Hawaii STEM Conference 2015
Wailea Marriott
April 17 and 18, 2015

Cybersecurity Breakout Overview
Dr. Debasis Bhattacharya, @uhmcabit, UH Maui College
Mario Canual, UHMC Student and King Kekaulike graduate

Quote from WhiteHat Security web site - www.whitehatsec.com
"The reason ethical hacking exists is because somebody less ethical in a different country will hack your systems and not tell you - that is going to happen no matter what," says **Jeremiah Grossman**, Founder and CTO of WhiteHat Security. "So, ethical hacking is conducted to hack yourself first and fix the issues and vulnerabilities that remain to avoid being a headline like Sony."

Ethical hackers, then, attempt to exploit the IT security of a system on behalf of its owners by following certain polite rules, like getting a written or verbal consent from the owner of the system before the professional conducts the test. [Source: WhiteHatSec]

Phases of an Attack
1. Reconnaissance - preparatory phase where an attacker gathers as much info
2. Scanning - use details gathered during reconnaissance to identify vulnerabilities
3. Gaining access - enter through open ports, user download of malicious bot code etc.
4. Maintaining access - when most of the damage is usually done
5. Covering tracks - remove evidence of entry, install Trojan or rootkit etc.

Ethical Hackers
Ethical hackers
- Information security professionals who specialize in evaluating and defending against threats from attackers
- Possess excellent computer skills and are committed to using those skills in protecting the integrity of computer systems rather than hurting them
- Former black hats or White hats or Consulting firms

What do Ethical Hackers do?
Ethical hacker's evaluation of a client's information system security seeks answers to three basic questions:
- What can an attacker see on the target system?
- What can an intruder do with that information?
- Are the attackers' attempts being noticed on the target systems?

Ethical hacker must also remember to convey to the client that that it is never possible to guard systems completely
- However, they can always be improved

Conducting an Ethical Hack

1. Talk with the client about the importance of security and the necessity of testing
2. Prepare NDA (non-disclosure agreement) documents and have the client sign it
3. Prepare an ethical hacking team and create a schedule for testing
4. Conduct the test
5. Analyze the results and prepare the report
6. Deliver the report to the client

Steganography

Art and science of communicating in a way that hides the existence of a message. Hiding messages among irrelevant and obvious data - files, images, sound, video etc.

Big **r**umble **i**n **N**ew **G**uinea.
The **w**ar **o**n **c**elebrity **a**cts **s**hould **e**nd **s**oon.
Over **f**our **b**ig **e**cstatic **e**lephants **r**eplicated!

Tools of the Ethical Hacker

1. Security Scanner - Nmap - www.nmap.org
2. Network Sniffing - Wireshark - www.wireshark.org
3. Windows Internals - http://technet.microsoft.com/en-us/sysinternals/bb842062
4. Password cracker - Ophcrack - http://ophcrack.sourceforge.net/
5. Steganography - http://embeddedsw.net/OpenPuff_Steganography_Home.html
6. Passcracking + Network Sniffing - Cain & Abel - http://www.oxid.it/cain.html

Ethical Hacking Activities

1. Trace a route from your computer to a remote computer
    a. Tools - Tracert and Nmap
    b. Looking Glass Server - http://www.bgp4.as/looking-glasses
2. Discover live hosts and services running on a network - Tools - www.Nmap.org
3. Port scanning to discover open ports - Tools - Nmap
4. Send out Phishing email to test vulnerability and social engineering
5. Conduct Denial of Service (DoS) attack - tools - DoSHTTP www.socketsoft.net

Current and Future CyberSecurity Events

1. PicoCTF
    a. Sponsored by Carnegie-Mellon and NSA - http://www.picoctf.com/
2. CyberPatriot VIII - Cyber Competition for High Schools - October 2015 - Feb 2016
    a. Information page - http://www.uscyberpatriot.org/Pages/default.aspx
3. CAMS CTF
    a. Capture the Flag event created by the California Academy of Mathematics and science - http://camsctf.com/
4. UH Maui College
    a. Certificate of Competency - http://maui.hawaii.edu/cybersecurity

Cybersecurity Labs

1. **Microsoft System Internals -** This is a set of tools that provides great access to the internal working of your Windows computer. Test a few of these tools:
    a. **DiskView** - Hard Disk Analysis
    b. **ProcExp** - Process Explorer
2. **Ping** - This is a network tool used for testing whether or not a computer is online (locally or globally) It sends an ICMP packet that makes a round trip. If the packet is not returned, then the computer might be down or blocking ping packets. This tool also measures latency, or the amount of time taken for the packet to make a round trip.
    a. Click on the Windows logo on the bottom left corner of the desktop, and type in "**cmd**" and press enter.
    b. After you see the command shell or box, type in "**ipconfig**" (without quotes!)
    c. Type in "**ping www.hawaii.edu**" and press enter
    d. Type in "**ping www.google.com**"and press enter
        i. This shows the average round-trip time between you and the closest google server.
    e. Type in "**ping www.bbc.net.uk**" and press enter. Note the
    f. Type in "**ping 127.0.0.1**"
        i. This is the localhost, so average round-trip time should be 0ms.
    g. Type in "**ping www.eng.kremlin.ru**"
        i. This is the website for the president of Russia, notice the average round-trip time is a lot more than google, this shows high latency, which often has to do with the amount of devices your connection passes through as well as geographical factors such as distance.
3. **Zenmap: Traceroute** - This is a network tool that lists the hosts that your computer has to hop through in order to get to your destination. The internet is not as simple as just connecting directly to a server, but rather, you hop different networks in order to reach that server.
    a. Open Zenmap application and in **Profile**: select "**Quick Traceroute**".
    b. In **Target**: type in "www.hawaii.edu" and press **Scan**.
    c. In **Target**: type in "www.google.com" and press **Scan**.
    d. In **Target**: type in "www.bbc.net.uk" and press **Scan**.
    e. In **Target**: type in "www.eng.kremlin.ru" and press **Scan**.
        i. While Google has servers all over the US, the BBC is in the United Kingdom, so we will see the servers/routers your computer goes through to get there. Not surprisingly, the Kremlin takes the longest!
        ii. You'll notice a drastic jump in time (measured in milliseconds) in between hops, you can assume that's the time it took for the packets to move across the Pacific/Atlantic ocean, especially to the Kremlin.
    f. Click **Topology** to see a graph of the traces across the Internet. Click **Fisheye**.

4. **WHOIS**: Lookup Domain and IP Owner Information
    a. Open the Google Chrome browser
    b. Type in www.who.is
    c. In the WhoIs site, type the box: www.amazon.com and check out the results
    d. Click on DNS Records and on first row Type A, see under Content: 72.21.194.1
    e. Go to Google Chrome browser and in Search Box, type: 72.21.194.1
    f. In the WhoIs site, type the box: www.cern.ch and check out the results
    g. Click on DNS Records and on first row Type A, see under Content: 188.184.9.234
    h. Go to Google Chrome browser and in Search Box, type: 188.184.9.234
5. **Zenmap/Nmap: Port Scanning**
    a. Open Zenmap application and in **Profile**: select "**Quick Scan**".
    b. In **Target**: type in "72.21.194.1", click Scan & check out the results for Amazon
    c. Change Profile: select "**Intense Scan, no ping**" click Scan for a Stealth Scan
    d. In **Target**: type in "188.184.9.234", click Scan & check out the results for CERN
    e. In **Target**: type in "66.147.244.155", click Scan & check out MEDB.ORG
    f. Change Profile: select "**Intense Scan, no ping**" Note the various open ports
    g. Click on Ports / Hosts and Host Details for more information
6. **Wireshark: Packet Capture**
    a. Open Wireshark application, select WiFi and click on Start
    b. Click Capture - Options and ensure you have all the valid Interfaces
    c. Open a browser and generate some web traffic. Search for **Amazon.com**
    d. In the **Filter box**, type or select **http**
    e. Top Panel is Packet List, Middle is Packet Detail and bottom is Packet Bytes
    f. To search for Amazon, go to **Edit - Find Packet**.
    g. Check on Find By: **String.** In Filter: type **amazon**
    h. Select Search In: **Packet Bytes**, click **Find**. Find Next by clicking **Ctrl+N**
    i. Generate packets by searching for **www.MEDB.org** and doing the above steps
    j. You can stop your search and save packets as a pcap file by **File - Save As**
7. **OpenPuff: Steganography (optional)**
    a. Open the application Open Puff. Click on **Hide button**
    b. Use only one password for simplicity. **Uncheck Enable (B) and (C)**
    c. Type in a simple password such as MEDB2015
    d. Go to Carrier, where you will hide the file. Click Add and Select **boston.JPG**
    e. Go to Data, which is the payload in Carrier. Browse and select **Secret.txt**
    f. Click on **Hide Data**! Save to the Desktop
    g. The boston.JPG file is saved to the Desktop with a hidden text file
    h. Do the reverse process to Unhide the text file from the Carrier file
    i. You can also hide pictures within pictures, or video within pictures etc.