

Becoming a Hacker



Everett Stiles
evstiles@cisco.com
ASIG

Chris McCoy
cmm@cisco.com
ASIG

Nicholas Weigand
nweigand@cisco.com
ASIG

Sammy Tieng
stieng@cisco.com
ASIG

John Allbritten
jallbrit@cisco.com
ASIG

Omar Santos
os@cisco.com
PSIRT

Maxwell Schmidt
maxwschm@cisco.com
ASIG



Let's learn about each other!

- Who you are
- What you currently do and your history in Cisco
- Your experience in security and hacking
- What you'd like to achieve in this class

GET TO KNOW THE CLASS

GET TO KNOW ASIG

GET TO KNOW INSTRUCTORS

Agenda, Lab Access, & Materials

<https://training.becomingahacker.com>

<https://becomingahacker.com>

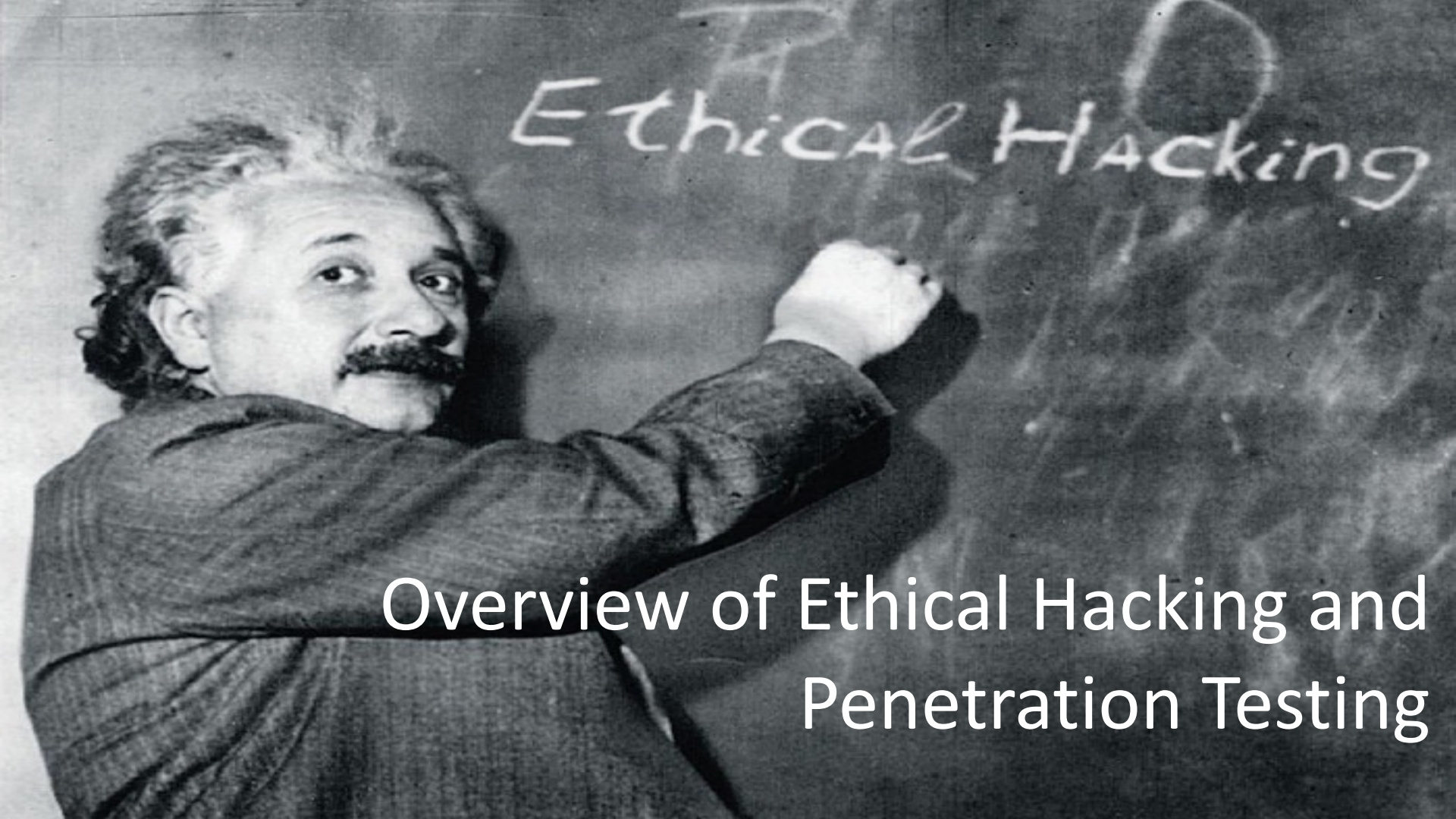
DISCLAIMER | WARNING

Do not hack your neighbor

The information provided on this training is **for educational purposes only**. The **author**, Cisco, or any other entity **is in no way responsible for any misuse of the information**.

Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.

Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

A black and white photograph of Albert Einstein, with his characteristic wild hair and mustache, wearing a dark sweater. He is standing in front of a chalkboard, looking back over his shoulder at the camera while his right arm is raised, holding a piece of chalk. The word "Ethical Hacking" is written in large, cursive letters on the chalkboard behind him.

Ethical Hacking

Overview of Ethical Hacking and Penetration Testing

What is Penetration Testing or Ethical Hacking?

- An ethical hacker is as a person who is hired and permitted by an organization to attack its systems for the purpose of identifying vulnerabilities, which an attacker might take advantage of.
- The sole difference between the terms “malicious hacking” and “ethical hacking” is the permission.

What is a White Hat Hacker?

- Security professionals or security researchers that perform ethical hacking.
- Such hackers are employed by an organization and are permitted to attack an organization to find vulnerabilities that an attacker might be able to exploit.

What is a Black Hat Hacker?

- Sometimes also referred to as a cracker, threat actor, bad actor, or malicious attacker.
- Uses his or her knowledge for negative purposes.
- Of course, they are often referred to by the media as *hackers*.

What is a vulnerability?

- A vulnerability is an exploitable weakness in a system or its design.
- Vulnerabilities can be found in protocols, operating systems, applications, hardware, and system designs.

What is a threat?

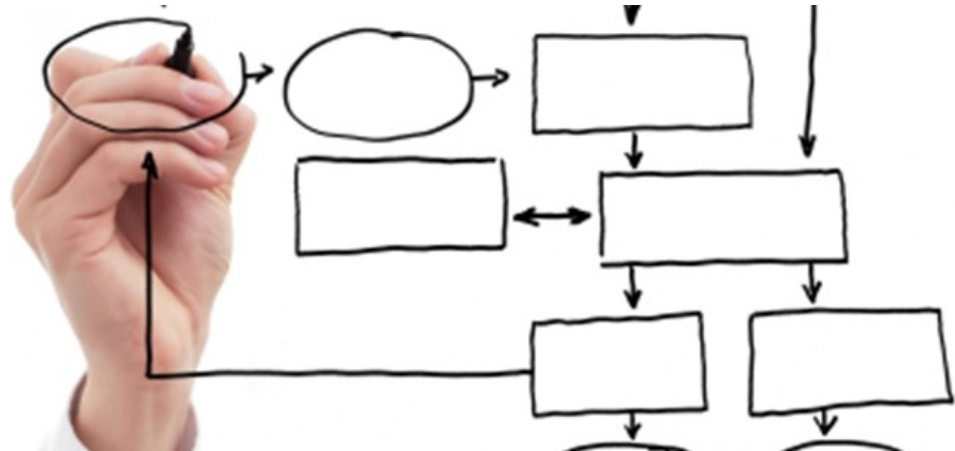
- A threat is any potential danger to an asset.
- If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known— “the threat is latent and not yet realized.”

What is an exploit?

- An exploit is software or a sequence of commands that takes advantage of a vulnerability in order to cause harm to a system or network.
- There are several methods of classifying exploits; however, the most common two categories are remote and local exploits.

Hacking is a lot more than cool tools...

- Methodologies
- Research
- Think like an attacker
- Combine social engineering with technical capabilities

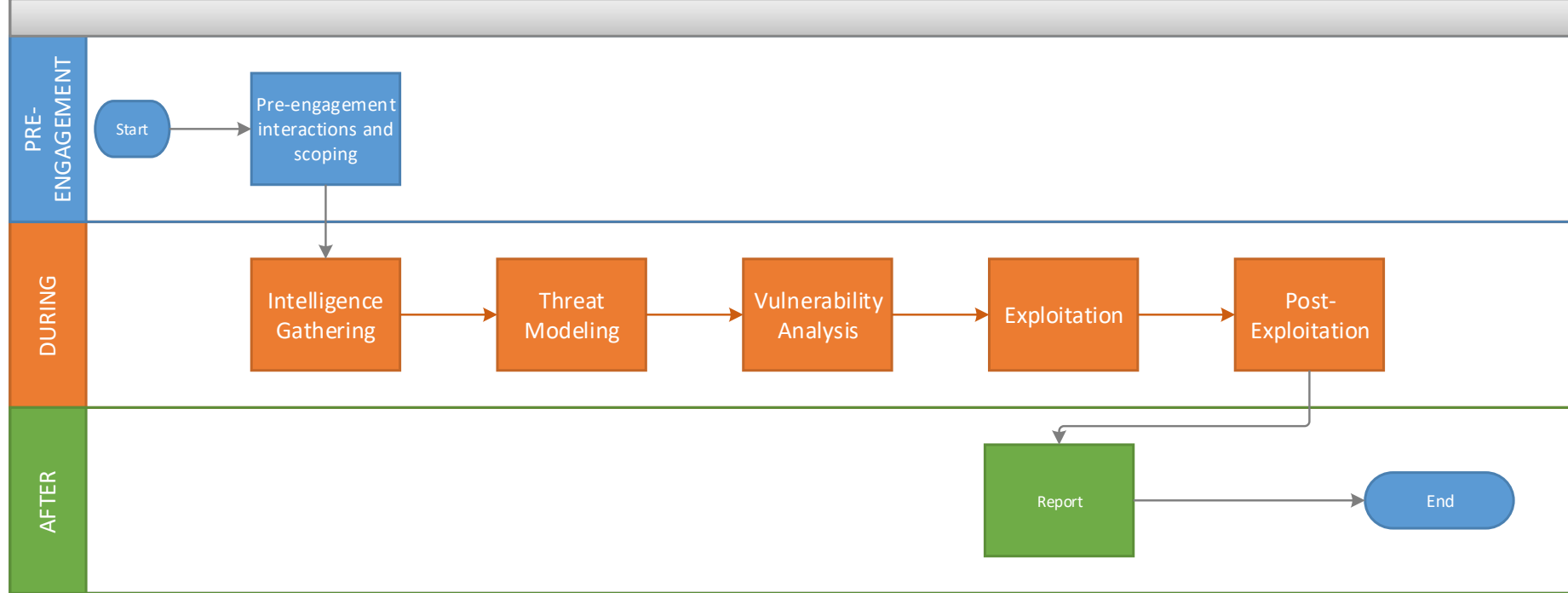


PEN TESTING METHODOLOGIES

- Penetration Testing Execution Standard
<http://www.pentest-standard.org>
- OWASP Testing Guide
https://www.owasp.org/index.php/OWASP_Testing_Project
- NIST 800-115: Technical Guide to Information Security Testing and Assessment
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- Open Source Security Testing Methodology Manual (OSSTMM)
<http://www.isecom.org/research/>

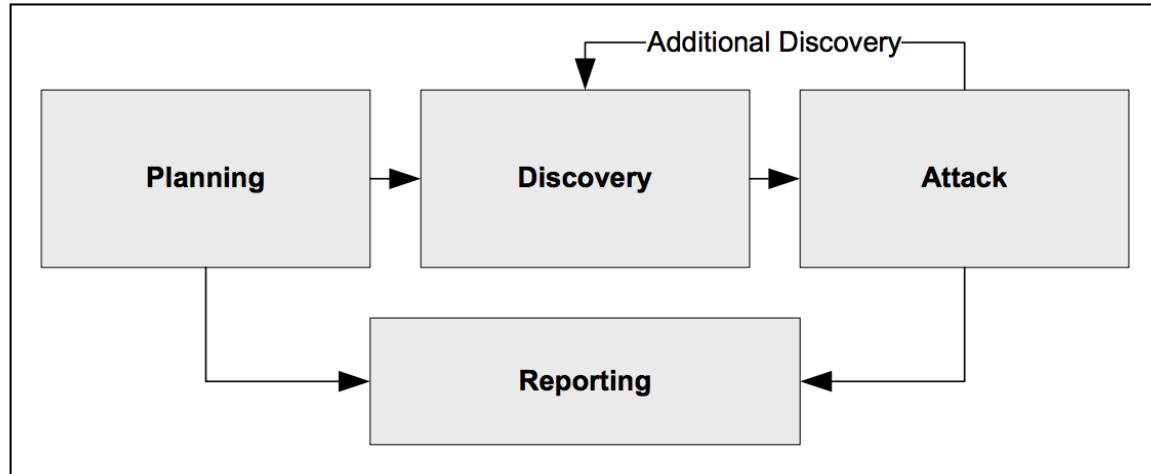


PEN TESTING LIFECYCLE



Aligned with: <http://www.pentest-standard.org>

NIST 800-115



<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>



Over 6000 resources! – h4cker.org/github