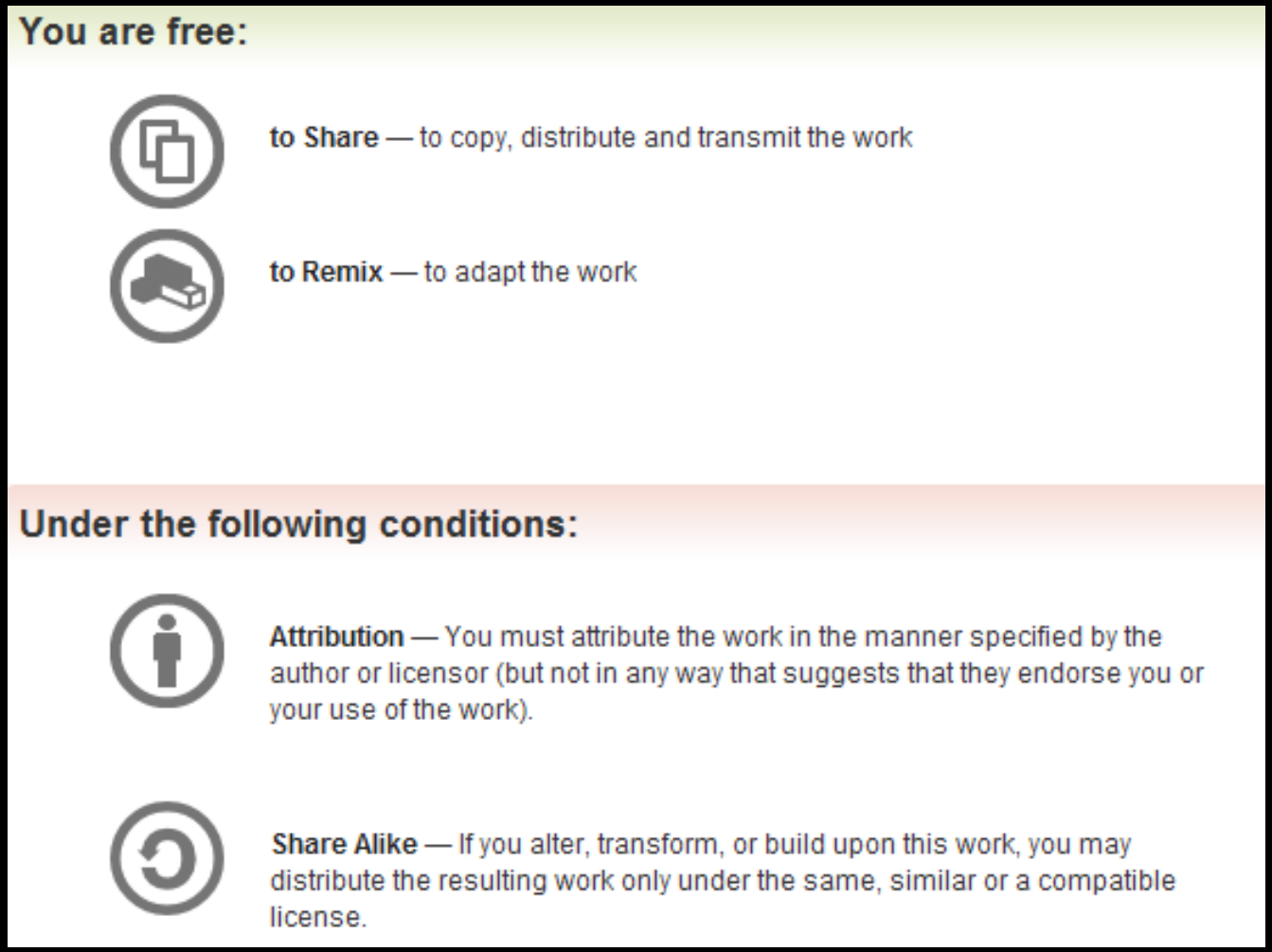
Hacking Techniques & Intrusion Detection

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

Pre-Engagement, and Reconnaissance

Outline – Pre-Engagement

Pre-Engagement Process:

- Scoping
- Goals
- Communication Lines
- Rules of Engagement
- Capabilities and Technology in Place

Scoping

- Scoping is arguably one of the more important and often overlooked components of a penetration test.
- Scoping is specifically tied to what you are going to test. This is very different from covering how you are going to test.
- A penetration test is not an activity to see if the tester can "*hack*" you. It should be about *identifying the business risk associated with an attack*.

Howto Scope

- Figure out exactly how you as a tester are going to spend your time.
- Some engagements will have a wide canvas of IP addresses to test and choose from to try and access a network as part of a test.
- Highly focused tests will spend weeks (if not months) on one specific application.

The key is knowing the difference!

Metrics for Time Estimation

- Much of this will be based upon your experience in the area you are going to test.
- Try to estimate consultant overhead.
  - Meeting Creep, Site problems, etc
  - Provide additional service if no overhead
- Specify clearly the starting and ending date and the hours required to work.

Scoping Meeting

- The goal of the scoping meeting is to discuss what it is you are to test. It is not to about RoE or Costs.
- In many cases the scoping meeting will happen after the contract has been signed.
- There are some blissful scenarios where you can cover many of the topics relating to scope before a contract is signed. For those situations an NDA must be signed before any in-depth scoping discussions occur.
- Need to ask them explicitly what IP ranges are in scope for the engagement.
- Need to identify which countries the target environment operates in.

Additional Support Based on Hourly Rate

- Anything that is not explicitly covered within the scope of the engagement should be handled very carefully.
- These tasks can easily eat the profits of your engagement and create confusion and anger with the customer.
- Additional requests has to be documented in the form of a Statement of Work that clearly identifies the work to be done.
- Clearly state in the contract that additional work will be done for a flat fee per hour and explicitly state that additional work cannot be completed until a new SOW is signed.

Questionnaires

- Communication starts with the customer by a set of questions that you will need answered before you can accurately scope the penetration test engagement.
- These questions are critical to ask and should give you a better understanding of:
  - what the client is looking to gain out of the penetration test
  - why the client is looking to have a penetration test performed against their environment,
  - and whether or not they want certain types of tests performed during the penetration test.

Check the Questionnaires document for examples.

Scope Creep

- Often one of the most effective ways that a penetration testing company can cease to exist.
- Couple of things to remember when battling scope creep:
  - If you have done a great job it is very common for a customer to request additional work.
  - Do not gouge your existing customers when they ask for additional work.
  - Specify start and end dates.
  - Put in contract retesting after final report (ex: 30 days).
  - Your best source for future work is through your existing customers. *Treat them well and they will return*.

Specify IP Ranges and Domains

- You must know what the targets you will be attempting to penetrate are.
- Targets obtained from the customer during the initial questionnaire phase.
- Targets can be given in the form of specific IP addresses, network ranges, or domain names.
- In some instances, the only target the customer gives you is the organization's name.
- Important to define systems that are between the target and the tester like: firewalls and IDS/IPS or networking equipment.

Dealing with Third Parties

- Some situations where you will be asked to test a service or an application that is being hosted by a third party.
- Important to remember that you may have permission to test from your customer, but you also need to receive permission from the third party!
  - Cloud Services
  - ISP
  - Web Hosting
  - Managed Security Service Providers (MSSP)
  - Countries Where Servers are Hosted

Verify the laws yourself, don't depend on others!

Define Acceptable Social Engineering Pretexts

- Social engineering and spear-phishing attacks are currently widely used by many attackers today.
- Most of the successful attacks use pretexts like sex, drugs and rock and roll some of these pretexts may not be acceptable in a cooperate environment.
- Obtain written approval for the pretext that will be used in the test.

DoS Testing

- Stress testing or Denial of Service testing should be discussed before you start your engagement.
- Many organizations are uncomfortable with due to the potentially damaging nature of the testing.
- If an organization is only worried about the confidentiality or integrity of their data:
  - stress testing may not be necessary
- If the organization is worried about the availability of their services:
  - stress testing should be conducted in a non-production environment that is identical to their production environment

Payment Terms

- **Net 30**

Total amount is due within 30 days of the delivery of the final report. Usually associated with a per month percentage penalty for non-payment.

- **Half Upfront**

Require half of the total bill upfront before testing begins. This is very common for longer-term engagements.

- **Recurring**

May have a recurring payment schedule. This is more of a long-term engagement.

Goals

- Every penetration test should be goal oriented.
- The test is to identify specific vulnerabilities that lead to a compromise of the business or mission objectives of the customer (not finding un-patched systems).
  - Primary – not compliance driven
  - Secondary – can be compliance driven
- Secondary goals mean something for compliance and IT. Primary goals get the attention of the C-O's.
  - Business Analysis - depends on maturity of the customer

Establish Lines of Communication

- One of the most important aspects of any penetration test is communication with the customer.

- How often you interact with the customer, and the manner in which you approach them, can make a huge difference in their feeling of satisfaction.

Emergency Contact Information

- Being able to get in touch with the customer or target organization in an emergency is vital.
- Create an emergency contact list.
- Not only do you need contact information from the customer, but they may need to contact you.
- The list should preferably include the following people:
  - All penetration testers
  - The manager of the test group
  - Two technical contacts at each target organization
  - One upper management or business contact at the customer

Rules of Engagement (RoE)

- Scope defines what it is you are supposed to test, the rules of engagement defines *how testing is to occur*.

- Timeline
- Locations
- Disclosure of Sensitive Information
- Evidence Handling
- Regular Status Meetings
- Time of the Day to Test
- Dealing with Shunning
- Permission to Test
- Legal Considerations

Capabilities and Technology in Place

- Testing the capabilities of the target organization in regards to the ability to detect and respond to:
  - Information gathering, foot printing, scanning and vulnerability analysis, infiltration (attacks), etc

- Important Note:

  when tracking this information be sure to collect time information.