Hacker Highschool

SECURITY AWARENESS FOR TEENS

LESSON 1
BEING A HACKER

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior highschool students, and highschool students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Pete Herzog, ISECOM

Marta Barceló, ISECOM

Chuck Truett, ISECOM

Kim Truett, ISECOM

Marco Ivaldi, ISECOM

Shaun Copplestone, ISECOM

Greg Playle, ISECOM

Jeff Cleveland, ISECOM

Simone Onofri, ISECOM

Tom Thomas, ISECOM

Dzen Hacks

For the Love of Hacking

Introduction by Pete Herzog

Whatever you may have heard about hackers, the truth is they do something really, really well: discover. Hackers are motivated, resourceful, and creative. They get deeply into how things work, to the point that they know how to take control of them and change them into something else. This lets them re-think even big ideas because they can really dig to the bottom of how things function. Furthermore, they aren't afraid to make the same mistake twice just out of a kind of scientific curiosity, to see if that mistake always has the same results. That's why hackers don't see failure as a mistake or a waste of time because every failure means something and something new to be learned. And these are all traits any society needs in order to make progress.

> Many people who have been called hackers, especially by the media, or who have gotten in trouble for “hacking” were not, in fact, hackers.

A hacker is a type of hands-on, experimenting scientist, although perhaps sometimes the term “mad scientist” fits better since unlike professional scientists, they dive right in following a feeling rather than a formal hypothesis. That's not necessarily a bad thing. Many interesting things have been designed or invented by people who didn't follow standard conventions of what was known or believed to be true at the time.

The mathematician, *Georg Cantor*, proposed new ideas about infinity and set theory that caused outrage amongst many fellow mathematicians to the point that one called his ideas a “grave disease” infecting mathematics.

Nikola Tesla is another person considered a “mad scientist” in his day, but he knew more about how electricity behaved than anyone else. He designed possibly the first brushless motor that ran on AC electricity but is mostly known for the Tesla effect and the Tesla coil.

Then there was *Ignaz Philipp Semmelweis* who figured out that doctors need to wash their hands between treating patients to keep diseases from spreading. He wondered if the diseases following him around between patients were his fault, so he decided to try washing hands between his patient visits and sure enough, the transmissions disappeared. His ideas went against both the scientific conventions of what was known at the time about germs (nothing) as well as the convenience of the doctors who felt it was too much hassle to keep washing their hands.

What you may think you know about hackers is that they can break into other computers and take over other people's accounts. They can read your email without you knowing. They can look through your web cam without your permission and can see you and hear you in the supposed privacy of your own home. That's not untrue.

Some hackers see network security as just another challenge, so they tinker with ways to trick or fool the system, but really what they're trying to do is out-think the network installers or designers. They discover as much about the network as they can, where it gets its instructions, the rules it uses, and how it interacts with operating systems, the other systems around it, the users who have access to it and the administrators who manage it. Then they use that to try different ways of getting what they want. This kind of hacking can be greatly beneficial to the world for understanding how to be safer and for building even better technology.

Unfortunately though, sometimes the hacking is done by criminals and what they want is illegal, invasive, and destructive. And those are usually the only hackers you read about in the news.

A hacker is not someone who posts to someone's account when they leave some social media page open or **shoulder-surfs** passwords and then logs into their account later. That's not hacking. A hacker also is not someone who downloads a **script kiddie** tool to break into someone's email. Those aren't hackers; those are just thieves and vandals.

> Hacking is research. Have you ever tried something again and again in different ways to get it to do what you wanted? Have you ever opened up a machine or a device to see how it works, research what the components are, and then make adjustments to see what now worked differently? That's hacking. You are hacking whenever you deeply examine how something really works in order to creatively manipulate it into doing what you want.

It just so happens that the way the Internet is designed and the huge number of different applications, systems, devices, and processes it has makes it the most common place to find hackers. You could say it was built by hackers so it's the best playground for hackers. But it's not the only place. You can find great hackers in almost every field and industry and they all have one thing in common: they spend time learning how things work, so they can make them work in a new way. They didn't look at something as the original designers did, but instead saw bigger or better potential for it and hacked it to be something new.

> Don't think you can just be a great hacker. Only by doing great hacks with great humility can you be great.

Hacking itself is not illegal. At least not any more than throwing a rock is illegal. It all comes down to intent. If you throw a rock and your intent is to injure someone, that's a crime. If your intent is not to hurt someone, but someone does get hurt, that may not be a crime, but you are responsible for your actions and will have to pay restitution. An ISECOM project called the **Hacker Profiling Project** found that the most damage from hacking comes from young, inexperienced hackers damaging other people's property by accident. That's like throwing rocks in the street just for fun but denting cars and smashing windows in the process. Maybe the damage is unintentional, but you can expect to be held responsible and pay for it. So do be careful when hacking around other people's property. Stick to hacking your own stuff.

It may be illegal to hack something you bought and own. There are hackers who have been punished for hacking their own devices and computers. There are hackers who hacked programs, music and movies they bought – and were prosecuted for it. In particular, you may not be allowed legally to hack software that you've purchased, even if it's just to check for yourself that it's secure enough to run on your own computer. This is because many of the things that you purchase may come with a contract or **End User License Agreement (EULA)** that says you can't. And you agree to it when you open or install the product, even if you can't read it or even know about it until after you've opened or installed the product. Keep this in mind when you are practicing your hacking skills on the things you purchased in the privacy of your own home.

-Pete Herzog

Why Be a Hacker?

Consider how scientists mapped the human genome: they used a method developed for decoding passwords. Passwords are usually stored in an encrypted form, so they're hard to steal. Hierarchical shotgun **brute-forcing** is a method of decrypting passwords by **cracking** their encrypted form. It breaks down the encrypted **hash** of the password, solves a few characters at a time, then stitches it all back together. Genome researchers adapted the same technique to map the entire 3.3 billion base pairs of the human genome.

Hacking has shown up in kitchens as chefs use liquid nitrogen as the cooling agent to make perfect ice cream or when they hack food to make tomato fries with potato sauce as the ketchup or just need to make something they don't have the right equipment for....

Chemists have been hacking elements and compounds for centuries. By nature molecules are finicky when it comes to how they behave in different environments (hot weather, cold weather, on mountains, or deep beneath the ocean), so chemists need to deeply understand the properties of the chemicals they have, so they can try to hack together the one they need. Nowhere is this more evident than in the invention of new pharmaceuticals, where hundreds of plants in a region are studied for their chemical properties from roots to fruits, and extracted and combined with others to make new medicines. Then they try again and again, sometimes for years, to get the combinations right and make it do what they want it to do.

Hacking is used in business to understand a market or the buying behavior of certain types of consumers. They research deeply into the forces that drive the area of business they're concerned with, and then they try to change or influence it to make it do what they want. Sometimes they're hacking the product, and sometimes they're hacking you (with advertising and **priming**, something you'll work with in the Social Engineering lesson).

Hacking has also become an increasingly critical part of warfare. Highly skilled soldiers are resourceful and creative in accomplishing their goals, which is exactly what hackers are. Code breakers, intelligence analysts and field officers use what are basically hacking skills to figure out what the enemy has, what they are doing, and how to take advantage of any weaknesses in their equipment. As more nations rely on computers and networks, the use of hacking in cyber attacks and defense has become a valuable part of a nation's armed forces and intelligence operations. National and international security agencies are even going to hacker conventions to recruit hackers!

The real reason to be a hacker is because it's really powerful. You can do some very cool things when you have strong hacking skills. Any deep knowledge gives you great power. If you know how something works to the point that you can take control of it, you have serious power in your hands. Most of all, you have the power to protect yourself and those you care about.

More and more of people's lives are online as relationships form, people find jobs, and money is made on the Internet. Information can be valuable – or threatening – and hackers can protect themselves better than anyone else. They can research what's happening to their data. They can make sure to reveal only what they want and just generally keep themselves safer and more private. That's a huge competitive advantage in school, at work, and in life, because the smallest negative perception will eventually be used against you. Count on it.

Hack everything but harm none.

Feed Your Head: Handles

What's a handle all about?

From the earliest days, hackers had handles. A handle is a made up name that a hacker goes by. This was mostly for fun because hackers in the early days were mostly kids. But later, this game of "playing someone else" became a tool that hackers could use to protect themselves by allowing them to be anonymous.

Early on, hackers chose names like "Erik Bloodaxe," "Mentor" and "Captain Crunch." Some hackers played on the spelling of words like Phiber Optik. Those are the names of some of the most notable, and each is now known publicly.

But hacker handles were meant to be like a super hero's secret identity. No one, or only close trusted friends should know the handle you use online. Why the need for this secrecy? Because sometimes, people don't understand how hackers help, and who we are.

For example, in the past many students who happened to be hackers discovered vulnerabilities in the very networks that they used everyday at school. Wanting to be helpful they reported these findings to school administration. Sometimes the administration was grateful for the information, and maybe even for help with fixing the flaw. But there are several cases when the student was expelled, or even prosecuted by the school system. That reaction comes from ignorance, but it's something that we have to understand and deal with.

Handles also promote free speech. As hackers, we need to say what's true to a world that sometimes doesn't want to hear it. It's a sad fact that some people that hold positions of authority may try to put pressure on a person to bend the truth or hide it when it doesn't agree with their personal views.

The utility of a hacker handle is that it allows us to be ourselves, without the worry of retribution from a well-meaning, but misunderstanding society.

So how does one get started with choosing a handle and establishing an online identity? Well, first things first. Choose a handle that means something to you, and try to make it unique. For example, "Batman" is not very unique, and means something to lots of people. But if you like Windows batch scripts, then BAT.mn is a step closer.

Many handles incorporate parts of **leet speak**. An example is the name used by the group **l0pht**. They chose that name for their group because they met in a rented loft. So you could decide to incorporate that into your chosen handle. If you've become pretty good at playing with Linux's iptables (a host based firewall) you might choose "fyr3w@ll". Just remember that whatever you use, you'll have to type it over and over, so don't go too overboard.

Once you have your handle all picked out, it's time to start establishing your online identity. The first step is the easiest. Go to one of the online providers of free email accounts and see if you can create an account with your new handle. You may find that someone else is using it already. If you do, you can tweak it to be different, change the handle altogether, or simply try the same handle with a different email service.

Once you have your email account established, you need to think about the forums, IRC channels and mailing lists that you want to subscribe to. Forums are a good way for you to establish your new handle. When you are new and inexperienced, you can get help from more seasoned hackers by posting questions to a forum. As you get more experience yourself, you can help others by answering posts that you have experience with. A word of caution here: always research thoroughly before posting questions. If you ask a question that has an obvious answer, you may get terse responses. Always try to be gracious if someone is rude. No one likes a **flame war**.

You can now hang out in IRC, or sign in to instant messaging clients with your new handle.

You can also start a blog, or web page, listing your new handle as the author/administrator. But remember that this will mean a commitment on your part to keep the content updated; so think hard before you commit to something that could be time consuming.

Having established your online secret identity, or handle, you should enjoy keeping it a secret. Don't ever mention yourself, or anyone that you know in your posts, comments or messages. It's easy to keep things anonymous in most cases. If you do accidentally discover that misconfigured webpage, server or computer, then you can send an email from your handle's account, and not worry about the fact that the person that owns it is your principal, club leader, or dad.

You may find, as many hackers do, that as you get older and respected in computer security circles, that you don't need your handle anymore. That you can use your real name and be taken seriously. If you work hard, become proficient and well regarded then you don't need to hide behind anonymity to be taken seriously any longer. And that day can be just as liberating as it was the day that you chose your handle.

-Dzen Hacks

Exercise

1.1 You may or may not choose to use a hacker handle, but you should think about it. As Dzen notes above, you may have a legitimate reason to maintain an alternate identity. So what would your handle be?

How about something dark and mysterious: Phantom Blade or Lightning Fury or Dark Summoner? Can you really live up to this persona? Do you even want to?

Maybe something light and non-threatening? Sk8ter? PonyGirl? Would you be worried about being taken seriously?

Okay, maybe a friendly name like FluffyBunny? Unfortunately, you might be giving the wrong impression about your interests.

The ideal handle is one that never gives you away, but says something about your interests and personality.

Choose a handle for yourself.

How to Hack

Telling you how to hack is like explaining to you how to do a backward flip on a balance beam: no matter how detailed the explanation is you won't be able to do it on your own the first time. You need to develop the skills, feeling, and intuition through practice or else you'll fall flat on your face. But there are some things we can tell you to help you along and encourage you to keep practicing.

First, you should know some little secrets about how hacking actually works. We're going to take these from the **OSSTMM** (www.osstmm.org). Hackers sound it out and pronounce it “aw-stem.” The OSSTMM is the **Open Source Security Testing Methodology Manual**, and while it may read like DVD player setup instructions, it's the main document that many hacking professionals use to plan and execute their attacks and defenses. Deep in that manual are some real gems that will open your eyes.

Two Ways to Get What You Want

For example, you should know that there are really only two ways to take anything: you take it or you have someone else take it and give it to you. That means all the taking in the world requires **interactions** between the person and the thing. Obvious, right? But think about it. That means that all protection mechanisms have to try to stop someone from interacting with the thing they are protecting. Unless you lock everything in a huge safe, you can't stop all interaction. Stores need to put stuff on shelves that shoppers can touch. Businesses need to send information through email clients that attach to mail servers and send messages to other mail servers.

All of these are interactions. Some of these interactions are between people and things that are familiar with each other, so we call those interactions **Trusts**. When the interactions happen between unknown people or systems we call these interactions **Accesses**. You can either use an access to take what you want yourself, or you can trick someone who has a trust with the target to take what you want for you and give it to you. If you think about that for a moment, it means that security means protecting something from both those it doesn't know and those it knows and trusts.

Exercises

1.2 What kind of interaction is using a search engine? Think carefully: is anyone giving Access? Is anyone giving Trust?

1.3 Give a simple example of using Access and Trust to take a bicycle locked to a bike rack.

1.4 Give a simple example of how you can use Access and Trust to log into another person's web-mail account.

Feed Your Head: Espionage

When hacking is used against a foreign government to commit criminal acts of breaking and entering, trespassing, theft, and destruction to get the edge in political or military information it's called **espionage**. But when the hacking is done from a foreign business against another business in a different country to get an edge in business, it's called **economic espionage**.

When hacking is used to get private and personal information on individual people to embarrass them publicly it's called **DoXing**. If public information is dug out to target a person or company for an attack, but no criminal acts are made to get the information, it's referred to as **document grinding** or **OSInt (Open Source Intelligence)**.

When hacking is used to understand a company network, systems, applications, and devices as the target of an attack without actually intruding or trespassing into the systems it's known as **network surveying**.

When hacking is used to deeply understand a competitor without breaking any laws (although what they do may be considered just plain mean or rude) it's called **competitive intelligence**.

You're probably dying to hear now what kind of mean and rude things they do that are still legal. Consider the example of inflicting stress and worry on someone to get information from them. As long as you don't kill them, telling them lies is still legal (although there are laws against causing panic in public places like yelling "Fire!" in a crowded movie theater when there is none).

Say the hacker wants to know where a company is planning to set up their new factory. They use document grinding to find out which people are in the position to make that decision. Then the hacker calls their offices to find out which cities they've been to and perhaps which factories they've visited. But of course that's private company information and nobody is just going to tell them that without raising red flags. So the hacker needs to trick the information from them. It's not hard to imagine the process.

> Hacker: Hi, I'm Dr. Jones, and I'm calling from the school about your daughter Nancy.
>
> Target: Oh really? What has she done now?
>
> Hacker: Well, she's got a persistent nosebleed we can't get to stop. I'd like to ask you about any chemicals she's been exposed to, manufacturing chemicals and such. These symptoms are rare except in people exposed to these chemicals. Can you tell me anything?
>
> Target: (spills their guts)

This is not really illegal in most places but it causes unneeded stress. Not to mention it's just mean to make a parent worry like that.

Hacking to Take Over Your World

Hacking isn't just about interactions. You know that. Some people say politics is about interactions. Maybe. But you probably thought hacking is about breaking security. Sometimes it is. What it's really about is taking control of something or changing it as well. Understanding interactions and what they mean in the real world, using the basic terms we've discussed, is useful when you're trying to infiltrate, discover, or even invent. Why would you do this? To have the freedom to make something you own do what you want. And to keep others from changing something you own in the name of what some people might call security (but we're not those people).

Sometimes you buy something and the company you bought it from will attempt to forcefully or sneakily make sure you can't customize it or change it beyond their rules. And you can agree to that, as long as you accept the fact that if you break it then you can't expect them to fix it or replace it. So hacking something you own does more than make it yours, it makes it irrevocably and undeniably yours. As scary as that may sound to some, it certainly has its advantages. Especially if you want to keep others out of your stuff.

For many, many people (we could put many more "manys" here to get the point across that we really mean "way way too many"), security is about putting a product in place, whether that's a lock or an alarm or a firewall or anything that theoretically keeps them secure. But sometimes those products don't work as well they should, or come with their own problems that just increase your **Attack Surface**, when a security product should be shrinking it. (The Attack Surface is all the ways, all the interactions, that allow for something or someone to be attacked.) And good luck getting that product improved in a mass-marketing, pay-as-you-go, crowd-sourcing, "you bought it as-is and that's what you have to live with" kind of world. That's why you hack your security. You need to analyze the product and figure out where it fails and how to change it so it works better. Then you might have to hack it some more to keep that company you bought it from, from changing it back to the default!

So when you think of hacking in terms of breaking security, remember that's just one area that hacking is useful for, because without being able to do that, you may have to give up some freedom or some privacy that you don't want to give up. (And yes we get it that you may not care right now about certain things you do or say or post, but the Internet has a long memory and it's getting better and better at helping others recall those memories of you. What goes on the net stays on the net. So consider this for the future you even if the you of today doesn't care.)

Now that you get the idea about interactions, let's get into them into more detail. You know the basic interactions as Access and Trust but have you heard of **Visibility**? That's the third type of interaction. It's just as powerful as the other two. In police language, it's simplified as *opportunity* but in hacking it's more about knowing if there is something to interact with or not. This interaction brings along a whole lot of new security techniques like deception, illusion, and camouflage, as well as all-new hacking techniques for avoiding and getting around security measures like deception, illusion, and camouflage!

When famous bank robber Jesse James was asked why he robbed banks, he said it's because that's where the money is. What he meant is that through Visibility he knew that the banks had money where other things he could rob might not. Banks have Visibility: people know what assets they hold. But not everything has Visibility. As a matter of fact Privacy is the opposite of Visibility and it's a powerful way to avoid being a target. Whether on dangerous streets, in the jungle, or on the Internet, keeping a low **Exposure** and avoiding Visibility is a way to keep from getting attacked in the first place.

Exercises

1.5 The Internet is so popular for creating myths and perpetuating false stories that it's hard to know what's real information and what is just a hoax. So if you want to learn to be a good hacker, get in the habit of checking your facts and learning the truth about things. That's why you're going to search and find out if Jesse James really did say that. And don't go easy on the answer by just going to the first web page you find, dig a little.

Now that you're getting used to looking things up, find the truth about these common things:

1.6 In the Inuit language where the word igloo comes from, what does it really mean? What kind of interactions did you use now to find out?

1.7 Many parents are quick to point out that sugar makes little kids hyper-active but does it really? What interactions are really occurring in their little bellies when children eat a lot of candy or sugary foods that make them act silly and hyper?

1.8 You might have heard that sugar causes cavities (caries) in your teeth but what is the real interaction that takes place – what really causes it? Is it sugar or not? Bonus points if you can say what brushing is as an interaction to fight the real cause and find the name of at least one of the chemicals that addresses the root of the problem (*hint: fluoride is wrong*).

Game On: A Hacker's First Toy

It was a cool afternoon at Jace's grandparents' apartment. Rain slammed down onto the outside world but didn't bother anyone in the building. The ten-year-old always enjoyed spending time with her grandfather because he enjoyed spending time with her. Her mother had woven her fine dark hair into a singe ponytail with a pink bow at the end. Three hours into playing and the pink bow was sideways and barely holding on to a few strands of hair. Jace was busy finding things to play with around the small home when she came across one of her favorite toys.

This particular toy was a small handmade box slimmer than a shoe box made of painted wood. There was a crank handle on one end. On the top of the box there was a small wooden wall with a tiny hole, a sleeping cat and a sleeping wooden old lady sitting in a chair. When Jace turned the box handle a mouse appeared from a hole in the wall and moved towards the sleeping cat. Once the mouse arrived at the cat, the cat leaped into the air and landed on top the sleeping ladies head. The surprised wooden lady would open her eyes and kick out her legs as the mouse watched in amusement.

Jace would wind the handle backwards to reset the automata machine and as soon as the mouse was hidden back in the wall, turn the handle forward to create the whole comical scene again. The ten-year-old would usually do this a few times before getting bored and turn her attention to something else. However, this time Grandpa was watching Jace and paying close attention to her expression. Jace didn't seem satisfied with just watching the mouse spook the cat and watching the cat land on the little woman's head. *She wonders how it works,* he thought, and decided to give her a surprise.

Crouching next to Jace in his gray work pants, he pushed his glasses back. He said, "I see you like the mouse causing all the trouble here. It is because the mouse is the smallest of the creatures in the cast or because the mouse is sneaky enough to surprise the cat and the woman in the chair?"

Jace didn't look behind her because she knew the smell of her grandfather and he always asked questions like this. His closeness to her made her feel comfortable but she didn't know the answer to his question. She had her own question but didn't know what that question was or how to ask it. She continued to turn the handle in both directions to see how each piece was moving. She answered into the air, "I don't understand how all the parts move. I like this but I wish I could see what's happening inside, what makes everything work."

Grandpa clapped his hands in delight. This was the moment he had been waiting years for, the moment Jace pushed her curiosity into his realm. Without getting up, Grandpa pivoted around on the orange carpet to sit next to the child. He gently pulled the toy away from her small hands and asked, "What if you can't open the box to look inside? What will you do?"

Jace studied the wooded container and simply said, "I'll break it open, then."

Grandpa's eyebrows knitted and he stared at Jace, who went wide-eyed. "This toy doesn't belong to you. You can play with it but you can't just go around breaking things that don't belong to you. If you want to see how it works, you need to find another way to do it. Criminals break things on purpose. You, my dear, are not a criminal. You are curious about things so I'm going to show you how to be a hacker."

Jace knew what a criminal was but had never heard of a hacker before. She squared her shoulders and sat up straight since this was turning into one of Grandpa's teaching talks. These were always fun. She asked her grandfather, "What's a hacker?"

"A hacker is someone who wants to learn how machines work. They read about them, build them, play with them. Hacking … at least when I was growing up, hacking didn't mean anything illegal. There are people who call themselves hackers but they're really criminals because they steal from other people, destroy things that don't belong to them

and hurt other people. Real hackers don't."

Child eyes looking into Grandpa's, Jace said, "Like when I said I would break the box open, that's something a bad person would do." She nodded: no remorse for her previous statement, just taking in the difference between one type of action versus another. The gray haired gentleman moved the box in his hands until he felt a spot on the bottom of the toy. Using his thumbnail, he carefully slide the side panel upwards to reveal in the inside of the box. Turning the box over, he did the same thing to open the other side panel.

The ten-year-old stared into the inner workings of this machine. Grandpa smiled, he watching her tilting the box and looking in from every angle. Inside were wooden gears, cams, a worm drive and small fishing rod weights: no longer a toy but a spectacular invention of moving parts. It reminded Jace of Grandpa's old pocket watch, with all the delicate gears and springs you could see in the back.

Grandpa said, "Go on, touch it. Move the pieces to see what happens. Watch how each piece makes other parts move. Check out the cat and mouse. What makes them move?"

Jace was baffled by the puzzle of motion in her hands. She reached into the exposed box and touched the pin wheel. A pin fell off the wheel and landed somewhere inside the box. When Jace tried to turn the crank, the mouse moved but the cat didn't. She looked up at Grandpa, stricken: the toy was broken!

Grandpa looked at Jace and softly said, "No, no, no. It isn't broken. We just have to put the pin back on the wheel. Well, we first have to find the pin. Shake the box until you hear something loose rattle around."

The child gently jiggled the box, then titled it up and down until the pin fell on to the carpet in front of her. Grandpa continued, "See, if we do accidentally break something it is our duty as hackers to fix it. If we come across something that's already broken, we either let the owner know it's broken or we fix it and tell the owner how we fixed it. We have to be responsible citizens, as hackers and as good people."

Jace handed the pin to her grandfather who handed the pin right back to Jace. He said, "You broke it, you fix it. I'll show you how."

He picked up the machine and took it over to the kitchen table where the light was better. Jace followed him and pulled up a chair alongside her mentor. Grandpa pulled a pencil out of his breast pocket and laid the box on its side so they could see the insides.

"See the crank handle on the outside of the box," he began. "When you turn that handle in one direction the mouse comes out of the wall and moves towards the cat. The mouse is moved because below the box surface, the mouse sits on a hidden track that is kind of like a corkscrew. The handle you turn causes the corkscrew track, what is called a worm drive, to rotate the mouse forward and also turn a pin wheel at the end of the track. The pin wheel has four pins on it."

Grandpa pointed his pencil at the pinwheel that was missing one pin. Jace opened up her small hand to reveal the lone pin. He continued, "You turn the crank four times and each time the mouse moves forward and the pin wheel makes one turn of a pin. Once the pinwheel moves four rotations, there is a cam connected to the fourth pin. It's called a drop cam even though it's shaped like an egg or a pear. The fourth rotation causes the drop cam to move to its highest point, which is connected to the cat."

Jace was looking at each mechanism but wasn't sure she understood how they worked together. Her grandfather moved his pencil to the cat, which rested on a wire hook. "See, when the drop cam hits its highest point on the fourth rotation, the wire is released and the cat jumps into the air on a curved path. The cat lands on the little woman's head. Now, if you look closely, you'll see the sitting lady has two buttons on top of her head. When the cat lands on her head, the cat pushed down on the two buttons in her hair. One button cause the woman's eyes to open and the other button causes her legs to pop forward in surprise."

Grandpa started the box at the first stage to show how a single turn on the crank made the worm drive push the mouse towards the cat and also move the pin wheel one rotation. This one rotation caused the drop cam to turn a quarter of a rotation. A second turn of the crank caused the mouse to move closer to the cat and the pin wheel rotated one more time, which made the drop cam complete a half rotation. The third crank turn did the same thing as the previous two turns. It wasn't until the forth crank turn that the mouse reached the cat, which turned the pin wheel to the fourth position. This also cause the drop cam to move to its highest point and released the cat. The cat flew on the wire and landed on the little woman's head as she sat sleeping in her chair.

The cat landed on the woman's head, the buttons pushed, that opened her eyes and made her legs swing out in surprise. Turning the crank in the opposite direction reset all the movements. Jace watched intently as she turned the handle slowly in one direction and then the other direction. Grandpa rested back in his kitchen chair and watched as Jace's mind absorbed all this mechanical movement information.

With her teacher looking on, Jace removed a pin or a part to see how that changed the toy's mechanics. Each change either had disastrous results or no effect at all. Several hours into the toy tinkering Jace began to ask a series of questions.

“Why not use a magnet instead?”

“How come the cat hangs on a wire when a spring would work better?”

“What happens if I turn the crank five or six times?”

“Why is a worm drive thing here, when you could use a curved track instead?”

“Does this work upside down?”

Grandpa interrupted Jace by raising his index finger to his lips. He looked with wonder in his eyes and repeated, “Why is a worm drive used when a curved track could be used instead? Is that what you just said?”

Jace nodded as she explored the pinwheel closer. Grandpa grabbed a piece of paper and started to draw on it. When he was done drawing a few drafts he slid the paper over to his granddaughter and asked, “Is that what you mean by a curved track?”

Jace took a quick look and said, “Yeah but you need to add a small piece to the mouse to keep it on the track. It would be smoother that way and easier to build.”

Grandpa's mouth worked but he said nothing.

Jace added, “Plus you can get rid of the pin wheel by cutting a slot at the end of the track. One less thing to go wrong. You won't need to turn the crank four times, either. When the mouse gets to the end of the track, the slot will trigger the wire to release. You can get rid of the drop cam too. Less parts to build. And why have two buttons on the top of the woman's head. Ya only need one to open her eyes and make her legs pop out.”

Grandpa's pencil hit paper and scribbled fast as he thought, *I just got schooled.*

Game Over

The Four Point Process

When you take the three types of interactions together, you have **Porosity**, the basis of an Attack Surface. And like the word implies, it's the pores or "holes" in any defenses you have to have in order for any necessary interactions to take place (as well as any unknown or unnecessary interactions taking place). For instance, a store still needs to put products on the shelves so people can touch them, put them in a cart and buy them. These are the interactions they need to sell things. But they might not be aware of the employees who are sneaking stuff out of the loading dock, which is an interaction that they don't want.

Porosity is something you need to know about to protect yourself or attack some target. But it's not enough to analyze something to hack it. To do that you need to know something deeper about the three types of interactions you just learned. This is another little secret from the OSSTMM and it's called the **Four Point Process (FPP)**. It outlines four ways these interactions are used to analyze something as deeply as possible, and by analyze we mean to mess with it so we can watch it and see what happens.

The Echo Process

We grow up discovering things and learning things by interacting with them directly. Little kids poke the dried-up squirrel with a stick to see if it's dead. This is called the **echo process**. It's the most basic and immature form of analysis. It's like yelling into a cave and listening for the response. The echo process requires throwing different types of Access interactions at a target and then monitoring its reactions to figure out what ways you can interact with it. The echo process is a cause-and-effect type of verification.

This is an odd way to test something, because although it makes for a very fast test, it also isn't very accurate. For instance, when using the echo process in testing security, a target that does not respond is considered secure. That's the same as not having Visibility. But we also know that just because something is non-responsive to a particular type of interaction that doesn't mean it's "secure." If this were true then opossums would never get killed by other animals when they played dead and everyone would be safe from bear attacks just by passing out in fear. But it's just not true. Avoiding Visibility might help you survive some types of interactions but certainly not all.

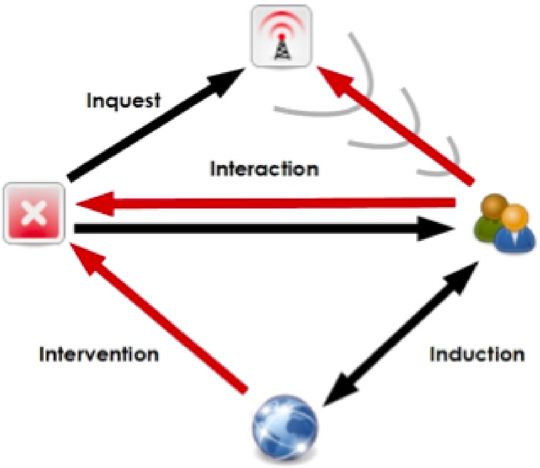

Figure 1.1: The Four Point Process

Unfortunately, the majority of ways people investigate things in their everyday life is through the echo process alone. There is so much information lost in this kind of one-dimensional analysis that we should be thankful the health care industry has evolved past the "Does it hurt if I do this?" method of diagnosis. If hospitals only used the echo process to determine the health of a person they would rarely truly help people. On the bright side the waiting room times would be very short. That's why some doctors, most scientists, and especially hackers use the Four Point Process to make sure they don't miss anything.

The Four Point Process has you look at interactions in the following ways:

1. **Induction**: What can we tell about the target from its environment? How does it behave in that environment? If the target is not influenced by its environment, that's interesting too.
2. **Inquest**: What signals (emanations) does the target give off? Investigate any tracks or indicators of those emanations. A system or process generally leaves a signature of interactions with its environment.
3. **Interaction**: What happens when you poke it? This point calls for echo tests, including expected and unexpected interactions with the target, to trigger responses.
4. **Intervention**: How far will it bend before it breaks? Intervene with the resources the target needs, like electricity, or meddle with its interactions with other systems to understand the extremes under which it can continue operating.

Back to our hospital example...the four stages of the FPP would look like this:

1. The **interaction** function is the echo process where the doctors poke the patients, talk to them, and test their reflexes on the elbows and knees and use other tools of the "Does it hurt if I do this?" method.
2. The **inquest** is reading **emanations** from the patient like pulse, blood pressure, and brain waves.
3. The **intervention** is changing or stressing the patient's homeostasis, behavior, routine, or comfort level to see what happens.
4. And finally **induction**, which is examining the environment, the places where the person visited before they got ill and how they may have affected the patient, such as what they may have touched, ingested, or breathed.

Exercise

1.9 As you can see, the Four Point Process lets you more deeply investigate interactions. Now you can try it. Explain how you would use the Four Point Process to know if a clock is working – and then if it's working correctly by keeping the right time.

What to Hack

When you're hacking anything you need to set up some ground rules. You need the language and the concepts to know what you're actually hacking. The **Scope** is a word we use to describe the total possible operating environment, which is every interaction that the thing you want to hack has.

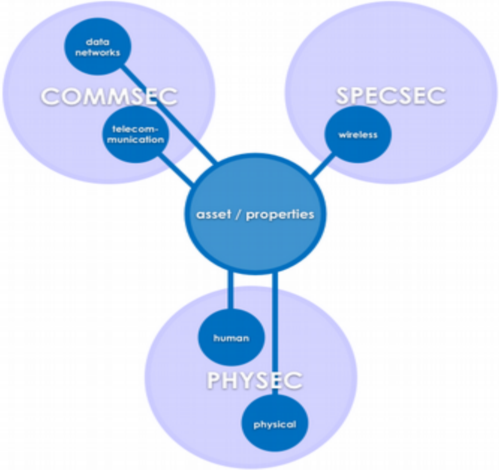

Figure 1.2: Scope

Feed Your Head: Classes and Channels

In professional terminology (also useful to hackers), the Scope is made up of three **Classes** that subdivide to five **Channels**:

Class	Channel
Physical Security (PHYSSEC)	Human
	Physical
Spectrum Security (SPECSEC)	Wireless
Communications Security (COMSEC)	Telecommunications
	Data Networks

Classes are not something you have to be too worried about but they are the official labels used currently in the security industry, government, and the military. Classes define an area of study, investigation, or operation. So if you're looking up more information on any topic, it's really good to know what the pros call it.

Channels are the common terms for the ways you interact with assets. It's not uncommon to hack a gadget by using the Four Point Process over each Channel. Yes it seems like a lot of work, but think of how thrilling it is when you discover a way to make it work that's not listed in any manual, or better yet not even known to the manufacturer!

An **Asset** can be anything that has value to the owner. It can be physical property like gold, people, blueprints, laptops, the typical 900 MHz frequency phone signal, and money; or intellectual property such as personnel data, a relationship, a brand, business processes, passwords, and something said over the 900 MHz phone signal.

Dependencies are the things beyond the asset owner's ability to provide independently. Not many computer owners generate their own electricity, for instance. Even if it's not likely someone will cut off your electricity, it is still within your scope.

The goal of security is **Separation** between an asset as well as its dependencies, and any threat to them.

We say **security is a function of separation**. There are four ways we can create this separation:

- Move the asset to create a barrier between it and the threats.
- Change the threat to a harmless state.
- Destroy the threat.
- Destroy the asset. (Not recommended!)

When we're hacking we look for places where interactions with the target are possible, and where they are not. Think of doors into a building. Some are necessary for workers;

others are necessary for customers. Some may be needed to escape fire. And some may not be necessary at all.

Every door, though, is a point of interaction, one that aids both necessary operations and unwanted ones like theft. When we come on the scene as hackers, we don't start out knowing the reasons for all these interactive points, so we analyze them with the Four Point Process.

Consider the example of a guy who wants to be totally safe from lightning. The only way to do this (while still on Earth) is to get into a mountain where it is completely impossible for lightning to get inside through all that dirt and rock. Assuming he never needs to go out again we can say his security is absolutely 100%. But if we start drilling holes in the mountain the lightning has one more point of access with every hole, and the porosity increases. The OSSTMM differentiates between being **Safe** from lightning and being **Secure** from it. The simple fact is that the more porosity there is, the more likely a hacker can make changes and control what they want.

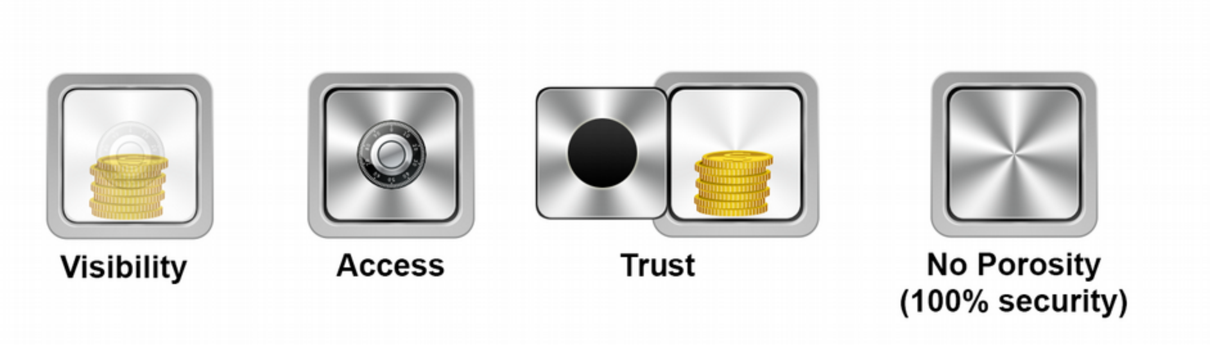

Figure 1.3: Porosity

Feed Your Head: Porosity

Here are some examples that describe how pores can be located, classified, and determined in the hacking process.

Term	Definition
Visibility	When police investigate a crime, they look for *means*, *motive* and *opportunity*. If an asset is visible, it can be attacked, but if it's not visible, it can't be targeted – though it could be discovered. Some security professionals like to say that **obfuscation** is poor security because it doesn't protect anything, it only hides it. But that's not a bad thing especially since you don't always need a permanent security answer. To that effect the **OSSTMM** offers this little gem: *"Security doesn't have to last forever, just longer than anything else that might notice it's gone."*
Access	Access is the number of different places where interactions can occur to the outside of the scope. For a building this could be doors to the street or windows and for a server on the Internet it could be the number of open network ports or services available on that computer.
Trust	Trust is when one entity accepts free interaction with another entity within the scope. It's why you don't ask your mother for ID when she comes to hug you. It's also why you don't suspect she's poisoned your food. You learn to trust the things inside your scope. Then one day if she gets taken over by

an alien race and replaced (*a lá* **Invasion of the Body Snatchers**) and does poison your food you'll eat it unsuspectingly. Thus trust is both a security hole and a common replacement for authentication, the way we can validate if someone is who we think they are. Trust is a strange topic because it's such a human thing to do and pretty valuable in society. Without trust, we'd never be able to interact freely. But because of trust, we are easily tricked, fooled, robbed, and lied to. OSSTMM research on trust shows that there are 10 reasons to trust someone called **Trust Properties** and if all ten reasons are satisfied then we can trust safely without any worry. But that same research shows that most people need only one trust reason to be satisfied and the really paranoid or cynical are okay with just three reasons to trust.

Resources

Effective research, learning and critical thinking are key skills for a hacker. Hacking, in reality, is a creative process that is based more on lifestyle than lesson. We can't teach you everything that you need to know, but we can help you recognize what you need to learn. Because science advances so quickly, what we teach today may not be relevant tomorrow. It is much better for you to embrace hacker learning habits, which are probably the most vital part of hacking, and which will separate you from the **script kiddie** (a hacker word that means a person who uses tools without really knowing how or why they work).

If you run into a word or concept you don't understand in this lesson, it's essential you look it up. Ignoring new words will only make it difficult for you to understand concepts in the coming lessons. You'll be asked to investigate a topic and then expected to use the information that you find to complete the exercises in that lesson – but those lessons won't explain to you how to do this research. So be sure to spend as much time as you need learning to use the various resources available to you.

Books

You might be surprised that we don't point you straight at the Internet, but books are a great way to learn the foundation and factual science of everything you want to explore. Want to know something about computer science, like the hardware details of your PC? Nothing will help you more than reading a current book on the subject. The main problem with books for computers is that they become out-of-date very quickly. The secret is to learn to see the fundamental structure underneath the thin skin of details. MS-DOS and Windows are clearly different, but both are based on principles of Boolean logic that have driven computers since Ada, Countess of Lovelace, wrote the first computer programs in the nineteenth century. Security and privacy concerns may have changed in the last 2,500 years, but **The Art of War** by Sun Tzu covers fundamental principles that still apply today. (By the way, there is no faster way to look like a **n00b** than by quoting Sun Tzu. Some things you should know how to apply but not say. And quoting The Art of War proves that you didn't really read The Art of War because Sun Tzu even says to keep your real knowledge a secret.)

Even though information found in books may not be as up to date as information that comes from other sources, the information you find in books is more likely to be better written than most other sources. Sometimes they are more accurate too. A writer who spends a year writing a book is more likely to check facts than someone who is updating a blog six times a day. (See the Sections on Zines and Blogs for more information.)

But remember – accurate does not mean unbiased. The sources of the author's information themselves might be biased. "History books are written by the winners" (look up that quote), and the same holds true when the politics and social norms of the time may prevent certain information from being published. This commonly happens with school textbooks that are chosen through a political process and contain only the information considered socially acceptable to know. Don't think you've found a golden truth just because you read it in a book. The truth is that anyone can write a book and any book can contain anyone's version of the truth.

> Don't look at a book and give up before you even start just because it's so big. Nobody reads most of these massive books that you see sitting around from cover to cover. **Think of them as prehistoric web pages.** Open one up to a random page and begin to read. If you don't understand something, go backward and look for the explanation (or skip forward to something that does make sense). Jump through the book, backwards and forwards, just as you would bounce from link to link in a web page. This type of non-linear research is often much more interesting and satisfying for hackers, since it's about satisfying your curiosity more than it is about reading.

Finally, one thing that book readers gain as a valuable skill is the ability to write well. This is a huge advantage whenever you are trying to understand and participate in a new field. It also makes what you have to say more credible to other readers, especially those who are in positions of authority.

Magazines and Newspapers

Magazines and newspapers are highly useful for providing concise, timely information. Both types of publications can be very short on details, though. Also be aware that every newspaper or magazine has its own audience and its own agenda or theme, regardless of any claims of being "fair and unbiased." Know the theme of the publication: a Linux magazine isn't necessarily a good source of information about Microsoft Windows, because Windows is a conflicting theme (a competing operating system), and frankly a Linux magazine's readers want to read about the superiority of Linux. Many of the specialty magazines employ **cherry picking,** the technique of highlighting only the positive aspects of something fitting the magazine's theme or highlighting only the negative aspects of the things that don't.

> Be aware of a publication's possible biases. That's where they give you opinions instead of facts or leave out facts from a story to fit their own opinions or so you can't form your own opinion. Consider the source! Even "neutral" appearing periodicals can be full of biases and speculation, a nice way of saying "educated guesses" but is more often just "guesses" on the part of the journalist.

There's is a huge movement in the medical field to have all medical and pharmaceutical trials published (or at least all publicly-funded trials) even if they failed so that doctors can make even more informed choices about what medicine and procedures to apply. While current medical journals may be publishing "facts" from research trials, the details and circumstances behind those facts are still cloudy. That's really important when you deal with subjects that rely on having root causes. Causation requires that the cause precedes and is the reason for the effect.

Other tricks used by periodicals (both inadvertently and purposely) are **anecdotal evidence**, which is opinions from people published as evidence regardless of whether they are experts or not; **authoritative evidence**, in which industry employees represented as experts give their opinions, or people who are authorities in one area offer their opinion in another area in which they have no expertise; and finally, **speculation**, dressing up something as true because "everyone" believes it is true, though there's no actual attribution to anyone specific.

The best way to deal with the issues of accuracy and agenda is to be well and widely read. If you read about an interesting issue in a magazine, look into it further. Take one side of the issue, and look for confirmations; then take the other side, and look for rebuttals. Some cultures do this by default. It's part of their social habits to seek other sides to the story. That's a really powerful cultural trait, especially if you're trying to assure a successful democracy.

Exercises

1.10 Search the Internet for three online magazines on the subject of hacking. How did you find these magazines?

1.11 Are all three magazines specifically about computer hacking? What else do they offer that might be helpful in other fields or other businesses?

Feed Your Head: Speculation

The following paragraph is from a newspaper article about a robbery. Can you find the Speculation? Note the areas that you suspect:

The Lake Meadow Bank and Mortgage Lender was robbed Tuesday afternoon when masked gunmen walked in just moments before closing and held the employees hostage for an hour before what appears to be making their get-away in a late model SUV. None of the hostages were reportedly injured.

No one could identify the gunmen which leads the police to believe that this may have been a professional job as moments after the robbery, the car was spotted behind the bank and heading south towards the dense woods of the Bluegreen Mountains. The police are now likely to be looking for experienced robbers who may have prison records and who also have relationships to people living in that area.

With an average of 57 thefts at banks being reported every day within this country and the Bluegreen county population reportedly to reach a population of over 50,000 by next year, this could be the start of a rash of bank robberies from that region. “This looks like the start of a trend.” said the police commissioner, Smith.

As we become more desensitized to speculation and remain functionally ignorant of the bias in statistical data and results, the future of all our news might as well just come from a single journalist speculating on news stories as they happen. In the short example above, there is only one real fact - a bank had been robbed on Tuesday afternoon. Now for the sake of obviousness, this is what it would look like if we changed all the speculation to make it more ridiculous:

The Righteous Bank and Mortgage Lender was robbed Tuesday afternoon when what appears to be masked chickens walked in just moments before closing which means they could have held the employees hostage for as long as a decade before what appears to be making their get-away in a hot air balloon shaped like a chicken coop. None of the hostages were reportedly covered in feathers.

No one could identify the chickens which leads the police to believe that they may have had a professional disguise artist among them in addition to an accomplished balloonist as moments after the robbery, a hot air balloon was spotted above the bank and flying south towards the tundra of Antarctica. The police are now likely to be looking for accomplished make-up artists who also have ties to balloon hobbyists.

With an average of 57 thefts at banks being reported every day within this country and the ballooning industry reporting sales to reach $47 gazillion by some future date, this could be the start of a rash of bank robberies using hot air balloons. “This looks like the start of a trend.” said the police commissioner, Gordon.

With the overwhelming use of speculation and statistics across all industries it is no wonder that it has entered the security industry with such force. The commonly used term in this industry is **FUD** which is an acronym for **Fear, Uncertainty, and Doubt**. It is how speculation and subjective risk analysis are used in security to gain attention for one's interests and sell security solutions. Unfortunately it plays very well with the primitive paranoia in the human psyche and a growing numbness to speculation. This has led to inappropriate security solutions, inappropriately applied security, reactive security controls, and false confidence in authorities. There is clearly a failure of critical thinking skills within the population and this is being exploited both by the commercial sector and the criminals.

Search Engines

Google is a well known search engine but it’s not the only search engine. Bing is very good with searches in the form of simple questions and Yahoo is good for doing thorough research. Be very aware that all these web services want to know everything they can about you, and probably know more than they should. They will record your searches and which websites you visit after you search.

There are engines like AltaVista and DuckDuckGo.com that may give you some – or a lot – of anonymity, which might be a good thing when you are looking into dark corners.

Websites are searchable while they're online and usually long after that. Typically they're preserved in the form of **cached pages**. An Internet cache is an online record of past versions of websites, or even of websites that have gone dark. Search engines and archive sites keep this information indefinitely, which in Internet terms is "forever." That's a valuable thing to remember before you ever put anything on the Internet: it isn't going away. Ever. You may have to look for a link to the cached copy of a page. Google, for instance, used to put a simple link labeled "Cache" alongside the regular link to a result. That has changed to a fly-out menu on the right, and may have changed again by the time you read this.

Besides the search engines, there are also useful public caches at places like the **Internet Archive at http://www.archive.org**. You can find cached versions of whole websites from over the years, which can be very useful for finding information that has "disappeared."

One final note on websites: don't assume you can trust a website just because it shows up in a search engine. Many hacker attacks and viruses are spread just by visiting a website or downloading innocent-looking programs, screen savers or any shared files. You can safeguard yourself by not downloading programs from untrusted websites, and by making sure your browser runs in a **sandbox**. But this may not be enough. A browser is a window to the Internet and like any window, bad stuff can float in just because it's open. Sometimes you won't even know until it's too late.

Exercises

1.12 There are many search engines out there. Some are good for getting to the **Invisible Web**, areas of the Internet that are hard for most search engines to dig through, like certain private databases. A good researcher knows how to use them all. Some websites specialize in tracking search engines. So find five search engines you haven't used or maybe even heard of before.

1.13 There are also search engines that search other search engines. These are called **meta search engines**. Find one of these meta search engines.

1.14 Search for "security and hacking" (including the quotation marks) and note the top three answers. How do the results differ when you DON'T use quotes?

1.15 It is very different to search for a topic than it is to search for a word or phrase. In the previous exercise, you searched for a phrase. Now you will search for an idea.

To do this, **think of phrases that might be on the page you're looking for**. If you want the search engine to give you a list of online magazines about hacking, you won't get far by searching for "a list of online magazines about hacking." Not many web pages will contain that phrase! You'll get some hits but not many.

Instead, you need to think, "If I was setting up a hacking magazine, what would a typical sentence in that magazine look like?" Put the following words and phrases into a search engine and find out which provides the best results for your search:

1. my list of favorite magazines on hacking
2. list of professional hacking magazines
3. resources for hackers
4. hacking magazine
5. magazines hacking security list resources

1.16 Find the oldest website from Mozilla in the Internet Archive. To do this you need to search on "www.mozilla.org" at the http://www.archive.org website.

1.17 Now to put it all together, let's say you want to download version 1 of the Netscape web browser. Using search engines and the Internet Archives, see if you can locate and download version 1.

Websites and Web Applications

The *de facto* standard for sharing information is currently through a web browser. While we classify everything we see as "the web," more and more what we really use are "web applications," since not everything on the web is a website. If you check email using a web browser, or get music through a web-connected service, you are using a web application.

Sometimes web applications require privileges. This means you need a login name and password to get access. Having access when you have a legal right to access is called having **privileges**. Hacking into a website to change a page may mean you have access, but since you have no legal right to be there, you don't have privileged access. As you continue to use the web, you'll find that many places give access to privileged areas by accident.

When you find something like this, it's a good habit to report it to the website administrator. However, beware of potential legal repercussions. Unfortunately, many administrators frown upon unsolicited vulnerability reports.

> To contribute to making the Internet a safer place while also protecting yourself, you should consider using an **anonymizer** service (e.g., Tor or anonymous remailers, etc.) for sending out vulnerability reports to these administrators. But be aware: all of these anonymous technologies have their weak points and you may not be as anonymous as you think you are! (More than one hacker has learned this the hard way.)

Exercises

1.18 Use a search engine to find sites that have made the mistake of giving privileged access to everyone. To do this, we'll look for folders that let us list the contents (a "directory listing"), something that usually shouldn't be allowed. For this we will use some Google command tricks at http://www.google.com. Enter this into the search box:

```
allintitle:"index of" .js
```

Scan the results and you may find one that looks like a directory listing. This type of searching is known as Google Hacking.

1.19 Can you find other types of documents in this way? Find three more directory listings that contain .xls files, .doc files, and .avi files.

1.20 Are there other search options like "allintitle:"? How can you find them?

Zines

Zines, also known as **e-zines**, are the descendants of **fanzines**: small, usually free magazines with a very small distribution (less than 10,000 readers) and often produced by hobbyists and amateur journalists. Fanzines were printed on paper. Zines on the Internet, like the famous **2600** or the **Phrack** web zine, are written by volunteers; often that means the producers don't edit content for non-technical errors. Sometimes strong language can be surprising for those who aren't familiar with this genre.

Zines have very strong themes or agendas, and tend to be very opinionated. However, they are also more likely to show and argue both sides of issues, since they usually don't care about or have to please advertisers and subscribers.

Exercises

1.21 Search the Internet for three zines on the subject of hacking. How did you find these zines?

1.22 Why do you classify these as zines? Remember, just because they market it as a zine or put "zine" in the title doesn't mean it is one.

Blogs

A **blog** can be considered an evolution of the zine, usually with a writing staff of one. Blogs are updated more often than most print publications or zines, and create communities tied to very strong themes. It's as important to read the commentary as the postings. Even more so than zines, on blogs the response is often immediate and opinionated, with comments from every side. This is one of their special values.

There are millions of blogs on the Internet, but only a small percentage of them are active. The information on almost all, however, is still available.

Exercises

1.23 Search the Internet for three blogs on the subject of hacking.

1.24 What groups or communities are these associated with?

1.25 Is there a security, law enforcement or academic theme to the blog?

Forums and Mailing Lists

Forums and **mailing lists** are communally developed media, a lot like a recording of conversations at a party. Be a little skeptical about everything you read there. The conversations shift focus often, a lot of what is said is rumor, some people are **trolling**, a **flame war** might erupt, and, when the party is over, no one is certain who said what. Forums and mailing lists are similar, because there are many ways for people to contribute inaccurate information – sometimes intentionally – and there are ways for people to contribute anonymously or as someone else. Since topics and themes change quickly, to get all the information it's important to read the whole thread of comments and not just the first few.

You can find forums on almost any topic, and many online magazines and newspapers offer forums for readers to write responses to the articles they publish. Because of this, forums are invaluable for getting more than one opinion on an article; no matter how much one person liked it, there is certain to be someone who didn't.

There are many mailing lists on special topics, but they can be hard to find. Sometimes the best technique is to search for information on a particular subject to find a mailing list community that deals with it.

As a hacker, what is most important for you to know is that many forums and mailing lists are not searchable through major search engines. While you might find a forum or list through a search engine, you may not find information on individual posts. This information

is part of the invisible web because it contains data that is only searchable directly on the website or forum.

Exercises

1.26 Find two hacker forums. How did you find these forums?

Can you determine the themes or topics of specialty of these websites?

Do the topics in the forums reflect the theme of the website hosting them?

1.27 Find two hacking or security mailing lists.

Who is the "owner" of these lists? Can you see the member list? (You might need to figure out the application the list has been developed on and then search the web for the hidden commands to see the list of members on that kind of mailing list.)

On which lists would you expect the information to be more factual and less opinionated? Why?

Newsgroups

Newsgroups have been around a long time. There were newsgroups long before the World Wide Web existed. Google purchased the entire archive of newsgroups and put them online at http://groups.google.com. Newsgroups are like mailing list archives but without the mail. People posted there directly like they do when commenting to a website. You will find posts in there from the early 1990s onward.

> Like the web archives, the group archives can be important for finding who really originated an idea or created a product. They're also useful for finding obscure information that never may have made it to a web page.

Newsgroups aren't used any less today than they were years ago, before the web became the mainstream for sharing information. However, they also haven't grown as their popularity is replaced by new web services like blogs and forums.

Exercises

1.28 Using Google's groups, find the oldest newsgroup posting you can on the subject of hacking.

1.29 Find other ways to use newsgroups. Are there applications you can use to read newsgroups?

1.30 How many newsgroups can you find that talk about hacking?

1.31 Can you find a current list of all the different newsgroups currently in existence?

Wikis

Wikis are a newer phenomenon on the Internet. Wikipedia (www.wikipedia.org) is probably the most famous one, but there are many others. Like many other sites wikis are put together by communities. Reports often claim that wikis are not accurate because they are contributed to by amateurs and fanatics. But that's true of books, mailing lists, magazines, and everything else too. What's important to know is that experts aren't the only source of great ideas or factual information. As the OSSTMM points out, facts come from the small steps of verifying ideas and not great leaps of discovery. That's why wikis are great sources of both professional and amateur ideas slowly and incrementally verifying each other.

> Wikis will often discuss many sides of a topic and allow you to follow how information is argued, refuted, refined and changed through a list of edits. So they are great places to dig up information, but often you have to go to the wiki's website to do searches.

Exercises

1.32 Search for "Ada Lovelace." Do you see results from wikis?

1.33 Go to Wikipedia and repeat this search. Take a look at the article on her. Was it included in your search results?

1.34 Check out the edits of that Wikipedia page and look at the kinds of things that were corrected and changed. What kinds of things were changed? Was there anything changed and then changed back? Now pick a popular movie star or singer you like and go to that page in Wikipedia and check the edits. Do you notice a difference?

1.35 Find another wiki site and do the search again. Did any of the results show up in your original search engine search?

Social Media

Do you use a social media site? Or more than one? As a hacker you're well aware of the popular social media sites of the moment. How about the ones that aren't as hot as they used to be? They still exist, and all their data is still available, in most cases.

> This means there is a huge repository of information about us, most of which we have freely given away. And it's going to be there pretty much forever.

Social media sites often have sub-groups or communities of interest. Sites with a professional theme frequently have cybersecurity groups, and sites with an "underground" theme frequently have hacker groups. On the professional sites you are (and everyone else is) expected to use your real name. On the hacker sites, not so much.

Most important of all, do you use your real name on social media sites, or do you use a "handle?" Is there any way your handle could be traced to your real name? Most people don't realize it when they use handles, but it's not uncommon for them to accidentally or sometimes on purpose post their real names, address, city, school, jobs, and so on when using the handle. If another hacker DoXes your handle then they can usually pretty quickly figure out who you really are because of such small mistakes. If you use a handle to be anonymous to those who don't know you, then make sure you take measures to keep it that way. And NEVER confuse your handles if you have more than one.

Exercises

1.36 Search for yourself. Do you get any results (that are actually you)? Are any of them from social media sites?

1.37 Go to a social media site you use. Don't log in, but repeat the search as if you were an outsider. How much can you find out about yourself?

1.38 Go to a social media site a friend uses. Again, don't log in if you have an account. Search for your friend. How much can you find out about your friend?

Chat

Chat, which comes in the forms of **Internet Relay Chat (IRC)** and **Instant Messaging (IM)**, is a very popular way to communicate.

> As a research source, chat is extremely inconsistent because you're dealing with individuals in real time. Some will be friendly and some will be rude. Some will be harmless pranksters, but some will be malicious liars. Some will be intelligent and willing to share information, and some will be completely uninformed, but no less willing to share. It can be difficult to know which is which.

However, once you get comfortable with certain groups and channels, you may be accepted into the community. You will be allowed to ask more and more questions, and you will learn whom you can trust. Eventually you can get access to the very newest hacking exploits (also known as **zero day**, meaning it was just discovered right now) and advance your own knowledge.

Exercises

1.39 Find three instant messaging programs. What makes them different? Can they all be used to talk to each other?

1.40 Find out what IRC is and how you can connect to it. Can you discover what network holds ISECOM's channel? Once you join the network, how do you attach to the isecom-discuss channel?

1.41 How do you know what channels exist on an IRC network? Find three security channels and three hacker channels. Can you enter these channels? Are people talking or are they bots?

P2P

Peer to Peer, also known as **P2P**, is a network inside the Internet. Unlike the usual client/server network, where every computer communicates through a central server, the computers in a P2P network communicate directly with each other. Most people associate P2P with downloading MP3s and pirated movies on the infamous original Napster, but there are many other P2P networks – both for the purpose of exchanging information, and as a means of conducting research on distributed information sharing.

The problem with P2P networks is that, while you can find just about anything on them, some things are on the network illegally. And other things are there legally but the companies that created them still feel that they should not be there and are happy to demand money from the owner of any **Internet gateway** where it's downloaded.

> At the moment there is not much agreement on whether the person whose Internet access was used to download content is responsible or if the police actually have to catch the person who did it. That's like saying that if your car is used to commit a crime the owner of the car, not the driver, goes to jail. Internet laws are currently not just and not fair so be extra careful!

Whether or not you are the kind of person who risks downloading intellectual property, there is no question that P2P networks can be a vital resource for finding information. Remember: there is nothing illegal about P2P networks – there are a lot of files that are available to be freely distributed under a wide variety of licenses – but there are also a lot of files on these networks that shouldn't be there. Don't be afraid to use P2P networks, but be aware of the dangers, and of what you are downloading.

Exercises

1.42 What are the three most popular and most used P2P networks? How does each one work? What program do you need to use it?

1.43 Research the protocol of one of those P2P networks. What does it do, and how does it make downloading faster?

1.44 Search for the words “download Linux.” Can you download a distribution (or distro) of Linux using P2P?

Certifications

There are OSSTMM Security Tester and Security Analyst certifications, various colors of “hacker” certifications, certifications based on one version of “best practices” or another and certifications with all kinds of crazy initials or pieces of punctuation.

> Why do you care about certifications? Because you can get some of them at any age, because you don't have to have a college degree to get them, and because they can put you in the position of the sought-after person, rather than the person asking for a gig.

The problem with best-practices based certifications is that best practices change often, because *best practices* is just another way of saying “what everyone else is doing right now.” Often what everyone else is doing is wrong this week, and will still be wrong when they update it next week.

Then there are research-based certifications, based on valid and repeatable research into human and system behavior. Needless to say our parent organization, ISECOM, falls squarely into the realm of research-based certification authorities. Whether from ISECOM or elsewhere, look for skills-based certifications and analysis-based or **applied knowledge** certifications that make you prove you can do what you say you've learned. That will be handy when you actually have to do it.

Seminars

Attending seminars is a great way to hear theory explained in detail and to watch skills in action. Even product-focused seminars are good to attend to see how a product is intended to be used, as long as you're aware that the event is a marketing pitch and their real job is to sell.

We would be remiss if we didn't mention that we can bring Hacker Highschool Seminars to many locations, and we can cover any of the available lessons. Seminars consist of professional hackers talking to students about hacking and being a hacker, both the bad and the good. These seminars take a sharp look at what real hackers are from research in the **Hacker Profiling Project**, a collaboration project with the United Nations to explore who hackers are and why they hack. Then you will go on to discover the bright side of hacking and how it's not always a dark thing.

One of the most powerful things we can help you find is the means to be as intellectually curious and resourceful as a hacker. Hackers succeed at what they do because they know how to teach themselves, go beyond the lessons available and learn the skills they need to go further.

You're also welcome to ask your parents and educators to learn how to help out and how to start a Hacker Highschool chapter at your school. Contact ISECOM for more information.

Microcomputer Universe: Introduction

Have you heard of the Raspberry Pi? It's a tiny single-board computer (**SBC**) about the size of a credit card, and about the price of a couple of pizzas. It's not a wimpy little thing, either: the P1 2 has a quad-core CPU, USB and HDMI video. A tiny microSD card serves as the hard drive, and swaps so easily you can use several operating systems.

Figure 1.4: a boxed Raspberry Pi, photo by Nico Kaiser

The Raspberry Pi isn't the only microcomputer out there. Other manufacturers sell the Banana Pi, the Orange Pi, the BeagleBone, the Radxa Rock – each with a unique set of features. Want built-in Bluetooth and wifi, for instance? One of the above offers exactly that. (Start researching.)

There are basically three types of microcomputers; the first is the Linux-based board that can act as a full computer or server. The next is an Arduino device that is more of a controller for sensors, robotic equipment, lighting control and basic items. The last type of microcomputer is the hybrid device that is built for specific purposes like controlling sensors but can also be a computer to a point.

The Raspberry Pi (RPi) is in the first category since it runs Linux. This computer has a 1GHZ Cortex Arm quad core processor with 1 gig of ram. The board includes a GPU, four USB ports, an ethernet port, HDMI video output, audio output and a 40-pin GPIO connector to add additional parts onto it. (The attachments have a fun name: because they are Hardware Attached on Top, they're called "HATs" - but that's only with Pies.) You can find them for well under $50, even lower for older models.

You can learn programming (python, scratch, java, php and others) on this device. It can also be used as a server for email, web, multimedia, VPN, or even a NAT firewall. One very popular use is as a Minecraft server. There is a huge collection of information available on the Internet for this device.

Arduino devices are made in Italy and were primarily built to teach coding, control sensors and robotic equipment. These devices are a bit more expensive and are more customized for specific jobs. These require some expertise to work with.

Hybrid devices include Udoo, Remix, Radxa Rock and others. The prices for these vary greatly but often include wifi and Bluetooth built in. Neither Arduino nor Raspberry Pi have these connections but it doesn't cost much to add them on (except the Arduino Yun which has wifi built in). The hybrids are built to act as controllers and computers on a much higher level than the RPi or Arduino. The Remix is a full blown computer that runs a special version of Android. The Udoo tries to replace the RPi and Arduino with a single device.

If you are looking to start out, we would suggest the RPi as your first step. It is cheap but requires a learning curve to set working. All of these devices use a microSD card to hold the operating system. Luckily, most devices allow you to choose which operating system you want to work with. Changing operating systems is as simple as swapping out the microSD card.

Most of the devices connect to a TV or monitor using HDMI. You can connect a wireless or USB keyboard to control your device or puTTY in based on the local IP address of the device.

We'll be working more with these microcomputer devices in Hacker Highschool in upcoming **Microcomputer Universe** sections.

Further Study

Now you should practice until you're a master of researching. The better you get at it, the more information you will find quickly, and the faster you will learn. But be careful also to develop a critical eye. Not all information is truth.

> Always remember to ask yourself, why would someone lie? Is there money involved in being dishonest or perpetuating a rumor or story? Where do the facts come from? And most importantly, what is the scope?

Like all hacking, research includes a scope. That's really important when you see statistics, like math that uses percentages and fractions and odds. Always look to see where the scope took place and recognize that the scope has to apply. A common place you see this is national crime or health statistics taken from a small sample in just one part of the country. Just because something affects 10% of people out of 200 studied in a single city doesn't mean that 10% of the whole nation has this same problem. So be smart about how you read information as well as how you find it. Figuring out the scope of the information always makes a huge difference!

To help you become a better researcher for the Hacker Highschool program, here are some additional topics and terms for you to investigate:

- Meta Search
- The Invisible Web
- Google Hacking
- How Search Engines Work
- The Open Source Search Engine
- The Jargon File
- OSSTMM
- ISECOM Certifications:
    - OPST (OSSTMM Professional Security Tester)
    - OPSA (OSSTMM Professional Security Analyst)
    - OPSE (OSSTMM Professional Security Expert)
    - OWSE (OSSTMM Wireless Security Expert)
    - CTA (Certified Trust Analyst)
    - SAI (Security Awareness Instructor)

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM