Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 19
HACKING PHYSICAL SECURITY

DRAFT

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 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.

Table of Contents

Contributors

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Bob Monroe, ISECOM

Dustin Craig

Matt Sloper

ISECOM

Introduction

Physical security is an often-underestimated aspect of information security. Hacking in this realm requires a unique blend of physical skill and technical knowledge. Hackers with solid knowledge of physical security concepts and applications carry a significant edge. Physical security can be loosely defined as the application of physical controls to prevent or reduce damage and unauthorized access of physical property. These controls include; **environmental design**, **access control**, **intrusion detection** and **personnel identification**.

Reality Check:

- If you are young, you are marked as a victim. You must learn to protect yourself.
- If you are female, you are marked as a victim.
- If you are naïve, and think people will protect you, you are marked. For life.
- You take this course: you are not quite so naïve and you think ahead.
- But, the "Bad People" have more experience than you.
- You may have seen a few Bad People.
- They have seen tens or hundreds of you. They ***know*** how to exploit you.
- Physical security is a starting point. Know the area. Know yourself. Know your enemy.
- Or lose.

What is Physical Security?

Physical security is all of these and more:

- Knowing where you are, who is around you, and how they are acting.
- Fences, Gates, Lights and Barbwire
- Walls, Windows and Doors
- Locks, Keys, Keycards and Passwords
- Guards, Armaments and Dogs
- Fire Alarms and Suppression Systems
- CCTV and Motion Sensors
- Employee Identification
- Organizational Procedures
- Building Construction
- Specialized Landscaping

How does Physical Security apply to Hacking?

Let's answer this question with an example. Suppose you are a hacker for hire and your client requests that you gain access to their competitors top-secret server. If there was little or no physical security in place you might be able to walk in and use your social engineering skills to keep you hidden in plain site long enough to extract the data you need, then exit without raising any alarms.

In the above scenario the lack of physical security allows you free access to the facility and you are able to bypass the firewall, walking directly into the server room and plugging into your target machine.

Upon your return, the client finds that the data was corrupted in transport. When you return to the facility for a second time they have learned from your previous intrusion and have significantly improved their physical security. To gain access to the facility the second time you must; scale a fence, sneak past armed guards, evade CCTV monitoring and impersonate a staff member to reach the server room undetected. Welcome to the realm of physical security!

Physical Security Foundations

Probably the most iconic physical security hackers of all time are the Ninja! These mountain warriors were carved out of the tough times of feudal Japan. They had quick feet and an even quicker wit. The Ninja were often grossly outnumberd and used a variety of tricks, or hacks (if you will), to overcome their opponent, the Samurai. Samurai were armored warriors, raised, even bred, to be the Shogun's killing machines. They ruled feudal Japan with an iron fist. The Ninja, were simple farmers who got sick of the Samurai's bullying. Now, I said they were fed-up, but they weren't stupid! The Ninja knew that they could not rise up against the Samurai, and survive, so, they got thinking.

The Plan; farmer by day, Ninja by night! The Ninja disguised themselves in dark clothing and spent their evenings battling their Samurai foes. In The Art of War Sun Tzu describes three levels of winning; fighting to win, winning before the fight and winning without fighting. When a ninja decided on a target he developed strategies based on the highest level; winning without fighting.

One such example follows. The setting is a small farming village, set in the mountains of feudal Japan. The locals get word that a band of Samurai have been traveling through their mountain range, raiding nearby villages and collecting “taxes” for the Shogun. They will arrive in this small town in just five short days.

The Ninja Farmers know better than to oppose the Samurai, so they scheme, plot and plan. Ultimately, they decide to bring the fight to the Shogun. They reason that if they can mount enough of an attack on the Shogun's Palace he will recall his Samurai to protect him and will be too busy developing his defenses to bother with their little village.

A solid plan! So, a handful of Ninja set out for the Shogun's Palace! When they arrive they spend the first night quietly watching the goings-on; carefully counting the footsteps of each sentry, observing their mealtimes, waiting for the weak link to reveal itself. Hours pass before their moment of opportunity presents itself; the changing of the guard. The guard on shift in the north/east tower is a bit chatty and isn't in a big hurry to get to his next post, so he and his replacement spend a good three minutes in conversation. The Ninja see an opportunity. The second night the Ninja prepare their explosives, surrounding the palace with small long-fused bamboo cannons. The third night is THE night! The moment comes and with the Sentries distracted in conversation one Ninja scales the stone wall and plants an explosive under the Palace before escaping into the dark.

It's time. The four remaining Ninja's run through the forest igniting the cannons before they too disappear into the dark. The first explosion startles the Shogun and puts the Samurai on high alert! While the Samurai are looking inside for the sabouteur, the first set of cannon fire, and then the second, and then the third and finally the fourth! The Shogun's Palace is under attack! By the time the Samurai collect themselves and begin their defense, they are firing their cannons into an empty forest and the Ninja are on their way home.

Planning for Security

The Shoguns of today have much more than stone walls and sentries! Likewise, today's hacker's have a much more complicated task than their Ninja counterparts. Secured facilities can be protected by electrified fences, armed guards, guard dogs, CCTV and intrusion detection systems. As with anything though, you are only as strong as your weakest link. As a Hacker you will need to determine what types of physical security controls are in place and how to best avoid, or exploit them. If you know this, you will know the area, what is around you, and what people should normally do. You can blend in and become one of "them", rather than stand out and be a victim. You do not have to "be" one of "them"; you only have to look like you are one of "them", so they pass you over and go to someone. Wherever it says "hacker" below, it might be you, or it might be "them".

Diversity of Skill

Like the Ninja of feudal Japan today's Hacker's (they? You?) will spend days, if not weeks, planning an attack. The Physical Security domain requires a diverse skill and knowledge base combined with patience, physical fitness and agility. In order to be effective in the realm of physical security a hacker must be physically fit, mentally acute and have knowledge and experience in the following subject areas; psychology, electrical engineering, computer science, telecommunications, environmental design and standard security procedures.

Exercise:

1. As part of a Ninja's martial training, she would be required to know how many steps she takes between her front door and her bedroom door. This skill would come in handy when she was on a mission and needed to precisely time her enemies' movements. Today, Hacker's time movements with stop watches. Using a stop watch time yourself. How long does it take to walk to the nearest exit and back?
2. The Ninja would know to their bones how many different ways they could get into, or out of, any given place. Assume an adversary who is not authorized to be there, and who can overcome normal barriers like windows, doors, locks, guards and alarms. How many ways can someone get into your bedroom? Your home? Your school?

Site Selection and Facility Design

Site selection can be the most important implementation of physical security principles. Selecting a site that meets the facilities requirements in terms of environment, population and access is an important first step. During facility design further consideration may be given to the principles of **environmental design** and **defensible space**.

Perimeter Security

Securing the **perimeter** is a necessary first step in terms of a facility's physical security. Perimeters may be secured with: berms, fences, walls, barriers, gates, guards, guard dogs and security personnel to name a few. These may be further backed up through the application of **access control** and **intrusion detection** technologies at the perimeter.

Perimeters are enforced as part of the **defense in depth** strategy. The effectiveness of a security perimeter can be negatively impacted by poor planning during the site selection and design phases. An example may be a very large perimeter that is surrounded by a

forest where trees limbs extend to the inside beyond the perimeter fence. An agile Hacker might scale a tree to bypass this physical security perimeter. (Another one might flip a large piece of carpet over the fence and barbed wire, run up the carpet, jump over the top and land on the inside.)

Exercise:

1. Go online and research "defense in depth." How does this concept apply to physical security?
2. How might a hacker's knowledge of "defense in depth" help them to gain access to a secured facility?
3. How might a hacker's knowledge of defense in depth help them gain access to where you normally are? What means might you use to frustrate them or slow them down?

Internal Security

This refers to how well an organization is protected from attacks being implemented from within their facility. This may be a disgruntled employee or a nefarious hacker who has circumvented your physical **security perimeter** and **intrusion detection** technologies.

A physically secure organization will use multiple layers and types of **internal security** to prevent unauthorized access to critical infrastructure and data. Some of these methods, such as **intrusion detection and response**, **procedural access control** and **personnel identification** will be discussed further in later sections.

Exercise:

1. How might an organization's internal security practices impact their regular business? (If it is hard to get in, can the customers get in?)
2. What obstacles might internal security practices pose for a hacker trying to gain unauthorized access to the system?

Facilities Security

These types of security controls are typically intended to protect against property damage and personal harm. While they may be triggered in response to an attack, their purpose is not specifically related to preventing an attack. In fact, these types of security controls exist in facilities that are publicly open, such as; schools, shopping centres, malls, etc,.

We are talking about fire and explosive protections, and weather related controls placed on systems to prevent damage due to pressure, moisture, heat or extreme cold. These security features are not necessarily implemented to prevent attack; their purpose is to prevent or reduce damage to property and loss of life.

But, a knowledgeable hacker can observe, learn from and exploit these controls. For example: Where are the lights placed after dark? Are there any shadowed spots that might be used? Where is the trash taken? Might it be "dumpster dived" for information? Where are the security cameras? Are there any blind spots? If there is a fire, where are the fire extinguishers and fire hoses? Might those be used to cause internal damage? Are there storm shelters? Can they be used to shelter from an attack? Can they be used to contain an attack (can you run the attacker to ground in the shelter, preventing them from fleeing)?

Exercises:

1. Discussion Question – List facility security features that you might find in your daily life. (Home, school, mall, shopping area, transportation.)
2. What is the difference between facility security and internal security?
3. How might a Hacker exploit facility security features?

Environmental Design

Environmental design refers to physical protections that are built into facilities and landscapes as a means to prevent property damage and deter crime. The principals of **environmental design** are usually applied prior to building construction and are best included during the planning phase of development.

The key concepts in environmental design are; **natural surveillance**, **natural access control** and **territorial reinforcement**.

Environmental design includes natural protection from flood, wildfire, thunderstorms, hurricanes, tornadoes, blizzards, perhaps riots or civil unrest.

Natural surveillance: what can you see from this place? Can you see in every direction? If not, where are the blind spots? What can you do to reduce or protect from those blind spots?

Natural Access Control: Look at the old monasteries. They were difficult to reach for a reason. If they are hard to reach, invaders might avoid them. And if invaders come, they are easily defended.

Territorial reinforcement: If the attackers come, is their way easy, or hard? Are there cliffs, fences or walls to scale? Rivers, dykes, or swamps? Will their passage through the area raise alerts (pea fowl make nice alarms, as do geese).

Exercises:

1. Brainstorm. What physical security controls do you think can be built into a facility landscape?
2. Search the web for information on **natural surveillance**. How does the idea of natural surveillance differ from more other **monitoring** methods, such as, CCTV.
3. In your own words explain the principle of territorial reinforcement.
4. Describe how a Hacker might exploit the principals of environmental design to gain unauthorized access to a facility?
5. In terms of environmental design there are two distinct, yet closely related methods **Crime Prevention Through Environmental Design** and **Defensible Space**. Research them online, then discuss their differences and similarities with your friends.

Access Control

Access control is simply controlling who has access to, or can interact with, a resource. Access is controlled by an authority. The resources being controlled can be just about anything: buildings, computer networks, server rooms, cars, parking lots, or soft-drinks in a vending machine. We see access control everywhere in day-to-day life: anything with a

key, anything that accepts a password, and anything that accepts payment, are all forms of access control.

In physical security, the resources being controlled are generally physical areas: buildings or rooms, and the authority is typically concerned with people, but could also involve cars or animals. It's all about who can access what, where and when.

In order for access control to be effective, there must be a way to enforce it. This can be accomplished in two ways, using people (guards/cashier), or most commonly with devices such as locks and keys. Access will be granted by providing some kind of token, or credential, ie., a key or keycard.

Access Control Points

Access is usually controlled at specific access control points, such as entrances/exits to the building or room, but can also be at every doorway when security is very important. Usually once through the access control point the person is then considered "cleared" for the building or room they are entering. A great example of this is at the airport. After purchasing tickets people must go through an access control point where the person and their belongings are checked for threats, and then allowed into the terminal. Once the person has been checked they can roam freely within the terminal, and are considered safe until they leave.

Mechanical Access Control

Mechanical access control devices have been around for a very long time. The typical example is the lock and key. With these types of devices, access is either granted or denied, the lock is open or closed. The lock has no way of knowing who is using it; as long as the correct key is inserted anyone can open the lock. This can present some problems because it requires a physical object, which can be lost, stolen, or duplicated. Also, once you give someone a key, it is hard to revoke, he/she may be unwilling to give it up or could have made copies. Mechanical locks have also been exploited for a very long time, you might have even done it virtually in The Elder Scrolls: Skyrim, it's called lock picking!

Lock Picking

Picking a lock is a simple concept. The majority of locks are **pin tumbler** locks, they have two cylinders, one inside another, and by rotating the inner cylinder a mechanism opens the door. The door is locked because small metal pins block the cylinder from turning. When a key is inserted, the pins rise to the correct height, the cylinder is free to rotate, and the lock opens. Under ideal circumstances, ALL the pins must be set to the correct position at the same time, but due to slight defects during manufacturing, you can set pins one by one using a pick. Really cheap locks (typically found in filing cabinets, medicine cabinets, etc.) can be picked with ease using nothing more than two bobby pins.

See http://www.wikihow.com/Pick-a-Lock.

Electronic Access Control

Electronic access control gives much finer control than traditional mechanical devices. They can accept many different types of tokens and credentials, and can revoke them much more quickly and easily. Electronic devices can also be aware of who is requesting access, are able to restrict access within certain time frames, and can be aware of incorrect access attempts, which could then trigger an alarm.

Exercises:

1. What are the benefits of biometric access control?
2. How can biometric access control be defeated?
3. How does biometric access control differ from proximity card access controls?
4. How does a privilege elevation strategy act as a form of access control?

Procedural Access Control

Procedural Access Control refers to security procedures that control how employees can access critical areas and information within their organization. This physical security control prevents unauthorized individuals from accessing areas and information that are critical to the organization's business.

Procedural access control processes may include recording the information of the individual seeking access and monitoring their access to the controlled area or system. Facilities where visitors may be allowed on premises will have a procedure for recording and tracking visitors. In some cases visitors are issued security escorts to monitor their activities while on premises.

Exercise:

1. Why might an organization implement procedural access control?
2. How might an organization implement procedural access control?
3. Discuss the benefits of procedural access control from a security perspective.
4. As a hacker, how might you circumvent procedural access controls?

Credentials

Credentials are used to control who gets access, there are many types of credentials, but they can all be categorized into three main types:

1. Something you know, like a password
2. Something you have, such as a key
3. Something you are, like your fingerprint (biometrics)
4. (sometimes someone you know can be considered a factor as well, if the controller knows who you are)

Passwords can be entered onto a keypad, an RFID badge can be scanned, a magnetic strip card can be swiped, or a person's fingerprint can be read. Any type of access control point requiring one of these forms of authentication is called single factor authentication. Most credentials can be easily shared, with the exception of biometrics, so where high security is required, two factor authentication should be employed, ensuring a user must know something (password) as well as have something (a key). In this case, if the key is lost or stolen, an attacker would still need to know the password and entry would be denied.

Intrusion Detection and Response

In the days of the Samurai intrusion detection was the job of the Sentry and was prone to human error. Today intrusion detection refers to an **Intrusion Detection System** (IDS), which scan networks and monitor facilities with **CCTV** and motion detection technology.

Intrusion Detection Systems (IDS)

An IDS is a device or application that monitors a network or system for known malicious actions or policy violations. A level of sophistication has been added in this domain with the introduction of Intrusion Detection and Prevention Systems (IDPS). While an IDS simply monitors and logs events on a network, an IDPS will attempt to interrupt or otherwise prevent an attack on the network.

Exercises:

1. What is the difference between an IDS and an IDPS?
2. What are the three main types of Intrusion Detection Systems (IDS)?

CCTV and Motion Sensors

Closed Circuit Television (CCTV) is the industry standard for video surveillance monitoring. The cameras are controlled by security personnel in a Control Room where video captured by the CCTV system is displayed on monitors.

To enhance monitoring capabilities Pan-Tilt-Zoom (PTZ) cameras are used in areas where moving the camera is required. Cameras can be programmed to pan automatically, move in the direction indicated by a motion sensor or can be operated manually by security personnel.

New technology is perpetually pushing the bounds of what is possible. In recent years facial and gait recognition technology was integrated into CCTV systems. Most recently the United States Department of Defense has begun what they are calling Project Hostile Intent. The project intends to build an application that will recognize when a person is experiencing an extreme emotional reaction.

While CCTV Monitoring typically requires the presence of human security personnel, motion sensors can be used to alert the security system of a potential intruder or a stray cat.

CCTV systems sometimes have "blind spots" the cameras cannot see. The cameras are often installed in small, dark hemispherical housings; you may be able to spot them in banks or stores. Many times, the cameras are wireless; sometimes they are web-based. Wireless or web-based cameras can be exploited by tapping in to their communications. Wireless cameras can have their signals jammed.

Exercises:

1. How does motion sensor technology differ from CCTV monitoring?
2. What might be a limitation of CCTV?
3. How might a hacker exploit motion sensor technology?
4. Where have you seen CCTV or Motion sensor technology used? Is it useful at that location? Why, or why not?

Response Procedures

The most important aspect of intrusion detection is the response, but like our Samurai friends demonstrated, not just any response will do. Developing effective response procedures requires that you know what the attacker is after and can anticipate his movements. Intrusion detection can only signal that there is a problem. Each detected intrusion should trigger a response from a system or security personnel. The response could be as simple as raising an alarm or as complicated as activating mechanical locks, or even issuing a call to law enforcement.

Exercises:

1. Where do you see intrusion detection in action in your daily life?
2. What good is intrusion detection without a response plan?
3. Discuss differences between IDS and CCTV monitoring.
4. Search the web for criticisms of intrusion detection technologies.
5. How might knowing the response for an intrusion detection system or technology give a hacker an advantage?
6. How might people react if the IDS or alarm system frequently gave false alarms?

Personnel Identification

While the Shogun's Samurai were easily identifiable by their uniforms today's organizations provide employees with identification badges and user ids to uniquely identify them while they perform their duties. As you may know, computers maintain a record of who has created and modified files and directories. Organizations also maintain records of employee movements and access to privileged areas and systems.

Identification

Identification extends beyond regular staff to temporary contractors and even visitors. At a secure facility it is standard procedure to issue visitors a 'visitors badge' and an **escort**. Photo identification cards are a standard identifier that is widely used. Another form of identification is your user id which uniquely identifies you to the system and system administrators.

Exercises:

1. Discuss Personnel Identification – What is the purpose of personnel identification?
2. Discuss how personnel identification procedures strengthen an organization's physical security.
3. How might a Hacker exploit personnel identification?

Authentication

Authentication is the means by which the system identifies that *"you are who you say you are"* Your identity can be verified in one of three ways; ownership factors, knowledge factors or inherence factors.

Ownership factors refer to objects that only you should have (ie., company badge)

Knowledge factors refer to things that only you should know and this is probably the most common and most familiar form of authentication. Knowledge factors can be; passwords, PINs, or challenge questions.

Inherence factors refer to fingerprints, DNA (biometrics) or even a signature. This form of authentication is often considered the most secure.

Two-factor authentication requires that you provide two or more means of identication. A simple example of this is the bank card + PIN combination. The bank card is something you have (ownership) and the PIN is something you know (knowledge).

Exercises:

1. How might a hacker authenticate themself through exploitation of the ownership factor?
2. What is the benefit of two-factor authentication?
3. File Encryption Exercise:
   - **A** Open a terminal and create a text file
     ```
     $gedit my_text_file.txt
     ```
   - **B** Write a secret message into your text file, save it and close it.
   - **C** In the open terminal use the Gnu Privacy Guard to encrypt your file
     ```
     $gpg--force-mdc --output my_encrypted_file.gpg --symmetric
        my_text_file.txt
     Enter Passphrase:******
     Repeat Passphrase: ******
     ```
   - **D** Use gedit to view my_encrypted_file.gpg
     ```
     $gedit my_encrypted_file.gpg
     ```
   - **E** Close my_encrypted_file.gpg
   - **F** Use Gnu Privacy Guard to decrypt my_encrypted_file.gpg
     ```
     $gpg --output my_decrypted_file.txt --decrypt my_encrypted_file.gpg
     Enter Passphrase:******
     ```
   - **G** Use gedit to view my_decrypted_file.txt
     ```
     $gedit my_decrypted_file.txt
     ```
4. What type of authentication is used in the exercise above?

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