

# Ethical Hacking Introduction

## Table of Contents

What Is "Ethical Hacking"?	2
Why Perform "Ethical Hacking"?	6
The Certified Ethical Hacker (CEH)	9
Information Security Reports	10
Internet Crime Complaint Center (IC3)	11
Data Breach Investigations Report (DBIR)	13
Types of Data Stolen	16
Effects of Hacking on Business	18
Notices	20

## What Is "Ethical Hacking"?

---

**Ethical Hacking** - The learning, developing, and use of tools and techniques to exploit vulnerabilities in systems or networks with the purpose of hardening and securing a system or network.

# H4CK3RZ

**CEH Definition** - To help organizations take preemptive measures against malicious attacks by attacking systems themselves, all the while staying within legal limits.



\*\*006 So if you had to define ethical hacking what would it be? Without looking at the slide up here, somebody or multiple people tell me, what would be your definition of an ethical hacker? If I came up to you and said I'm an ethical hacker what would you think I did during the day? Anyone want to offer up an answer? Sir?

Student: You've been hired by someone, you've been authorized by someone to find vulnerabilities in their system and try to get into the system and acquire information.

Chris Evans: That's a good definition. I heard two important things in there: "hired" and probably more importantly

"authorized". What else? Anybody have a different definition? Sir?

Student: You follow all the laws, eagerly accepted it.

Chris Evans: Okay you follow all the laws, by definition of being "ethical" right? You're guided by some type of legal structure or legal framework or at least some type of moral compass, okay? What else?

Student: If you develop a system or a network somehow exposing [inaudible] I would like to make sure it's hard [inaudible] maybe close possible doors and make sure it's secure enough to protect actual hackers.

Chris Evans: Okay, excellent answer. And so what you're getting at there is that you're looking at systems from the standpoint of attacking it so that we can turn around and fix it and defend that system.

And so with ethical hacking we've talked about you've been hired, you've been authorized to do this, you're doing this from the standpoint of fixing things. Contrast that to an unethical hacker. There is no such thing but pretty much any hacktivist hacker cybercrime guy out there fits into this bucket. What would be an unethical hacker? Anyone? Sir?

Student: Somebody who breaks into machines for profit.

Chris Evans: Okay hacking for fun and profit, yes. What else? Think of all the bad actors out there that you know of in the

cyber world. What do they do? What are they motivated by? Money is a big one. What else are they motivated by?

Student: Challenge.

Student: Ego.

Chris Evans: Yep those are big ones. What else?

Student: Destroying somebody's-

Chris Evans: Sabotage? Sabotage is a good one. There's one big one that I'm looking for.

Student: Fame just in the hacker world.

Student: Revenge.

Chris Evans: Yep, those of you who work in the in cyber threat world probably know quite a bit about that. Sir?

Student: Political statement.

Chris Evans: Political statement, the recent stuff with Anonymous is pretty huge about making a political statement, Occupy Wall Street.

Student: Because you can.

Chris Evans: Because you can, absolutely.

Chris Evans: Okay. Actually that's kind of what I was getting at so patriotism, the whole espionage route. I work for a major company and we have intellectual property that I want to safeguard and make sure that nobody else gets a hold

of. Laurie works at a competitor of mine and she doesn't want to spend the resources in developing a competing technology to me so why not just steal it? Pretty much everything we do nowadays is kept on a computer system somewhere, right? So you see that quite a bit with corporate espionage and certainly at the national level there's a whole lot of espionage going on there. Patriotism certainly, but more so it's acquiring information, resources, whatever else just because you can leverage the fact that somebody else has done it, why do I need to go out and do it myself? That is very clearly unethical hacking.

With ethical hacking you're looking at developing your own tools, using tools that are already out there to find vulnerabilities in systems to fix them and make your systems more hardened and more resistant so that when the unethical hacker comes along you don't fall victim to that.

The official definition of it is right here and that's "To help organizations take preemptive measures against malicious attacks by attacking systems themselves." Again, difference between ethical hacking and unethical hacking. Ethical hacking you're doing it from the standpoint of "I want to fix the system here before somebody comes along and takes advantage of it." Unethical hacking is "I don't care. This computer has something on it that I want and I'm going to get it."

## Why Perform “Ethical Hacking”?

---

### **Non-malicious tools can be used for malicious purposes.**

- Using psexec.exe to open a shell on a remote box, done by an administrator...perfectly harmless, done by a hacker with malicious intent, very harmful.

### **Malicious tools can be used by network administrators to harden their networks.**

- Using an attack framework, like Metasploit, to ensure a patch really fixes a known vulnerability.



\*\*007 So why would you perform ethical hacking? Well there are two different schools of thoughts to this. One is that there are non-malicious tools that can be used for malicious purpose. Take a look at for those of you that are in a system administrator role, you have a set of tools that you use during the day. Maybe it's various active directory tools if you're in a Windows environment. Maybe there are command line tools. Maybe they're GUI tools, whatever the case may be, but you've got a set of tools that you use during the day. And so the first school of thought is well, these tools are great for system administration but they can also be used for malicious purposes as well, right? So any tool that you have as a

system administrator makes a great tool for me or a great resource for me as a hacker. Because one, it's already installed on the systems, it's probably already configured because you as administrator use it. It's there so once I get into the system I can use that as a malicious entity.

The other school of thought here is that malicious tools can be used by network administrators to harden their systems and this is really the basic premise of ethical hacking. It's being able to use tools that are out there on your own networks to increase the security of it, to defend those networks and make sure they're secure. So if you think about it, logically it kind of makes sense. You know that there are bad guys out there doing stuff to your networks. You know that they're hacking in. You know that they're running certain tool sets. Why not take that tool set and apply it to your own network to see, one, how your network responds to it, how your own defenders respond to it; can they detect this stuff? Can they respond to it? Do they analyze it correctly?

What would be one down side of using these malicious tools? Let's say you go out to the Internet and grab super hacking tool 1.0 as a network administrator and you go "I'm going to secure my system." You download this tool, you run it on your network. What would be one potential downside to that?

Student: The tool is already a malicious tool maybe [inaudible] in their system. How do you trust that tool?

Chris Evans: How do you trust that tool? How do you know it's doing what you think it's doing, right? Okay excellent, why else? Any other thoughts on that? There really is a danger in just going out and grabbing tools off the Internet. There's a type of hacker out there known as a script kiddie and so if you're just going out to the Internet and downloading these malicious tools and running them on your network, what are you? You probably are a script kiddie if you had no idea what that tool is doing, that kind of impact it's creating on your network and what it's really doing behind the scenes. And so if you're going to go and take this approach of using these malicious tools to attack your own systems, I would urge you to actually take a look at that tool, run it in a virtual machine environment, run it in a closed network, whatever the case may be, but understand what that tool is doing and make sure you know what is going on behind the scenes before you actually fire it off on your network because there are plenty of tools out there who which will say that they do this. Well they also do a couple of things over here that you're not really aware of: opening up backdoors, exfiltrating information, a bunch of other stuff can happen there, so if you're going through this just be cognizant that there are things out there that don't always do what they say they do and do a little bit more.

## The Certified Ethical Hacker (CEH)

---

The purpose of the CEH credential is to

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures
- Inform the public that credentialed individuals meet or exceed the minimum standards
- Reinforce ethical hacking as a unique and self regulating profession



\*\*008 The purpose of CEH as a credential is really to establish minimum standards meaning the CEH is designed to give you an understanding of what an attacker does at a very rudimentary level, arm you with enough information so that you can go out and start learning to do this on your own and that's really what CEH was designed to do.



# Information Security Reports

\*\*009 We'll talk a little bit about information security reports. So in ethical hacking there's a lot of talk about vulnerabilities, about weaknesses and that sort of thing. So where would you actually go to find this type of information?

# Internet Crime Complaint Center (IC3)

Partnership between FBI and National White Collar Crime Center (NW3C): <http://www.ic3.gov>

Provides means to file Internet-related criminal complaints for deferral to appropriate agencies for investigation

Produces annual state and national Internet Crime Reports

### Complaint Characteristics

During 2010, the non-delivery of payment or merchandise was the most reported offense, followed by FBI-related scams and identity theft.

Table 3: Top 10 Crime Types

Type	Percent
1. Non-delivery Payment/Merchandise	14.4%
2. FBI-Related Scams	13.2%
3. Identity Theft	9.8%
4. Computer Crimes	9.1%
5. Miscellaneous Fraud	8.6%
6. Advance Fee Fraud	7.6%
7. Spam	6.9%
8. Auction Fraud	5.9%
9. Credit Card Fraud	5.3%
10. Overpayment Fraud	5.3%



\*\*010 There's an organization out there called the Internet Crime Complaint Center, IC3. This is kind of a, oh, I knocked over the mascot. Shame on me. So IC3 is kind of a partnership between FBI and the National White Collar Crime Center. And this is a venue that's kind of been established to provide a way for people to file complaints about things they've seen on the Internet or been taking advantage of. It's just kind of a clearing house for this.

Take a look at the types of crimes that this center is actually tracking. At the top of the list there is non-delivery of payment or merchandise meaning you ordered something off the Internet and it didn't arrive or they took your money and ran,

right? The next one on the list, FBI-related scams. Identify theft, computer crimes, miscellaneous fraud, What is this really telling you? When you look at the world of hacking, what do you think of? We already talked about espionage, sabotage, a little bit about financially motivated stuff. What are most of these in the top list? They're almost all financially motivated, right? Why would you go out and do identity theft? Because you're a great person and I want to be you? Nope. Because you have money and you have credit cards and you have other things that I want access to. The vast majority of hacking out there is not the breaking into national security systems. It's cybercrime, it's financially motivated.

# Data Breach Investigations Report (DBIR)

Annual study conducted by Verizon RISK Team with cooperation from US Secret Service

## 2011 Report Highlights:

- Over last 3 years, decrease in total records compromised  
— 361 million >> 144 million >> 4 million

Who is behind data breaches?	How do breaches occur?
<b>92%</b> stemmed from external agents (+22%)	<b>50%</b> utilized some form of hacking (+10%)
<b>17%</b> implicated insiders (-31%)	<b>49%</b> incorporated malware (+11%)
<b>&lt;1%</b> resulted from business partners (-10%)	<b>29%</b> involved physical attacks (+14%)
<b>9%</b> involved multiple parties (-18%)	<b>17%</b> resulted from privilege misuse (-31%)
	<b>11%</b> employed social tactics (-17%)

\*source: [http://www.secretservice.gov/Verizon\\_Data\\_Breach\\_2011.pdf](http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf)

\*\*011 The next one on the list here is the Data Breach Investigation reports. Every year the combination of Verizon and Secret Service publish a data breach report where they talk about the various things that they've seen during the year, the types of attacks, the various crimes that they've seen. And here if you look at the report that was published in 2011 "A decrease in the total number of records compromised" meaning the amount of information on you, your Social Security number, your credit card information, that amount of information that's being stolen is decreasing. Why do you think that is? I'll give you two choices. We're getting better at security, or the bad guys are getting better at their jobs so that nobody

is detecting it. How many people say we're getting better at security? How many people say the bad guys are getting better? Unfortunately I think it's more of the latter case there.

Look at this column here, who's behind these various data breaches? Ninety-two percent stemmed from external agents. And what's right here "Up 22 percent" so meaning compared to the last years, the report before this, the number of attacks has increased from external agents by 22 percent. Implicated insiders only 17 percent of attacks, down 30 percent, business partners and involved multiple parties. What is this trending towards? This is kind a key point. What is this showing? This is showing that most of the attacks are coming from the outside and even here implicated insiders is decreasing. Why is that? Because people are realizing that you know what? I don't have to be sitting at this computer to hack into it. I can sit in a hotel room halfway across the world and get into this system.

What are my chances of being arrested convicted if I'm sitting at a computer here hacking away and somebody walks in the door and goes "What are you doing here?" Maybe pretty good. Certainly better than if I was in a hotel room halfway across the world hacking into a system. The cost to the hacker for doing some type of sitting at the keyboard hacking inside your target is very, very high. The cost to the attacker sitting in a hotel room on the other side of the world is what? Miniscule, absolutely miniscule because it's very hard to catch them and actually prosecute them.

If you look over here the various types of breaches and how those are actually occurring some form of hacking as a general term, and we'll talk about the different types of that in a little bit. Half of them incorporate some type of malware. Twenty-nine percent involve physical attacks. How would you define a physical attack? What would a physical attack be? I'll give you a demonstration. A big hammer? Unfortunately he didn't scream. He was supposed to but he didn't. A physical attack is something where you're physically altering this system. Again, take a hammer to it, physically take it, steal it, walk out the door with it. Privilege misuse and social tactics, I think this is probably a little bit low because if you look at how as we go through the ethical hacking methodology you'll see that one of the easiest and probably cheapest from a risk standpoint to an attacker, cheapest methods to actually get into systems is with some type of social engineering attack.

## Types of Data Stolen

# Types of Data Stolen

	Number of incidents	Percent of incidents	Percent of records
Payment card numbers/data	593	78%	96%
Authentication credentials (usernames, pwds, etc)	339	45%	3%
Personal Information (Name, SS#, Addr, etc)	111	15%	1%
Sensitive organizational data (reports, plans, etc)	81	11%	0%
Bank account numbers/data	64	8%	<1%
Intellectual property	41	5%	<1%
System information (config, svcs, sw, etc)	41	5%	unknown
Classified information	20	3%	unknown
Medical records	4	1%	unknown
Unknown	7	1%	0%

\*source: [http://www.secretservice.gov/Verizon\\_Data\\_Breach\\_2011.pdf](http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf)



\*\*012 Types of data stolen, again, look at the top of the list. What do the top entries have in common? You have payment card, authentication credentials, personal information, bank account numbers, what does all this have in common?

Student: Money.

Student: Financial.

Chris Evans: Financial, right it's all financially motivated. If you look at the scope of hacking incidents that are out there that are reported, the vast majority of them are financially motivated. Now there's a whole category of attacks and things that go on out there that aren't

reported that aren't tracked at this in these types of reports and it's clearly the espionage level and so you won't see that up here. I think the other reason you won't see that up here is imagine I'm a large company. I get hacked into my intellectual property gets stolen do I tell anybody about that?

Student: Are you in a state where it's legally required?

Chris Evans: Am I in a state where it's legally required? Maybe, but if it was my intellectual property that was stolen not my personal information, there are very few laws actually governing that if any. Personal information yeah, you bet, if you're in California or Massachusetts yep, you get a nice letter in the mail. I've gotten many of those actually that say your personal information has been compromised. But if I have super widget 1.0 here and it's got a whole set of plans and design specifications, if that information gets stolen do I have to report that? Do I report that? Well it's going to influence my stock price. Can I keep it quiet? Can I just kind of shovel it under the bed and not tell anybody about it? Maybe, all that sorts of stuff happens but I think that's why you don't see more of the intellectual property listed in here.

## Effects of Hacking on Business

---

### Loss of competitive advantage

- Theft of Intellectual Property

### Loss of revenue

- DDoS attack against a major online store, like amazon.com

### Embarrassment

- Website defacement

### Negative reputation

- Customer Social Security Numbers or other PII stolen from a “trusted” company



\*\*013 The effects of hacking on business, this really goes to motivation for why you might want to be an ethical hacker and how you can actually support the various organizations that you might work for. Loss of competitive advantage: again, this is what people are going after. They're looking for to make a statement against you. Imagine a distributed denial of service against a major online retailer like Amazon. If it actually knocked the servers off line and Amazon has a very, very robust system so the idea of somebody being able to distribute a denial of service to them is pretty limited. But imagine a retailer like that who gets hit with a distributed denial of service attack where their servers that they process that they

take customer orders from and process all that are offline. How much money do you think they lose every minute those servers are down? Millions, probably. Amazon, certainly. So that's why they've spent millions of dollars on a very robust system. So loss of revenue is pretty big. Embarrassment, certainly with website defacements and negative reputation again as an ethical hacker if you have been hired or you've been chartered by your organization to actually go out and do this, these are the things that you want to look at preventing with your actions. Again, you're not just going out as an ethical hacker and saying yep, I'm going to scan the network. I'm going to do a pen test. We found all these things, we're going to fix it that's it we're done. You want to frame it from the standpoint of these types of things here because these are the things that make an impact on the business or on your organization. If you're with a government organization you might have a different set of goals, confidentiality of information, maybe integrity, maybe availability. We'll talk about those in a little bit.

## Notices

# Notices

---

Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.