# 3. Testarea securităţii reţelelor

# Obiective

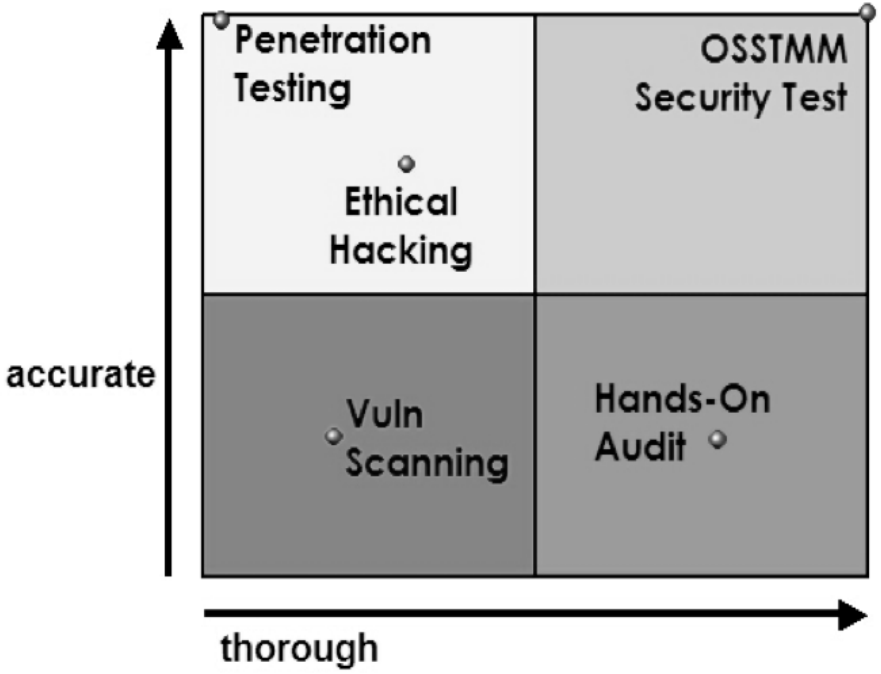
- Testarea securităţii sistemelor folosind unelte şi tehnici similare cu ale potenţialilor atacatori
- Cunoaşterea adversarului şi a tehnicilor folosite de acesta
- Evaluarea capacităţii de a face faţă la atacuri

- Offensive security vs. defensive security

- Abordări:
  - Penetration Testing
  - Etical Hacking
  - Red Teaming

- Acţiunea trebuie autorizată de managementul organizaţiei!
- Cod de etică profesională!

# Obiective (cont.)




- Un test de penetrare oferă o imagine de moment (snapshot) a stării curente de securitate a unui sistem
- Acţiune limitată în timp

# Scop

- Ce se poate testa / Care este ţinta?
  - infrastructura IT&C
    - obţinerea controlului asupra Active Directory
  - o aplicaţie critică
    - ERP, e-banking, etc
  - un proces de business
    - billing
  - o facilitate
    - obţinerea accesului fizic în clădire / data room
  - angajaţii
    - social engineering
- Pentru ce se face testarea?
  - lansarea în producţie a unui nou sistem critic
  - verificarea periodică a sistemelor
  - măsurarea eficienţei sistemelor de securitate implementate
  - măsurarea impactului pe care o breşă de securitate în poate avea asupra organizaţiei
  - asigurarea complianţei cu reglementările în domeniu

# Tipuri de teste

- Funcţie de cantitatea de informaţie pusă la dispoziţie echipei de testare:
  - black-box test (fără nici un fel de cunoştinţe despre ţintă)
  - gray-box test (cunoştinţe parţiale despre ţintă)
  - white-box test (cunoştinţe complete despre ţintă)
- Funcţie de locaţia din care se desfăşoară testele:
  - external tests (Internet)
  - half-in, half-out tests (DMZ)
  - internal tests (LAN)
- Funcţie de gradul de informare al echipei interne
  - cu anunţarea echipei interne
  - fără anunţarea echipei interne

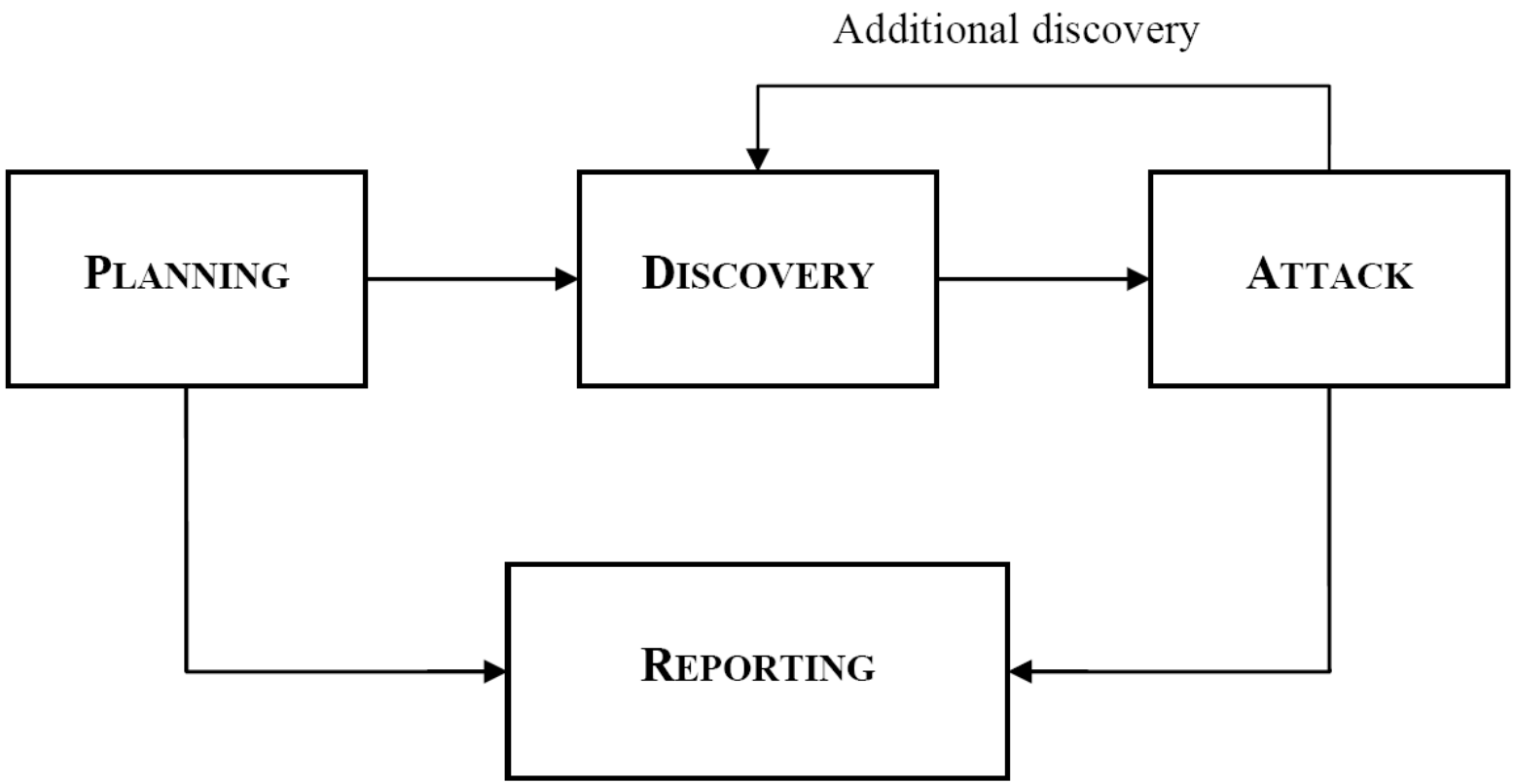
# Metodologii de testare

- Open Source Security Testing Methodology Manual (OSSTMM)
  - http://www.isecom.org/osstmm/
  - creată de Pete Herzog
  - abordare foarte practică
    - checklists cu ce trebuie testat şi în ce ordine
    - listă de unelte
- NIST SP 800-115 “Technical Guide to Information Security Testing and Assessment”
  - http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
  - prezentare principii, metode şi tehnici de testare a securităţii sistemelor
  - nu intră în foarte multe detalii tehnice (face referire la OSSTMM)
- Information Design Assurance Red Team (IDART)
  - http://idart.sandia.gov/
  - red teaming
- Information Systems Security Assessment Framework (ISSAF)
  - http://www.oissg.org/issaf/
  - stadiu incipient (drat)
- Open Web Application Security Project (OWASP)
  - http://www.owasp.org/
  - framework pentru asigurarea securităţii aplicaţiilor Web

# Certificări profesionale

- Certified Ethical Hacker / Licensed Penetration Tester
  - EC-Council
  - http://www.eccouncil.org/certification/certifications.aspx
- GIAC Certified Penetration Tester (GPEN) / GIAC Web Application Penetration Tester (GWAPT)
  - SANS Institute (SysAdmin, Audit, Networking, and Security)
  - http://www.giac.org/certifications/security/
- Certified Penetration Tester (CPT)
  - Information Assurance Certification Review Board (IACRB)
  - http://www.iacertification.org/aboutus.html

# Etape



# Planificarea

- Obţinerea aprobărilor din partea managementului organizaţiei
- Semnarea NDA (Non Disclosure Agreement)
- Definirea scopului şi a planului de testare
- Stabilirea metodologiei de testare şi alegerea uneltelor

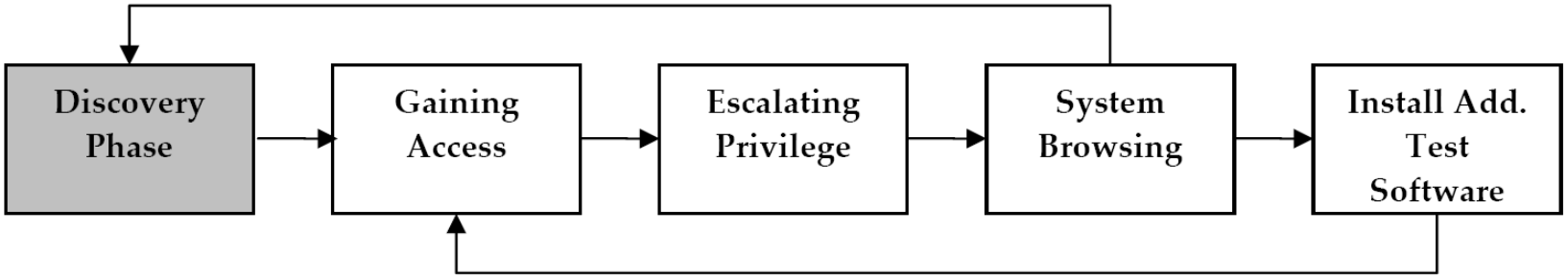
- Rules of Engagement

# Descoperirea

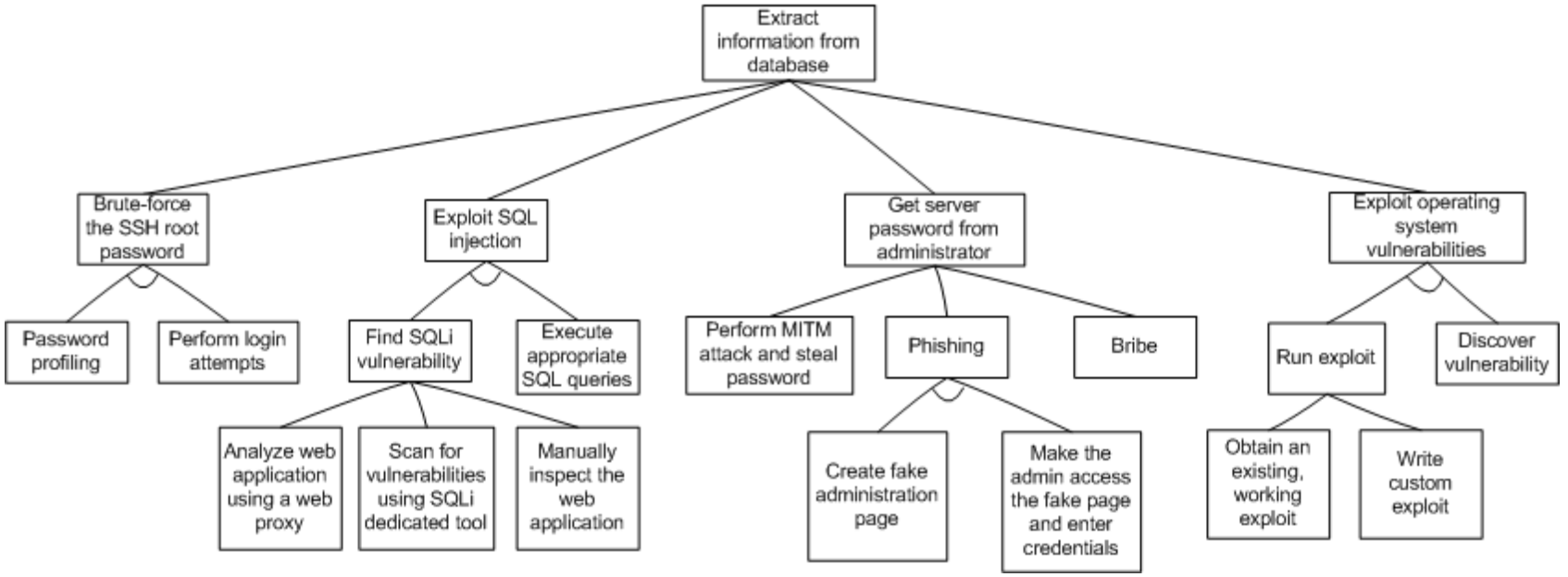
- Culegerea de informaţii (recunoaşterea)
  - cunoaşterea ţintei (sedii, infrastructură IT&C, angajaţi, parteneri, etc)
- Scanarea şi enumerarea
  - determinare sisteme active, porturi, servicii, sisteme de securitate, etc
- Identificarea vulnerabilităţilor
  - sisteme ne-updatate, greşeli de configurare, drepturi de acces, etc

# Atacul

- **Exploatarea vulnerabilităţilor**
  - exploit-uri de securitate
  - poate duce la blocarea funcţionării sistemelor!
- **Obţinerea accesului în sistem**
  - control asupra sistemului (parţial / total)
- **Escaladarea privilegiilor**
  - obţinere privilegii de super user (root / administrator)
  - folosire sistem compromis pentru a ataca alte sisteme



# Arborele de atac




- introdus de Bruce Schneier şi formalizat de S. Mauw şi M. Oostdjik
- Construire scenarii de atac pentru fiecare obiectiv de atins
- Acţiuni conjunctive / disjunctive
- Pentru fiecare nod se pot defini atribute: cost, timp de desfăşurare, unelte necesare, etc

# Raportare

- Conţinutul raportului de testare
  - Executive Summary
  - Probleme identificate
    - Descriere detaliată
    - Nivelul de risc asociat
    - Impactul asupra organizaţiei
  - Recomandări
  - Concluzii
- Descrierea detaliată a fiecărui tip de atac desfăşurat şi a rezultatelor obţinute (chiar dacă a avut succes sau nu)
- Prezentarea raportului în faţa clientului

# Resurse

- Live distributions CD
  - BackTrack (http://www.backtrack-linux.org/)
  - Knoppix STD (http://s-t-d.org/)
- Site-uri web
  - http://www.offensive-security.com/
  - http://www.vulnerabilityassessment.co.uk/
  - http://sectools.org/
  - http://www.remote-exploit.org/
  - http://packetstormsecurity.org/