |
| Threat Hunting | Monitor SIEM logs for suspicious activity and investigate incidents. | Kshitij Patil | Incident report with findings and recommendations. |
| Phishing Email Analysis | Analyze phishing emails for indicators of compromise (IOCs). | Athrav  Katkar | Phishing analysis report with IOCs and threat intelligence. |
| Incident Response | Create a report of an incident and suggest remediation. | Aditya Dange | Incident response report with root cause analysis and remediation plan. |
| Security  Awareness  Training | Develop and deliver a security awareness training program for employees. | Kshitij Patil | Training materials, feedback report, and improvement plan. |
| Penetration Testing | Perform a penetration test on a target system and document findings. | Athrav  Katkar | Penetration testing report with vulnerabilities and recommendations. |

Detailed Assignments

1. Vulnerability Assessment

Assigned to: Aditya Dange Tasks:

* 1. Install and configure Nessus on a virtual machine.
  2. Perform a full vulnerability scan on the target system.
  3. Analyze the scan results and prioritize vulnerabilities based on severity.

Deliverables:

● A detailed scan report with:

* + 1. Executive summary.
    2. List of vulnerabilities with severity levels.
    3. Recommendations for mitigation.

1. Threat Hunting

Assigned to: Kshitij Patil Tasks:

* 1. Set up a SIEM tool (e.g., Splunk or ELK Stack).
  2. Monitor logs for unusual login attempts or suspicious activity.
  3. Investigate and escalate any confirmed threats.

Deliverables:

● An incident report with:

* + 1. Description of the suspicious activity.
    2. Key findings from the SIEM logs.
    3. Recommendations to prevent future incidents.

1. Phishing Email Analysis

Assigned to: Athrav Katkar Tasks:

* 1. Collect phishing emails from a spam folder or simulated campaign.
  2. Analyze email headers and content for phishing indicators.
  3. Identify and document indicators of compromise (IOCs).

Deliverables:

● A phishing analysis report with:

* + 1. Summary of the phishing email.
    2. List of IOCs identified.
    3. Recommendations to improve email security.

1. Incident Response

Assigned to: Aditya Dange Tasks:

* 1. Document the details of a simulated incident (e.g., phishing attack, malware infection).
  2. Analyze the root cause of the incident.
  3. Suggest remediation steps to prevent future incidents.

Deliverables:

● An incident response report with:

* + 1. Overview of the incident.
    2. Root cause analysis.
    3. Remediation plan.

1. Security Awareness Training

Assigned to: Kshitij Patil Tasks:

* 1. Identify key topics for security awareness training (e.g., phishing, password security).
  2. Develop training materials (e.g., presentations, handouts).
  3. Deliver the training to a group of employees.

Deliverables:

● Training materials, including:

* + 1. Presentations and handouts.
    2. Feedback report from participants.
    3. Improvement plan for future training.

1. Penetration Testing

Assigned to: Athrav Katkar Tasks:

* 1. Plan and execute a penetration test on a target system.
  2. Use tools like Metasploit or Nmap to identify and exploit vulnerabilities.
  3. Document the findings and provide recommendations.

Deliverables:

● A penetration testing report with:

* + 1. Overview of the test.
    2. List of vulnerabilities identified and exploited.
    3. Recommendations for mitigation