



Penetration Testing 101


Definitions, Methodologies, and Examples

Matthias Vallentin

`vallentin@icsi.berkeley.edu`



Penetration Test

- ■ Method to **evaluate security** of a network/computer system
 - ■ Simulates an attack conducted by a malicious user (e.g. cracker)
 - ■ Active analysis of the target, testing for
 - ■ Vulnerabilities
 - ■ Misconfigurations
 - ■ Operational weaknesses
 - ■ Security issues are thoroughly assessed and presented
- 

Methodologies

- ■ Open Source Security Testing Methodology Manual (**OSSTMM**)
 - ■ Peer-reviewed international standard for security testing
- ■ Information Systems Security Assessment Framework (**ISSAF**)
 - ■ Fairly new categorization of security assessment into domains
- ■ NIST Guideline on Network Security Testing
 - ■ Likely to be accepted by regulatory agencies

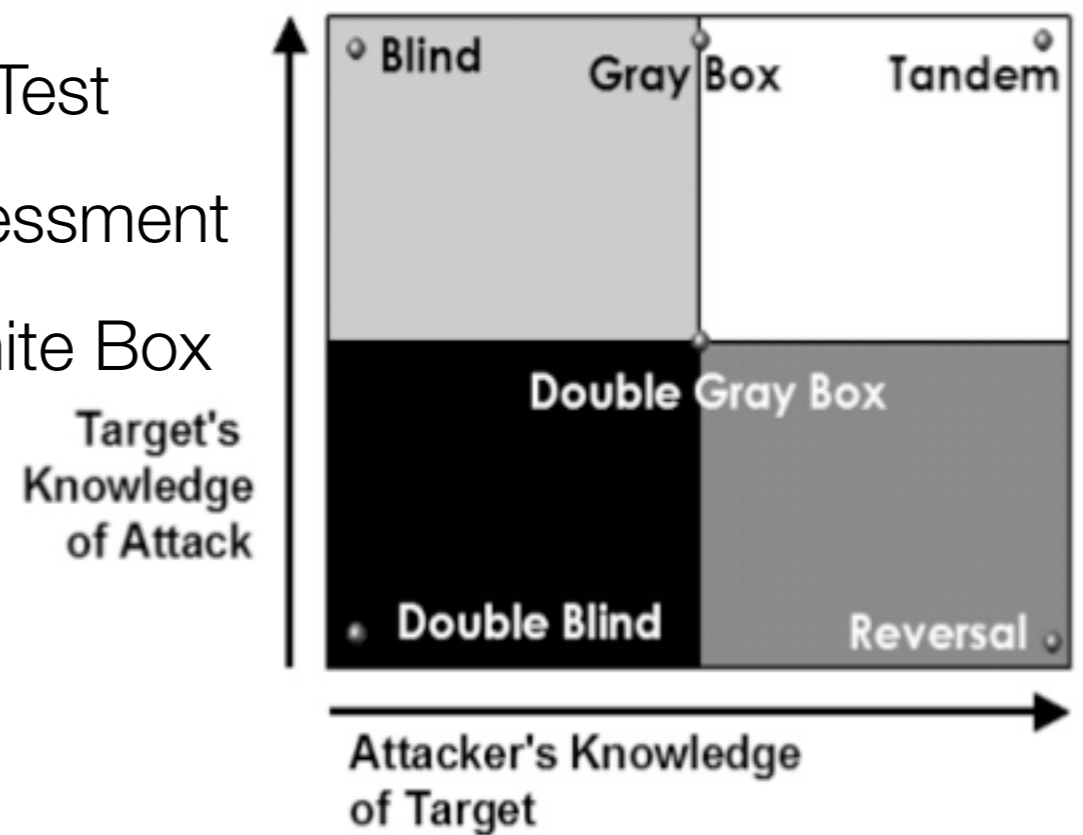


Web Application Security

- ■ **Open Web Application Security Project (OWASP)**
 - ■ Open-source application security project
 - ■ Not affiliated with any technology company
- ■ Notable documents
 - ■ OWASP Guide - how to build secure web applications
 - ■ OWASP Top 10 - current 10 most critical security flaws

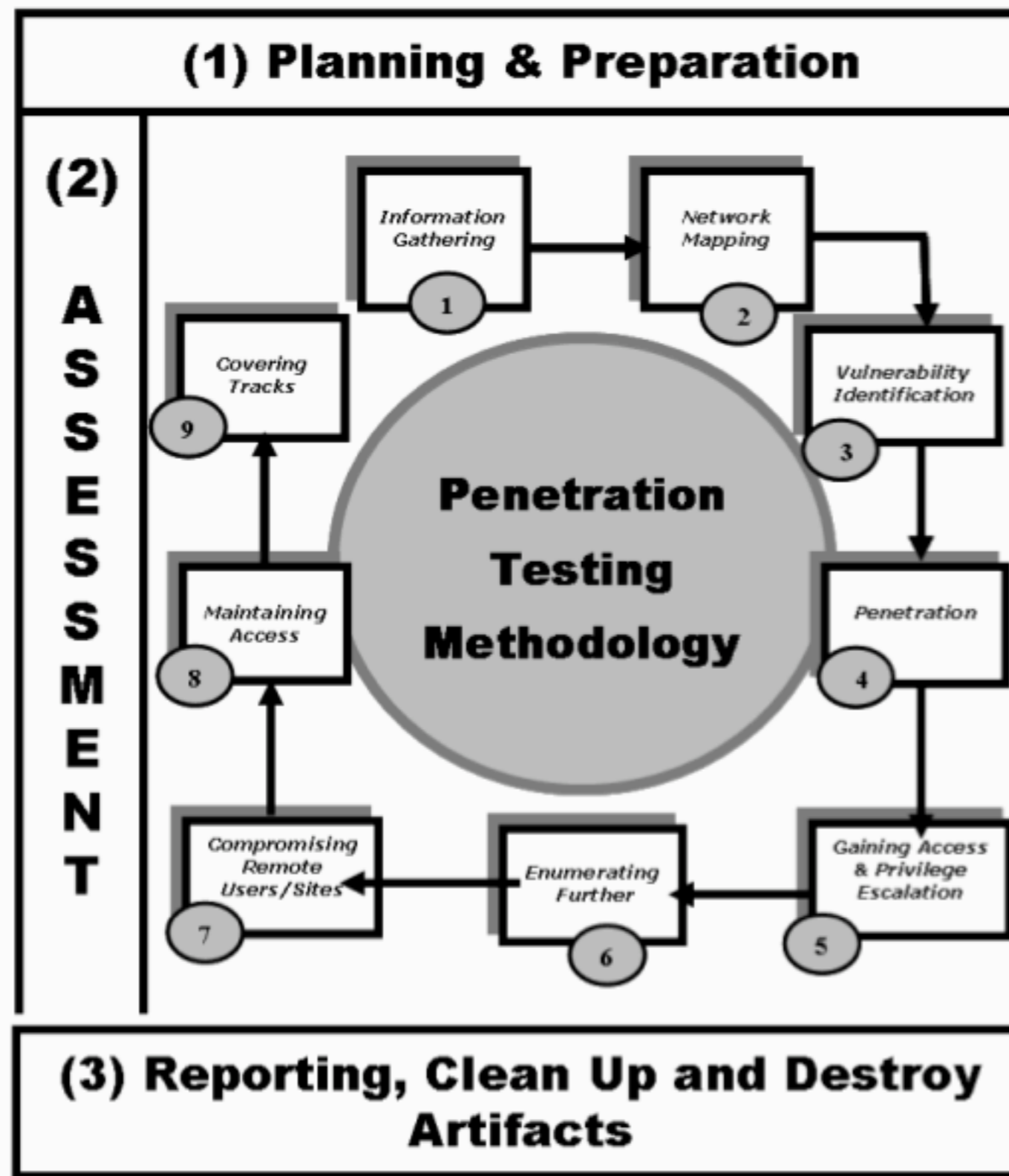
OSSTMM Test Types

- **Blind:** War Gaming, Role Play
- **Double Blind:** Penetration Test
- **Gray Box:** often a Self Assessment
- **Double Gray Box:** also White Box
- **Tandem:** also Crystal Box
- **Reversal:** Red Team



Source: The Vision of the OSSTMM

ISAFF Approach & Methodology



Example Toolkit

■ Information Gathering:

- old: Google, whois, zone-transfers, reverse DNS lookups
- shiny: Maltego, Metagoofil, CentralOps.net, DigitalPoint.com, DomainTools.com

■ Network Mapping

- basic: nmap, Hping3, p0f, Xprobe2, amap
- shiny: trigger SMTP bounces, Brute force HTTP vhosts, watch outbound DNS, email users

Example Toolkit

- Vulnerability Identification

- `basic`: Nessus, commercial tools

- `web`: `hackvertor`, `Nikto`, `WFuzz`, `w3af`, `HttpRecon`, `WebScarab`

- Penetration

- `basic`: `milw0rm`, `bugtraq`, exploit databases

- `shiny`: `Metasploit`, `FastTrack`, `Inguma`, `Karma`, `wesside-ng`

Example Toolkit

■ Privilege Escalation

- `basic`: john, Hydra, Medusa, Ettercap, tcpdump
- `nice`: Scapy/Scrubby, FPGAs (WPA2), Rainbowcrack, NTLM relays, social engineering, `dhcpcd -h WPAD -i eth0`

■ Maintaining Access

- `basic`: VNC, B02k, hxdef, Adore-ng, netcat cronjob
- `tunneling`: CryptCat, nstx, socat, vstt, ht[sc], icmptx

FIN

Matthias Vallentin



<http://matthias.vallentin.cc>



<http://feeds.feedburner.com/security-loop>