

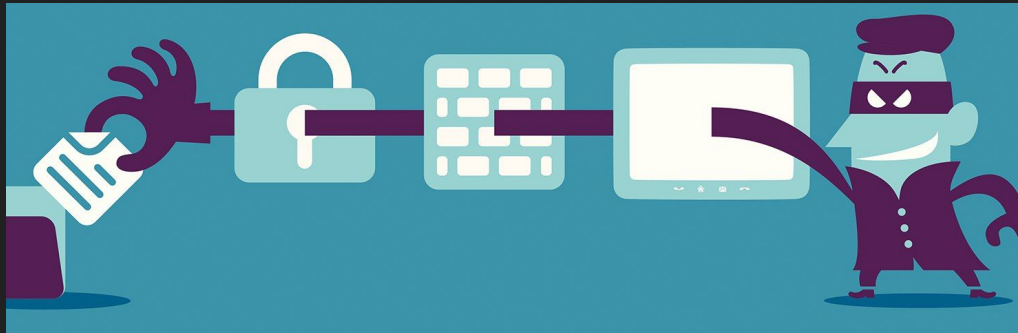







White Hat

Ethical Hacking
and Information Security

What is Hacking?

Exploiting a system's vulnerabilities and security controls to gain access to system resources and features outside of the creator's original purpose.



<p>Script Kiddie</p>		<ul style="list-style-type: none"> • Considered widely as “a class of wannabes” • Mostly rely on readymade applications and copies of software.
<p>Green Hat</p>		<ul style="list-style-type: none"> • Aspiring hackers with limited knowledge; • Use premade tools and applications, BUT try to understand what they are doing and learn.
<p>White Hat</p>		<ul style="list-style-type: none"> • THE GOOD (ethical) GUYS of the internet; • Hold down high paying jobs to thwart the actions of cybercriminals. • Act with purpose and within legal bounds and are paid to hunt for them.
<p>Black Hat</p>		<ul style="list-style-type: none"> • Cyber criminals • Often responsible for data breaches, security hacks, malware, virus distribution, • Use extensive knowledge of systems to gain illegal access and wreak havoc.
<p>Grey Hat</p>		<ul style="list-style-type: none"> • Not generally criminals, • BUT not particularly heartbroken or afraid if they need to hack a system or two, as long as the ends justify means to them.



What is Ethical Hacking?

- ❖ The use of hacking methods and tools to discover weaknesses for system security.
- ❖ Ethical hackers are contracted and deployed by the entity being hacked. They always have permission prior to the penetration test.

Parts of a Pen Test

1. Defining and documenting the scope of test.
2. Researching the entity.
3. THE HACK!
4. Documenting and reporting of ALL results.



The Hack - Breaking it Down

Reconnaissance Phase - Finding the target

Scanning Phase - Identifying systems, mapping out hardware

Gaining Access Phase - Entering via network, OS or application

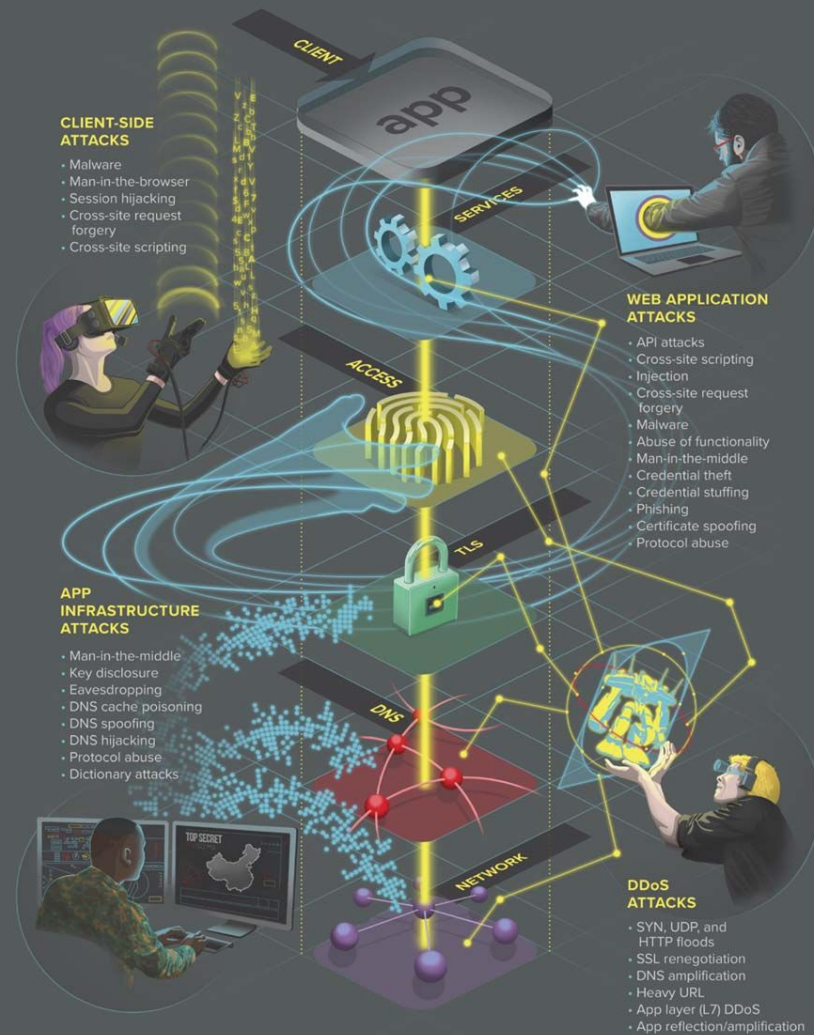
Maintain Access Phase - PWNing the system

Clearing Tracks Phase - Destroying any proof

Basic Ethical Hacker Techniques

- ❖ Password guessing and cracking:
- ❖ Session hijacking
- ❖ Session spoofing
- ❖ Network traffic sniffing
- ❖ Domain Name System (DNS) Poisoning
- ❖ Exploiting buffer overflow vulnerabilities
- ❖ SQL injection

The techniques do consist of qualities that are similar to others; lines are blurred, qualities will seem shared, and lists will not be all inclusive.



A Closer Look: Password Cracking Technique

- ❖ Three basic types of password cracking test tools:
 - **Dictionary:** file of words run against the accounts
 - **Hybrid:** similar to dictionary attack, but adds simple numbers or symbols
 - **Brute force:** tries every combination of characters until password is broken



Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.



Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.



Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.



Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.



Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Shoulder Surfing

Observing someone typing their password.



Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.



Blacklist the most common password choices



Monitor failed login attempts... train users to report suspicious activity



Prioritise administrator and remote user accounts



Don't store passwords in plain text format.



Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks



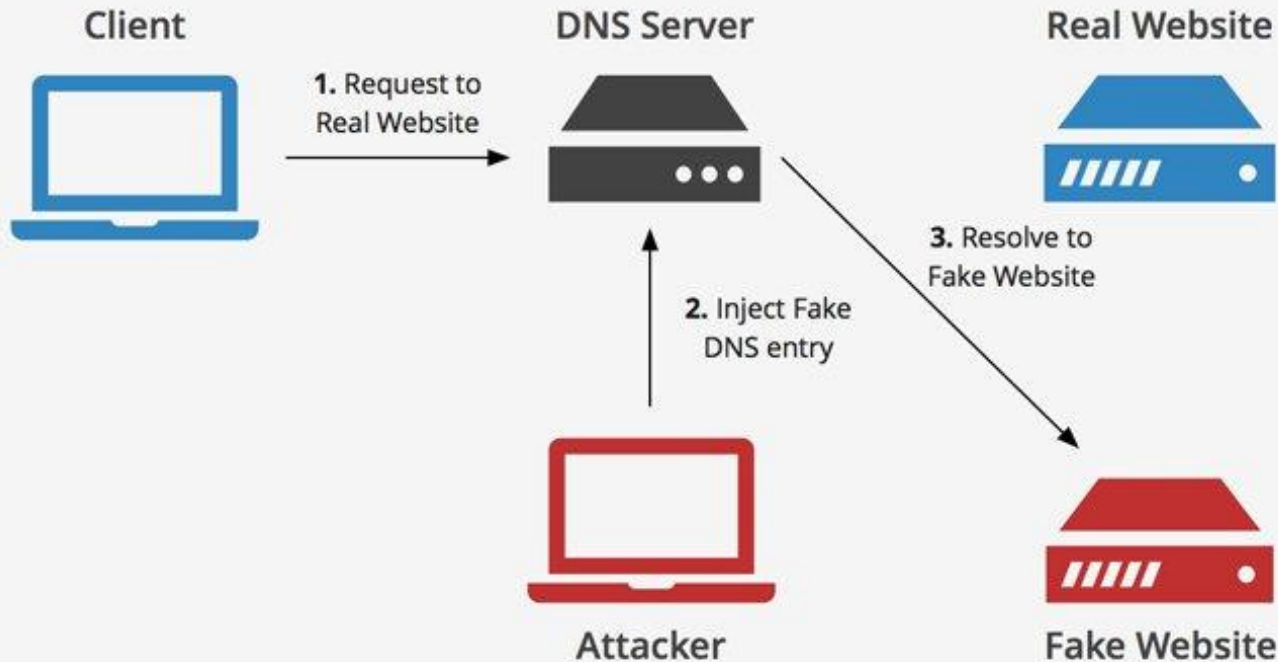
A Closer Look: Network Traffic Sniffing Technique

- ❖ The process of monitoring and capturing all data packets passing through a given network using sniffing tools.
 - Data packets are used by diagnostic admin for troubleshooting, BUT hackers use them too.
 - A packet sniffer is a program that can see all traffic over the network flowing back and forth.
- ❖ It is also considered a form of “phone tapping” or wiretapping.
- ❖ What could be sniffed?
 - Email traffic, passwords, web traffics, router config, chat sessions, DNS (domain name system) traffic
 - Basically, any data that is passed over the network in clear text is vulnerable to sniffing.
- ❖ Sniffers are ethically used to help investigate network problems, filter network traffic, and discover misuse, susceptibility, etc



Lawful Interception (LI) is the legally sanctioned official access to private communications, such as emails and phone calls. In generally, LI is the security process in which network operators give law enforcement access to the communications of individuals or organizations. Remember, these things are already being logged...

A Closer Look: Domain Name Server (DNS)



Ethical Hackers: Top 10 Tools



- ❖ Nmap ([Network Mapper](#)) - originally a simple scanning utility, now a full pentesting platform
- ❖ Metasploit - essentially a security framework
- ❖ Burp Suite - integrated platform for attacking web applications with functionalities like Spider, Proxy, and more.
- ❖ John the Ripper - popular offline password cracking pentest tool - dictionary attacks
- ❖ THC Hydra - similar to John the Ripper, but an online tool - dictionary & brute force
- ❖ OWASP Zed Attack Proxy (ZAP) - integrated pentest tool for find vulnerabilities in web apps
- ❖ Wireshark - network protocol analyzer tool allowing for live capture and analysis of packages
- ❖ Aircrack-ng - wireless hacking tool with effectiveness in password hacking
- ❖ Maltego - digital forensic tool used to deliver a cyber threat picture/graphical layout
- ❖ Cain and Abel - an ethical password recovery tool for Microsoft Operating systems
- ❖ Nikto Website Vulnerability Scanner - a web server scanner performs intense tests against servers for multiple items, such as dangerous files, outdated versions, etc.



- ❖ Social Engineering: The **'Secret Shoppers'**
 - Secret Shoppers pose as business clients
 - Third party contracted business
 - Internal shopper (auditor)
 - Contact service centers to make sure security protocol is followed.
- ❖ Secret Shoppers contact banks too:
 - Common Red Flag Examples of a Fraudster:
 - International Wires: Esp. China, Russia, Middle East
 - Recent changes to Personal Information
 - New bank account on file prior to withdraw request
 - New Phone number
 - New Email



The Need for Ethical Hacking

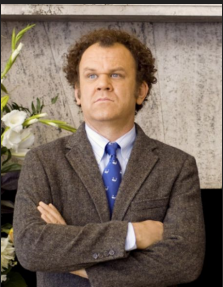
Social Engineering as The CEO

A Fictional Case Study,

Based On A Common Social Engineering 'Hack'



- The scam targets a business that regularly performs wire transfer payments. May be carried out by compromising legitimate business email account or spoofed accounts. Goal is to 'hack' or gain access to an CEO or another authority figure's email.
- Once the cybercriminal spoofs or gains access to a company email account and impersonates an executive, they fool an employee into executing unauthorized wire transfers.
- Unless the fraud is spotted within 24 hours, the chances of recovery are small.



Interested?

❖ Background/Education Requirements:

- A bachelor's/master's degree in compSci, information security, or math would provide a strong base.
- A military background is also highly recognized by hiring managers.
- Skills needed: communication, problem solving, secure tech and organizational skills, impeccable judgement, etc.
- Have the ability to think like a black hat, but function within the ethics and legality of the law.

❖ Certifications

- Recommended starting point is the Certified Ethical Hacker (CEH) certification from the EC-council.
 - Will need to have at least 2 years of work experience in the info security domain.
 - Apply for the exam
 - Take the exam (125 multiple choice questions for 4 hours) and “pass”.
 - There is no specific general passing score; it depends on the difficulty of that sessions questions.

❖ FYI: There are also physical aspects of the job

- See if you can tailgate through an access gate
- Get someone to hold a badge access door open so you bypass security



Professional Development for Hackers

DEFCON

- Annual hacking convention in Las Vegas, Nevada
- Activities:
 - “Voting Machine Hacking Village”
 - “Capture the Flag” (Jeopardy or Attack & Defense)
- Recruiters (like the NSA) come to find candidates

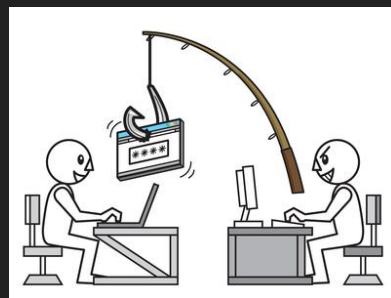
CERTIFIED ETHICAL HACKER (CEH)

- Demonstrates knowledge of “using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system.” - Wikipedia



DEMO 1 - *DO NOT TRY AT HOME*

Spear phishing or whaling:



- Domain squat on a similar domain, i.e., zipcodewilrnington.com
- Send a targeted email from this domain w/ link to a “spoofed” login portal
 - For example, Zip Code uses G Suite, so a Google login portal would be ideal
- Credentials entered would be POST’d to servlet
- Professional tools: [GoFish](#) (Go), [Kingfisher](#) (Python)

DEMO 2 - *TRY IT AT HOME!*

OWASP JUICESHOP <https://goo.gl/FMF3Ac>



- an intentionally insecure webapp for security trainings written entirely in JavaScript which encompasses common security flaws.

“Certified Ethical Hacker.” *Wikipedia*, Wikimedia Foundation, 24 Nov. 2018, en.wikipedia.org/wiki/Certified_Ethical_Hacker.

Grimes, Roger A. “What Is Ethical Hacking? Penetration Testing Basics and Requirements.” *CSO Online*, CSO, 24 Jan. 2018, www.csoonline.com/article/3238128/hacking/what-is-ethical-hacking-penetration-testing-basics.html.

“Hacker Tools: Sniffers.” *InfoSec Resources*, 21 May 2018, resources.infosecinstitute.com/hacker-tools-sniffers/#gref.

KnowBe4. “CEO Fraud.” *KnowBe4*, www.knowbe4.com/ceo-fraud.

Meredith, Dale. “Ethical Hacking: Understanding Ethical Hacking.” *Sign In - Pluralsight*, Pluralsight, 1 Aug. 2018, app.pluralsight.com/library/courses/ethical-hacking-understanding/table-of-contents.

“Password Cracking Tools and Techniques.” *SearchITChannel*, searchitchannel.techtarget.com/feature/Ethical-hacking-tools-and-techniques-Password-cracking.

Tangent, The Dark. “DEF CON Hacking Conference.” *DEF CON® 24 Hacking Conference - Speakers*, www.defcon.org/.

Tittel, Ed. “How To Become A White Hat Hacker.” *Business News Daily*, 24 Apr. 2018, www.businessnewsdaily.com/10713-white-hat-hacker-career.html.

tutorialspoint.com. “Ethical Hacking Sniffing.” *Www.tutorialspoint.com*, Tutorial Point,

Clickable Source Links List

- <https://searchitchannel.techtarget.com/feature/Ethical-hacking-tools-and-techniques-Password-cracking>
- https://en.wikipedia.org/wiki/Certified_Ethical_Hacker
- <https://www.defcon.org/>
- <https://www.csoononline.com/article/3238128/hacking/what-is-ethical-hacking-penetration-testing-basics.html>
- <https://app.pluralsight.com/library/courses/ethical-hacking-understanding/table-of-contents>
- <https://app.pluralsight.com/player?course=ethical-hacking-session-hijacking&author=troy-hunt&name=ethical-hacking-session-hijacking-m1&clip=0&mode=live>
- <https://www.knowbe4.com/ceo-fraud>
- https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm
- <https://resources.infosecinstitute.com/hacker-tools-sniffers/#gref>
- <https://resources.infosecinstitute.com/category/certifications-training/ceh/ethical-hacking-tools/>
- <https://www.businessnewsdaily.com/10713-white-hat-hacker-career.html>