ADMIN SOP - Distributed pentesting

DO NOT SHARE THIS DOCUMENT UNLESS IT IS WITH MANAGEMENT

Reviewed by

This document has been reviewed by

Reviewers	Date reviewed	Remarks or OK	Remarks creator
@ James Beers (Unlicensed)	07/16/2022	Yes, tech lead assigns scope to team and responsibilities to senior members then oversees the project while working with the member doing logic testing. brainstorming during meetings while all the minds can think on a issue. Communication is KEY make sure organization includes communication.	Added the deliverables clause
@ Brandon Lachterman	7/16/22	This looks very good, and I agree wholly with this, although I will add this will vary slightly with the TYPE of pentest we are engaged in, as a network pentest does not need to necessarily adhere to the OWASP 10 specifically. This will develop over time though. As an SOP, this is great.	Added the network pentest clause

If we distribute our pentesting, we need to set up a strict line of things for every endpoint that needs to be tested. We also need to appoint 1 person to business logic depending on the required coverage level.

What needs to be done

- Create a coverage document, this should contain either every endpoint or every functionality
  - Public or private function
  - Gut level security risk (in human words)
  - Security level (low/med/high)
  - % covered
  - A total % covered versus need to be covered
- A test plan needs to be drafted
- Endpoint/function documents need to be created (see next)
- Weekly/daily meeting needs to be set up with client
- Budgeted hours need to be set vs timeline and roster has to be assembled

Endpoint/function document creation process

I can not stress this enough, management or tech leads determine what gets tested

- We create 1 document per endpoint/function
- We mention the OWASP top 10 or the specific things to test for on a port/target
  - In case of network pentest, we either divide per IP or per port depending on the scope
- We mention exactly what to test per top 10 item
- Can be either API top 10 or web top 10

Peer reviews

THERE SHALL BE NO DOCUMENTS GOING OUT TO ANY TESTER THAT HAVE NOT BEEN REVIEWED **AND SIGNED OFF** BY ANOTHER SENIOR.

Deliverables

The senior is responsible for acquiring the deliverables from the tester. They should contain:

- All the things that have been tested (in checklist style)
- Any remarks while testing
- Tester per remark

Every week or day depending on the project, we will have a standup meeting.