Post-Exploitation

Santiago Hernández Ramos
@santiagohramos

POST-EXPLOITATION

- The post-exploitation phase involves determining the value of the resources that have been compromised in the earlier stages of the process.

- The value of a resource can be assessed based on the sensitivity of the information it stores or the potential it provides an attacker to compromise additional resources within the organization.

- It must be ensured that the client's business processes are not exposed to a greater level of risk due to the execution of the hacking.

RECOMMENDATIONS

- ✓ Unless there is an express request from the client, critical services should not be assessed or modified.
- ✓ Any modifications and configuration changes made must be documented and reverted.
- ✓ A detailed list of all actions taken against the client's systems and the timeframe in which they were performed must be delivered.
- ✓ Any private or personal information discovered can be used to gain more privileges or obtain additional information only if express authorization is granted by the client and the owner of the information.
- ✓ Passwords (even if encrypted) must not be included in the final report.
- ✓ Persistence mechanisms must not be established on a machine without the express consent of the client.
- ✓ All information collected during the audit must be encrypted on the analysts' devices.
- ✓ All collected information must be destroyed once the client accepts the final report.