

Vulnerabilità e Difesa dei Sistemi Internet

A.K.A. ETHICAL HACKING

FRANCESCO MANCINI- francesco.mancini@uniroma2.it

The class

Structured as a hands-on survey of topics

- Topics hand picked from a variety of resources
- Hands on through in-class/homework assignments

Will transform n00bs into hackers in ≈60 hours?

- Absolutely not...
- ...it will introduce you to a new vision of security
- Practical projects will help you to master tools
- Start to do something impressive:
 - Make a difference on the security community
 - Expand existing tools
 - Design new tools
 - Explore cutting edge tools / techniques / skills

Prepare your equipment

Laptop/PC needed in most of the lessons!

Virtualization Platform:

- Virtualbox: <https://www.virtualbox.org/wiki/Downloads>
- VMWare Workstation Player: <https://www.vmware.com/content/vmware/vmware-published-sites/us/products/workstation-player/workstation-player-evaluation.html.html>

Operating System:

- Kali Linux: <https://www.kali.org/get-kali/#kali-platforms>

Approximate Schedule

Introduction

Tools and Best Practices

- Kali Linux and Metasploit

Information Gathering

- Social Engineering

Vulnerability and Scanning

Network Hacking


Password security

Wireless security

Web Application exploitation

Privilege escalation

Post-exploitation



Defensive point of view?!

#whoami



Contacts

E-mail:

- Francesco Mancini: francesco.mancini@uniroma2.it
- Pasquale Caporaso: pasquale.caporaso@uniroma2.it
- Pierciro Caliendo: pierciro.caliandro@uniroma2.it
- Sara Da Canal: sara.da.canal@uniroma2.it

Telegram: <https://t.me/+UPNIM93E-g5MjNk>

Volunteer collaboration for

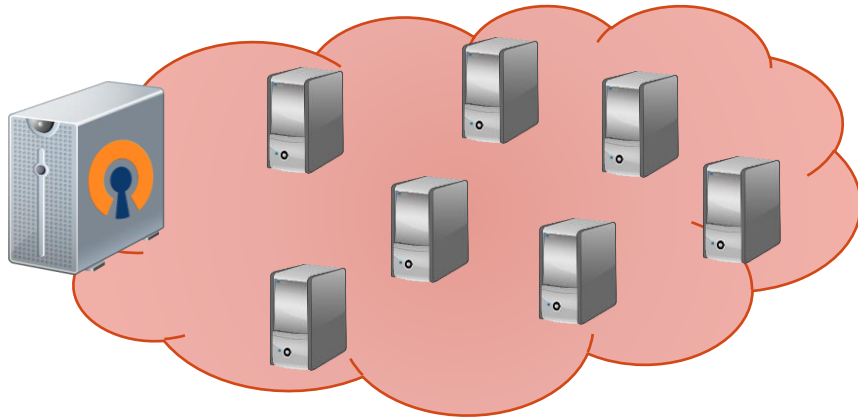
- Security news and opinion
- Technical analysis of security threats (hacking news, etc.)
- Project outcomes

Teams: [BIANCHI-8039415-VULNERABILITA' E DIFESA DEI SISTEMI INTERNET | General | Microsoft Teams](#)

Test and Improve skills practically

VPN with network to hack:

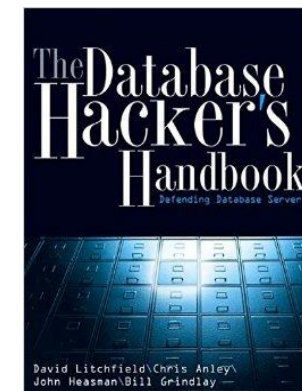
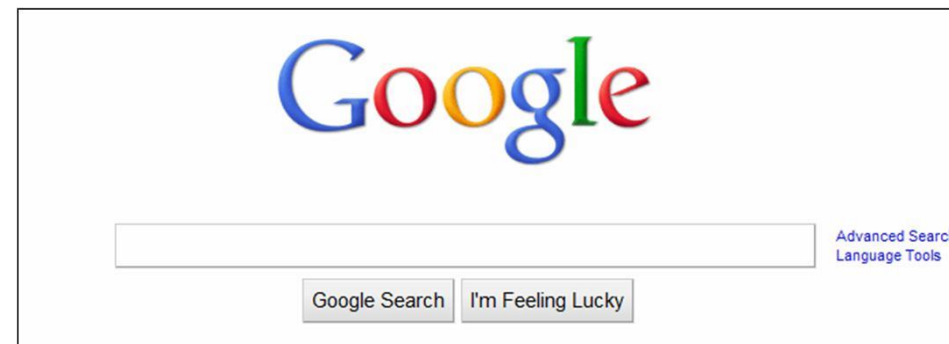
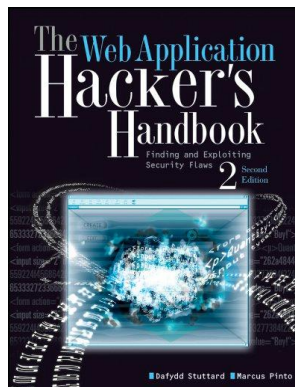
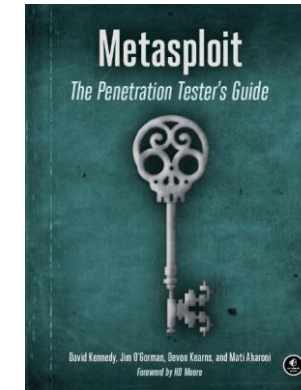
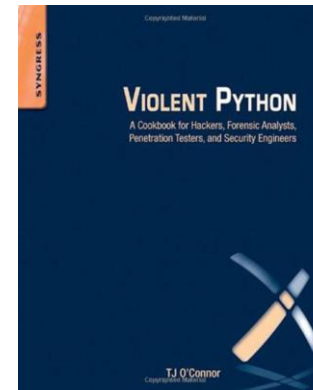
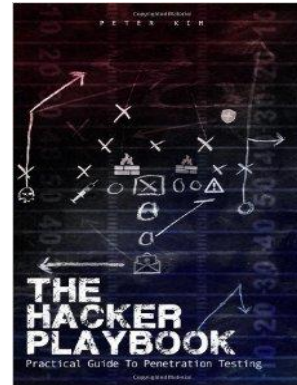
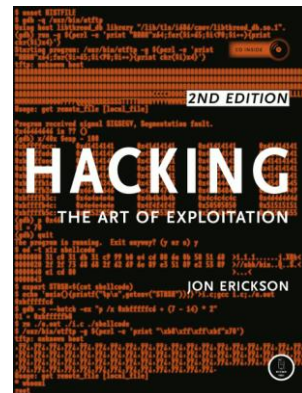
- <https://tryhackme.com/>
- <https://www.hackthebox.com/>



CTF challenges? <https://ctftime.org/>



Suggested readings



Vulnerabilità e Difesa dei Sistemi Internet

WHAT HACKING IS?

DDoS vs Hacking

Currently around the World....

- <http://www.digitalattackmap.com/>
- <http://map.ipviking.com/>



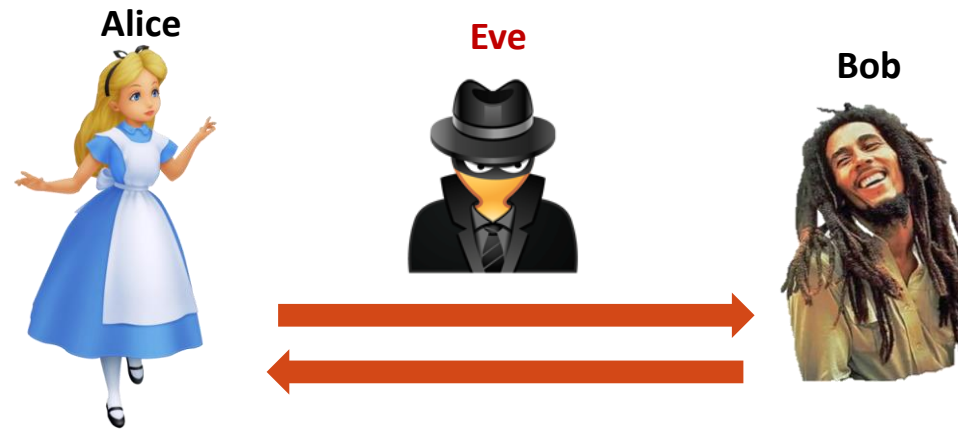
But these are just DDoS...We are going to thoroughly explore more interesting techniques...

- Learn to gain (un)-authorized access
- With the final aim to detect and prevent it

Security with Alice and Bob

How can Alice communicate securely with Bob?

- When Eve can modify or eavesdrop on the communication?



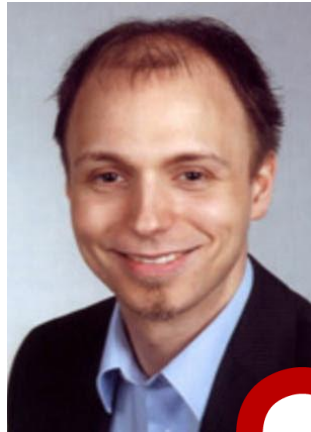
Security with Alice and Bob

How can Alice communicate securely with Bob?

- When Eve can modify or eavesdrop on the communication?
- Use a secure communication channel (e.g. TLS/SSL)!



The real world



[projects](#) / [openssl.git](#) / commit

[summary](#) | [shortlog](#) | [log](#) | [commit](#) | [commitdiff](#) | [tree](#)
(parent: [84b6e27](#)) | [patch](#)

PR: 2658

```
author    Dr. Stephen Henson <steve@openssl.org>
          Sat, 31 Dec 2011 23:59:57 +0100 (22:59 +0000)
committer Dr. Stephen Henson <steve@openssl.org>
          Sat, 31 Dec 2011 23:59:57 +0100 (22:59 +0000)
commit    4817504d069b4c5082161b02a22116ad75f822b1
tree      7a85f6af852e34e5b80080b50d80741f6ab36c5a   tree | snapshot
parent    84b6e277d4f45487377d0159e82c356d750e1218   commit | diff
```

PR: 2658
Submitted by: Robin Seggelmann <seggelmann@fh-muenster.de>
Reviewed by: steve

Support for TLS/DTLS heartbeats.

20 files changed:

What heartbleed is?

Exploits a vulnerability in OpenSSL

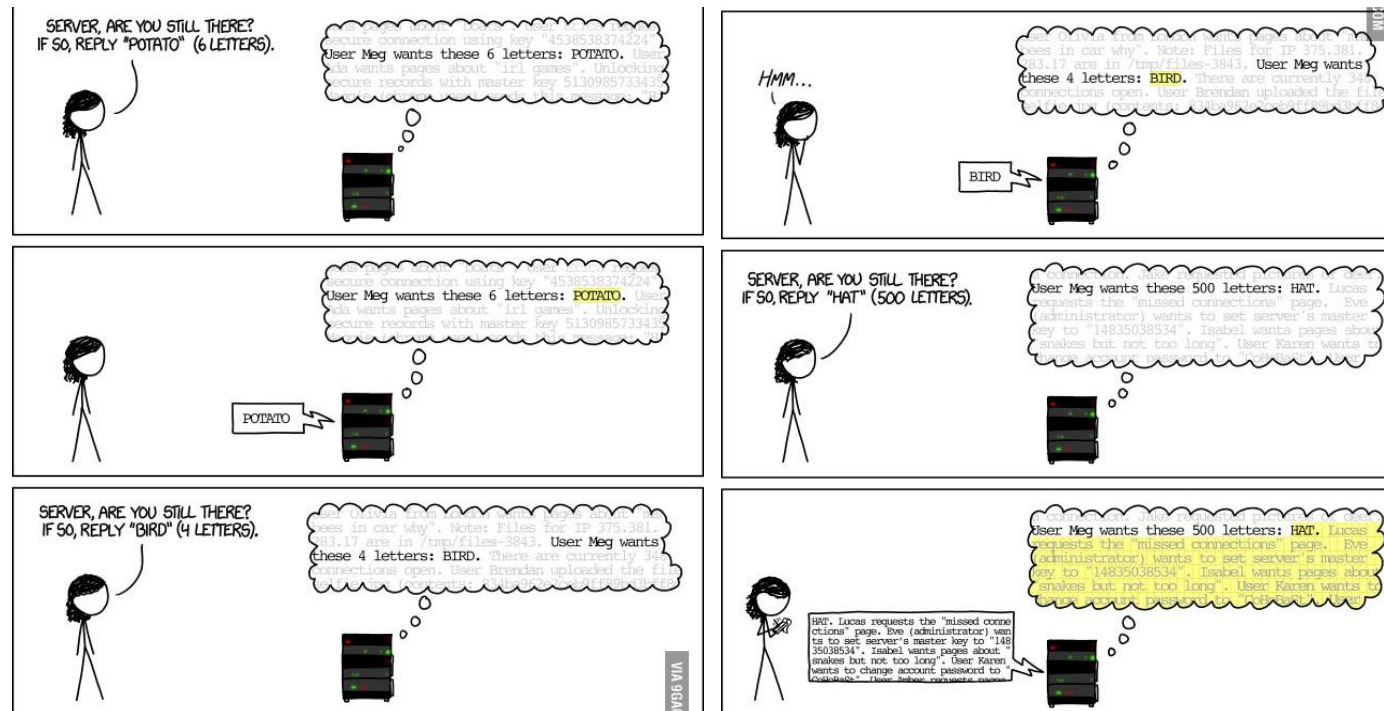
- used to implement the Transport Layer Security protocol
- used in web, mobile, instant messaging, etc.

Exposes

- User's passwords
- Cookies and other data to the attacker
- Server's **PRIVATE KEY!**

It is not a malware!

How it works?



Take-home messages

User input may:

- Have the wrong value
- Have the wrong size or format
- Be from an authorized but malicious user
- Be from an unauthorized user (or have been modified by an malicious user)

User input must be validated in form and content:

- Security functions should never rely on un-validated user input
- Malicious input to functions which aren't themselves security related can still cause security failures

It is hard to maintain software:

- It does not always implement what we expect
- It is configured by humans
- It is subject to errors

Take-home messages

Theory
≠
Real World

Vulnerabilità e Difesa dei Sistemi Internet

HACKERS VS PENETRATION TESTERS

Black, White, Gray, Red, Blue...hat?

SCRIPT KIDDIES

Use borrowed programs to attack networks and deface websites in an attempt to make names for themselves.



HACKTIVISTS

Some motivated by politics or religion, while others may wish to expose wrongdoing, or exact revenge, or simply harass their target for their own entertainment.



Black, White, Gray, Red, Blue...hat?

WHITE HAT HACKERS

These are the **good guys**

- Still operates illegally unless otherwise stated

Computer security experts

- Specialized in penetration testing
- To ensure that a company's information systems are secure
- Seeks out security flaws and vulnerabilities not for exploitation, but so that their discovery will result in their correction, benefitting the common good

BLACK HAT HACKERS

These are the **bad guys**

- Typically referred to as just plain hackers
- Seeks **un-authorized** access to systems **without acquiring legal permission**

Motivation is for personal benefit

- Material wealth creating spambots and botnets, acquiring lucrative information, blackmail
- Vendetta (website defacement or vandalism just for fun)
- Generally to get paid



Black Hat means...

State Sponsored Hackers

- Governments around the globe realize that now it's all about controlling cyberspace
- Have limitless time and funding to target civilians, corporations and governments

Spy Hackers

- Corporations hire hackers to infiltrate the competition and steal trade secrets
- They may hack in from the outside or gain employment in order to act as a mole
- Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid

Cyber Terrorists

- These hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures
- Cyber terrorists are by far the most dangerous, with a wide range of skills and goals
- Cyber Terrorists ultimate motivation is to spread fear, terror and commit murder

Penetration Tester vs Hacker

What is the difference between a Pen Tester and a Hacker?

- PenTester's have prior **approval** from the **client**
- Hackers have prior **approval** from **themselves**
- PenTester's social engineering attacks are there to raise awareness
- Hackers social engineering attacks are aimed into divulging sensitive information about the whereabouts of their target

PERMISSION

Without permission, its ILLEGAL

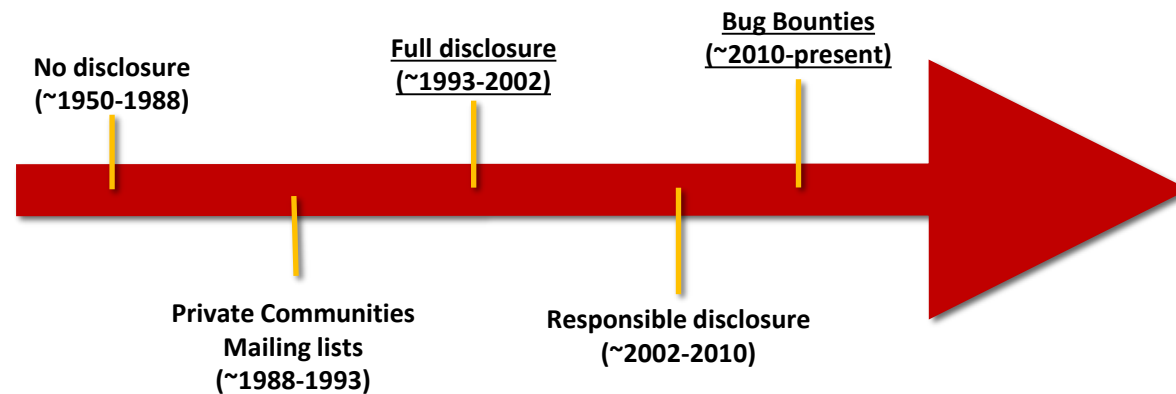


Ethics and Vulnerability Disclosure

Say you find a security problem

Who do you tell? And how?

- How would they react?
- Would they sue you? patch it? or ignore it?
- What if you worked hard to find it?



Bug Bounty Programs

Company	Scope	Bounty	URL
Google	Web & Apps	\$500-\$20,000	http://www.google.com/about/appsecurity/reward-program/
Facebook	Web	\$500+	https://www.facebook.com/whitehat/bounty/
Mozilla	Web / Mobile/ Apps	\$500 - \$3,000	http://www.mozilla.org/security/bug-bounty.html

What motivates hackers?

Black hat: “It’s their own fault.”

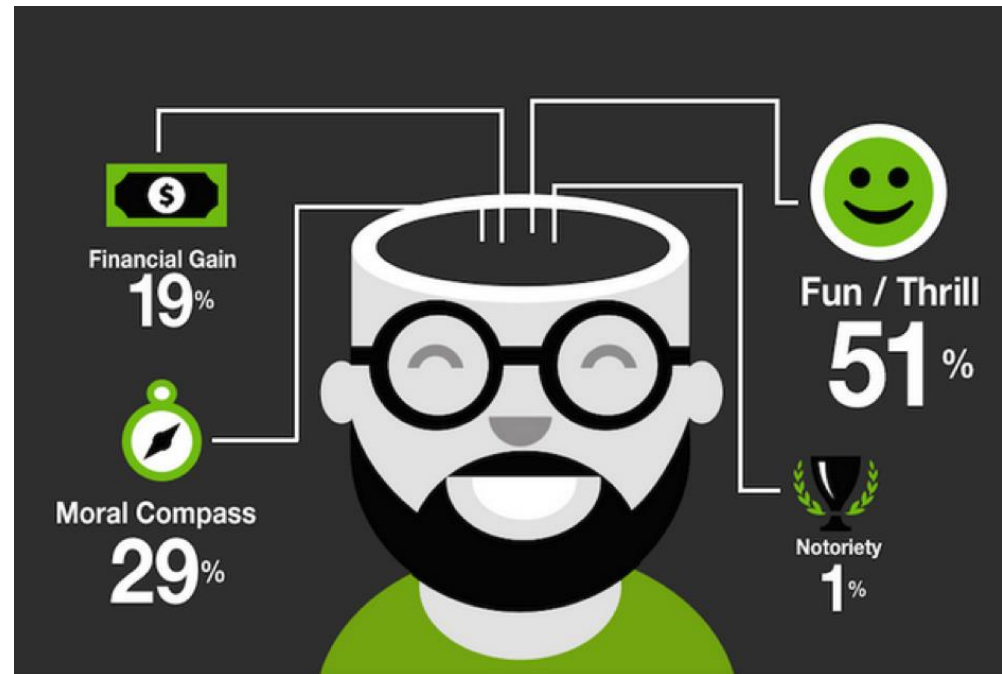
White hat: “Yeah, but it’s our responsibility to help them.”

Grey hat: “I want to help, but I don’t want to get in trouble...”



Not pictured: Grey hat

What motivates hackers?

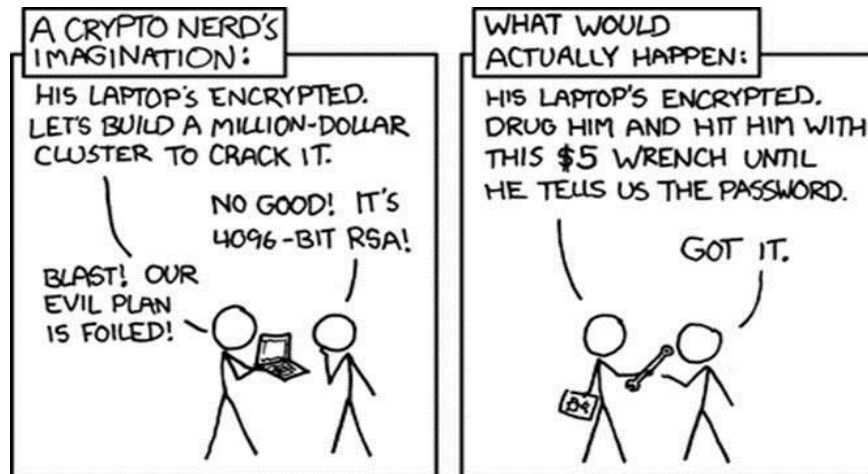


What motivates an ethical hacking course?

Teaching only defense is like teaching people personal defense
when you don't even know how a punch looks like

Most security education focuses heavily Cryptography...

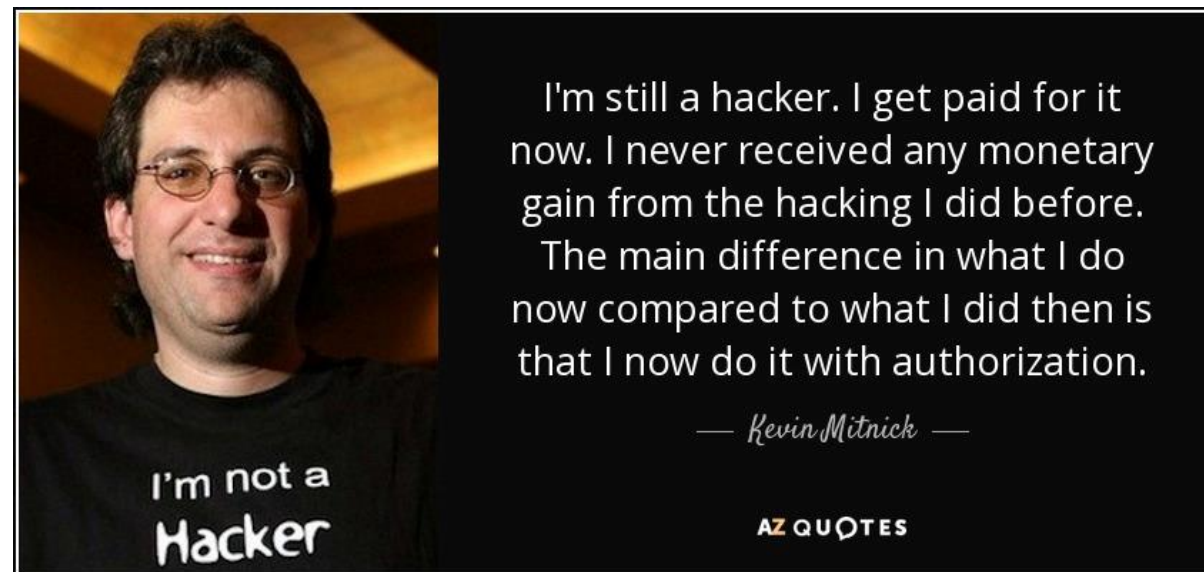
...but to break into most systems, you don't have to break crypto



What motivates pentesters?

Penetration testing is fun

- ...and you get paid for hack!!!



What motivates pentesters?



What motivates pentesters?



Hacker skills

Basic Computer Skills

- These skills go beyond the ability to create a Word document or cruise the Internet...

Networking Skills

- DHCP, NAT, Subnetting, IPv4, IPv6, Public vs Private IP, DNS, Routers and switches, VLANs, OSI model, MAC addressing, ARP, etc.
- The better you understand how they work, the more successful you will be

Linux Skills

- It is extremely critical to develop Linux skills to become a hacker. Nearly all the tools we use as a hacker are developed for Linux
- Linux gives us capabilities that we don't have using Windows

Security Concepts & Technologies

- The only way to overcome the roadblocks established by the security admins is to be familiar with them
- The hacker must understand such things as PKI (public key infrastructure), SSL (secure sockets layer), IDS (intrusion detection system), firewalls, etc.

Hacker skills

Scripting

- To develop your own unique tools, you will need to become proficient at least in one of the scripting languages
- These should include one of Perl, Python, or Ruby.

Web Applications & Databases

- The more you understand about how web applications work and the databases behind them, the more successful you will be.
- In addition, you will likely need to build your own website for phishing and other nefarious purposes.

Advanced Networking & Cryptography

- You must understand in intimate details the networking protocols stack and fields
- Although one doesn't need to be a cryptographer to be a good hacker, the more you understand the strengths and weaknesses of each cryptographic algorithm, the better the chances of defeating it.

Reverse Engineering

- Reverse engineering enables you to open a piece of malware and re-build it with additional features and capabilities

Hacker skills

Think Creatively

- There is ALWAYS a way to hack a system and many ways to accomplish it. A good hacker can think creatively of multiple approaches to the same hack.

Problem-Solving Skills

- A hacker is always coming up against seemingly unsolvable problems. This requires that the hacker be accustomed to thinking analytically and solving problems.
- This often demands that the hacker diagnose accurately what is wrong and then break the problem down into separate components. This is one of those abilities that comes with ***many hours of practice.***

Persistence

- A hacker must be persistent. If you fail at first, try again. If that fails, come up with a new approach and try again.

It takes time

Script kiddies or packet monkeys

- Young inexperienced hackers
- Copy codes and techniques from knowledgeable hackers

Experienced penetration testers write programs or scripts using these languages

- Practical Extraction and Report Language (Perl), C, C++, Python, JavaScript, Visual Basic, SQL, and many others

This class alone won't make you a hacker, or an expert

- It might make you a **script kiddie**

It usually takes years of study and experience to earn respect in the hacker community

- It's a hobby, a lifestyle, and an attitude
- A drive to figure out how things work

Vulnerabilità e Difesa dei Sistemi Internet

PHASES OF AN ATTACK/PENETRATION TEST

What is Penetration Testing?

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker.

– Wikipedia

The intention is to find security weaknesses and:

- Potentially gain access to the system
- Exploit functionalities of the system
- Obtain un-authorized data

Penetration tests can be **automated** with software applications or they can be performed **manually**.

The process includes:

- gathering information about the target before the test (**reconnaissance**)
- identifying possible entry points (**port scanning**)
- attempting to break in (**either virtually or for real**)
- **reporting back the findings**

Penetration Testing vs Vulnerability Assessment



Penetration Testing vs Vulnerability Assessment

Vulnerability Assessment:

- Typically is general in scope and includes a large assessment
- Predictable (I know when those darn Security guys scan us)
- Unreliable at times and high rate of false positives (I've got a banner!)
- Vulnerability assessment invites debate among System Admins
- Produces a report with mitigation guidelines and action items

Penetration Testing:

- Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
- May be unpredictable by the recipient (Don't know the "how?" and "when?")
- Highly accurate and reliable (I've got root access!)
- Penetration Testing = Proof of Concept against vulnerabilities
- Produces a binary result: *Either the team owned you, or they didn't*

Scope of Penetration Testing

Targeted Recon

- Targeted exploitation of vulnerable software

Social Engineering

- Hi HelpDesk...I'm Mr. Jones...Can you tell me what my password is?

Physical facilities audit

- Hmm, I forgot my badge... but there's 200 yards of fence missing on the east side of the center

Wireless War Driving

- Detection of rogue or weakly encrypted AP's

Dumpster Diving

- How much fun can I have in the dumpster...whoops...I've found someone's notes paper with passwords

Why Bother?

Active pen-testing teaches you things that security planning will not

- What are the vulnerability scanners missing?

Are your users and system administrators actually following their own policies?

- host that claims one thing in security plan but it totally different in reality
- Audit Physical Security
- Just what is in that building no one ever goes in?
- The strongest network based protections are useless if there is a accessible unlocked terminal, unlocked tape vault, etc.

Raises security awareness

- I better not leave my terminal unlocked because I know that those security guys are lurking around somewhere.

Helps identify weakness that may be leveraged by insider threat or accidental exposure.

Provides Senior Management a realistic view of their security posture

Great tool to advocate for more funding to mitigate flaws discovered

If I can break into it, so could someone else!

Why conduct a penetration test?

Prevent data breach

Test your security controls

Ensure system security

Get a baseline

Compliance



Steps of penetration test

Planning

Information gathering

- Reconnaissance
- Discovery
 - Port scanning

Vulnerability discovery

- Vulnerability scanning
- Taking control
 - Exploitation
 - Brute forcing
 - Social engineering
- Pivoting

Reporting

- Evidence collection
- Risk analysis
- Remediation



Some Considerations

Scope

Internal or external

In-house or outsourced

Selecting a pen-tester (white hat hacker)

White hat hacker vs Black hat hacker



How to prepare a penetration test?

A discussion with the client establishes the following:

The type of penetration test

- Physical access or just remote access?
- Is social engineering allowed?
- Covert or Overt?

Rules of Engagement

- What is off limits?
- Threat model (insider threat, ex-employee, outsider, etc.)?
- Specified targets?

Timeline

What to expect from the report

Penetration testing methodologies

WHITE BOX MODEL

Tester is told everything:

- The network topology
- The network technologies
- The company hierarchies

Tester is authorized to:

- Interview IT personnel and company employees
- Access the company physically

Makes tester's job easier...

BLACK BOX MODEL

Company staff does not know about the test

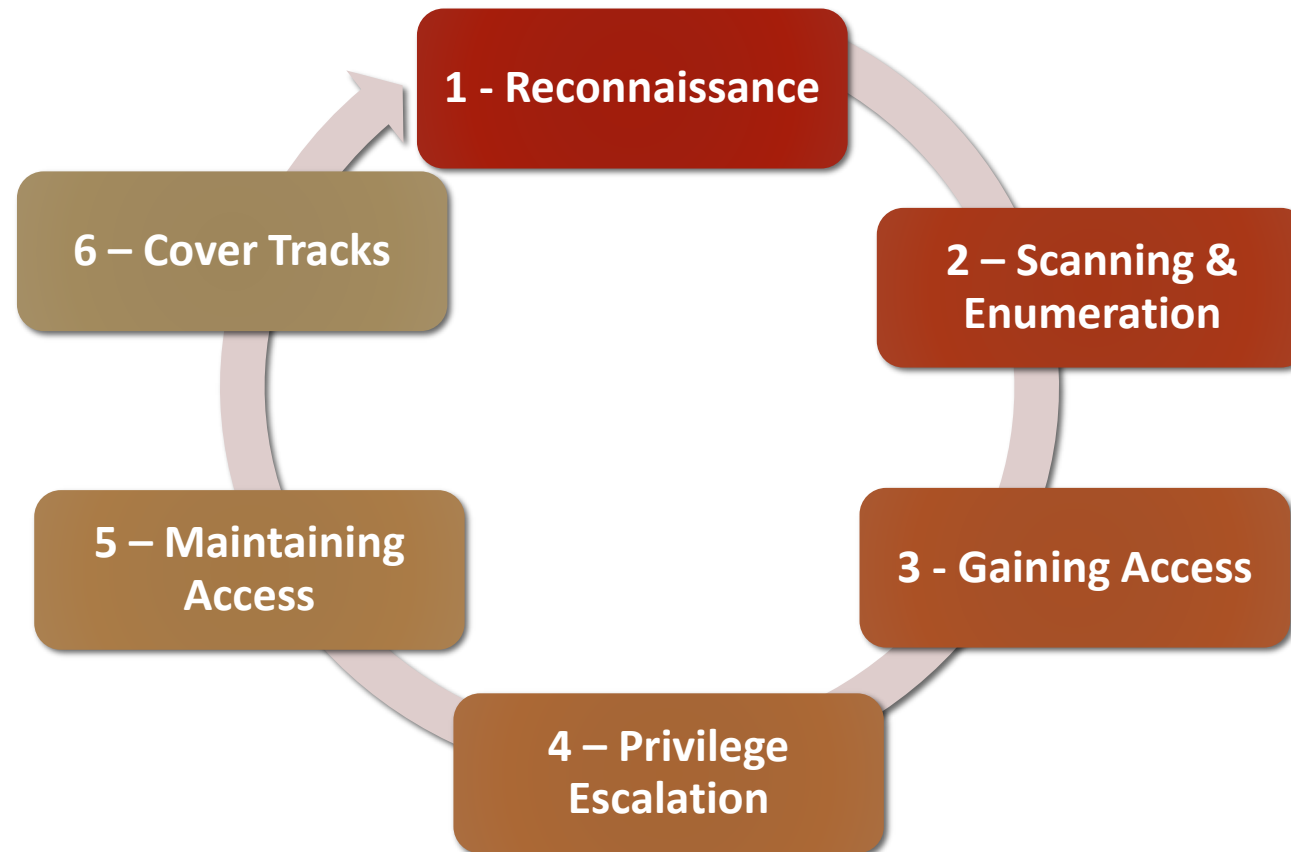
Tester is not given details about the network

Burden is on the tester to find these details

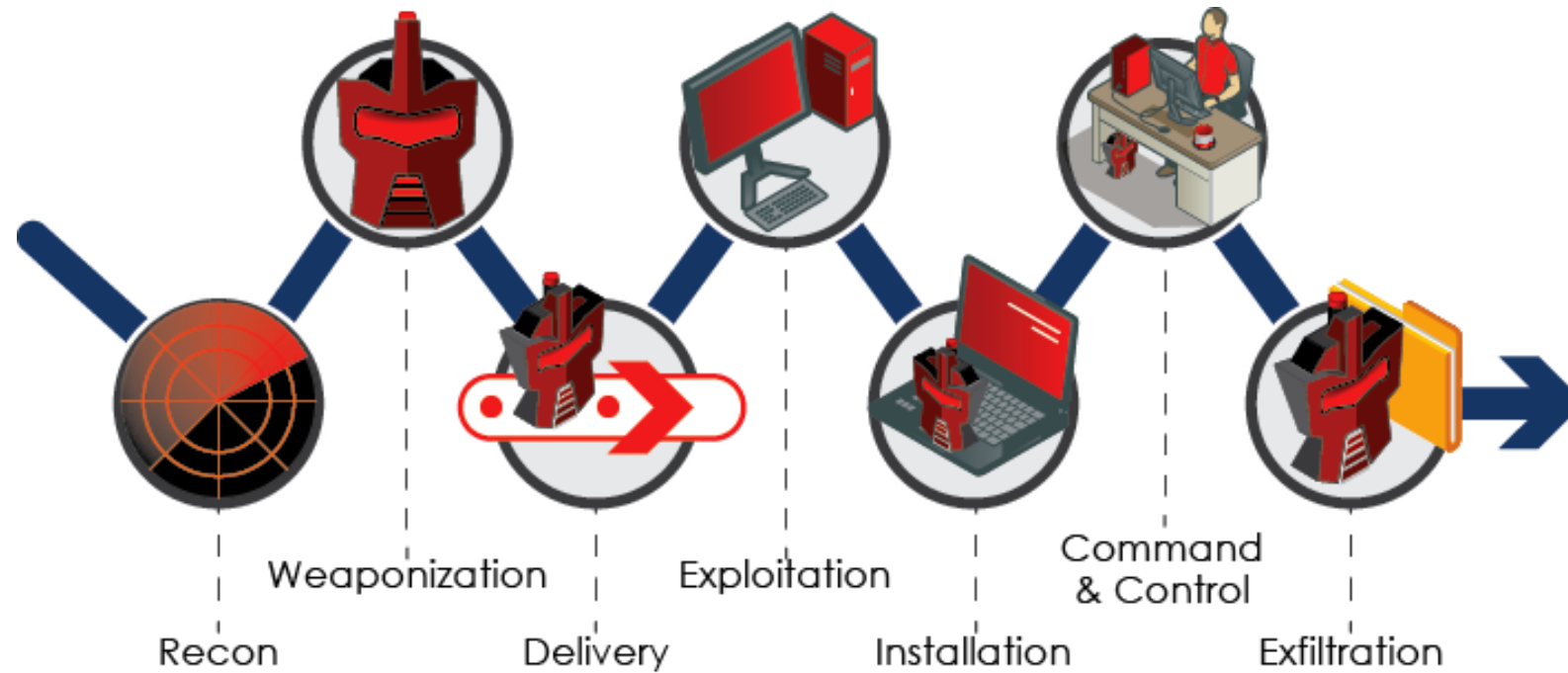
Tests if security personnel are able to detect an attack

Exactly like an external attacker...

Hacking phases



The Killchain Model: APT



The Killchain Model: APT

Reconnaissance. The attacker gathers information on the target before the actual attack starts. He can do it by looking for publicly available information on the Internet.

Weaponization. The attacker uses an exploit and creates a malicious payload to send to the victim. This step happens at the attacker side, without contact with the victim.

Delivery. The attacker sends the malicious payload to the victim by email or other means, which represents one of many intrusion methods the attacker can use.

Exploitation. The actual execution of the exploit, which is, again, relevant only when the attacker uses an exploit.

Installation. Installing malware on the infected computer is relevant only if the attacker used malware as part of the attack, and even when there is malware involved, the installation is a point in time within a much more elaborate attack process that takes months to operate.

Command and control. The attacker creates a command and control channel in order to continue to operate his internal assets remotely. This step is relatively generic and relevant throughout the attack, not only when malware is installed.

Exfiltration. The attacker performs the steps to achieve his actual goals inside the victim's network. This is the elaborate active attack process that takes months, and thousands of small steps, in order to achieve.