Penetration Testing

January 28, 2016

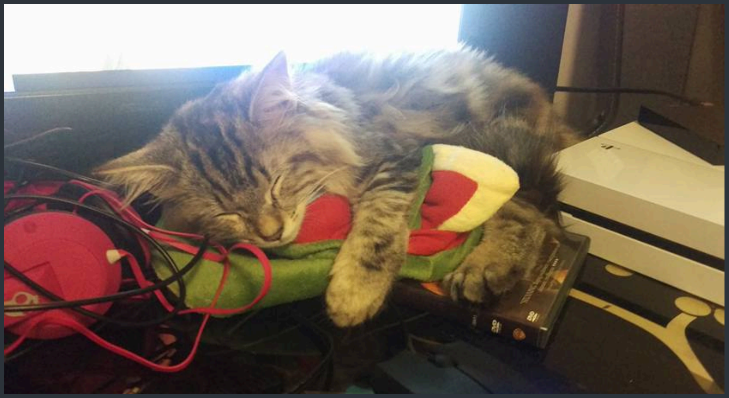
Marissa Nishimoto

First things first

- Not a good enough reason to use the word “penetration” → “pen testing”

A Bit About Me

- Undergrad: B.S. in Applied Computational and Mathematical Science (Focus EE Digital Signal Processing)
- Graduate: M.S. Cybersecurity (in progress)
- Working in an engineering rotation program
- That’s my cat →



National institute of standards and technology (NIST)

- Four Stages
  - Planning: this stage includes information gathering and scanning (network ports, services, etc.)
  - Discovery: vulnerability analysis stage
  - Attack: verify previously identified vulnerabilities by attempting exploits
  - Reporting: the paperwork

Planning

- Goal: Defining the pentest with whoever has contracted the tester. Also includes figuring out general information about the environment of the system.
- physical recon also included
- tools: nmap, wireshark
- 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
- White box vs Black box pentest
- Other sorts of techniques things available off of social media sites (Facebook, Instagram, linked-in), job postings (to figure out what technology they are using).

Discovery

- Goal: Find out what they have in a detailed fashion. Should be able to draw a picture of the target system.
- Tools:
  - Network: nmap, telnet, netcat, unicornscan, python, scapy, wireshark, tcpdump, nessus, nexpose, qualys,
  - Wireless: kismet, fern, airmon, aircrack-ng suite.
  - Web: Burp, ZAP, skipfish, nessus, nexpose, qualys, cenzic
- This is also the asset identification and enumeration

Attack

- 4 Stages:
  - Gaining Access
  - Escalating Privileges
  - System Browsing
  - Install Additional Tools
- Goal: Compromise the system
  - This will look different for different systems and requests

Categories of Vulnerabilities

- Misconfigurations: change settings of a node on the system
- Kernel Flaws
- Buffer Overflows: able to introduce arbitrary code due to a lack of adequate length checking of input
- Insufficient Input Validation: opportunity for SQL injection, or other database contamination
- Symbolic Links: often used to trick privileged programs into running, accessing, modifying, or listing incorrect files
- 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
- Race Conditions: usually used to take advantage of something given temporarily elevated privileges
- Incorrect File and Directory Permissions

Attack (weapons)

- **Gaining Access**
  - Social Engineering Toolkit (SET)
  - Code Cave Injections
  - Open network jacks
  - Wireshark
  - Arp Cache Poisoning
  - Net-Bios MITM

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

Attack (weapons)

- **System Browsing**
  - “hunting sysadmins”
  - Net * commands
  - Lots of manual searching

- **Install Additional Tools**
  - Scheduled tasks
  - Startup scripts
  - Metasploit, Veil, Powershell, Net,
  - Look to take advantage of kerberos based authentication
  - Golden Ticket attack (http://www.infoworld.com/article/2608877/security/fear-the-golden-ticket-attack-.html)

Reporting

- Goal: Help the customer understand what you did and the consequences of any weaknesses found
- Not a lot of tools, but some collaboration tools to help
  - Lair has an easy to use front end that allocates your scan data into a spot. You can add notes and easily track your progress as you go.
  - Assign 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.

Red team / blue team

- Red Team: Offense
- Blue Team: Defense

Miscellaneous resources if you like breaking stuff

- Wargame sites for fun: http://overthewire.org/wargames/bandit/ → this is a very good wargaming site for anyone interesting in learning linux. Provides guidance for new people.
- Conferences - Defcon, shmoocon, derbycon all these conferences post videos online. Free!
- Hak5.org has some awesome tutorials, blogs, nerd toys (for the use of cybersecurity professionals and friendly enthusiasts)
- Return Oriented Programming (ROP): http://smashthestack.org/index.html
  - IO is the ROP one, there are other flavors listed on the left
- Of course… Kristina ☺

What’s NOT Allowed

Blue

- Air strikes
- Police on standby

Red

- Air strikes
- Total destruction