COSC 458-647
Application Software Security

Automating Penetration Tests

Today

- The Penetration Test
- Problems in the current Penetration Test practice
- Automating Penetration Tests
- The Technical Challenges
- Overcoming the Technical Challenges
- Conclusions

The Penetration Test

- What is it?
- What is it good for?
- How is it actually done?

The Penetration Test

- Rationale:

“Improving the security of your site by breaking into it”,

Dan Farmer & Wietse Venema, 1993
http://www.fish.com/security/admin-guide-to-cracking.html

- A plausible definition:

“A localized and time-constrained attempt to breach the information security architecture using the attacker’s techniques”

Terms

- “Localized”
  - Implies definition of scope
- “Time-constrained”
  - A pentest does not last forever
- “Attempt to breach the security”
  - A pentest is not a full security audit
- “Using the attacker’s techniques”
  - Implies definition of the attacker’s role

Requirements and Goal

- Scope
- Security architecture
- Attacker’s profile
- Results

The goal

- To improve information security awareness
- To assess risk
- To mitigate risk immediately
- To reinforce the IS process
- To assist in decision making processes

The Scope: What will be tested?

- IT infrastructure
- Security architecture
  - Prevention capabilities
  - Detection capabilities
  - Response capabilities
  - Policies and procedures
- Business processes

The Scope: When it will be tested?

- Weakest/Strongest moment
- Normal operational state
- Periodically, random date within limits
- Before/After specific projects

Security Architecture

- Security Infrastructure (PKI/FWs/IDSes)
- Network security
- Host security
- Workstation security
- Application security
- Physical security
- Human security

The Attacker’s Profile

- External
  - With zero previous knowledge
  - With some degree of knowledge
- Internal
  - With zero previous knowledge
  - With some degree of knowledge
- Associate

The Result: Final Report

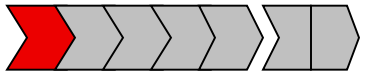
- Clear description of scope and methodology
- Reproducible and accountable process
- High level analysis and description (suitable for upper/non technical management)
- General recommendations and conclusions
- Detailed findings

How is it usually done?

1. Information Gathering
2. Information Analysis and Planning
3. Vulnerability Detection
4. Penetration
5. Attack/Privilege Escalation
6. Analysis and reporting
7. Clean-up

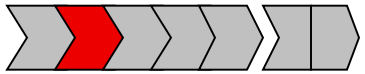
Information Gathering

- Organizational intelligence
- Access point discovery
- Network discovery
- Infrastructure fingerprinting



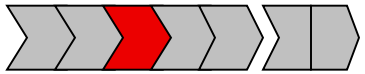
Information Analysis and Planning

- Understanding of component relationships
- High level attack planning
- Target identification
- Time & effort estimation
- Alternative attacks



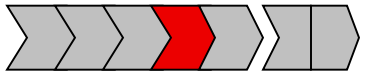
Vulnerability Detection

- Automated vulnerability scanning
- Manual scanning
- In-house research
- Target acquisition



Penetration Phase

- Known/available exploit selection
- Exploit customization
- Exploit development
- Exploit testing
- Attack



Attack/ Privilege Escalation Phase

- Final target compromise: SUCCESS!
- Intermediate target: full compromise, pivoting
- Intermediate target: partial compromise, pivoting
- Point of attack/attacker profile switching
- Back to information gathering phase