Techniques for Penetration Testing of Infrastructures

Ilias Boutsikakis, Nikolaos Tsalis

{boutsikakhsh, ntsalis}@aueb.gr

Information Security & Critical Infrastructure Protection Research (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece

Thesis scope

- Five major penetration testing methodologies: ***ISSAF***, ***NIST***, ***OSSTMM***, ***PTES*** and ***PTF***
- **Comparison** analysis of methodologies on specific criteria
- Proposal of a unified **penetration testing methodology**
- Proposal of a **penetration testing tools set**
- Lab Setup and Results Analysis of a Penetration Testing **scenario**
- Development of a **Nessus parser**, written in Java, for automatic results exportation
- Proposal of a **Penetration Testing Report template**

Penetration Testing Methodologies

ISSAF	NIST	OSSTMM	PTES	PTF
Technology oriented	Theoretical	Theoretical and new terminology	Technology oriented	Technology oriented
Security Assessment methodology	Security Assessment methodology	Metrics based	Penetration testing methodology	
	Social Engineering extended	Security Assessment methodology	Extended analysis of all stages	

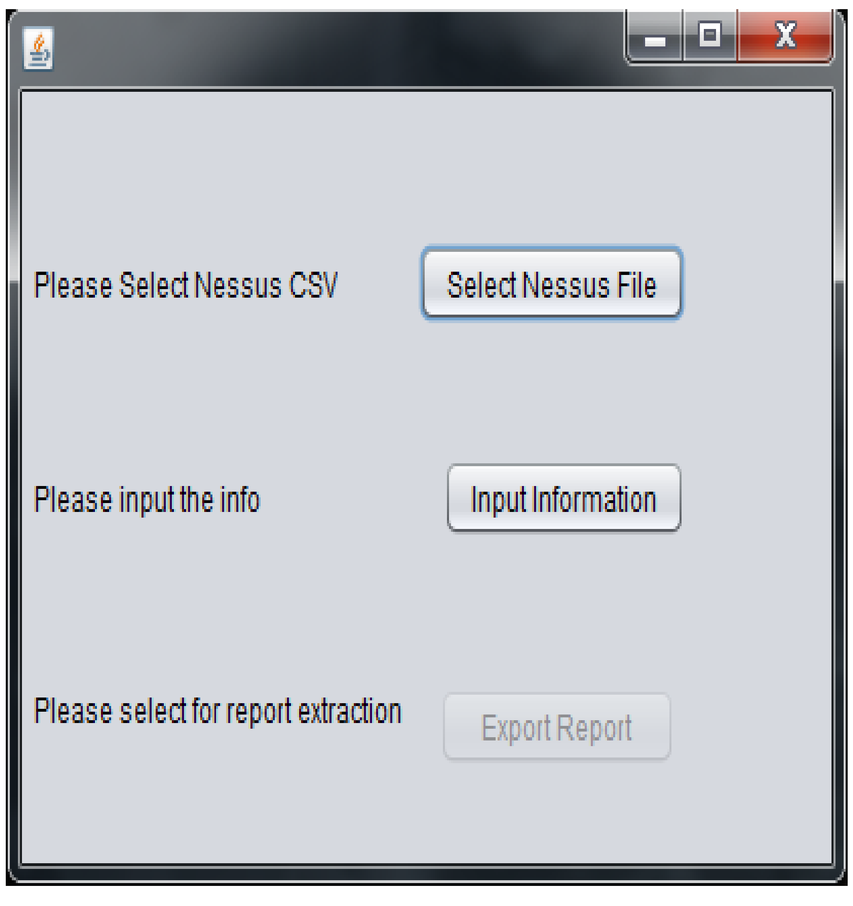
Basic Principles

- There is no perfect methodology suitable for any purpose
- All phases of a penetration testing methodology are equally important
- The success of a stage depends on the success of the previous stages
- Technology is no help for a penetration tester without a proper methodology
- The results of a penetration testing must be concise, clear and fully understood by the management

Penetration Testing proposed Methodology: Stages

Planning and Preparation	Information Gathering	Vulnerability Identification	Exploitation	Maintaining Access	Report
• Agreement between parties • Rules of engagement	• Passive and Active • Network Mapping	• Automated tools • Specific purpose tools • Techniques for validation	• Optional	• Password cracking • Backdoor installments	• Concise • Clear • Self-explanatory • Remediation actions

Nessus parser and report compilation



The Nessus tool parser opens a .csv file, and reads it. Each line represents an object of a class. These objects - lines are printed in a .docx output file created automatically by the parser. The parser creates the output according to these rules:

- The vulnerabilities are grouped by each host.
- The vulnerabilities are shown in a descending form, Critical – Medium – Low – Informational.
- The fields shown are IP address, Description, CVSS, CVE, port, synopsis and solution.

Penetration Testing Proposed Methodology: Tools

Information Gathering	Vulnerability Identification	Exploitation	Maintaining Acess
Wireshark	Nessus	Metasploit	Cymothoa
Nmap	Core Impact		John the Ripper
Maltego	OpenVas		Hydra
Fierce	Nexpose	Immunity Canvas	Cain and Abel
TcpFlow	TripWire IP360		
The harvester	BeyondTrust Retina		
Fping			
Hping			
Creepy			

Conclusions

- **Planning** and **Preparation** are usually overlooked by the penetration testing team.
- **Information Gathering** stage is the stage that provides the next stages with information.
- **Vulnerability Identification** stage results must be verified through Validity processes.
- **Exploitation** occurs only after there has been an agreement with the tested party.
- **Maintaining Access** involves password cracking and installation of backdoors.
- The **preparation and creation of the report** is a procedure that must be written and presented in an understandable way.
- All tasks must be executed by well-**trained personnel**.

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. *Information System Security Assessment Framework 0.2.1.* (2006). [online] Available at: http://www.oissg.org/files/issaf0.2.1B.pdf [Accessed 25 Sep. 2014]
3. 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.
4. 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.
5. 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].
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, 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*. 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.