Penetration Testing techniques in web applications

Dimitris Mandilaras, Nikolaos Tsalis

{mandhlarasd, ntsalis}@aueb.gr

Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business, Greece

Predefined Rules

1. Penetration testing should be executed by experienced and authorized personnel.
2. The penetration testing process must be consistent of the rules of engagement that have been agreed from both sides (tester and organization).
3. The steps of the framework must be followed in the predefined order and every step must be complete in order to proceed in the next one.

Comparison Analysis

- ❑ Every framework/methodology follows a **different way in execution**. For instance, some of them focus on wireless testing, physical security testing, password cracking, social engineering, network testing etc.
- ❑ Every organization has its own specific cause of the different **objective and scope**. The tester must be aware of these elements and understand the purpose of the test in order to choose the right approach.
- ❑ All **methodologies** initiate penetration testing with the information gathering phase, while ISSAF includes this phase in the second step. In the second phase they differentiate from vulnerability analysis, while the same applies to the exploitation phase. They all have the basic steps, e.g. information gathering, vulnerability analysis, exploitation. but they also include some additional phases or steps.
- ❑ In addition, some frameworks are created for different **objectives**. For example OWASP, PTES and a part of ISSAF focus on web penetration testing. while NIST, OSSTM and PTF include a more generic approach.

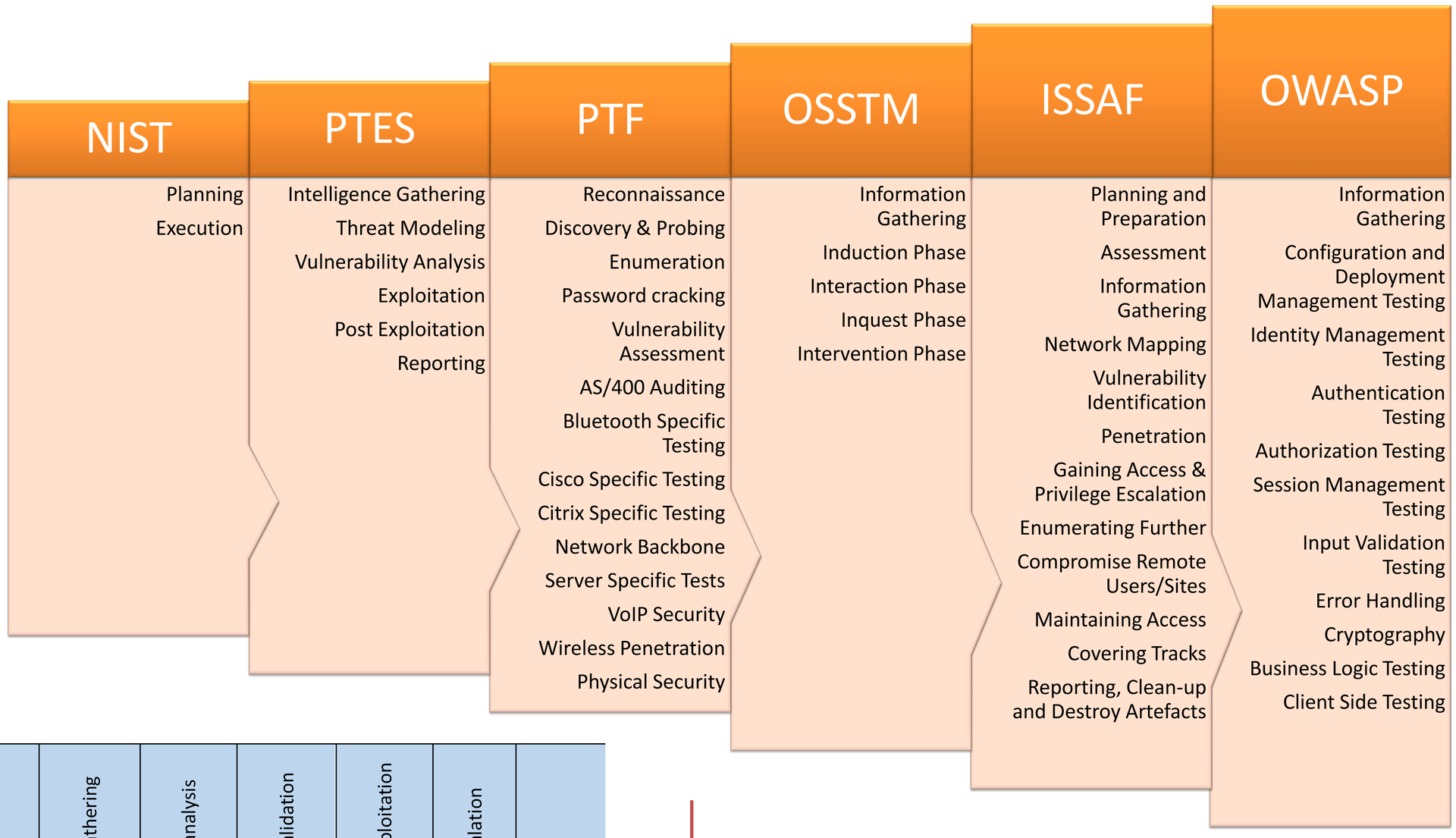

Figure 1: Penetration testing methodology phases

Phases / Tools	Planning & Preparation	information gathering	Vulnerability analysis	vulnerability validation	Vulnerability exploitation	Privilege escalation	Report
Acunetix		X	X	X	X	X	X
Burpsuite		X	X	X	X	X	X
Dirbuster		X	-	-	-	-	X
Nmap		X	-	-	-	-	-
Netsparker		X	X	X	X	-	X
Nikto		X	-	-	-	-	X
OWASP Zed Attack		X	X	X	X	X	X
Paros		X	-	-	-	-	X
Skipfish		X	X	-	X	-	X
SqlNinja		-	X	-	X	X	X
Vega		X	X	-	X	-	X
W3af		X	X	-	X	-	X
Wapiti		X	X	-	X	X	X
Webinspect		X	X	-	X	X	X
WebScarab		X	X	-	X	-	X
Websurgery		X	X	X	X	X	X
Websecurify		X	X	X	X	-	X
Websploit		X	X	-	X	-	X
Wikto		X	X	-	-	-	-
Powerfuzzer		-	X	-	X	-	-

Figure 2: Tools per penetration testing phase

Figure 3: Penetration testing phases

References

1. Herzog, P. “OSSTMM 3 – The Open Source Security Testing Methodology Manual”. [online] Available at: http://scadahacker.com/library/Documents/Assessment_Guidance/OSSTMM-3.0.pdf [Accessed 23 Sep. 2014]
2. Kandias M., Stavrou V., Bozovic N., Mitrou L., Gritzalis D., "Can we trust this user? Predicting insider’s attitude via YouTube usage profiling", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing* (ATC-2013), pp. 347-354, IEEE Press, Italy, 2013.
3. Kandias M., Stavrou V., Bosovic N., Mitrou L., Gritzalis D., “Predicting the insider threat via social media: The YouTube case”, in *Proc. of the 12th Workshop on Privacy in the Electronic Society* (WPES-2013), pp. 261-266, ACM Press, Berlin, November 2013.
4. Lawson, L. “Penetration Testing Framework 0.59”. [online] Vulnerabilityassessment.co.uk. Available at: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html [Accessed 23 Sep. 2014].
5. Muller, A. “OWASP Testing Guide v.4:. [online] Available at: https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf [Accessed 19 Sep. 2014].
6. Mylonas, A., Tsalis, N., Gritzalis, D., “Evaluating the manageability of web browsers controls”, in *Proc. of the 9th International Workshop on Security and Trust Management*, pp. 82-98, Springer (LNCS 8203), United Kingdom, 2013.
7. Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D., “Smartphone sensor data as digital evidence”, *Computers & Security*, Vol. 38, pp. 51-75, October 2013.
8. Pentest-standard.org, (2013). PTES Technical Guidelines - The Penetration Testing Execution Standard. [online] Available at: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines [Accessed 15 Sep. 2014].
9. Technical guide to information security testing and assessment. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.
10. Theoharidou, M., Papanikolaou, N., Pearson, S., Gritzalis, D., “Privacy risks, security and accountability in the Cloud”, in *Proc. of the 5th IEEE Conference on Cloud Computing Technology and Science*, pp. 177-184, IEEE Press, United Kingdom, 2013.
11. Theoharidou, M., Tsalis, N., Gritzalis, D., “In Cloud we Trust: Risk-Assessment-as-a-Service”, in *Proc. of the 7th IFIP International Conference on Trust Management*, pp. 100-110, Springer (AICT 401), Spain, 2013.
12. Tsalis, N., Theoharidou, M., Gritzalis, D., “Return on security investment for Cloud platforms”, in *Proc. of the Economics of Security in the Cloud Workshop*, pp.132-137, IEEE Press, United Kingdom, 2013.
13. Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Mobile devices: A phisher's paradise", in *Proc. of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pp. 79-87, ScitePress, Austria, 2014.
14. Virvilis N., Gritzalis D., “Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?”, in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing* (ATC-2013), pp. 396-403, IEEE Press, Italy, 2013.