Security Testing

Luigi Gangitano
gangitano@openconsulting.it

Il processo di sicurezza

Terminologia

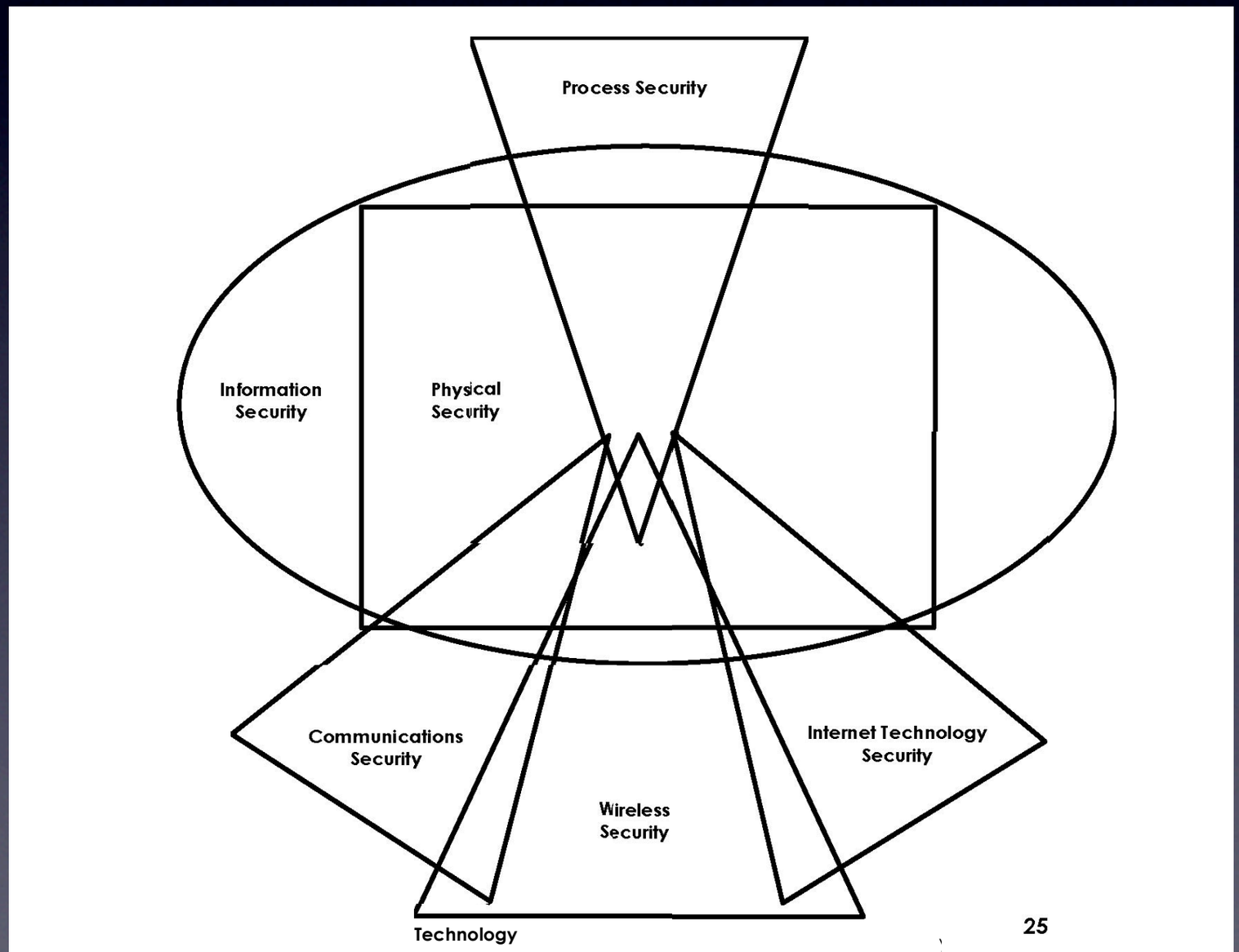
- Vulnerability scanning (automatico, Nessus)
- Security Scanning (VS e analisi professionale)
- Penetration Testing (esiste almeno un varco?)
- Risk Assessment (sulla carta)
- Security Auditing (verifica delle misure di sicurezza)
- Ethical Hacking (PT multipli, a tempo)
- Security Testing

OSSTMM

- Open Source Security Testing Methodology Manual
  - Standard *de-facto* del Security Testing
  - Processo di revisione del manuale OpenSource
    - Copre tutte le fasi del progetto di verifica della sicurezza, dalle indicazioni sul marketing al formato dei documenti di progetto
    - Certificazioni (Tester, Analyst, Expert)
    - Diverse revisioni disponibili (la più aggiornata è a pagamento)
    - http://www.isecom.org

OSSTMM

- Copre tutte le aree della sicurezza delle informazioni



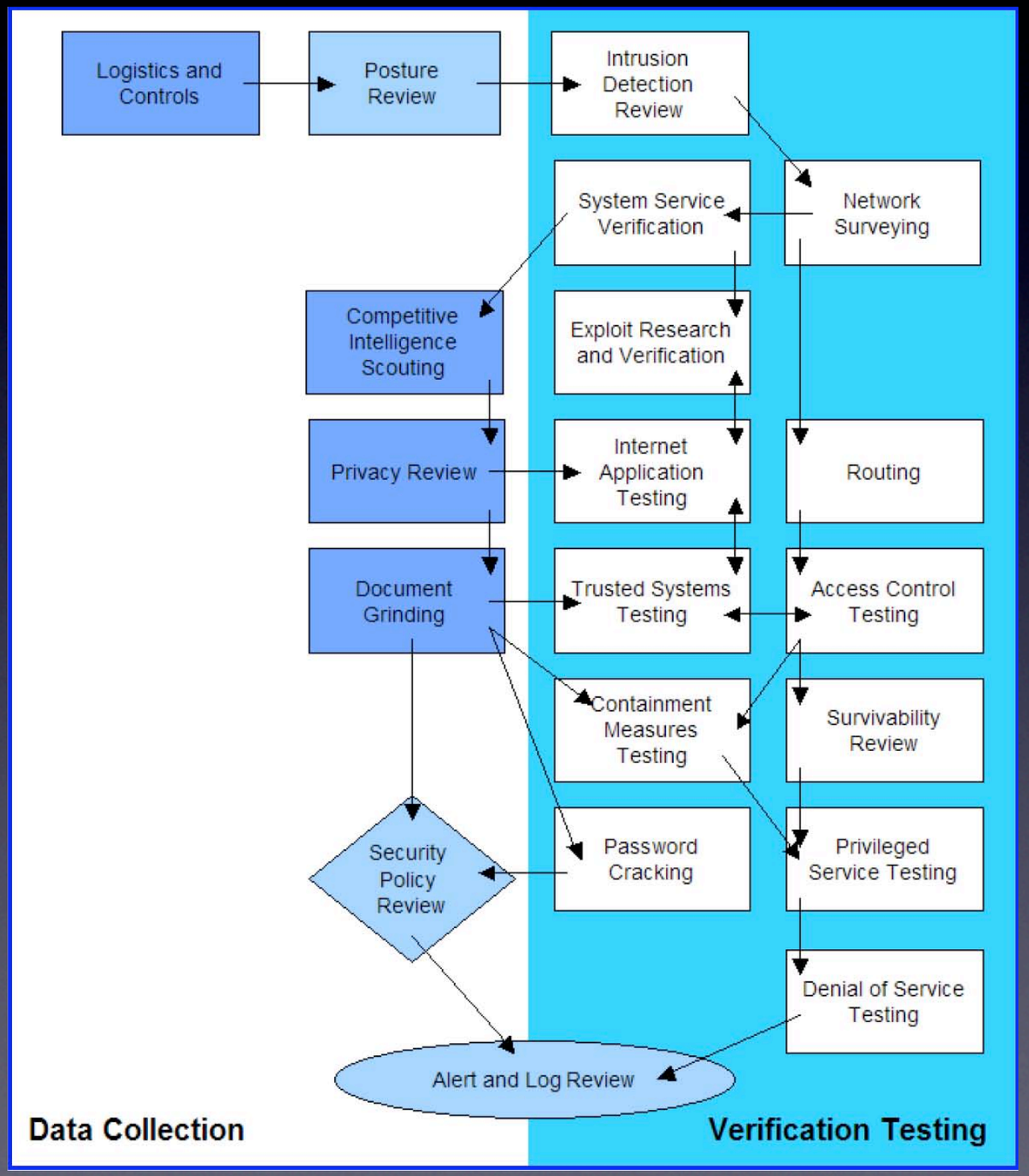
OSSTMM

- 6 Moduli:
  - Sicurezza delle informazioni
  - Sicurezza dei processi
  - Sicurezza delle tecnologie Internet
  - Sicurezza delle comunicazioni
  - Sicurezza dei canali Wireless
  - Sicurezza Fisica
- Per ciascun modulo sono indicate diverse attività
- Tutte le attività di un modulo devono essere svolte

Metodologia

- Definizione dello stato dell'arte della sicurezza per l'ambiente oggetto di analisi
- Raccolta di informazioni
- Esecuzione dei test di sicurezza
- Misurazione dei risultati (attraverso RA, distanza dallo stato dell'arte)
- Documentazione dei risultati

Un esempio



Dettaglio di un test

- Definizione dei risultati attesi
  - Eventuali vulnerabilità
  - Elenco delle politiche non rispettate
  - Elenco dei metodi utilizzati per i test
  - Dati raccolti durante i test
- Esecuzione delle procedure indicate nel test
  - Attraverso l'uso di strumenti automatici
  - Attraverso la verifica manuale dello stato dei sistemi

Report

Server Information Template

IP Address	domain name

Port	Protocol	Service	Service Details

BANNER(S):

Port	Protocol	Banner

TCP SEQUENCING:

TCP Sequence Prediction
TCP ISN Seq. Numbers
IPID Sequence Generation
Uptime

CONCERNS AND VULNERABILITIES:

Concern or Vulnerability
Example
Solution

Aree di analisi

- Security testing non è solo nmap + nessus
- Sicurezza fisica (accessi, controlli, allarmi, CCTV)
- Sicurezza delle comunicazioni (PBX, Wardialing)
- Sicurezza dei canali Wireless
  - 802.11*, Bluetooth, DECT, RFID, IR, Tempest
- Social Engeneering
  - Richieste informazioni, inviti, impersonamento

Pre-requisiti

- Accordi commerciali
- Definizione dei limiti delle verifiche
- Definizione della durata dei test
- Non Disclosure Agreement

Diversi livelli di ST

- Blind, Double blind
- Gray box, Double gray box
- Tandem
- Reversal