Incident Response Playbook

Unauthorized access via Web attacks

Phase 1: Preparation

Define incident response team roles and responsibilities: Identify the members of the incident response team and their roles and responsibilities in the incident response process. The team should include representatives from IT, security, legal, and management.

Create incident response plan and procedures: Develop an incident response plan that outlines the steps to be taken during an incident and the procedures to follow. This should include contact information for team members, stakeholders, and external partners, as well as a clear chain of command.

Implement security controls and monitoring systems: Implement security controls and monitoring systems to detect and prevent unauthorized access via basic web app attacks. This should include firewalls, intrusion detection and prevention systems, antivirus software, and web application firewalls.

Train incident response team members and stakeholders: Ensure that all team members and stakeholders are trained in their roles and responsibilities during an incident. This should include regular training and awareness programs to educate employees on security best practices.

Perform regular system backups and ensure their availability: Regularly back up all critical systems and data and ensure that backups are available and easily accessible in the event of an incident.

Phase 2: Identification

Monitor system logs and alerts for suspicious activity: Monitor system logs and alerts for any unusual activity that may indicate unauthorized access via basic web app attacks.

Investigate reports of unusual web app behavior or security incidents: Investigate reports of any unusual web app behavior or security incidents and take appropriate action to contain the incident.

Collect evidence of the incident and document it for later analysis: Collect and document all evidence related to the incident, including system logs, network traffic, and any other relevant data.

Phase 3: Containment

Isolate affected web app(s) from the rest of the IT infrastructure: Isolate the affected web app(s) from the rest of the IT infrastructure to prevent further damage.

Disable any compromised user accounts and/or revoke access tokens: Disable any user accounts that may have been compromised and revoke any access tokens associated with the affected web app(s).

Limit further damage by stopping malicious processes or closing vulnerable ports: Take steps to limit further damage by stopping any malicious processes or closing any vulnerable ports associated with the affected web app(s).

Phase 4: Analysis

Conduct a thorough investigation of the incident and its root cause: Conduct a thorough investigation of the incident to determine how the unauthorized access via basic web app attacks occurred and identify the root cause of the incident.

Analyze the collected evidence to determine the scope and impact of the incident: Analyze the evidence collected during the investigation to determine the scope and impact of the incident and identify any additional systems or data that may have been compromised.

Identify and prioritize systems that need to be repaired or restored: Identify and prioritize the systems that need to be repaired or restored as part of the incident response process.

Phase 5: Eradication

Remove any malware or unauthorized files from affected systems: Remove any malware or unauthorized files from affected systems associated with the affected web app(s).

Close any known vulnerabilities and apply security patches or updates: Close any known vulnerabilities associated with the affected web app(s) and apply security patches or updates to prevent similar incidents from occurring in the future.

Restore web app(s) and data from backups if necessary: Restore the affected web app(s) and any compromised data from backups if necessary.

Phase 6: Recovery

Restore the affected web app(s) and data from backups: Restore the affected web app(s) and any compromised data from backups, ensuring that data integrity is maintained.

Verify that all security controls and monitoring systems are functioning correctly: Test all security controls and monitoring systems to ensure they are functioning correctly and able to detect any future unauthorized access via basic web app attacks.

Reconnect the repaired or restored web app(s) to the IT infrastructure: Reconnect the repaired or restored web app(s) to the IT infrastructure and ensure that they are functioning correctly.

Conduct a post-incident review: Conduct a post-incident review to identify any areas for improvement in the incident response process and make necessary adjustments to the incident response plan and procedures.

Phase 7: Reporting

Notify relevant stakeholders: Notify all relevant stakeholders, including executive management, legal, and regulatory bodies, of the incident. This should be done as soon as possible to minimize the potential impact on the organization.

Provide a detailed report of the incident: Provide a detailed report of the incident, including a timeline of events, the root cause of the incident, and the steps taken to contain and mitigate the incident. The report should also include any recommendations for improvements to the incident response plan and procedures.

Review and update incident response plan: Review and update the incident response plan based on the lessons learned from the incident. This should include any changes to the roles and responsibilities of the incident response team, as well as any updates to the security controls and monitoring systems in place.

Conduct follow-up activities: Conduct follow-up activities, such as providing additional training to employees or conducting additional security assessments, as needed to ensure that the incident does not recur. These activities should be documented and tracked to ensure that they are completed in a timely manner.