AST

Audit de Sécurité Technique

2.5

Rapport et communication

Jean-Marc Bost

jean-marc.bost@heig-vd.ch

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Scoping – SoE

SoE = Scope of Engagement

- Objectives
  - Business risks (e.g. reputation versus business discontinuity)
  - Priorities (e.g. based on a threat scenario)
  - Constraints (e.g. no impact on business hours)
- Scope
  - Hosts, network ranges and applications
  - Exclusions: incl. hosts, network ranges and applications which should not be tested
  - Third-parties owning systems and applications (as applicable)

Scoping – RoE

RoE = Rules of Engagement

- Activities
  - Description, ownership (group), estimated effort, hypotheses
- Timeline
  - GANTT chart, Work Break Structure (WBS) for every task you have identified
- Location(s) where the project will be conducted
  - Place and prerequisites (VPN, keys, place of work…)
- White box vs black box?
  - Decision motivations
  - Communication plan: who, when, why
- Coordination
  - Contact information
  - Status meetings
- Sensitive data and viewing policy

Scoping – permission to test

Memorandum for File

Subject: Vulnerability Assessment and Penetration Testing Authorization

Date: MMDDYY

To properly secure this organization's information technology assets, the information security team is required to assess our security stance periodically by conducting vulnerability assessments and penetration testing. These activities involve scanning our desktops, laptops, servers, network elements, and other computer systems owned by this organization on a regular, periodic basis to discover vulnerabilities present on these systems. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. To that end, the undersigned attests to the following:

1) [Insert name of tester], [Insert name of tester], and [Insert name of tester] have permission to scan the organization's computer equipment to find vulnerabilities. This permission is granted for from [insert start date] until [insert end date].

2) [Insert name of approver] has the authority to grant this permission for testing the organization's Information Technology assets.

[Insert additional permissions and/or restrictions if appropriate.]

Signature: _____ Signature: _____

[Name of Approver] [Name of Test Team Lead]

[Title of Approver] [Title of Test Team Lead]

Date: _____ Date: _____

Scoping – NDA

- Preferably, use the customer's one
- Otherwise
  - \\eistore1\profs\ARS\cours\AST-2019\3. Docs\nda.txt

Results – report

- PDF document with:

1. Table of contents
2. Executive summary (context, facts and risks)
3. Project summary (objectives, scope and methodology)
4. Project results summary (done/not, major findings, recommendations)
5. Detailed results (discoveries, vulnerabilities, exploits, risks impact)
6. Next steps and recommendations

Appendices (any relevant documents like raw output from vulnerability scans)

Results – presentation

- 25' max for:
  1. Scope, goals and timeline at a glance
  2. Executive summary for customer
  3. Statistical presentation of work done and findings
  4. Major results/findings
  5. One or two examples in deeper technical details
  6. Recommendations and next steps

Deliverables, milestones, owners

#	Deliverable	Type	Signed by		Delivered to		Approved by	
1	Project proposal	f	-		P	< 11.10.2019	P	13.10.19
2	NDA	c	SPA	< 25.11.19	C	25.11.19		
3	Permission to test	c	C	< 25.11.19	SP	< 25.11.19	P	25.11.19
4	Scoping	p[1,2]	-		P(C)	< 25.11.19	PC	25.11.19
5	Results	r[2]	-		PC	19.01.19	P	11.02.19
		p[1,2]	-		P(C)	19.01.19	P	11.02.19

f = form
c = contract
r = report
p = presentation

P = profs
C = customer
S = student
A = assistant

(optional)

PLEASE, INFORM YOUR CUSTOMER THAT:

1. **one single presentation, with or without customer, at HEIG or customer's premises**
2. **no censorship by customer**

Q&A sessions

- Every Friday, from 1:15 to 3:40 PM