



Ethical Hacking as a Career

Dr. Debasis Bhattacharya | debasisb@hawaii.edu | @uhmcabit | maui.hawaii.edu/cybersecurity

"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 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 - most of the damage is usually done
- 4 Maintaining access - remove evidence of entry, install Trojan or rootkit etc.
- 5 Covering or erasing tracks, deleting log files, removing traces of entry and access

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

Ethical hacker categories:

- Former black hats or White hats or Consulting firms

Pay Ranges for Ethical Hackers – Average Salary is \$71,000, with max range to \$111,000

Companies that hire ethical hackers – banks, insurance, hospitals, government, education etc.

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 (nondisclosure 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.

Example: Big rumble in New Guinea. The war on celebrity acts should end soon.

Over four big ecstatic elephants replicated!

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](http://embeddedsw.net/OpenPuff%20Steganography%20Home.html)

Ethical Hacking Activities

- 1 Trace a route from your computer to a remote computer
 - a Tools - Tracert (on Windows), Traceroute (MacOS) and Nmap
 - b Looking Glass Server - <http://www.bgp4.as/looking-glasses>
- 2 Discover live hosts and services running on a network - Tools - Nmap
- 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

Sample Exercises

1. Tracert (Windows) – a) www.google.com b) 127.0.0.1 c) www.bbc.co.uk
2. Ping (Windows or MacOS) – a) www.google.com b) 127.0.0.1 c) www.bbc.co.uk
3. WW Looking Glass Servers: <http://www.bgp4.as/looking-glasses> Sample Looking Glass Server in North America NTT <https://www.us.ntt.net/support/looking-glass/>
4. www.MxToolBox.com - a) www.google.com b) meethawaii.com c) grandwailea.com
5. The HoneyNet Project – www.honeynet.org and MHN - <http://threatstream.github.io/mhn/>

Upcoming CyberSecurity Events

- 1 UH Maui College Summer 2017 - Cyber Camps, <http://maui.hawaii.edu/cybersecurity>
- 2 GenCyber Camps in Hawaii Summer 2017 – Details at <https://gencyber-hi.org/>
- 3 UH Maui College, NSA GenCyber Beginner Camp – June 5-9, 2017
- 4 UH Maui College, NSA GenCyber Intermediate Camp – June 12-16, 2017
- 5 UH Maui College, US Air Force Association CyberPatriot Camp – June 19-23, 2017