Introduction to Penetration Testing

Reading:
Bishop Section 23.2 Penetration Studies pg 647-660

Prep:
Nothing to download unless you want to follow along with the Kali Linux demonstrations that will be shown in class in which case you'll need a distro of Kali Linux

http://docs.kali.org/downloading/kali-linux-live-usb-install

First of all, not a good enough reason to use the word penetration, so shall henceforth be referred to as "pen testing"

There are different methodologies but NIST is commonly accepted in the US.

National Institute of Standards and Technology (NIST)

- The full document is listed here: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- Four-Stage PenTesting Methodology
    1. Planning
    - this stage includes information gathering and scanning (network ports, services, etc.)
    - physical recon also included
    - tools: nmap, wireshark,
    - In a full up pentest, the first step is always an initial kickoff meeting with the correct higher level stakeholders. At times its not good to bring in engineering level personnel because they'll create and establish extra security controls for the pentest. This doesn't give the customer a "true" report of what condition their environment really is in.
        1. Goals:
            - Establish ROE (very important) - you need to figure out what the left and right bounds are for a test
            - Establish Timeline
            - Establish POC in case you bring down a server
        2. White box vs Black box pentest:
            - White box - the tester has full knowledge of the system provided by the subject of the test
            - Black box – the tester has no knowledge of the system that cannot be found by the public
    - Any sort of passive recon is okay here. Normally online lookups, things available off of social media sites (Facebook, Instagram, linked-in), job postings (to figure out what technology they are using).

2. Discovery
    - this is the vulnerability analysis stage
    - list of publicly available databases included in the full document
    - tools: Nessus, Nexpose,
    - This is also the asset identification and enumeration. For instance for a network based pentest you'll be looking for assets out on the network, identify hosts look to group them in attack categories and run real basic button pressing tools to do quick surveying. Note: if you are trying to be quiet this can take a long time. IDS systems can be configured to catch these common toolsets (listed above). You may have to go back to the basics.
        a. Example: Symantec endpoint protection is configured to trigger alerts off of a port scan. Even if you use telnet to connect to 3 or more ports it will trigger the alert.
    - A big part of the industry is trying to commoditize pen testing. PCI / HIPPA type certifications generally don't go past this stage. Generally all they require is vulnerability analysis followed by "remediation of red/yellow findings".
    - Extra Tools:
        a. Network: nmap, telnet, netcat, unicornscan, python, scapy, wireshark, tcpdump, nessus, nexpose, qualys
        b. Wireless: kismet, fern, airmon, aircrack-ng suite.
        c. Web: Burp, ZAP, skipfish, nessus, nexpose, qualys, cenzic
3. Attack (the fun part)
    - verify previously identified vulnerabilities by attempting exploits
    - 4 stages
        a. Gaining Access
        b. Escalating Privileges
        c. System Browsing
        d. Install Additional Tools
    - Categories of vulnerabilities that get exploited
        a. Misconfigurations: change settings of a node on the system
        b. Kernel Flaws
        c. Buffer Overflows: able to introduce arbitrary code due to a lack of adequate length checking of input
        d. Insufficient Input Validation: opportunity for SQL injection, or other database contamination
        e. Symbolic Links: often used to trick privileged programs into running, accessing, modifying, or listing incorrect files
        f. File Descriptor Attacks: file descriptors used in place of file names to keep track of files, if a privileged program assigns an incorrect descriptor then it is vulnerable
        g. Race Conditions: usually used to take advantage of something given temporarily elevated privileges

    h. Incorrect File and Directory Permissions

- tools: John the Ripper, Burp Suite, Aircrack-ng,
- Tools into the 4 broken categories
    a. Gaining Access
        - Social Engineering Toolkit (SET)
        - Code Cave Injections
        - Open network jacks
        - Wireshark
        - Arp Cache Poisoning
        - Net-Bios MITM

    b. Escalating Privileges
        - DLL injections
        - User created scripts
        - Set UID/GID to root (run as admin scripts)
        - Metasploit
        - Powersploit
        - Veil

    c. System Browsing
        - I call this stage “hunting sysadmins”
        - Net * commands
        - Lots of manual searching

    d. Install Additional tools
        - I think this section refers to lateral movement and persistence
        - You’ll want to make sure you have a way back into a system that you’ve comprised
        - Scheduled tasks
        - Startup scripts
        - Metasploit, Veil, Powershell, Net,
        - Look to take advantage of kerberos based authentication
        - Golden Ticket attack

4. Reporting
    - this phase happens in conjunction with the other 3 phases, logs, notes, and results are to be recorded for later record
    - the report is the official collection of the logs and notes taken through the other phases and they should include at least what was done, why, and results
    - tools: outta luck here, gotta write stuff -
    - Collaboration - Lair is a dba with a easy to use front end that allocates your scan data into a spot. You can add notes and eaisly track your progress as you go.
        a. Assign rbac roles to various pentesters or analysts on the job.

        - Dradis will take your scan data and import it into a word document for you. Lots of up front work is required to make the word template but if you are doing repetitive testing this thing will save your life.

- Wargame sites for fun: http://overthewire.org/wargames/bandit/ → this is a very good wargaming site for anyone interesting in learning linux. Real easy and provides guidance for new people
- Conferences - Defcon, shmoocon, derbycon all these conferences post videos online. That you can watch for free.

Red Team/ Blue Team

- This is a simulated exercise in which a group of security professionals try to infiltrate a system (red team) while another team tries to defend (blue team)
- Red Team: Offense
- Blue Team: Defense