Hacker Highschool

SECURITY AWARENESS FOR TEENS

LESSON 20
HACKTIVISM

DRAFT

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 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 high school students, and high school 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 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Table of Contents

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Contributors

Pete Herzog, ISECOM

Marta Barceló, ISECOM

Bob Monroe, ISECOM

Dominique C. Brack

Craig Steven Wright

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Introduction

The Internet and the opportunities it presents to millions of people across the globe are enormous. Many companies today rely on the web for their businesses' operation and transactions online. However, within the shadows of the Internet, behind the computer monitors, looms some grave dangers that are not easily detectable, as hackers sneak in like thieves and you only realize you have been hit after the damage has been done. Privacy online is never guaranteed. Someone may be watching and recording every keystroke you make on your personal computer.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Key Elements of Hacking

The five motivation factors for hacking:

1. **Curiosity:** Hacking into a poorly-protected Web site or computer to see what is there, or to learn how to do so.
2. **Fame:** Hacking attacks motivated by ego ideology, and a sense of personal fame. An example is attacking a poorly-protected system and defacing the content with the help of tools. Attacks create huge amounts of traffic and sometimes Denial of Service attacks DoS.
3. **Personal Gain:** Hacking for financial gains, including organized crime syndicates from around the world. Hacking into corporate and enterprise systems to steal information that has monetary value like credit card information or intellectual property.
4. **National Interest:** Hackers who work on behalf of governments, often are highly skilled and command virtually unlimited resources.
5. **Global/ Political Interests:** Most hacking activities orchestrated are politically motivated with the hackers motivated by a political agenda.

It is important to note that there are individuals and groups who will attack organisations for many reasons. In today's society it is just not rational to believe that an organisation is safe because there is modest external perception. Both large and small organisations are targeted for a variety of reasons. Some examples are listed below;

- Mitsubishi has been a target of activists for using rainforest timber in some of their vehicles,
- Care International has been targeted by groups who believe that they are spying for the US,
- The Red Cross has been targeted by religious fundamentalists
- Many US organisations have been targeted (for example by Chinese Hacking groups) as a protest against the US government.

Remember, just because an organization is not well known, doesn't mean it's not a target for hackers.

Hacktivism

Hacktivism is the fusion of hacking and political or religious activism; politics and technology. Numerous instances of hacktivism have been reported in the recent past as it is much easier to launch a cyber-protest than to organize masses of people for street demonstrations. More specifically, hacktivism is described as hacking for a political cause.

Hacktivists, or hacker activists seek to advance or enforce their political or religious views through attacks on the information infrastructure. These groups are similar to the activist groups of the Sixties, but focus on using electronic means. Some examples include;

- Protestors who attacked financial web sites during the G8 summit;
- Attacks against the web sites and infrastructure of logging companies by pro-green groups.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

- Online attacks carried out by religious fundamentalists in protest of events or activities in other nations.
- “Patriotic” hackers attacking the financial or information infrastructure of another nation in protest of events or in retribution for other events.

Some of the common methods used by these groups include;

- Holding virtual sit-ins
- Visiting a site *en masse* in order to shut it down (a Denial of Service)
- Bombing email inboxes (mailbombing means sending vast amounts of email to the target)
- Forming a virtual blockade (denying legitimate traffic to the target)
- Defacing web pages to post messages of political or religious protest

Today, there are several organized groups that champion different causes. One of the most common reasons for organized hacking of prominent people’s accounts has been to protest bad leadership. Just like activism, where civil and human rights groups use all means possible to champion their courses, hacktivism involves the use of the Internet by hackers to send out serious targeted messages to governments, individuals and groups that try to gag the internet, overall bad leadership and bad policies. Most importantly, they demand the freedom of the cyberspace.

Up until recently, cyber-criminal gangs were behind record-breaking data breaches that resulted in the theft of millions of customer records. Today, hacktivists have outrun cyber-criminals. Hacktivists have drastically changed their game plan. They have moved beyond simple website defacements into highly sophisticated DDoS attacks and large-scale data theft operations.

They have been very effective in launching attacks on government websites and their motivation increases with each successful attack. Even TIME Magazine included **Anonymous** (well-known hacktivists) in their list of 100 Most Influential People for 2012.

What is this list? It names the people who inspire us, entertain us, challenge us and change the world. They are mostly the breakouts, pioneers, moguls, leaders and icons. It includes, among others:

- Barack Obama (US President)
- Lionel Messi (Soccer player)
- Shakira (Pop star)
- Mark Zuckerberg (Founder of Facebook)

It may appear odd to find Anonymous as an organization on this list. Some experts ask themselves –since it was a poll on the Internet – what is the surety that Anonymous itself didn’t help swing the poll in their favor?

The governments across the globe must be learning a lesson the hard way. Even though the police intelligence services are trying everything possible to bring the hackers to book, they are constantly hitting dead ends. There are so many hacking organizations in the world today and tracking and arresting all of them is an effort in futility. The more they are arrested, the more they perfect their game. They are now coming together and forming alliances across the World Wide Web and Internet and show no chance of relenting in their quest for a freer web and a just society. The public supports and funds the hacktivist when they believe in their causes.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Feed Your Head: Who or What is Anonymous?

Anonymous isn't a person. It's not even a group of people in any well-defined sense. Members have reportedly attacked sites ranging from the Vatican's to those of major companies such as PayPal and Sony; they apparently released 75,000 credit-card numbers belonging to customers of research firm Stratfor. Arrests of dozens of suspected participants in multiple countries haven't shut down the leaderless organization. There is no doubt that the group is comprised of the sharpest brains and internet gurus. With members spread across the world, "Anonymous" agitates for the freedom of the internet and is against internet related legislations and gagging. Anonymous is known for their philosophy and the symbol of a mask.

The Anonymous Philosophy

We Are Anonymous.

We Are Legion.

We Do Not Forgive.

We Do Not Forget.

Expect Us.

The Guy Fawkes mask

The Guy Fawkes mask is a stylized depiction of Guy Fawkes based on the movie V for Vendetta, released in 2006. After appearing in Internet forums, the mask was worn by participants in real-life protests such as the Occupy movement.

The Goal of Hacktivism

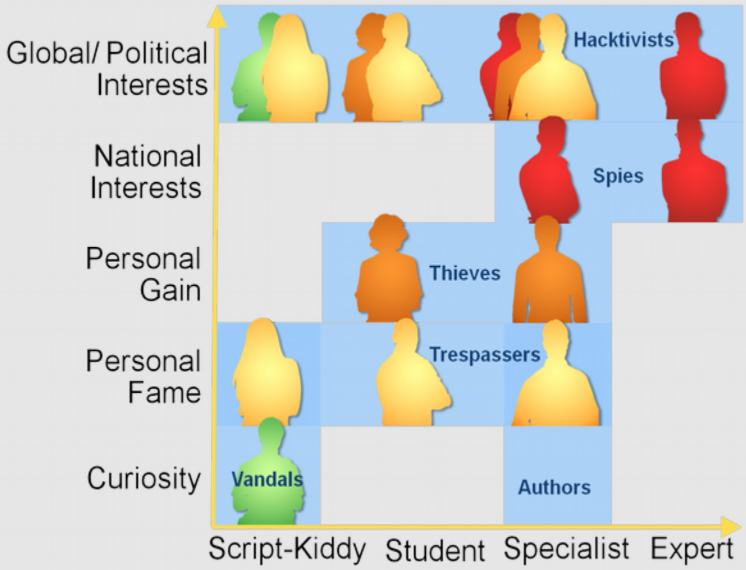
Hacktivists are committed to securing the Internet as a platform of free speech and expression. This ensures that the Internet remains a medium for activism and an environment that facilitates the free flow of information.

Feed Your Head: The Hacker Hierarchy

Initially, hacking was mostly for grins. People would hack into other people's accounts and laugh at whatever they discovered, especially private information. Competing businesses found a clue and would engage the services of the hackers to either fish out information from their competitor's websites or even bring them down. Celebrities have always been the most vulnerable group with hackers sneaking into their personal email accounts to get any information that they deem fit for the ever hungry ear and roaming eye of the public, through the media. People have made lots of money from this practice.

To get an idea of the kind of people involved in hacking, you can build a chart where the vertical axis represents motivation (from "Curiosity" to "Global/ Political Interest") and the horizontal axis represents expertise and resources (from the entry-level "Script-

Kiddy" to the formidable "Expert").



Where do Hacktivists fit into the broader picture of the hacker culture? Who are the people behind these Hacktivists in organizations like Anonymous?

At the low end of the threat picture, you have the Vandal. This is the person who, for example, hacks into a poorly-protected Web site and defaces the content.

Farther up the scale, you get Trespassers. These people are more capable than Vandals and they're motivated by ego and a sense of personal fame. Their intentions are relatively benign, but they can cause significant problems. The hackers who create many of the worms and viruses that make news usually fall into this category. Because their attacks create huge amounts of traffic and sometimes Denial of Service attacks, their actions can result in serious material damage to computer users, businesses and other organizations. However, they often do not include seriously harmful "payloads" that destroy data or enable theft.

A critical player in the hacker world is the Author. This is the highly-capable hacker who has the tools and expertise to reverse-engineer a patch and write exploit code, or find vulnerabilities in security software, hardware, or processes. Authors are generally motivated by ego, ideology, and/or personal fame.

Authors create the building blocks for criminal hackers, and their work scales out in all directions. For one, the tools and code they produce are usually readily available to the less-sophisticated. This means that the hacktivists, vandals and the script-kiddies are able to cause a lot more trouble with little efforts. More frighteningly, however, their efforts benefit the Thieves. This makes the Author a very interesting person to law enforcement organizations, which play an increasingly important role in helping to combat criminal hackers.

Up the scale, we find the Thieves. These are people who are in it for the money, and they include organized crime syndicates from around the world. Thieves are active and effective in hacking into corporate and enterprise systems, sometimes to steal information that has monetary value (such as credit card numbers), sometimes to divert cash into their accounts, and at times to extort payments and prevent their systems or data from being exposed to the public.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Next on the ladder are the Spies, who work on behalf of governments, highly skilled, and having virtually unlimited resources at their disposal.

At the far end of the scale, there are the Hacktivists. Their motivation is global and/or political. This group is a conglomerate of all the others! Driven by ideology this group engages in unlawful activities, hacking websites, executing denial of Service, DoS attacks and stealing data.

In terms of total hacking effort, Vandals constitute the largest group, or area of activity. However, the greatest financial losses are being incurred because of the web thieves.

In order for Hacktivists to execute large scale DoS/ DDoS attacks, a large number of participants are necessary. The participants execute the DoS/ DDoS attacks with the help of automated tools developed by the Authors. So, recruitment is an important task.

Recruiting for Hacktivism With the Help of MICE

MICE recruiting is commonly used in recruiting new spies. MICE, stands for-Money, Ideology, Coercion, and Ego. All these factors help recruit for their “cause”. If a single motivational factor is not enough, a combination of factors hitting the right mix for an individual usually convinces the recruited. Carefully applied social engineering techniques also help to convince an individual to join forces with the hackers.

Money: Some recruitment just works fine with money as the driving factor; we all want high value assets like cars, watches and other pecuniary items. Money as a reward will motivate the some, but not all.

Ideology: Prospective Hacktivists motivated by ideology are committed to a belief system that places them at odds with their own governments. Such Hacktivists may risk everything for the “cause” even imprisonment or money.

Coercion: Can be used against unwilling participants, blackmailing, loss of income, or threats i.e. potential consequences to their families and friends.

Ego: Entice or entrap participants based on their social standards within the community. This is made possible through offers of positions/ tasks of power and influence.

How Could You Be Enticed?

Try to apply what you have learned based on the following scenarios. Think about what you would offer in terms of MICE to the following prospects. You can use the coding, compare and discuss with your neighbor what the best approach is. Also discuss the order of preference, Ideology and Ego first? Coercion, as the last resort, or the other way round? Do you need only one motivational factor or all of them together?

Exercises

21.1 Evaluate each scenario.

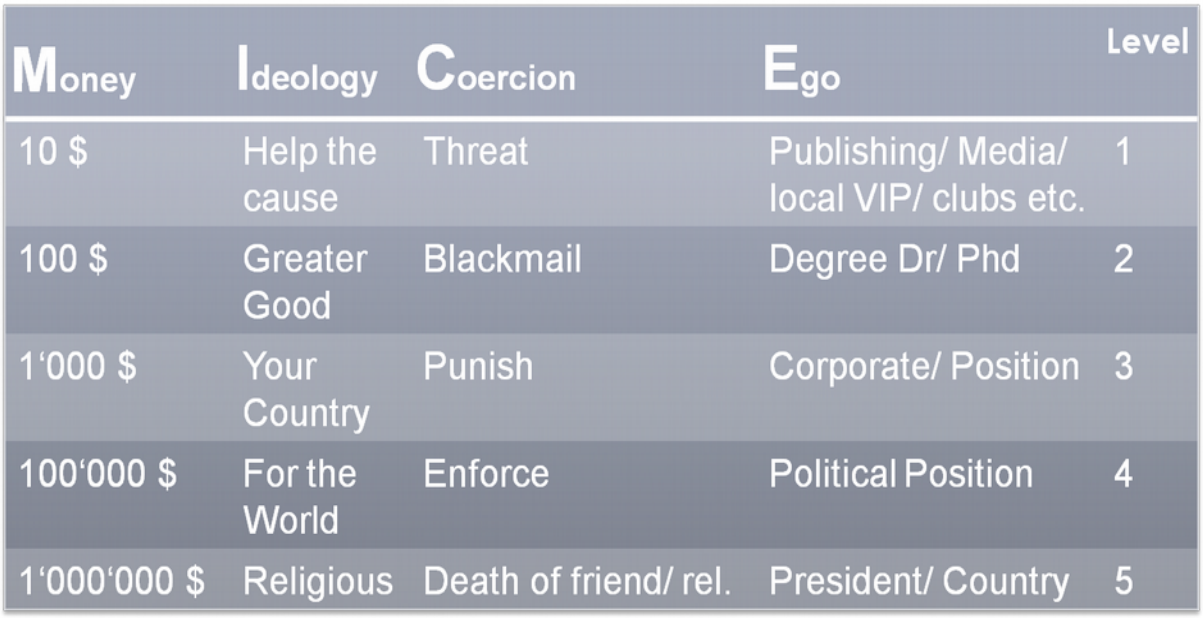
Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

S 0	Example: Pete is a very successful IT career professional. Engaged in not-for-profit work and volunteer programs, he uses his after-work hours to contribute to a volunteer project called Hacker High School. What would you offer Pete? See the table on the left for my approach.	Level 1-5 M - I 2 C - E 1 or 3

S 1	Mike is a 17 year old high school student from Moab (Utah). He is an avid mountain biker and spends every free minute on the slick rock trails. He tries to save money for the latest full suspension bike and dreams of going to Europe for a holiday with his long time girlfriend, Alice. She works for the new datacenter in the area and has a security clearance. **What are you offering Mike?**	Level 1-5 M I C E
S 2	Bob is a very successful public speaker and an information security expert. He is a frequent flyer all over the world due to his expert status and speaking engagements. Since he is never at home, his 20 year wife divorced him just recently. To overcome his loss, he just bought himself a fine Italian sports car, a Ferrari FF. **What are you offering Bob?**	Level 1-5 M I C E
S 3	There is Klaus, a very secretive government employee. He works for the department of defense and has access to top secret information. He can't be found on any social media platforms or on Google. He seems to have a family and relatives close by. Other than golfing, he hasn't been seen engaging in any other sports activity. **What are you offering Klaus?**	Level 1-5 M I C E

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Use the following table to think of how each person in the scenarios could be enticed or forced to cooperate? Levels 1-5 define how strong you are applying each motivational factor.



Money	Ideology	Coercion	Ego	Level
10 $	Help the cause	Threat	Publishing/ Media/ local VIP/ clubs etc.	1
100 $	Greater Good	Blackmail	Degree Dr/ Phd	2
1‘000 $	Your Country	Punish	Corporate/ Position	3
100‘000 $	For the World	Enforce	Political Position	4
1‘000‘000 $	Religious	Death of friend/ rel.	President/ Country	5

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

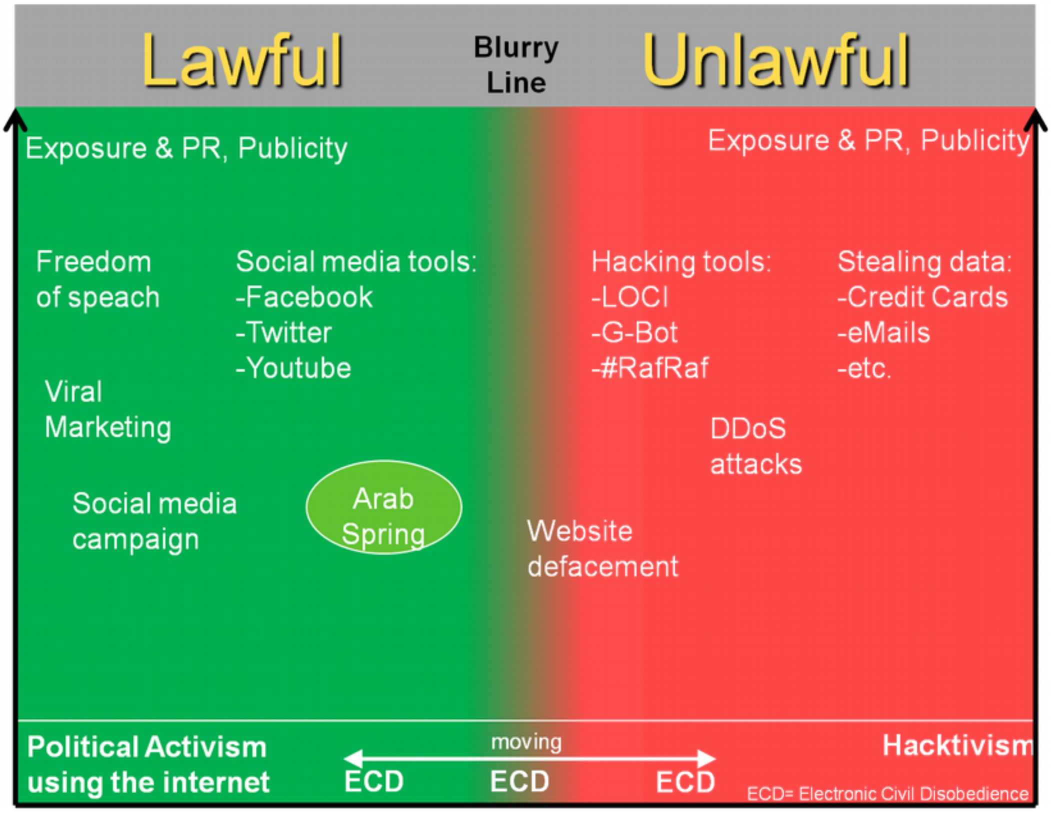
Lawful and Unlawful Hacktivism

Hacktivism is an activity that often gives rise to criminal prosecutions but does not in itself constitute cybercrime.

For this reason, hacktivism (using a computer and hacking skills to accomplish political activism objectives) is therefore technically not designated as a crime. It is considered to be a technical non-offense.

However, even though the law has never recognized a crime called "hacktivism" Hacktivists may possibly face penalties for other crimes deemed to be punishable by law.

The following graphic depicts the difference between lawful and unlawful activities. The difference between a lawful and unlawful activity is a blurry line. When someone is drawn into activities without clearly understanding what the activities actually entail, people can become part of an unlawful engagement without their knowledge (or lack thereof) and their explicit consent.



Both interest groups, political activism and hacktivism and in between the ECD, have the goals of exposure, public relations and publicity. The only difference is in how they achieve their means, either through lawful or unlawful activities. In terms of effectiveness both approaches can be similarly successful. In terms of efficiency, unlawful activities may look like a tempting shortcut. At the end, it comes down to everyone's ethical consciousness to determine what is okay and what is not.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Political Activism Using the Internet

This is activism without the "H" in front. Organizations with a political agenda like Greenpeace, for instance, are using social media to communicate their message or draw the focus to current failings or wrongdoings. Because social media can "**go viral**," a very successful campaign has been launched by Greenpeace. Greenpeace has recently taken on Nestlé because of its Indonesian palm oil supplier with very questionable environmental practices (killing orangutans to raise palm trees). The palm oil is used in making of the Kit Kat chocolate snacks. Interestingly, Nestlé not only apologized for its heavy-handed approach, but, in the wake of the Greenpeace controversy, also cut all ties with its Indonesian palm oil supplier.

This is one of most successful social media pressure campaigns. Using social media as the platform for political purposes can be extremely successful and is within legal boundaries. Social media also played a very important role during the Arab Spring where the citizens of countries like Egypt organized themselves through social media. It is believed without the use of social media it would have been much harder to organize protests and keep the people informed about the current situation.

Electronic Civil Disobedience

Electronic Civil Disobedience (ECD) is a form of non-violent, direct action utilized in order pressure institutions. ECD aims at disrupting target sites without causing serious damage. ECD activities can take the forms of virtual sit-ins. The hacker/hacktivist community passionately opposes the virtual sit-in tactic, suggesting that there is no difference between a virtual sit-in and a DDoS attack and this is where ECD becomes unlawful.

Hacktivism

Hacktivists are using different hacking and attack techniques in order to achieve their goals. Ranging from website defacements over DDoS attacks up to stealing data like credit card information, -mails and other related sensitive and secure information. All of these activities are unlawful and sometimes ethically questionable. Current statistics indicate that Hacktivism has become one of the most feared threats for an organization.

The Mechanics of Hacktivism

Hackers may learn their trade in underground forums that feature tutorials, videos and other instructional material. These sites are usually comprised of information on how to hack, forums for new hackers and discussion groups around new exploits. In essence, the purpose is clear: Release easy to use hacks for people that are semi technical.

Hacktivism, as practiced under the name Anonymous, is about public relations opportunism. Any organization could become a target if a political rationale can be found.

The PR impact: from the media and press perspective, it really doesn't make a difference whether a significant site has been taken down or an insignificant one. From a PR point of view, the target doesn't matter. Whatever happens, the hack will generate media coverage for the cause.

When the hacktivists are not successful in hacking a site using a web application vulnerability, they move on to the DDoS option, because ultimately DDoS doesn't need any vulnerability for it to be successful. You just have to create enough traffic in order to take the site down.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks

Denials of Service attacks aren't technically "hacks," since they can be done without breaking into any systems. Typically, DoS attacks overwhelm a website's servers by flooding them with requests. That makes websites unreachable or unresponsive.

To bring down bigger sites, attackers will sometimes use botnets, or large numbers of infected computers, to send requests all at once, distributed across the Internet. There's not much that companies can do to prevent that kind of attack. While there are numerous motives for DDoS, such as revenge, extortion (demanding 'protection money' to allow a DDoS'd site to come back up or not attack in the first place), competitive advantage, and protest, ideologically and politically motivated DDoS attacks have dramatically increased; in fact, half of DDoS attacks are attributed to political motivation.

Ethics

How does one make the right decisions in terms of engaging in intentionally in unlawful hacking activities? This depends on your personal and professional work ethic. The topic of what *ethics* means is monumental. Often you are forced to make quick and rational decisions in an area you are just starting to learn about. To help make the right decision, there are three major factors that one has to seriously analyze by reflecting on three main questions. This is in no way scientific, but it extends the frame of reference and helps you to consider more than one point of view.

The bubble and me.	Put yourself in the following position: Think of your best friend or your family and imagine that your decision will make front-page news and be posted on every billboard in town, even making it to the local TV news and late-night shows. Would you be happy for best friend or your family to hear, see, and experience this?
The future and me.	Picture yourself sitting back, enjoying the fruits of your labour and achievements. Now think about the best decisions you have made in the past. Does your current decision stack up with those? Is it in line? Some of the best jobs in world require you to have a squeaky clean record.
The society and me.	Think of your mentor, an inspiring leader, or someone else you admire. If you have to explain your decision to this person, will it be understandable or reasonable in his or her context?

In authoring this paper we thought exactly the same things: we asked ourselves if the content of this lesson is ethical and acceptable as per today's standards. Is it appropriate to share this information with a large community and publicly?

Exercises

21.2 Website defacement

Sorry, we shan't demonstrate how to deface websites. But we can sure share different sources and problems associated with website defacement. Web defacement is a serious problem and shouldn't be belittled. Unfortunately, most people focus too much on the defacement rather than the fact that their web applications are vulnerable to this level of exploitation. What happens if the defacers decide not only to alter some website content but instead do something more damaging such as adding malicious code to infect clients?

The following website is a great source for website defacements and statistics thereof. http://www.zone-h.org/

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

1. Go to http://www.zone-h.org/

2. Click on *Archive*

3. Now you will have a list with defaced websites. In order to view a defaced website you choose a website of your liking and click on *mirror* (far right).

4. You now will see what the defaced website looks like. Click on a few other sites to get an impression how the different sites have been defaced differently. Some defacements are just plain text others have pictures or even music.

5. Now use the search box in top right corner and enter anonymous as the search term. Click <enter>.

6. You need to enter the captcha displayed to you.

7. On the results page you will see two or three sections: News, Events, and Defacements.

8. Go to Defacements and select one of the notified by Anonymous links.

9. If you go to more than one link you will realize not all defacements look the same, even if all have been notified by Anonymous.

21.3 Additionally, if you want to check how a website looked years ago, you can go to www.archive.org or to www.waybackmachine.org. Type in your preferred website URL and click on the Take Me Back button to show the selected website over a period of time.

1. Go to the www.archive.org website.

2. Enter www.hackerhighschool.org URL and click on the Take Me Back button.

3. Go to November 28, 2004, 1 snapshot 15:03:15

4. Look at the website's appearance and feel (quite different from today)

5. Click on Lessons on the website

6. Register how many were available then! And in how many languages!

7. Repeat step 4 -6 with the following date: July 26, 2011 2 snapshots 13:51:56, 13:52:08

8. Excellent, well done!

Sources of Hacktivism: Twitter Feeds

It is important to know what is going on in the hacktivist realm. To possibly be as close as possible to what is going on, stay connected to media. For instance, Anonymous is quite reliably communicating through their Twitter channel.

Checking the Anonymous Twitter Channel:

1. Connect to https://twitter.com/#!/anonops. @anonops is one of the Anonymous Twitter channels.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

2. Try to obtain the following information:
   - how many Tweets have been sent:_________
   - Who is AnonOps following:__________________
   - How many followers has AnonOps:__________
3. Browse through the tweets and see what AnonOps is tweeting.
4. Advanced tip: You are maybe able to correlate tweets to website defacements. You have learned how to use http://www.zone-h.org/ to identify website defacements. This combined with the twitter feeds let's you combine the two information resources.
5. Under the *Following* tab you will see who AnonOps is following. Mostly other Anonymous sections, the FBI, Facebook, Stratfor, Wikileaks etc. This gives you an idea what they think is relevant to follow.

Feed Your Head: Great movies about social engineering and/ or hacking

Sneakers - 1992

Most memorable quote: (Cosmo) There's a war out there, old friend. A world war! And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information!

Hackers - 1995

Most memorable quote: (Cereal Killer) We have just gotten a wake-up call from the Nintendo Generation.

The Net - 1995

Most memorable quote: (Angela) Just think about it. Our whole world is sitting there on a computer. It's in the computer, everything: your, your DMV records, your, your social security, your credit cards, your medical records. It's all right there. Everyone is stored in there. It's like this little electronic shadow on each and every one of us, just, just begging for someone to screw with, and you know what? They've done it to me, and you know what? They're gonna do it to you."

The Matrix Trilogy - The Matrix, The Matrix Reloaded, The Animatrix, or The Matrix Revolutions

Most memorable quote:

Trinity: Do you know what happened to Neo?

The Oracle: He is trapped in a place between this world and the machine world. All I can do is tell you that your friend needs your help. He needs all our help.

Neo: What is the Matrix?

Trinity: The answer is out there, Neo, and it's looking for you, and it will find you if you want it to.

Swordfish - 2001

Most memorable quote: (Gabriel) You know what the problem with Hollywood is? They make shit. and as an extra bonus!!!

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

Code Hunter - 2002

Most memorable quote:

Nick's Mom: That computer is for school only.

Nick 'Jester' Chase: It's no big deal.

Nick's Mom: No big deal until I have the FBI breaking down the door.

Nick 'Jester' Chase: That's not gonna happen.

Nick's Mom: Good, because I'll kill you.

Firewall - 2006

Most memorable quote:

Jack Stanfield: I just hacked into your accounts.

Bill Cox: That's impossible.

Jack Stanfield: You just lost twenty million. Now you know what it feels like to lose what you love.

The Social Network - 2010

Most memorable quote: (Erica Albright) You are probably going to be a very successful computer person. But you're going to go through life thinking that girls don't like you because you're a nerd. And I want you to know, from the bottom of my heart, that that won't be true. It'll be because you're an asshole.

1.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.

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

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 2012, ISECOM