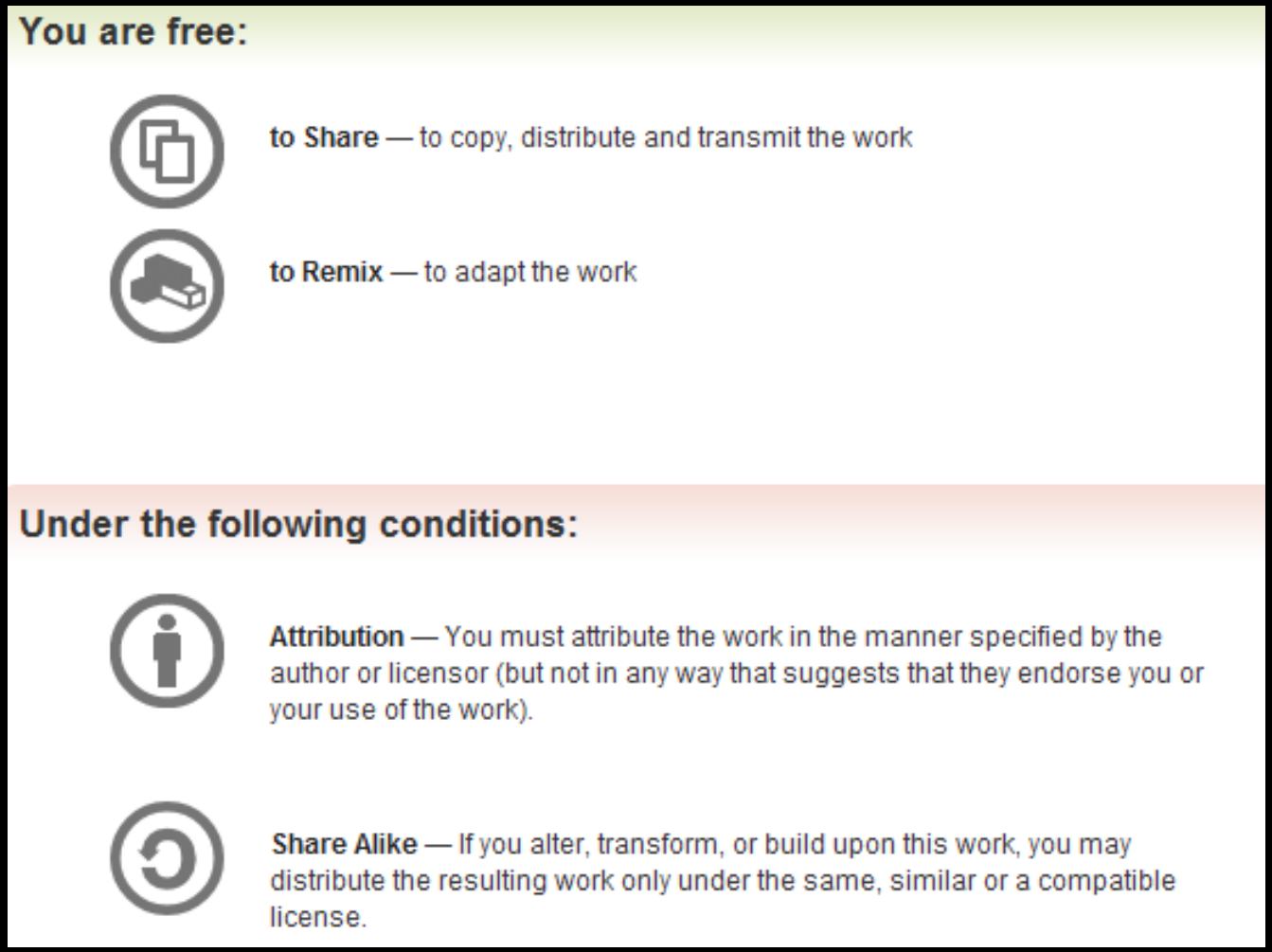
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

Physical Pentesting

What good is your firewall or IDS/IPS if I can grab your box?

Outline – Physical Pentesting

- Intro.
- The Process
- Techniques

Overview

- A Physical Penetration Test identifies the security weaknesses and strengths of the client's physical security.

- The goal of the test is to demonstrate the existence or absence of deficiencies in operating procedures concerning physical security.

Continue…

Did You Know?

- Physical Security is often overlooked in an organization
- Physical Security breaches can have the same impact as computer breaches
- Physical Security Attack & Penetration Tests should be conducted on high value facilities and locations annually
- Physical Security Attack & Penetration Tests should be conducted by qualified personnel with years of experience

The Process

- Building an Operating Team
- Project Planning
- Rules of Engagement
- Conducting Preliminary Research
- Evaluating Risk
- The Test Plan
- Legal Issues and Documentation

Building an Operating Team

- Operator – all are operators
- Team Leader – onsite/HQ
- Coordinator or Planner – offsite/HQ
- Social Engineer
- Computer Intrusion Specialist
- Physical Security Specialist
- Surveillance Specialist

Project Planning

Plan your project, create a workflow to be sure that you cover all aspects of the assignment. A recommended approach (Wil Sopp):

- Receiving the assignment – contracts signed and certain legal formalities observed.
- Negotiating the Rules of Engagement – Define what you can and can't do during testing and their purpose is usually to limit testers to a certain scope.
- Performing Preliminary Research – Pursue the initial IG phase.
  - Determining Risk – Very important to accurately gauge the risk a project poses both to the company and to the team members executing it.
  - Writing a Test Plan – A formal (but flexible) test plan is a good idea from both project management and legal perspectives.
  - Gathering Equipment – Important for the team to take gear that's appropriate to the test without being over encumbered.
- Providing documentation and legal requirements – Once the planning stage is complete you will have a not insignificant amount of documentation.

Rules of Engagement

- Determine areas of security the client considers to be weak and wants tested.
- Determine areas of testing the client wishes to avoid for legal reasons, such as close surveillance of staff.
- Agree on team members that will carry out testing (Clearances might not be given to all).
- Agree on test duration, or the maximum time permitted.
- Agree about the information given in advance {white, grey, black} box testing.
- Agree on the target assets (overall goals): something the team must acquire, identify, gain access to, or photograph. Examples include network operation centers, passwords or target personnel.
- Agree on test success, failure, and abortion circumstances.
- Agree on the actions to be taken directly following successful, failed and aborted tests.
- Determine a schedule for presentation and post testing report.
- After agreement is reached, document the RoE to be added to the project documentation.

Conducting Preliminary Research

- Human Intelligence (HUMINT).
- Signals Intelligence (SIGINT).
- Open Source Intelligence (OSINT).
- Imagery Intelligence (IMINT).

Evaluating Risk

- Team leader's responsibility to determine what constitutes an acceptable level of project risk. If level of risk is too high then the RoE should be reassessed or the test should not be carried out.

RISK acronym – COLE:

- Contractual Risks
  - Unable to complete assingment
- Operational Risks
  - Inexperienced team members, technical communication failure
- Legal Risks
  - Getting arrested
- Environmental Risks
  - Presence of machinery or high voltage
  - Climbing and falling
  - Guard dogs
  - Extremes of heat or cold
  - Confronting armed security

The Test Plan

- **Strategic:**
  - High-level view of the project that details the goals, assets, team members, potential COLE risks, and necessary equipment.
- **Tactical:**
  - List of milestones and the order of completion.
- **Operational:**
  - Requirements to complete each milestone and how its completion will affect the whole engagement.

Legal Issues and Documentation

Includes but not limited to:

- RoE
- Test plan
- Signed contracts
- Copies of ‘get out of jail free’ cards
- Scan of official ID of operating team members (passport, driving license)

Techniques

- Practical physical security testing
- Site exploration
- Tactical approaches
  - Tailgating to Gain Entry
  - Clothes Maketh the Man
  - Visiting a Nonexistent Employee
- Badge security
- Security mechanisms

Physical Pentesting

- Countermeasure
- Mitigation
- Remediation

?

SUMMARY

- The importance of physical penetration testing, and why it must not be overseen,
- Howto prepare for a physical pentesting,
- Techniques used for physical pentesting,
- Countermeasures, Mitigation, and Remediation for physical pentesting.

References

[-] Lock picking info., http://www.lockwiki.com/index.php/Main_Page

[-] Lock picking tools, http://toool.us/

[-] Learn Lock Picking, http://www.learnlockpicking.com

[-] Video on Lock picking, http://video.google.com/videoplay?docid=-8536478434720082857&ei=8sKpSrG0J5jqqwK4tsytAw&q=lock+picking+physical+security&hl=en

[-] Journal of Physical Security (JPS), http://jps.anl.gov/

[-] Hardware Tools for Physical Pentesting, http://www.darkreading.com/vulnerability-management/167901026/security/vulnerabilities/231600749/tech-insight-three-hardware-tools-for-physical-penetration-testing.html