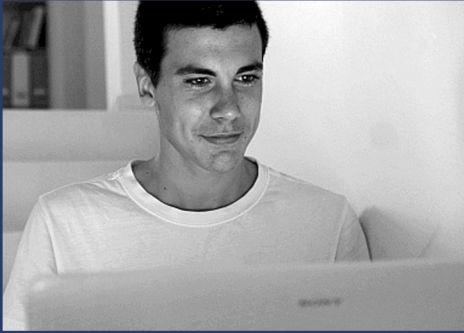


# Hacker Highschool

## SECURITY AWARENESS FOR TEENS



## LESSON 12 DEFENSIVE HACKING



HACKING IS LEARNING  
www.hackerhighschool.org

ISECOM

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG



## 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 has not been enough research on the 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 contained 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

WARNING.....	2
Introduction.....	5
Common Threats: This Week's Top Contenders!.....	6
What Do Attacks Look Like?.....	12
Attack Trees.....	12
From Trees to Logs.....	13
Like Tears in the Rain.....	15
Go Phish.....	16
Game On: Bad Computer, No Cookie for You.....	18
Attack Monitoring.....	20
Feed Your Head: SOC and Roll.....	20
SOC Mission.....	22
Lessons from the Trenches: The Social Virus.....	22
Why Be a SOC Analyst?.....	22
Bucket List.....	23
Lessons from the Trenches: Shame Game.....	24
Team Work!.....	24
Lessons from the Trenches: Chatbot.....	25
Mountain Dew Overload.....	25
Your Tool Shed:.....	26
Cuckoo Clock.....	26
Ollydbg is a Horrible Name for a Sandwich.....	27
Wiresharknado.....	27
Mimikatz and Dogs.....	27
PowerShell, Bash, Terminal, vi and Command Prompt.....	27
May the X-Force Be With You.....	28
Who's Your Data? Splunk Is.....	28
Watson You Say.....	29
Security Analysis as a Sport.....	30
Walk in My Shoes, err Socks (Day in the Life).....	30
Making Good Security Analysis.....	31
How to Start Doing Cybersecurity Analysis.....	34
Feed Your Head: Thinking Like the Enemy.....	37
Where Security Falls Short.....	39
Game On: Bad Computer, No Cookie for You, Part 2.....	40
Getting the Help You Need.....	42
News & Opinion.....	43
Reddit.....	43
Blogs.....	44
Useful Things.....	44
Organizations.....	44
Other Resources.....	44
Conclusion.....	45



## Contributors

---

Pete Herzog, ISECOM  
Bob Monroe, ISECOM  
Marta Barceló, ISECOM  
Chris Griffin, ISECOM  
Cor Rosielle, ISECOM  
Michael Menefee, ISECOM  
Nigel Hedges, ISECOM  
Marco Ivaldi, ISECOM  
Mike Wenzel, ISECOM  
Cassy Lalan, IBM  
Heather Ricciuto, IBM  
Stephen E. Keim, IBM  
Chelsea Balch, IBM  
Adam L Griffin, IBM  
Darren Lawless, IBM  
Jonathan Crowe, Barkly  
Craig Hand, Ziffen



## Introduction

---

Everyone has something that somebody else wants.

Maybe you don't have a fancy car or a big bank account, but there's probably someone around you who wants those cool shoes you've got, or that sparkly phone, or your jet black laptop bag- with the laptop inside.

It's no different in the cyber world.

Maybe you think it won't be a big deal to lose fifty dollars worth of your preferred cryptocurrency, but what about everything else that's on-line? Maybe someone empties your bank account- that's bad. Maybe someone uses your bank account to apply for a credit card in your name- now money that you didn't even have has been stolen from you and your credit history is trashed.

What about your media? Don't you have a cloud full of music and movies that you've paid for? What if someone steals your user ID? Now someone else has your music and movies.

What about your personality? You've spent years growing your followers. What happens when someone hacks your account and posts nothing but pictures of toe fungus? What happens if your account becomes a stream of limericks written in iambic pentameter? Your online personality that you worked so hard to not look like you worked hard on is now gone.

And what about your secrets? You think you're safe from malware just because you don't have any money to steal? You've got secrets. Do you want everyone to read those dark, moody poems you keep on Google Docs? Do you want your parents going through your Netflix history and seeing that you watched that snail documentary six times? Do you want your friends to learn about your nostalgic fondness for Kidz Bop songs?

We all have secrets, and thousands of our secrets are up on the Internet. We think these secrets are secure because we have PINs and passwords but, just as we become more accustomed to regularly using these, other people become accustomed to stealing them. Every day there are data breaches, financial information leakages, and thefts of personal data. The media calls them hackers, but we know they're criminals.

During the last eleven lessons, we've covered a wide range of topics on security and network fundamentals. Now it's time we wrap all that up into a lesson on how to defend yourself. No, not ninja stuff. This is Defensive Hacking, where you learn how to protect your digital environment as only a hacker can.

The first step: don't focus on threats. The media will offer up a new danger every week, maybe even every day, but you can't think about your security as being a frantic subscription to the 'Virus of the Month' club. You'll wind up chasing your tail, or worse, biting off a chunk.

Instead of looking at threats, look at your assets and protect them. Assets can be hardware like printers, servers, routers, and smart phones, or assets can be data and information like those poems of yours. Even the way that your data interacts with your hardware should be considered an asset. You can't control threats from others but you should be able to control your assets.

The second step: start asking questions. Criminals don't play by any set of rules, so you need to think differently. You're not here to learn how to be a criminal, but you need to learn to ask the questions that the criminals will ask.

For example:

- Can the fax function on an All-in-One printer be used to take over a server?
- Can a simple Powershell script open up a connection from your home network to the outside?



- Can an email user use their email account to gain system administrator rights?

You're not going to do these things- but the criminal looking to steal your information is, so you need to know what the answers to these questions are.

In this lesson, we will be looking at what types of attacks you can expect to see and what they might look like. You will be introduced to defensive hacking tools and given basic instructions on how to use them. We will also look at ways to make your computer and network more secure and at ways to reduce your overall visibility on the Internet.

And, understanding that your biggest asset is you, we will also be looking at the human aspects of defensive hacking: social engineering.

The things you will learn in this lesson (deconstructing threats, deconstructing security controls, and deconstructing an attack) will not only make your environment safer but also put you in a prime spot to work in cybersecurity. So we'll make sure you go through the same exercises and use the same tools as a professional SOC analyst (that's SOC as in "Security Operations Center" not as in SOCK "to collect foot sweat").

Let's turn up the music and get learning.

## **Common Threats: This Week's Top Contenders!**

As we said, you can't focus on the threats, but you've got to be familiar with them. That means knowing what they're called and what they actually do. This way you can be that obnoxious person at the party that says, "That's not a virus, it's a worm." And that's totally the kind of party we all want to be at!

The following threats and attacks are popular now, and knowing about them will give you a good start at making yourself more secure, but, remember, this week's top hit might be tomorrow's one hit wonder, so an attack that is common today, may be rare overall.

Here, in no particular order, is a sample of the most common threats along with a brief description of a defensive position needed for each:

### **Phishing**

Phishing is an attempt to compromise a system or steal information by tricking a user into responding to a malicious message. The most common phishing attacks involve emails containing links to infected websites or malware hidden in attachments, although phishing can be conducted via voicemail, text messages, and social media, too. Phishers can take over legitimate email accounts or spoof email addresses to make it look like messages are coming from a trusted source. And some phishing attacks, known as "spear phishing" attacks, can be extremely well-targeted and will look just like emails from your tech-clueless neighbor or nosy cousin. And they'll read just like them too. That's why the best of these attacks don't provide any red flags at all. They are *that* good.

First line of defense: *Trust no one*. If your sister, who only ever sends you memes over social media, sends you an email with a link to the cutest cat picture ever, think before you click. When you hover the cursor over the link in an email, you should see the URL for the link. If the link doesn't make sense in any way, don't click on it. And, if your cousin sends you a surprise attachment, *don't open it*. People rarely send unexpected attachments. If you weren't expecting an attachment from someone, then you should assume that it is dangerous. Send a text or walk over to them and confirm that it's a valid file.

### **Social Engineering**

There are two ways to steal anything — you either take it yourself or you get someone else to give it to you. Social engineering is a broad umbrella term for any tactics designed to

exploit and manipulate trust so the victim hands the attacker what they want. Think fake customer service calls designed to reset passwords or a criminal spoofing your email address and convincing your friend to send money. And they will likely fall for it.

Evidence shows that everyone — repeat, everyone — can be conned, defrauded, fooled, or manipulated. Being vulnerable can sometimes come down to a lack of training or experience, but more often it will simply come down to distraction and mental fatigue. So the best defense against social engineering is to relax. Don't take on more than you can handle or let someone's emergency become your stress. And the biggest cause of social fatigue, which I'm sure you don't want to hear, is socializing. That's right. Chatting, posting, texting, talking, gossiping, and everything like that will tax your brain like you wouldn't believe! Socializing is the mind killer and primary distraction of all humans. So when you need to be careful and vigilant, which is pretty much always, don't socialize at the same time.

## Ransomware

This is malicious software designed to encrypt a victim's files and then demand payment, generally in "anonymous" Bitcoin, in exchange for unlocking the files. As with other malware infections, ransomware attacks typically start with employees falling victim to phishing emails or visiting compromised websites. Unlike other malware infections, however, the primary goal of ransomware isn't to gain stealth and persistence for long periods of time. Instead, its priority is to spread as quickly as possible, encrypt as much data as possible, then actively alert victims of its presence.

```
-.+_|$**.._
.$--$||-_$=
$_.=|+|=
```

**!!! IMPORTANT INFORMATION !!!!**

All of your files are encrypted with RSA-2048 and AES-128 ciphers.  
 More information about the RSA and AES can be found here:  
[http://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))  
[http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.  
 To receive your private key follow one of the links:

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [g46mbrzpfzsonuk.onion/G89R3DIQEJJIUAXZ](https://g46mbrzpfzsonuk.onion/G89R3DIQEJJIUAXZ)
4. Follow the instructions on the site.

**!!! Your personal identification ID: G89R3DIQEJJIUAXZ !!!**

```
_=-*_*-|_~+
-$~|++-*
```

Ransomware will lock up any drive the infected user has access to, including connected USB drives and network shares. Once files are encrypted, the only way to regain access to them is to a) have a reliable, up-to-date backup; b) hope a security researcher has cracked the encryption and made a decryption tool available; or c) hold your nose and pay the ransom. Paying up is anything but a sure thing, because, well, ransomware authors are criminals. Being dishonest is what they do. They're also occasionally less than



spectacular at coding, so there's also the risk of paying the ransom only to find your files were accidentally destroyed or rendered unrecoverable.

One reason ransomware is hard to protect against is because it's built to turn a strength (making files easily accessible) into a weakness. Additionally, with ransomware developing into a billion-dollar industry, there's plenty of incentive for criminals to continue investing in delivery and evasion tactics to keep their business model humming. That means they can change faster than your signature-based security solutions can keep up.

The best way to protect yourself from ransomware is to require authentication to access anything at any time. Of course, that's a pain to do so the next best thing is to use the process of "whitelisting" to permit only trusted applications access to your system. Another option is to use software that detects and blocks any use of encryption in order to stop the ransomware in its tracks, but this is far from foolproof. Or you can buy a commercial security product, cross your fingers, and hope that it will catch everything. Easy, but the least effective option. You have hopefully noticed an important trend in security – generally, the less painful something is the less effective it is. Regardless of the option you choose, it is always wise to keep regular backups of your important data outside of your computer or network.

### Drive-by Downloads / Download Hijacking

In nature, the big predators hang out at common water holes and wait for their prey to come by. On the Internet, the big predators find ways to turn popular website visits into covert attacks. In some cases, they inject code through comments that force unsuspecting visitors to automatically download malware. In other cases, they've compromised the web server and injected malicious code into seemingly legitimate downloads. Another trick is to utilize exploit kits, programs designed to actively probe the website's visitors' browsers for vulnerabilities so they can take advantage of them when they show up and infect their systems.

Not only do attackers have the element of surprise in these situations, they also have a collection of tricks to make sure they're successful. If you update your browser, they'll update their code. If you patch a vulnerability, they'll move on to a new one. It's also not as if we're talking about strictly sketchy websites. Some of the web's most popular sites (The New York Times, the BBC, AOL, the MSN homepage) have been compromised in the past. And you usually can't expect to stop visiting websites altogether. That's what makes this attack so effective.

The best way to defend against these kinds of attacks is to make sure you have a small attack surface. The fewer plugins, applications, and devices you have active, the less likely an enemy will have something to attack you with. Make sure your system does not have a direct connection to the Internet and that your applications are separated from the operating system either through whitelisting or sandboxing. Some browser add-ons have things like Flash, which has been a dangerous attack vector for many years. Enabling Click-to-play settings keeps certain content inactive until you click it to view it, protecting you from content running without your knowledge. You may think just keeping your software up-to-date and running AntiVirus is enough, but it's not. Those are things you do for added security, not for security itself. Just like rubber boots are something you wear for added protection against the rain- but they don't make you rainproof.

### Malvertising

Marketers aren't the only ones who like to utilize advertising to get in front of the crowds of website visitors. Criminals do the same thing, inserting malicious code into ads so they can quite literally capture their audience. This code they insert can do many things, but it's most common that they try to steal passwords saved in cookies or hijack things open in other tabs on the browser. But that's not all as they can actively attack with full-on malware and take over your system.





Online advertising is already incredibly prevalent, and chances are it's only going to grow more aggressive. At the same time, people are also becoming increasingly used to ads, including pop-ups, etc. and they're no longer viewed with as much mistrust. In terms of protection, the quick knee-jerk reaction is to use ad-blocker software. Unfortunately, many websites don't work unless you deactivate it. And if you have to choose between using an ad-blocker and the best of Fail videos...

Currently the only way to defend against these attacks is sandboxing or whitelisting components of your web browser. But getting people to do that is hard, so an alternative is to make sure people use different browsers for different activities like banking, shopping, and surfing, and not just different tabs in the same browser. And while good, this unfortunately still won't help against malicious ads that, if clicked from a smartphone, subscribe you to "premium services" (for which you usually pay weekly!). Disabling such premium services should be handled through your mobile provider.

## Zero-Day Attack

Traditionally, a zero-day refers to any undisclosed vulnerability that attackers can exploit before victims become aware of it and have the chance to patch it. The term "zero-day attack" is also sometimes more broadly applied to attacks that utilize new tactics, exploits, or malware variants that haven't been seen before, giving them an advantage over people who rely on crystals, dream catchers, and signature-based security software to stay secure.

It's difficult to protect yourself against something you've never encountered before, especially if it blindsides you because you didn't see it coming. Signature-based security solutions are particularly susceptible to getting bypassed by zero-day attacks since the way they identify malicious files is by matching them to a list of previously captured malware samples. If an attack is using a never-before-seen exploit or piece of malware, there's a good chance it's going to claim a victim.

The best defense against zero days, once again, is a reduced attack surface. If you have less that can be attacked then you have less zero-days that will be valid for your systems and services. While you can separate and harden systems on your network, this gets much harder when gadgets (a la IoT, the Internet of Things) and mobile multi-devices, like smartphones, add dynamic, interactive areas into your network and increase your attack surface in ways you have no idea about. This leaves you with really only two options: continuous monitoring for changes or creating a hostile environment in your network for anything that's not already there. Usually the go-to option for most is the first one since intrusion detection software, honeypots, and SIEMs are so prevalent today. But the second option is actually better despite being more work to build because it requires much less maintenance over the long term.

## Password Cracking

A login and password form isn't what most people think it is. It's actually a complicated set of processes that can involve multiple systems, secure transport to and from the servers, a trusted network of server identity assurance and revocation, code to evaluate the complexity of the user-generated password, more code to make sure the person entering the code is indeed a human, a secondary factor of authentication, and a means to sign-up to start with and later recover lost passwords. So password cracking is more than just running a program to guess the password — it's about cracking the password process to take over a user's account.

Any system that allows users to access it from anywhere and also requires those users to make, safeguard, and remember their own passwords is a system that's going to be difficult (if not impossible) to defend. According to what OSSTMM researchers refer to as the "Somebody Sequence," the more interaction somebody has in the security process, the greater its attack surface. Asking people to manage their own passwords is like giving



them full control over the keys to an important lock. You can make sure it's one of the strongest locks money can buy, but how secure can it ultimately be if there are keys for it floating around everywhere?

The ways people currently protect against password cracking is by making harder passwords and adding more steps to the process like limiting the number of guessing attempts that can be made at once. But as we said, passwords are a sequence of events, a process, and not just a thing you remember and type in. So the password you know is just one part of that greater process. Securing that whole process requires breaking it down so you know what each sequence is and does and securing it in layers. How, you ask? There's no way you actually asked that. You probably asked, what do you mean? For each part of the process, see if you can take the human out of the process. For example:

Human In the Sequence	Human Out of the Sequence
Person makes passphrase	Computer generates passphrase or gives a digital certificate
Person types in password to website	Computer with password manager submits password or digital certificate only to pre-authorized websites
Person requests forgotten password	Computer with password manager doesn't forget this stuff. Or else computer with password manager requests a password change.
Person carries a card with a table of numbers to add to the password as part of 2-factor authentication.	Person carries a smartphone that generates a unique code used for 2-factor authentication.

When it comes to security, the Somebody Sequence is important because we know just how we can start building better security to manage specific types of threats.

### Distributed Denial of Service Attack (DDoS)

There's really only so many packets a computer system can process before it starts to slow down and queues build up. By gaining control over a large number of hijacked systems and devices (referred to as a botnet), attackers can direct all these systems to send a continuous stream of packets to a single target all at once, with the intention of knocking it offline. This is the closest a cyber attack will ever get to a physical attack since the packets here are literally forcing an overload on the system.

The larger the botnet, the more damage a DDoS attack can do. Recent record-breaking attacks have leveraged a botnet estimated to be comprised of over 150,000 hijacked video cameras and IoT devices, capable of launching attacks of 1.1 terabits per second. The best you can do to prevent an attack is be subscribed to an anti-DDoS service that can reduce the flood. But if it's anything approaching that level of magnitude, there's little hope even they'll be able to handle the flood. The truth is that there is no free defense against DDoS and what you pay for defense can only help you to a certain level of flooding.

To make matters worse, sometimes attackers will contact their targets ahead of time and threaten to knock them offline unless "protection money" is paid up front. It can be difficult to discern whether such threats are real or are simply scams, and — as is the case with ransomware — giving in to criminal extortion demands never comes with a guarantee.



## Scareware

You've probably seen the pop-ups — "Warning! A virus has been detected on your computer. Download VirusBlaster to clean and remove it." That's scareware. The malware that really infects your computer is the program that warning is trying to trick you into downloading. Scareware can come in a variety of forms from fake antivirus programs to fake browsers or OS updates.

We know that social engineering works because it preys on the distracted and mentally fatigued. Combine that with fear and thus begins the "good intentions" downward spiral that leads people to make really bad decisions. Once scareware gets inside the system, it has all the privileges, passwords, and logins of the employee who installed it. Getting it out may be as easy as just wiping the system and starting fresh or recovering from backup. Or it may be more difficult and time-consuming if the malware spreads to other systems.

Protecting yourself from scareware starts with not overreacting to fear. Can we be tricked into thinking we have a virus? Sure, it happens all the time. Many hackers who play and test software tend to get paranoid when the disk drive starts grinding for no apparent reason and immediately power off. Then they boot with another disk and start to look for malware. No scareware even necessary! That seems like overreacting but it's not- it's a little paranoid but the process is right- something's funny then power down and investigate that disk from another system or booted disk. Overreacting is downloading some strange software and installing it. That's where fear makes stupid. So if you get scared, follow protocol and not random Internet advice.

## SQL Injection

While it is unlike all the user-based attacks previously covered in the list, we include this here because it's such a common attack that it wouldn't be a list of common attacks if it wasn't here. But really as a user, there's nothing you can do to protect yourself from it since the attacks are against the servers you use and not your own computer.

SQL injection is when a website has an input box or entry form (like when you're entering in your username and password, or your credit card number if you're buying something) into which an attacker can try inserting structured query language (SQL) code to gain access to or make changes to the stored data. SQL injection exploits a trust between the web application and its database to let the attacker do pretty much whatever it wants with the database. If all you can think of is "delete data" then you're underestimating the depths to which a criminal can stoop.

Besides adding, removing, and changing data, and in addition to stealing info like client credit card numbers and health records, there's also the possibility of inserting malicious code to be passed back to users when they use the form, instead of the data they're looking for. Once criminals start using that tactic they can abuse popular websites to do their dirty work for them like distributing drive-by downloads, building a botnet army, even hijacking DNS requests to send visitors to malicious versions of the websites they know to collect even more info (aka "Your credit card failed please try another and another"). If the login form is vulnerable, SQL injection can even help with password cracking by bypassing the login altogether.

Any place where a user can input information into a website with a database, it has the potential to be SQL injectable, which unfortunately makes it a widespread problem. It's not like you can just remove all user-input interactions from your website and still get any purchases or feedback.

Protecting against SQL injection is all about input and output sanitation on the server side. That means that any characters or types of requests that are not valid for answering the question, the reason of the input, should be removed or changed before they even reach the database. The most effective way of doing that is using prepared statements with parameterized queries (a mouthful!) in the development of the app. That basically means



the app can tell the difference between a command and the data that's being input so it can't be fooled by injection. Remember, when you are putting a trust interaction between two systems you control and the strangers on the Internet then you better control what they're sending and receiving because you can't trust them to always have good intentions.

### Exercises

- 12.1 Nowhere in this list did we just say "virus" or "worm". They aren't among the top 10 for a reason. It's because they are actually a tactic to increase the success of an attack. It's something that's used to deliver an attack. Of this list of 10, which could use a virus or a worm as a tactic to improve attack success?
- 12.2 Malvertising is a very specific thing. However, if the advertisement doesn't deliver malware, could it still be dangerous? How else can an advertisement be "weaponized" to harm rather than just inform? Try to think out of the cybersecurity box for a moment.
- 12.3 This is just a sample of the numerous types of threats out there. Yes we were being facetious by saying "This Week's" because some of these threats have been around for years. So describe one that we didn't cover and explain what they are and how to defend against it.

### What Do Attacks Look Like?

I know you're asking yourself this. And if this was a book on martial arts self defense we could show you pictures of a person in a ski mask mugging a person in a dark alley. Or you could just watch any Batman movie. But this is different. This is about packets that are invisible to the eye and attackers who are deliberately trying to be sneaky using obfuscated code. The point is that it's not that easy to show you attacks in action.

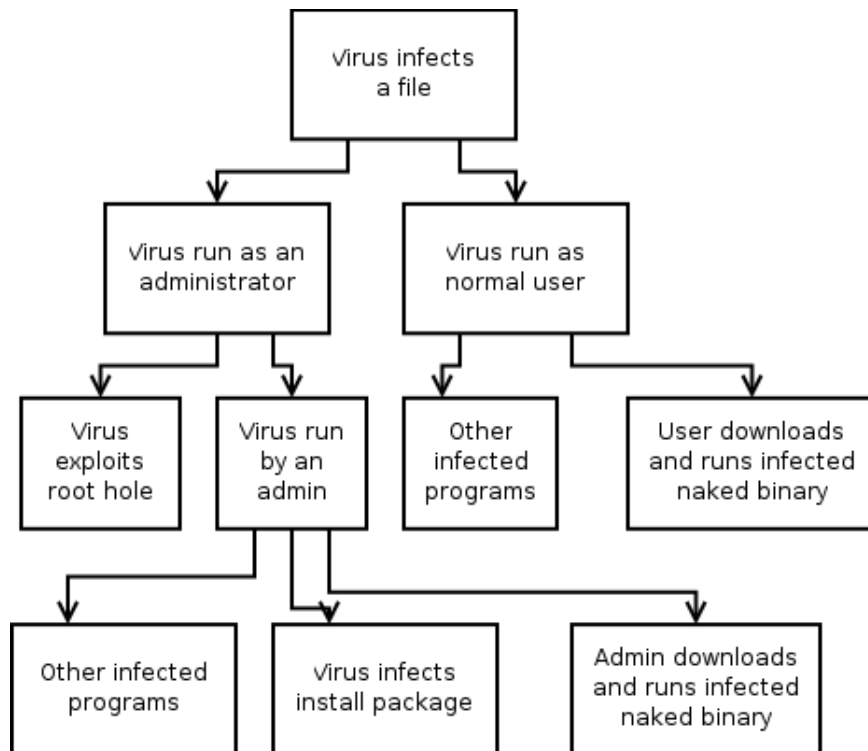
If anything, you're more likely to recognize an attack AFTER it happened. And if it was sneaky and successful, you may never see it. But if it was malicious, you may notice the hard drive working harder than normal, a large increase in network traffic, or even the computer randomly crashing. That's not fun!

So let's talk about a few of the ways that security analysts work with attacks as they're happening.

### Attack Trees

We pretty much know what you visualized: a slim oak with a katana gripped tightly in one leafy branch and a semi-automatic in another. Okay, well if you didn't, you have now!

What you need to know about them is that many security practitioners use attack trees (also sometimes called threat trees) to help determine where vulnerabilities might be in a system. However, a security analyst may use attack trees as a guide for determining possibilities of actions and reactions based on the types of threat. Sort of like trying to visualize a puzzle by connecting the clues. By graphically diagramming a flow chart of causes and possible effects, a security analyst can both see how the attack went down as well as determine where they have holes in their defenses.



## Exercises

- 12.4 Ransomware is one of the most common types of attack now. There's been many of them and they all have names. Research three of them and explain what they are, what they do, and how they work. If you find any interesting facts about them, like maybe the decryption key that people paid for didn't work or it was designed by someone in Florida, throw that in too!
- 12.5 When we look at attacks we really only see the representations of the packets passing through the network unless the attack is successful and then we also see the damage. Get online and discover what is the latest malware that's going around. Now diagram that malware into an attack tree to show what it does.
- 12.6 Is portscanning an attack? Why or why not? Can it be diagrammed into an attack tree? Try it!

## From Trees to Logs

Realtime log analysis is exactly as fun as it sounds. YMMV. But it's a way to see attacks roll out as they happen. Many times this is integrated into a SIEM and you will be at a SOC where it's correlated instead of just a raw file like below. So take a look at this log file from the Hacker Highschool webserver:

```

193.201.224.186 - - [02/Nov/2015:05:28:22 -0500] "GET
/wp-content/plugins/akismet/akismet.js HTTP/1.1" 404 5355 "-" "Go 1.1 package
http"
193.201.224.186 - - [02/Nov/2015:05:28:23 -0500] "GET
/wp-content/themes/classic/rtl.css HTTP/1.1" 404 5355 "-" "Go 1.1 package http"
193.201.224.186 - - [02/Nov/2015:05:28:23 -0500] "GET
/wp-content/themes/twentyeleven/readme.txt HTTP/1.1" 404 5355 "-" "Go 1.1 package
http"
193.201.224.186 - - [02/Nov/2015:05:28:23 -0500] "GET
/wp-content/themes/twentyten/style.css HTTP/1.1" 404 5355 "-" "Go 1.1 package
http"
212-51-138-149.fiber7.init7.net - - [02/Nov/2015:05:28:23 -0500] "GET /books.html
HTTP/1.1" 200 7962 "http://hackerhighschool.org/getting-started.html"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11) AppleWebKit/601.1.56 (KHTML, like
Gecko) Version/9.0 Safari/601.1.56"
193.201.224.186 - - [02/Nov/2015:05:28:23 -0500] "GET
/wp-includes/css/buttons.css HTTP/1.1" 404 5355 "-" "Go 1.1 package http"
193.201.224.186 - - [02/Nov/2015:05:28:23 -0500] "GET
/wp-includes/js/scriptaculous/wp-scriptaculous.js HTTP/1.1" 404 5355 "-" "Go 1.1
package http"

```

What can you figure out in there? Well, you should see the IP Address at the start, the date and time of the requests, what was requested, what version of HTTP was used, the result of the request, and then the HTTP client user agent. But you should know that by now. So what makes this an attack? There's 2 big hints. Take a moment to look and figure it out before you read on.

Okay, so you can't wait to know? The first may not be obvious, but as a security analyst you would have done it- look at the website [hackerhighschool.org](http://hackerhighschool.org) and see what it's made of. It's NOT Wordpress yet all those "wp-" requests are asking for Wordpress pages. So it's clearly a scan looking for something to attack. You can see we don't use Wordpress because all those responses in the log saying 404 are really just saying "nothing like that here!". The second big hint is that the user agent is "Go 1.1 package http". That's not a regular browser.

## Exercises

- 12.7 Do a little online research and explain why this attacker is searching for Wordpress.
- 12.8 Since you're still so curious, what is the user agent "Go 1.1 package http" and why does it show up here?
- 12.9 Is every line in that web log above an attack or is there legitimate traffic in there? If so, what is it and why?



## Like Tears in the Rain

If you've spent enough time looking at packet captures, you'll have probably seen more attacks than you can count. And not because you failed counting in first grade but then again, that might have contributed to it. It's just that you've seen them and maybe not known they were attacks. The truth is that it's a case of "unless you know something's wrong and are looking for it, you'll never realize what exactly you're supposed to be looking for."

For example, take a look at this pretty little capture:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:50:54:7c:eb:3d	00:50:54:7c:eb:3d	LOOP	60	Reply
2	10.000279	00:50:54:7c:eb:3d	00:50:54:7c:eb:3d	LOOP	60	Reply
3	20.000798	00:50:54:7c:eb:3d	00:50:54:7c:eb:3d	LOOP	60	Reply
4	30.061149	00:50:54:7c:eb:3d	00:50:54:7c:eb:3d	LOOP	60	Reply
5	30.069467	00:50:54:7c:eb:3d	01:00:0c:ccc:cc:cc	CDP	333	Device ID: gramirez-isdn.tivoli.com Port ID: Ethernet0
6	30.292923	10.0.0.6	151.164.1.8	DNS	78	Standard query 0x7d9e A picard.uthscsa.edu
7	30.612811	151.164.1.8	10.0.0.6	DNS	289	Standard query response 0x7d9e A picard.uthscsa.edu A 129.111.30.27 NS ke...
8	30.614993	10.1.1.1	129.111.30.27	IPv4	70	Fragmented IP protocol (proto=UDP 17, off=0, ID=00f2) [Reassembled in #9]
9	30.615348	10.1.1.1	129.111.30.27	UDP	38	31915 → 20197 [BAD UDP LENGTH 36 > IP PAYLOAD LENGTH] Len=28
10	35.285494	00:40:33:d9:7c:fd	00:00:39:cf:d9:cd	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
11	36.285487	00:40:33:d9:7c:fd	00:00:39:cf:d9:cd	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
12	37.285485	00:40:33:d9:7c:fd	00:00:39:cf:d9:cd	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
13	38.285500	00:40:33:d9:7c:fd	ff:ff:ff:ff:ff:ff	ARP	42	Who has 10.0.0.254? Tell 10.0.0.6
14	38.287366	00:00:39:cf:d9:cd	00:40:33:d9:7c:fd	ARP	60	10.0.0.254 is at 00:00:39:cf:d9:cd
15	40.061851	00:50:54:7c:eb:3d	00:50:54:7c:eb:3d	LOOP	60	Reply
16	47.973426	10.0.0.6	10.0.0.254	ICMP	98	Echo (ping) request id=0xc41b, seq=0/0, ttl=64 (reply in 17)
17	47.977697	10.0.0.254	10.0.0.6	ICMP	98	Echo (ping) reply id=0xc41b, seq=0/0, ttl=255 (request in 16)

... 0101 = Header Length: 20 bytes (5)  
 ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 56  
 Identification: 0x00f2 (242)  
 ▷ Flags: 0x01 (More Fragments)  
 Fragment offset: 0  
 Time to live: 64  
 Protocol: UDP (17)  
 Header checksum: 0xaf37 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 10.1.1.1  
 Destination: 129.111.30.27  
 [Source GeoIP: Unknown]  
 [Destination GeoIP: Unknown]  
 Reassembled IPv4 in frame: 9

```

0000 00 00 39 cf d9 cd 00 40 33 d9 7c fd 08 00 45 00  .9...@3]...E.
0010 00 38 00 f2 20 00 40 11 af 37 0a 01 01 81 6f  .8...@.7.....
0020 1e 1b 7c ab 4e e5 00 24 00 00 00 00 00 00 00  .|.N.$.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040 00 00 00 00 00 00  .....
    
```

## Exercises

- 12.10 What you're looking at here is a Teardrop attack recorded by Wireshark. Take a moment to investigate what that is exactly and describe it in your own words full of that technical detail you like to use.
- 12.11 Now that you know what a Teardrop attack is, where, as in which line number in the packet capture, is it happening? How is Wireshark here showing it?
- 12.12 With your best artistry line-drawing skills, draw out what the attack would look like. Make sure it's understandable-- no Dali artwork here please, packet traces are surrealistic enough on their own!

### Go Phish

There's tools and then there's tools. Qradar is one of those professional tools that makes a security analyst's job almost easy (it's never completely easy when you're working with your eyes full of tears of joy that you get working in cybersecurity). So here's an attack seen through a super analysis tool. It will help you visualize attacks but you still need to have some imagination. For example:

Now there's an attack in there. Actually, there's more than one:

The screenshot shows the IBM QRadar Security Intelligence interface. The main content is a table of network activity logs. The table has the following columns: Content\_Subject (custom), SMTP HELO (custom), Originating\_User (custom), Recipient\_Users (custom), Content\_Type (custom), File\_Hash (custom), File\_Name (custom), and File\_Cus. The data rows show a pattern of emails from 'Jyn Erso' to 'cassianandor@gmail.com' with subject lines like 'Secret Plans'. The file hashes and names are also visible for each entry.

Content_Subject (custom)	SMTP HELO (custom)	Originating_User (custom)	Recipient_Users (custom)	Content_Type (custom)	File_Hash (custom)	File_Name (custom)	File_Cus
Secret Plans	cveairh1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	cveairh1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	cverogu1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	cverogu1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	rhadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	rhadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	chadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	2mtrwide	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	2mtrwide	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	cveairh1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	cveairh1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	cverogu1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	rhadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	rhadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	chadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	chadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Secret Plans	2mtrwide	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	2mtrwide	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	cveairh1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	cveairh1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	cverogu1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/html	82fbd8305...	body_content	462
Secret Plans	cverogu1	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448
Secret Plans	rhadwin7	"Jyn Erso " <jynerso@ca.outlook.com>	<cassianandor@gmail.com>	text/plain	e0e1b4da0...	0.txt	1448

### Exercises

12.13 Just by using your keen analysis skills, describe what you are looking at in the above image. Be specific.

12.14 Keep using that finely honed analysis engine in your head and describe what kinds of attacks could be delivered in this way. There's no wrong answers here because you're using your imagination to complement your analysis skills. However, there are still stupid answers so don't give any of those.

Now if your keen analytical skills fail you, and you have no idea where the attack is hidden above, then you should know that Qradar does know where it is. It knows because it follows rules and patterns that expert security analysts have set to help beginner security analysts get it right. Those rules look like this:





There are many rules by default in there which is why this is such a helpful analysis tool. And you're thinking, "Well, if all the rules are there why do I need to learn any of this?" and "Won't all security analysis jobs be taken over by robots eventually anyway?" and maybe "Where's my left sock?" but that last one might just be some of you. The thing is, because there's ALWAYS a thing, how do you think those rules got there?

## Exercises

12.15 How do those rules get there?

You know that there's a near infinite number of ways an attack can happen, don't you? No? Well, if you didn't, let us tell you that there's a near infinite number of ways an attack can happen. Well, not infinite. But from off-the-cuff calculations on a napkin, it turns out for a small business network of about 15 computers there's about  $10^{120}$  different ways. Yes, we used a really big napkin. Actually it was the tablecloth. But that's not what's important. What's important is that there are many more ways an attack can play out on a small business network than there are hydrogen atoms in the observable universe. Yes, atoms. Count them if you don't believe us. That means that no number of rules you can write will cover all the types of attacks, especially new attacks that haven't been seen yet. That's why you need to know how to analyze security too because, as great as the tools are, they'll always need more rules made. And as you use them, you'll be the one eventually custom making rules too!

There's another thing too. The up side. When you have an analysis tool that complements your abilities as a security analyst and does the heavy lifting for you- things like counting flows, tracking sessions, and correlating interactions across a huge number of IP addresses- then you can focus on making sure incident response gets handled and are free to investigate the more tricky stuff coming in. Eventually, you'll be writing rules for it too.



For now though, while you're training to be an expert security analyst, having a system that can break it down for you like this is a great way to learn while doing:

The screenshot shows the IBM QRadar Security Intelligence dashboard. The main content area displays details for 'Offense 267 (Summary)'. The interface includes a navigation menu on the left with options like 'My Offenses', 'All Offenses', and 'By Category'. The main view shows a summary table for the offense, including its magnitude, domain, description, source and destination IP addresses, and duration. Below this is an 'Offense Source Summary' table and a 'Last 5 Notes' section which currently shows 'No results were returned.' The system time is 7:21 PM.

Magnitude	[Progress Bar]			Status		Relevance	5	Severity	7	Credibility	3	
Domain	Default Domain											
Description	Potential Spam/Phishing Subject Detected from Multiple Sending Servers					Offense Type	Source IP					
Source IP(s)	10.40.40.105 (10.40.40.105)					Event/Flow count	5 events and 46 flows in 2 categories					
Destination IP(s)	54.165.58.142					Start	Oct 15, 2016, 11:49:09 AM					
Network(s)	other					Duration	7h 30m 36s					
						Assigned to	Unassigned					

Offense Source Summary			
IP	10.40.40.105	Location	Server_Network_Personnel_Records
Magnitude	[Progress Bar]	Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	10.40.40.105	Weight	0
Offenses	2	Events/Flows	58

Last 5 Notes		
Notes	Username	Creation Date
No results were returned.		

There are many, many more tools that the security analyst can and will use daily. This is just a sample. The most important take-away here is to realize that nobody does all this analysis in their hands. There's a lot of data, a lot of ideas to follow up on, and a lot of trails to follow so don't think you need to do it without analysis tools.



### Game On: Bad Computer, No Cookie for You

These are the kind of days that worry Jace the most: nothing happened. Her morning alarm clock went off at the right time. The bus was on schedule (and she had the correct change). School was uneventful. The weather seemed pleasant for a town located on the outskirts of an industrial complex. "Don't expect birds to be chirping on your shoulder, this ain't no fantasy movie," she reminded herself. Jace always kept her coffee brown hair tucked to the right to cover her face. After years of hiding her looks, she was pretty good at accepting the occasional stray hair that either got caught in her eye or between her lips.

The public bus pulled away from the curb and, instead of the usual lungs filled with



exhaust, the wind blew the black and gray pollution away from Jace. She noticed little details like that and those types of things bothered her. "Maybe it's my lucky day, yeah, right," she muttered to herself as she tilted her head up to get a better view of her neighborhood before heading up to the apartment she stayed at with Sweet G. A red robin flew past Jace from left to right, almost running into her, singing as it dashed off between the cars on the dirty street.

If Jace owned a pistol, she would have pulled it out from sheer fright. Luckily, guns were illegal in her country. The bird and all the normalcy began to spook the teen. She pivoted on her left sneaker near a tall bush next to her building and took two steps towards the back of the bush. The apartment complex wall had a tiny path between the exterior wall and the bushes. Jace paced herself, moving up and down as she use the foliage to hide herself from the action on the street.

As quietly as she could, Jace moved up the six sets of stairs to arrive on the third floor of her apartment complex. The teen looked up the hallway to the fourth door (her apartment), but everything still seemed perfectly fine. No key was needed to enter the small two-bedroom place she shared with her grandmother. Jace yelled out, "Hi, I'm home," in the direction she guessed her grandmother might be in. The teen turned the corner and entered her domain, her room. Reflexes caused her to kick off her shoes, toss down her backpack, slide across her bed, and hit the power button on her computer all in one smooth action.

It was the end to an odd day so her stomach told her to switch gears and head to the kitchen. Jace had made it within three steps of the kitchen counter before she realized something was wrong. It was a sound. Jace turned to face her bedroom, confused. "Was that...was that the Windows Logon sound," she asked herself. The slim teen crept to see that her computer was at the Windows Logon prompt. A chill went down her spine since her computer was set to boot to Linux first. Her computer could only run Windows if it was selected at bootup since Linux was the primary operating system. Jace placed her hand on the top of her computer and felt its warmth. Her computer had been running already. Something was very wrong with her system.

Jace reached down and performed a hard reboot of her computer by holding down the power button for several seconds. The computer screen did not respond. She thought through all the basic possibilities for this type of error and none of them looked good in her mind. Her next step was to reach around the back of the computer to see if anything else was plugged into ports, like a USB keylogger or a forgotten bootable USB drive. Her DVD drive was empty as well.

Unsure of herself, she physically pulled the electrical power cord from the outlet to the computer. The computer shut off. The teen bit her lip and worked her mind through possible options. Was she under attack? Did she have malware? Did some part of her computer break? Had the RAM gone bad? Maybe part of her hard drive was corrupt?

The front door opened with a blast of warm air and the delightful smell of Sweet G's perfume. "Honey, I'm back. How was school today," her grandmother asked as she entered the apartment and headed towards the kitchen. Jace poked her head out from behind her door and responded, "Have you seen anything going on with my computer lately?"

Her grandmother had her back towards the granddaughter since she was busy unloading some milk and vegetables in the kitchen. Sweet G replied, "No your computer has been quiet, or at least I think it has been quiet. How was your day?" A wide smile greeted Jace as her roommate turned to face her. "Is everything alright," Sweet G asked, a bit concerned by the look on Jace's face. The two of them always got along great even if grandma's dementia caused Jace to repeat herself several times or hear the same story twice in one meal.

Jace started to explain, "Well my computer was already on when I got home a few minutes ago. And it was running a different operating system than I normally use." The



teen looked at her grandmother for an answer or some insight. Sweet G just replied, "I'm sorry to hear about your computer troubles. Does it have anything to do with that package?"

Eyes wide, Jace asked, "What package?"

Her grandmother reached for the last few items from shopping that needed to be put away and said, "The small package that came for you the other day. I put it in your room next to your computer. I thought I told you about the box. There wasn't any address on it so I thought it must have been some computer device you bought online."

Jace's throat grew tight, "You put an unknown package next to my computer and forgot to tell me!" As angry as the teen was, she had to remind herself that it wasn't her grandmother's fault. She had a disease eating parts of her brain away. The computer geek asked, "Can you show me where this package is?"

Sweet G pointed to where she had put the package but it had fallen onto the floor. Jace pulled out her phone and turned on her WiFi scanner. The scanner would look for WiFi signals to identify them but not connect to them.

"There it is", Jace almost shouted.

"Do you see the box, dear," her grandmother asked, still looking around the small room for the box.

Jace responded, "No, not the package but I see two WiFi signals that are new and one Bluetooth signal. One signal is an access point but the other has a hidden identification. I don't understand what this Bluetooth signal is though."

**Game continues...**

## Attack Monitoring

Now if you want a front-row seat into seeing attacks happen then you want to get to the SOC early. A Security Operations Center, better known as the SOC, is an amazing and challenging environment. The center itself is a combination between an emergency room (with rapid response needed to save networks and data), a police detective's desk (where you are solving crimes by piecing together clues you need to discover), and an auto mechanics repair shop (with all kinds of equipment that require different fixes to get them working again). Luckily, there isn't nearly as much blood, grease, bullets, or paperwork in a SOC as there is in these other occupations. You can expect to get your mind stretched out though.

## Feed Your Head: SOC and Roll

The people who work in a SOC and do all the heavy lifting, like responding to incidents, are the SOC Analysts. And they do quite a bit more than incident response even though most of the work involves fifteen minute to one-hour long event situations. Those events can be malware dissection, hacking research, attack forensics, and real-time defense. An analyst works collaboratively with a team and the customer to pick out anomalies that occur across a cloud of data. Everyone in the SOC has a role to play.

This lesson essentially covers what a SOC Analyst is, does, and can become. We cover



the physical nature and the mission of the SOC. What makes a SOC a SOC. We talk about the events you'll encounter as a SOC Analyst and what it means to work in that world. We also discuss the technology aspects of your job and how you use the tools available to you in order to be successful. We make a big deal out of the SOC because, in defensive hacking, it is the most critical field to be in.

This job isn't for everyone. It needs people who can think quickly, be inquisitive, pay attention to the slightest detail, and be able to communicate with others. When an event (network abnormal behavior) happens, you will be expected to tell a story about that event from beginning to end. This requires analytical skills as well as interpersonal traits. But don't consider this lesson as a recruitment tool because we are going to tell you the cold hard truth about what it takes to be good SOC Analyst as well as the competitive environment you will be working in.

A high school graduate can work as an entry-level SOC Analyst and build their skills to move up the ranks. Security analysis is a skill, and a tough one to master, but if you're dedicated and like figuring stuff out like this then you can get really good, really quickly.

According to global labor statistics, 80% of jobs available do not require a college degree. Being a SOC Analyst is one of those jobs that does not mandate any degree, certification, or technical college background. You just have to know a bit about security and be trainable. Most of the people who work in this market started off as system administrators, call center help desk employees, web designers, programmers, or even students right out of high school.

Many people in this career field are self-taught. Having the drive to learn on your own has huge advantages in the cybersecurity world. Since the field of security is so large, there are unlimited topics that you can learn about. When it comes time to interview for a job, however, some people tend to underestimate their knowledge and capabilities. These folks feel like impostors because they don't have a bunch of initials after their name or a degree from a college.

As long as you can communicate, are a bit tech savvy, are able to investigate, and are willing to learn, then you are the perfect person for being a SOC Analyst. Nobody expects you to know everything. Don't feel out of place just because you don't know the answer to a question. There is an entire team working at the SOC to help each other out.

There is nothing wrong with being self-taught. In many cases it means you have a passion and motivation for cybersecurity far beyond most other professionals in this field. In 2016, LinkedIn analyzed over two million member profiles to determine which soft skills (non technical) are most in demand. The researchers found that the main skills that employers are looking for in potential employees are communication, organization, teamwork, punctuality, critical thinking, social skills, creativity, adaptability, and a friendly personality. Most of these skills are part of your personality. Luckily, cybersecurity professionals have never been known for their interpersonal communications or friendly personality so neither of these skill shortfalls should count against you if you are already passionate about technology.

So if you like a challenge and working with some of the smartest people on the planet, then pay attention to the SOC elements in this lesson.



## SOC Mission

A mission statement is usually one or two sentences that tell others why that business is a business. These are brief but powerful ideas that underlie the reason for a company to exist. Since a company is considered a living entity, you could say the mission statement is the purpose for its life. A SOC will have a mission as well. This mission supports the overall concept for the company.

Some SOCs provide their services for hire to other companies. Other SOCs are specific to one entity such as the military or government. Each SOC has unique capabilities, culture, processes, terminology, and most importantly, different people. The strength of a SOC or even a company is through its people, the employees. Everyone works together to accomplish the mission.

Yeah, you'll have that 30% of employees who don't seem to do anything all day. Then, you'll have that 30% who are the overachievers. The last 40% make up a range of different personalities, from management, to suck ups, to overlooked workers, to those with pure genius flowing through their veins.

SOCs tend to be made up of high achievers and those with genius exhaled with every sentence they speak. You'll be learning from those people for the first couple of years in the SOC. Your knowledge base will expand to unknown limits unlike any other job you may have had before.

### Lessons from the Trenches: The Social Virus

Cor Rosielle tells this story:

One morning a virus suddenly spread through the company like wild fire. The reason was an e-mail claiming to have a naked picture of a woman and had attachment called `annakournikova.jpg`. I think nearly everyone in the company tried to look. But what they saw was not Anna. If you watched carefully you could see the VBS-script in action. In those days your PC was not held for ransom like it is today, instead it sent a copy of the e-mail to all the contacts in the victim's address book. That's how it spread. Well, we got this outbreak under control pretty soon by deleting it off the mail servers. But since it was an incident, the HR department requested a list of all the people who opened the attachment to send them an e-mail with some threat or warning or something. Gathering this information, I noticed that one of the names was a member of my SOC team. I took him to the side and told him that I was disappointed about this. I told him that I expect some such behavior from end users but he should have been much smarter. After all, as a domain admin, he simply had to act more wisely and responsible. He assured me it wouldn't happen again.

Until that afternoon at least, when he couldn't resist trying to take a peek at `shakira.jpg.vbs`.

### Why Be a SOC Analyst?

Wherever you are in your security career, a great move to increase your value and knowledge is to work in a Security Operations Center (SOC). There aren't many jobs out there that are as diverse and challenging as a SOC Analyst. The money isn't bad either. As a SOC Analyst, you will be working across dozens of different cybersecurity specialty fields. Depending on where you work, you may be eligible for a security clearance. The security



clearance and experience you gain as a SOC Analyst will launch your career into whatever direction you choose.

You may have read some of the job postings looking for a SOC Analyst and thought you didn't have any of the skills the job description asked for. Maybe you were intimidated. Most job postings ask for too many skills for any normal human to have. Even a post looking for a sanitation worker will sound like they are looking for Hercules on amphetamines with a high IQ. The key to any job placement is knowing what you can and can't do.

As a SOC analyst, you will be facing challenges such as network intrusion and breaches that will require you being able to identify and evaluate the various approaches to solving the problem.

Imagine you are inside the SOC and you are sitting at your console. The software detects an anomaly in a file attachment sent to one of your network customers. You receive the file and sandbox it. Virus Total (VT) doesn't seem to have this listed as a known malware nor do other research organizations. You decide against reverse engineering this file to save some time. Opening Cuckoo, you ask the program to analyze the abnormal file.

Cuckoo shows you the processes that the file executes when it is activated. This file makes a couple GET requests and attempts to disable any anti-virus software running. One of the GET requests downloads a DLL file and unpacks a larger file within the program. You're intrigued by this new malware so you dig deeper. Cuckoo shows you two web sites that are built into the package, both are known to VT as a previously identified malware site. The file was compiled two days ago according to the sandbox. That explains why the anti-virus software didn't detect it.

The payload activates Winsock which gives the payload networking capabilities. The network request contacts a distribution point for a known malware. The hash value matches a known malware that has already been reverse engineered. It's a year-old program that sneaks into the network and sets up a connection to a command and control communication point. Luckily, everything happens inside that sandbox so Cuckoo can record every action the file makes.

If that doesn't sound cool to you maybe you are perfectly happy sitting in your parent's basement playing Doom all day. There is nothing wrong with that except for the cobwebs growing under your armpits. A SOC Analyst comes across all kinds of events like this each day. Some situations involve breaches, attacks, malware, insider threats or other anomalies.

## Bucket List

As a SOC Analyst you can think of your job as being charged with watching over a large bucket filled with blocks. Each block is something of value. One block might be gold, while the next block could be intellectual property. Other blocks could be financial information or inventory data for all the equipment owned by the company who handed you the bucket. The bucket itself is made of maybe plastic or steel. The bucket is sturdy but there are holes in the material at the molecular, atomic, and quantum level.

Your job is to protect the contents of that bucket. Unauthorized people want access to items in that bucket so they'll try all kinds of ways to gain access inside the container. Some may poke tiny holes in the bucket from outside while others will attempt to trick blocks in the bucket into opening holes for them from the inside.

It is up to you to block each unauthorized attempt and investigate how successful holes were created. If an outsider (or insider) gains access to any of the block in the bucket, you need to stop the event from getting worse, protect the block, and repair the hole. You will have the best tools available to you including an entire team of experts to assist you as you work to protect each block in the container. Your view of the bucket will be at the



quantum level all the way up to the human eye level so you can scale up or down as needed to see everything that happens in and around your container.

Every breach, attack, malware threat, insider hazard will be called an “event.” You are part of a team that stops these events and investigates anomalies so they can be communicated to other bucket holders around the world. Each day you need to be creative, resilient, and technically proficient to keep up with the evolving world. There is nothing repetitive or boring about this line of work. You will be pitted against some of the smartest people in the world on a daily basis.

### Lessons from the Trenches: Shame Game

Mike Menefee tells this story:

We were monitoring web browser usage using some algorithms we wrote to catch things like online gaming, which back then were considered more of a problem than they are now. Anyways, we caught a high-level manager playing online games during office hours, lots of them, hours upon hours a day. So I forged an email that made it look like it came from some new automated system we put in place, figuring he would be ashamed enough to stop and never mention it. Well that dude stormed up to the SOC and literally yelled at us at the top of his lungs for having put such systems in place. He said what we did was inappropriate. We were young and SOC employees really had no power in the company back then so we had no idea how to respond. Now I know a thousand different things I should have told him. Still bugs me to this day.

### Team Work!

Almost every job out there advertises teamwork as part of the job requirements. You won't find many jobs that ask for an employee to work from a hidden remote cave high in the mountains. The commute would be killer, plus how would you get inner office mail delivered? The annual office holiday party would be really weird, too. SOC Analysts typically sit at a console with several monitors around them. As events occur, the analysts work on that event with the support and assistance of a team.

Each person on the team has particular skills that help the team as a whole to work on the events. Maybe Jamal is really good at reverse engineering. Ingrid is terrific at network protocols. Tori excels at packet interpretation. Junta specializes in attack vectors and has an awesome Deathmatch set up at his house. Each person contributes to solving and protecting data in the SOC. You can expect to learn from each of these people and others you will be working with. Your own skills will add to the team tremendously as you mature in your position.

With the help of the team you will be able to figure out the following:

- Is this a new event, a related event, or an event that has already been identified (why reinvent the wheel)?
- What level of severity is the event?
- Who should be working to analyze and investigate this event (prioritization)?
- How much time and resources should be given to this event?

Job qualifications vary for each company but most are looking for an intelligent person who can communicate and is trainable. Employment posting will cite requirements for an





entry level position that rival the requirements needed to run an entire country. The reality is that a SOC Analyst should have technical experience such as networking, database design, web servers, programming languages, domain administration, or even basic computer science. The non-technical skills needed are communication (oral and written with the ability to take a situation and create a story about that event), analytical skills, data collection, critical thinking, ability to snoop around corners to see what you might find (working by a playbook but also knowing when to dig around on your own), and problem solving.

The most valuable employee is anyone with a passion for security. Those of you who are totally geeked out with technology are perfect fits for this type of work. You could be into video games or scripting but your true love is learning about technology. There are many of us out there so you are not alone. Your entire team will be made up of similar people who love a challenge.

Most of your work will be aided by automation technology (Artificial Intelligence, Machine Learning, event log auditors, Intrusion Detection Systems and so forth). Even with all these cool tools, your brain (gray matter) will be the most powerful resource available to the team. Your work shifts will be made up of long segments of routine operations punctuated by sudden bursts of crisis management (kinda like combat). Your work shift can move between the two different environments several times in a day.

### Lessons from the Trenches: Chatbot

Chris Griffin tells this story:

While working in a global SOC we were monitoring and collecting traffic at all our offices around the world including Botnet traffic over IRC. Well, apparently a high-ranking company executive in Germany also used the same channel to chat and tell her contact about her very private weekend. Well, we didn't translate it, we just put it in the report as "botnet" evidence. Which then made its way to Germany. Needless to say we had to turn off chat collection after that and our boss almost got canned (but that wouldn't have been so bad either).

### Mountain Dew Overload

Working as a SOC Analyst means you'll be doing respectable work that would even make your own mother proud. The pay is great, the job is a challenge, the benefits are very nice, and you'll be learning from many experts in their field. The SOC runs 24 hours a day, 7 days a week. This means you'll be part of shift work. Some organizations run 8 hour shifts, other run 10, and a few operate on 12 hour shifts. The places that run 12 hour shifts will have you working 3 days on and 3 days off so you won't be chained to your desk. Your shifts will rotate every couple of weeks or months.

The days of cramming down caffeine-laced drinks to stay awake are over with. Your body may go into withdrawals once you stop chugging the energy drinks, but at least you'll be much healthier. SOC Analysts sit in a semi-private pod with one to three monitors in front of them. Each analyst is surrounded by the best tools and smartest people available. No more windowless dark dungeons located in the basement. Modern SOC's allow for better collaboration and more openness among team members. Some SOC facilities even have windows to look outside.

The key to success is collaboration. It's not in school where you are put in a group for a project and only two people actually do the work for the whole team. In the real world,



you'll be expected to contribute your opinion, expertise, insight, wisdom or at least get the meeting room ready. Every person on your team will expect you to know your part. There are no "free passes" here.

Luckily, security professionals are much better at sharing information than they have been in the past. You'll have access to millions of documents, research papers, blogs, Twitter posts, and global alerts. Unless you really want to (or you are working an evening shift), you won't be spending all-nighters trying to fix a problem. You may even have the advantage of using cognitive skills to assist you. We'll talk more about that later.

## Your Tool Shed:

---

As with any trade craft, there is no one tool for all the different jobs you'll be doing. You could be using Cuckoo to dissect malware. Next, you might find Ollydbg useful for reverse engineering some code thrown in your network. Wireshark is great for capturing and analyzing data packets. Or maybe you'll just create your own tools. We'll talk about each tool in just a second. One of the most critical aspects of your job will be to know the capabilities and limitations of the tools you use.

Do not become overly reliant on any one tool. Do not use a tool for the first time on a live network. That is a good way to become the topic of lunchroom discussion or causing a meeting with your supervisor. You may be familiar with tool sets like Kali or Metasploit but the tools in those kits are kids play compared to what you'll be using in some SOCs.

Expect to using tools for asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and security identity and event management (SIEM)/security analytics. SIEM sounds like a cool word, huh. You were in a dark alley late at night when 12 SIEMs came out of nowhere and tried to steal your Jello pudding. Oh sorry, got a little carried away there. SIEM just means identifying an event and then managing that event. You will find that security folks like to use fancy words for simple things. As a SOC analyst, you'll be working with all kinds of tools.

## Cuckoo Clock

Like all our lessons, we usually only talk about free open source software (FOSS). Free stuff is good, plus there is an active community that works on these tools to make them better. You can read the source code yourself to see what the tool does, unlike proprietary software. Cuckoo is an example of FOSS.

The program sets up a sandbox environment where you can run any file you want inside of it safely. The file cannot escape and infect your system. The next thing Cuckoo does is it watches and reports what that file tries to do. These are broken down into stages. If the file tries to call up APIs or DLLs, that is recorded and reported to you. If the file attempts to make a network access request, that too is identified and reported. Certain malware will try to install its own network tools in an attempt to contact the file's mothership (command and control server). Cuckoo identifies this action, stops it and reports the behavior. The best part of Cuckoo is that it is modular so you can customize the tool for your environment as well as add your own scripts to make Cuckoo even more powerful.

You can find Cuckoo here:

```
git clone git://github.com/cuckoosandbox/cuckoo.git
```



## Ollydbg is a Horrible Name for a Sandwich

You know a tool is old when it says it can run from a floppy disk. Just because a tool is old doesn't mean it should be discarded, though. Sometimes you need a simple disassembler. In case you're wondering what a disassembler is, it's a tool use for debugging programs but also can be used to see how a program was written if you don't have the source code. This is very useful for reverse engineering DLLs, APIs, malware, system calls, constants & strings, and most importantly, analyzing software.

Ollydbg was last update in 2014 and runs at 32 bit. What it lacks in fancy graphics it makes up for in ease of use. The program was written with Windows in mind. This is one of many different disassemblers available out there but it is one of the oldies and goodies for binary code analysis.

Ollydbg is freely available at: <http://www.ollydbg.de/>

Since we're on the topic, another debugger you may want to try is x64dbg at: <http://x64dbg.com/>

## Wiresharknado

Let's be blunt here for a moment. If you don't know what Wireshark is, then perhaps you are in the wrong field. Much like Nmap, Wireshark is a primary tool for every security geek out there. The USB drive in your pocket must have Wireshark and Nmap already loaded on it. If it's not there then it must be loaded onto your rooted Android phone.

Okay, okay, for those of you who have been hiding in a cave their whole lives, Wireshark is a network protocol analyzer. It is THE network protocol packet analyzer. There are others out there but none match the power (and free cost) of Wireshark. The best part about this tool is there are plenty of free tutorials available to teach you how it works.

Wireshark can be located at:

<https://www.wireshark.org/#download>

## Mimikatz and Dogs

Most folks know that Windows stores passwords and those passwords are not in plain text. What few people understand is that Windows is a huge memory hog so tricks have been created to make the OS faster. One of the tricks is to store commonly used passwords in memory for quick retrieval. This is how Mimikatz is able to recover common passwords in Windows.

It's not a bad idea to run Mimikatz on your machines to see if your systems are storing passwords that can be recovered using this free software. Both Mimikatz v1 and v2 are integrated into Metasploit's Meterpreter (use of the "kiwi" extension is recommended over the older "mimikatz" extension).

Mimikatz v2 is located at: <https://github.com/gentilkiwi/mimikatz>

## PowerShell, Bash, Terminal, vi and Command Prompt

Ready for some earth shattering news? Apple computers have a Unix shell inside the operating system. Yup, People complain about the lack of customization on all Apple products but hidden deep in the underbelly is a terminal ready to run some (not all) bash functions. Of course, this is nothing new to all you Linux users since the terminal is where



you get all the real work done. GUI is nice but the power of any operating system is inside the terminal or command line.

Windows users will want to get comfortable with the command prompt and PowerShell. The command prompt has as much use as the iOS terminal but the PowerShell is where Microsoft keeps the heavy guns. PowerShell commands are very difficult to disable because they are pretty high up on the food chain for execution authority. It almost has the same level of power as the kernel does in Linux.

Vi is a Linux terminal text editor but trying to figure out how to shut it down is worthy of a PhD in astrophysics (hint: type “:q”). There are plenty of other text editors available such as DASH, Notepad, Nano, and even some can be program editors like KATE, Gedit and jedit. The importance of all these types of tools are their ability to debug, change functions, view source code and execute commands at root level (in some cases).

Just make sure you back up your files before you start changing anything.

### May the X-Force Be With You

Sometimes you need a bit of help from others. Maybe your DVD drive stopped working or you can't connect to a URL with .IO in the name, or it could just be you have a huge problem that only super experts from IBM can help to solve. You can think of X-Force as all purpose collection, repository, information booth, and open source intelligence network that happens to deliver critical information right to your email box. Sounds cool, right? Plus, it's free.

This web site will send you information about the newest malware, botnets, vulnerabilities, forum dialogs, and all the high level security issues we work with every day. Some of the data is pulled/vetted by IBM's Watson which means when someone asks you about a particular problem that was on the nightly news, you'll have all the insider knowledge about that event and what is being done to fix the issue. It will make you look really smart.

IBM offers a web dashboard where you can customize your notifications, drill down into events, cross-reference code that may have been used from another attack, or just provide you with a remedy so your network doesn't fall prey to that critical problem.

IBM X-Force Exchange is located at: <https://exchange.xforce.ibmcloud.com>

### Exercises

12.16 So let's see if you have what it takes to research like a security analyst: what is the difference between the RFC for Ethernet (802.1) and WiFi (802.11)? Good luck because there is no RFC for either, since both are hardware standards covered under IEEE.

12.17 Here's another: in a networked machine, what is port 0 used for?

12.18 And another: what is ARP? Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. So then what is ARP spoofing and why does it matter?

### Who's Your Data? Splunk Is

Never mind the funny name, in 2003 Splunk was created for one purpose: to make sense of machine generated log data. There is a ton of log data flowing across networks. From a

security perspective, it would be impossible to view all the event logs or firewall logs without the assistance of filters, algorithms, and machine learning. We already talked about artificial intelligence looking at unstructured data; machine learning looks at structured data. Log files are structured data while Twitter comments are unstructured because logs are easy for computers to understand, while natural language used in Tweets is very hard for a computer to figure out, OMG.

Machine Learning can examine the information much quicker, and with a greater degree of accuracy, than a human can. Imagine having to sift through millions of these event logs each day! Computers are much better at repetitive tasks like this because it is structured data. Programs like Splunk are designed to inspect large volumes of data and provide the user with the specific information they request.



As you can see in *the data above*, a computer has a difficult time understanding the grammar, poor punctuation, and incredible humor in Chuuch's transportation issues. Just try to categorize it and you come up with several labels that might fit this Tweet such as "Humor", "Tragedy", "Music", "Rap", "Cool Grandmas". Splunk would come in handy with structured data but not so much with unstructured.

As a SOC Analyst, you'll need plenty of help with all the log files that you will be dealing with. Once Splunk processes and extracts the relevant data from sensors, websites, applications, firewalls, routers, network devices and so forth, you will be able to easily locate where and what the problems are. The program is able to pull data from multiple systems as the events occur. This is probably the biggest selling point for using Splunk or QRadar. It is better to know what is happening as it happens rather than after it happens. You will often hear this term called "Real-Time" because it sounds cool.

Like QRadar, Splunk can use input data from a variety of sources and formats. Although it doesn't compare directly, Splunk is often associated with ELK or SumoLogic for capabilities. ELK is nice because it is entirely open source and easy to customize but event notifications can be a bit difficult to implement versus Splunk or QRadar. SumoLogic is entirely cloud-based which means your data has to go some other place to be analyzed. Both Splunk and QRadar can be built entirely within your own network if needed.

## Watson You Say

IBM provides the Qradar Suite which can work with the Watson Artificial Intelligence (AI) to assist in sniffing out all the threats as well as giving you accurate analysis for proper courses of action. Even with the enormous power of those tools, you'll still be working hard to safeguard hundreds of networks as part of a SOC team. Since 80% of a SOC Analyst job is performing research, Watson can help out by reviewing millions of resources for you. That way, this tool can help predict the next stage of a malware attack or which nodes will be affected if a certain router is turned off.



## Security Analysis as a Sport

The beginning of your shift usually starts with a briefing from the outgoing analyst that covers current activities like breaches, malware attacks, insider threats, network anomalies, and issues that are under investigation. The briefing could be either in crisis mode or casual mode depending on the events. The ideal briefing is to have the previous shift's situational update under casual circumstances but that isn't always possible due to network activities. Kinda like it's better to catch an attacker before they get into the network, but that isn't always the case.

### Walk in My Shoes, err Socks (Day in the Life)

Your role in the SOC will depend on what information you are given from the outgoing team. Don't worry, as you gain experience you will be given more responsibility and more information. The team leader should assign you a starting point for that shift. With large networks, there is too much information to just jump in so you need to have an entry point to begin your work. You may have to use your tools to scan the event logs for areas of the network that need attention. This is where the intrusion detection systems and cognitive security programs can help based on the information provided by the outgoing analyst.

If the network is currently under attack, you'll work as a team to develop the case file (or incident report), remediate the attack, gather evidence for forensic collection, and work to keep the assets secure. This could include rerouting compromised machines, blocking segments of that network, moving to other protocols in an attempt to stop the attack from spreading, and other tactical maneuvers which will allow your clients to continue their work uninterrupted. Once the attack is controlled, the investigative team will sort through the data to answer questions about data damage, who is responsible, how the attack can be prevented in the future, and if law enforcement needs to be contacted.

It isn't very often that you'll see an entirely new attack or new malware. Much of the time you'll be seeing the same type of intrusion event just conducted in a slightly different way. X-Force Exchange and other places are used for Indicators of Compromise (IoCs) that will allow you to determine if that event is an actual attack or just a false positive. QRadar advisor can investigate every IoC for you so you won't be tied up chasing down each event. One of the first things QRadar does is group events into an "Offense" so it reduces the number of single events an analyst need to work on.

An Offense is given a priority based on the organization's own policy, risk assessment, asset value, and other criteria. Just like anything else, you'll want to work on the highest priority items first.



IBM QRadar Security Intelligence

admin Help Messages IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Watson User Analytics System Time: 5:42 PM

Offenses

All Offenses > Offense 776 (Summary)

Offense 776 Summary Display Events Connections Flows View Attack Path Actions Print

Magnitude		Status		Relev...	0	Seve...	10	Cred...	4
Description	Potential WCry Detected	Offense Type	Source IP						
		Event/Flow Count	72 Events and 654 Flows in 8 Categories						
Source IP(s)	192.168.0.136 (192.168.0.136)	Start	May 25, 2017, 1:27:03 AM						
Destination...	Local (8) Remote (4)	Duration	2m 27s						
Network(s)	Multiple (3)	Assigned To	Unassigned						

Offense Source Summary

Username	charles_britt		
MAC Address	Unknown NIC	Hostname	Unknown
Last Known ...	Unknown	Last Known Machine	Unknown
Last Known ...	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	24	Events/Flows	726

As you can see in this image, Offenses shows 72 different events under QRadar. Anything with 72 events is a high priority, even more so since these events are identified as possible ransomware “WannaCry”. The QRadar dashboard seen here allows you, as a SOC Analyst, to find high priority issues and drill down to see more information about each event.

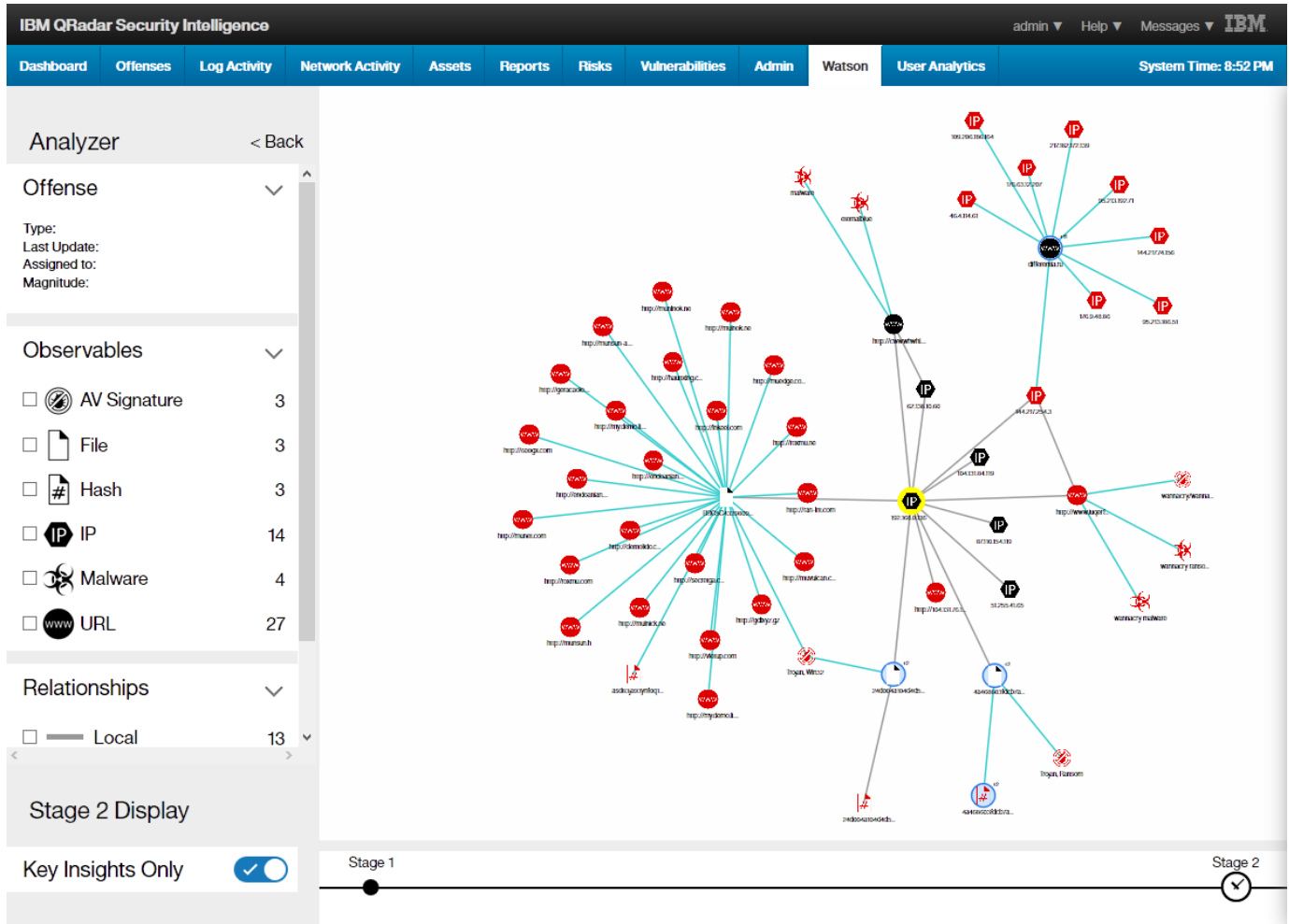
Both QRadar and Watson provide you with a tremendous amount of information which saves you research time and allows you to make decisions based on the SOC Playbook (How to Handle Every Situation). The Playbooks are established rules and procedures that cover how incidents are managed. It would be nice if somebody wrote a playbook for life, but at least you have them for your work so you don't have to guess how to remediate a situation.

QRadar even sets up templates for form letters that might need to be sent out to clients, law enforcement, or government compliance entities for reporting that incident within the mandatory reporting time. This is very handy because you won't be filing out letters, just filling in the blanks according to the Playbook for that Offense.

80% of your day is spent performing research. Believe it or not, Google is a very useful tool for locating information on incidents. Don't always believe what you read on Google but it is a great reference place to start with.

### Making Good Security Analysis

With all the tools available to you, your most valuable one will still be that gray blob between your ears (not ear wax, your brain). Tools can do all kinds of work for you, but they can't think for you. That is your critical task: to think. Whether the SOC is using rabbits with pocket calculators or multi-million dollar super computers, they can easily be misconfigured. Firewalls, routers, Intrusion Detection Systems, rogue wireless detection programs, or any similar device has to be set up correctly and maintained.



Companies know this and they're trying really hard to close the gap with tools like Watson, shown above. The truth is there's a lot of computers out there to secure and not enough of you to go around.

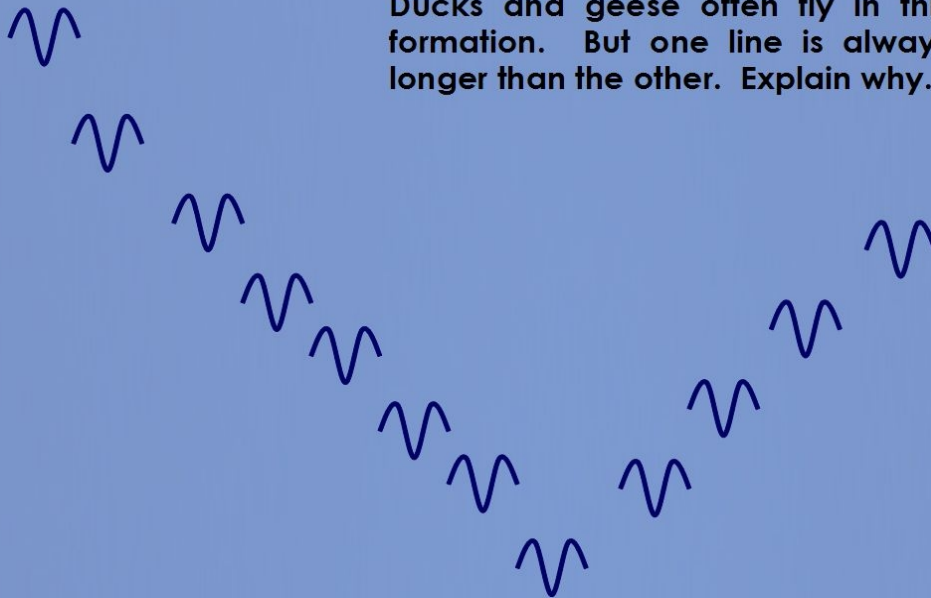
So it's not uncommon for a SOC to have piles of security products stacked up in a closet somewhere, unused because somebody else thought it would be a great idea to buy that product. A SOC runs on a budget like everything else out there. Unlike most company assets, a SOC doesn't produce income but instead protects those assets that do produce for the company. This is a business concept called "Return on Investment" or ROI. SOCs don't have ROIs but they can handle APTs by IDSes using SIEM ASAP. Not every place you work will have a war room with three monitors per person. Not every place you work will listen to your ideas on how to remediate a potential threat either. You may come across the same issue week after week but no matter what, do your job.





## Quiz

Ducks and geese often fly in this formation. But one line is always longer than the other. Explain why.



5



Copyright 2013, ISECOM. Any information contained within this document may not be modified or sold without the express consent of ISECOM. [www.isecom.org](http://www.isecom.org) – [www.opsa.org](http://www.opsa.org)



The above slide is a popular one in analysis classes. Created by Pete Herzog, it challenges the analyst to answer the question despite having limited knowledge or experience in geese and duck migration. This slide exemplifies everything hard with security analysis because the answer is so easy. The problem isn't the answer, it's the question. Asking the wrong question will get you a perfectly correct, but perfectly useless answer. Which is why they make jokes about it:

*An attack takes down the web server. An office worker notices there's no response and calls IT support.*

*So the IT support guy goes to the server room. He sees the power is on and all the network cables look okay. He goes to the keyboard to login and sees there's no shell. Nothing. Where's the Operating System? He thinks they got hacked.*

*So he freaks out and calls the Security Operations Center, "We got hacked! The web server is dead. What do I do?"*

*The SOC Analyst answers, "Don't panic, I can help you. First, shouldn't we make sure it's really dead?"*

*The IT Support guy puts down the phone and then some loud smashing is heard. Back on the phone, the IT support guy says "OK, now what?"*



## Exercises

- 12.19 Is there such a thing as throwing too much money at cybersecurity? Is there a limit to how much security you can have before it doesn't make things more secure? Explain your answer.
- 12.20 The cybersecurity industry has a big problem, it can't define security. How do you know if something is secure if you don't know what that even means. How can you then measure if something is a little secure, too secure, or secure enough? So look online in different sources for cybersecurity and find 3 different definitions of security. Which one do you think is right and why?
- 12.21 One of the main complaints in cybersecurity is that it's not improving. Many security professionals say that technology moves too fast to be secured. What do they mean by that? Do you think it's true and why?

## How to Start Doing Cybersecurity Analysis

We've talked a lot about the subject and we talked a lot around the subject but doing the analysis and how you go about figuring stuff out in a SOC is something that we haven't exactly nailed down. And there's a reason for that. It's because it's not as straight-forward as painting a chair green. Who doesn't want a green chair?!

You will need to look at something and mentally compare it to what you know as good security. You will need to see something that is not being controlled and determine if it has good intentions or bad intentions. None of that is a single skill. None of that is a single body of knowledge. What it is though is being a good hacker-- be resourceful, studious, creative, and attentive. If you know how things work well enough to hack them, then you know them well enough to control them as well as when others are trying to change them.

## Make Good Security

As we've mentioned, security isn't something easily defined. We even know so little that we can't really measure it well. But we do know things that contribute to making something more secure and the process is pretty straight-forward. To make good security you need to do these three things:

1. Separate.
2. Reduce.
3. Control.

And that is every bit as true as it is abstract. You separate interactions between whatever you can. You reduce everything you don't absolutely need. You control everything you can't separate or reduce. So when you look at anything that needs to be secured you ask yourself, "How can I better separate, reduce, or control this?" If you can't answer that then you don't know well enough how it works and you need to figure that out first. Sometimes the best way to do that is asking the people who work with it every day. Notice I didn't say ask the people who built it?

The reason why you go to the people who work with it is that you actually work in Operational Security. You are trying to secure something that includes people and machines, and they interact with each other. It's a living thing. It's moving. That means it doesn't work in a vacuum- it sits in an ever-changing environment and interacts with ever-changing people and parts. The people who build it may not know how it's used or the processes behind its use. The people who use it will know that. And you can't secure something until you know how it's intended to work.



## Master Your Environment

As a security analyst in a SOC you'll be overseeing many of these systems in many different environments. It seems like an impossible task but you have the home field advantage.

Know what's happening on your network. This is probably your greatest home field advantage. To monitor your network for activity and have a clear picture of what's running at any time of day there are several technologies you can look into. Security information and event management (SIEM) products will consolidate log files from all your systems and real-time captures of network traffic. Intrusion Detection Systems (IDS), which are generally a blacklist technology, will monitor real-time network traffic and respond to some types of attacks.

Even without these technologies, however, tools like tcpdump and Wireshark will give you more than enough information to understand what's running on your network and where it's going. That will help you at least see if your zone defense is working. As a network grows, you may want to look into behavioral analysis network tools to help automate sniffing out anomalies, because not all malicious activity is obvious.

Know what should be on each default install of each hard drive, whether it's a desktop or a server. This allows you to recognize malware or non-standard software installs. If you prefer to use file integrity software you will be alerted to changes in various files and directories that can indicate malware or compromise. Integrity checking is most powerful on servers where it can immediately replace files placed by attackers.

Know what normal looks like. The way you do that is by knowing and understanding the employees, the vendors, the routines, the operating hours, and the policies. For example, if you know that no Microsoft Security center should be calling the office to allow them to remotely inspect your system for malicious activity because you never paid for such a service then you'll recognize it as a social engineering or phishing attack and be prepared to stop it quickly.

You should also get in the habit of proactively talking to employees and asking how things are running. Complaints such as a noisy hard drive, a slow system, or strange messages can then be immediately investigated. If you are prepared to perform quick recoveries, a system that is acting suspicious can be quickly wiped and reinstalled. In security, there's no reason to trust an unknown.

## Forget Strategy, Choose Your Tactics

A strategy is an integral part of any modern cybersecurity defense. So what exactly is a cybersecurity strategy? A cybersecurity strategy is a cybersecurity plan with a set of goals and objectives to get cybersecurity as a result.

People who are into cybersecurity strategy like to say it also includes specifics on tools and metrics. But that's really just a trick of adding tactics to the strategy so it doesn't sound so useless.

Yes, useless. Fun fact for you — a cybersecurity strategy is useless to a security analyst. The truth is that if you don't have one for your team it's because you've inherently got one already. Maybe nobody ever bothered to formally document it because it's so obvious. Like how you don't have a formal *not dying* strategy. If you were to have a formal cybersecurity strategy it would likely say you don't want threats of any sort affecting your assets of any sort now or in the future. Which is obvious to you, we hope!

So if it's useless, why is there such a focus on a cybersecurity strategy? Because tactics are hard. Unfortunately, your job in the SOC is 100% tactics. So why do people talk strategy? Partly because they are using the word wrong and actually mean to say tactics but don't know the difference. And partly because it's easier to make a cybersecurity strategy sound like something important despite meaning nothing than it is to make tactics that



work. A cybersecurity strategy can go on meaning nothing a really long time but tactics that mean nothing get noticed right away, in a bad way.

That's because cybersecurity tactics are when the rubber meets the road. They are the bat striking the ball. They are literally the packets smacking the server. They are the way you do the thing you do to the things you have to achieve cybersecurity. And that's hard to make happen and do every day. Which is why being a security analyst can be hard, but for all of us in the field it's the fun kind of hard, like a game with a strong competitor where you can keep playing until you win. This is how to play it to win it (and make it a lot easier on yourself):

1. You will have a whiteboard in the SOC. You need one. Use it to draw out the interactions and the separations between systems based on the packet activity you find on the network. It's like making a hybrid physical and logical network map with arrows of interactions based on protocol activity. Determine how anything that should be separated or controlled. Voila, that's you applying tactics!
2. List all of your network processes like server backups, server administration, remote desktop support services, etc. Know exactly what systems and people they can interact with, then determine what they should be interacting with. How you control that authorization is you applying tactics.
3. Do the same for wireless, physical room access, and telephone systems. Determine which tactics you need to assure control.
4. Now make sure that all of the tactics you chose fit with the overall company business strategy and resources. Now when there's an attack, you have a complete overview of what could be happening and where it could be going. You can even go so far as start writing rules in your analysis automation software to handle your specific environment!

## Exercises

- 12.22 When we talk about making good security as something that's straight-forward we mean Separate, Reduce, and Control. But those things are very abstract. You're going to make them less abstract. How would you apply those three things to a laptop that you use on public WiFi to make it more secure?
- 12.23 Time to fire up Wireshark and take a look at your local network traffic. How many systems can you identify in that traffic? If it's many, how many, and why are there so many? If it's very few, explain why, and what security is keeping you from seeing other systems on the network.
- 12.24 Don't shut off Wireshark just yet! Let's take a look the protocols on your network. Can you identify types of services or even operating systems from those protocols?
- 12.25 While you have Wireshark open, let's take a look at some packet captures. Go online and search for "pcap attack" to find files of packet streams from attacks that you can study. Another place to go is <https://wiki.wireshark.org/SampleCaptures> and see a huge variety of protocols and services in action at the packet level. Select any one of the packet captures you find and do an analysis on it. Be resourceful if you can't figure it out. Write up a simple play-by-play for the important interactions. As a security analyst, figuring out how to analyze what's happening is as important as your ability to communicate it.



## Feed Your Head: Thinking Like the Enemy

While so many security analysis concepts revolve around “Thinking Like the Enemy,” there’s something you need to know: it doesn’t really work like that. Even security professionals tend to think that learning to think like a criminal hacker will make them better defenders. That’s only half right. Learning the hacker part will make them better at security. But not so much having the mind of a criminal. Here’s why:

**1. The enemy is not homogeneous.** Just like there is not just one foreign language, there is not one type of enemy.

So which type of enemy are you learning to think like? The fanatic? The prankster? The desperate? The lonely? The zealous? The frustrated? The crazy? The poor? And even then, can you really think like them when they embody a mindset built from years of thinking and living a certain way? Can you really understand the motives of an attacker when your large fountain drink might equal a day of their wages? We like to think we can because movies tell us it’s possible. But it’s not.

**2. The enemy will invest much more resources in staging an attack than you think is worth it.**

First, the attacker likely doesn’t have the same financial value system you do. You have no idea what they value! Secondly, they don’t necessarily have the same motives as you which means you won’t necessarily agree on what you have that’s worth stealing.


So the enemy may go to a further extent learning your devices, and dive in deeper than even the product manufacturer’s own engineers, if they think you have something they need more than sleep itself.

Sometimes, they’ll spend years longer than what you think is the product life cycle. Since some engineers will be using toolkits and recycled code from other projects, often without knowing how it functions, the code and vulnerabilities will be around much longer than you expect.

Most importantly, to some types of attackers, things you have and don’t think much about, like reputation, ideology, political affiliations, representation, circle of friends, contacts, raw research data, customer details, or even your outspoken moral code, they may see as an asset more valuable than just credit card numbers. An attacker in it just for the kicks may be more interested in seeing you publicly eat crow than fencing your goods. And then there are some assets you don’t realize the value of until they’re gone or smeared all over the news. So of course they’ll put much more effort into it than you think you would if you were in their shoes because they think it’s worth more than you do. So obviously you can’t think like them.

**3. The enemy can and will readily exploit the one thing in your society that you think has made you so advanced and civilized: trust.** As children, our society makes us learn that it’s nice and polite to share. Then, in our teen years, it’s cemented in us by rewarding those who share their secrets with receiving the secrets of others. And knowing secrets makes us feel trusted and important. Even the typical romantic comedy movies focus on trust- showing it’s good and healthy to share with one another, then regret it, and then realize it doesn’t matter and fall in love all over again. This way we can also laugh and cry together. It makes a unified society.

So as you grow up you learn that it is polite and civilized to extend trust as a show of



good will. People who receive that trust without earning it feel important. And if you really think you are important, you're likely to expect and even demand to have access to the secrets of others and get mad at people who don't just trust you with them. Maybe you're even one of those people who believes the old expression that people who don't trust others can't be trusted. But we're all in it together in this society. And so sharing and extending trust brings us to be trusted in a nasty, vicious circle of trusting, love, and friendship. And self-importance.

And that's why people will click on that link that their old elementary school friend Tim sent them, despite the fact that they haven't talked to him in seven years. No, they weren't really friends then, but rather just had their desks near each other, but Tim has something he apparently really needs them to see-- so click click and zap, the malware is in. It wasn't really Tim.


So an enemy who isn't saddled with the same burden of sharing and trusting as part of being polite in their society can only see these trust connections as exploitable interactions. Meanwhile, you who did grow up with that burden won't completely be able to think like that.

**4. The enemy is very capable of planning and interweaving multiple attacks across multiple channels to get to their target.** It's harder to do, sure (see #2), but they aren't just thinking about what's easy to steal- your "low hanging fruit". They are thinking multiple steps ahead of your current security measures, aggregating different means of attack, and correlating their attacks across wireless, telephones, people, and physical infrastructure to get there. For example, an exploit may require that a user receive an e-mail, click on a link in that e-mail to receive a document type not allowed via e-mail, be willing to be interested enough in that document to over-ride any security warnings to view it, and then nest a dirty little bug within the operating system to send info to a foreign server camouflaged as normal traffic. And if you think, "But who would do all those steps?" re-read #3 and remember that the people who went to school with Tim probably would.

Nowadays, an attack which can be made directly, as in my exploit for your vulnerability, is "low hanging fruit" and expected to be the least bit of effort required in most security compliance documents. Which means anyone patching regularly will not be vulnerable for long. So attackers who are already making a large effort, will focus on more complicated but more certain attack methods that will be around a long time. So they will use precision timing, random-number guessing algorithms, back on back attacks like a flood followed by a specially timed buffer overflow, artificial intelligence, and a lot of trust manipulation all together on just one specific attack. And they might just call that Tuesday. While you might be able to think like that, you can't do it natively, and you certainly won't convince your boss to spend money to protect against this.

**5. The enemy probably doesn't have everything you have, but that doesn't mean that if we don't have it that they don't either.** In other words, don't think that if you can't afford a supercomputer to crack your super-strong encryption that it means your enemy can't use one. The enemy will get the things they need. They will. And they will use your own garbage to make the things that you thought you had to buy. Then there's the potential for state sponsorship of equipment for what they can't afford either. Then there's the enemy which is just a lot of people with a common goal (many hands make light work), who can just all download and run a program which causes a massive denial of service attack.

When you try to think like this enemy you not only can't really imagine what they have access to, but also what their diverse backgrounds teach them about how to solve problems like getting what they need. They can be resourceful to a level you can't imagine.



Consider the creation of the cantenna. While corporate security experts were making sure that no wireless laptop, even with a large, expensive antenna, could get on their internal wireless network from beyond their property line, the enemy is more than a kilometer away and currently attacking their network with a repurposed Pringles can they found in the garbage. Probably in their garbage.

**6. The enemy will take advantage of your superego.** That part of you which is defined by your society, culture, and way of living, which makes you want to be likable, is one of the ways that the attacker will evade detection.

Attackers know not to back anyone into a corner. They need to leave room for their target to think they can choose from various courses of action but really their leaving the best (easiest) choice to be the one where the security team does nothing. And by nothing, I mean, puff out their chest, stomp around, yell blame at others, and wave papers of compliance audits passed. But nothing as far as trying to actually catch the attacker.

That part of the attack often requires restraint not generally attributed to an enemy. Stealthy, yes. Smart, sure. But restrained? No, you automatically think that when you vanquished the attacker you did so before more damage could be done. Or else you think that the attacker was too stupid to know what they managed to get in to. That's your ego talking of course. But as light is cast on the attack and you need to take recourse, the superego defines what responsibility you must take and how you can make yourself accountable. So the normal societal response is to lie like hell.

Yes, once again, society has made it more attractive to deny any wrong-doing and avoid punishment than to learn and grow from a mistake. Just look to our role models in government and in Hollywood. It's because our society wants us to punish those victims who didn't do all they could do. So if you don't lie in the corporate setting, they'll fire you. So you follow the golden rule: deny when caught. The enemy knows this but you don't think they know this. Because you can't think like them.

## Where Security Falls Short

Security is like your laundry, you will always have something that needs to be cleaned (even the clothes you are wearing). No matter how often you get your stuff cleaned up, there is forever something else that needs to be done. Security is much more than applying patches, using good malware protection, encrypting data, password management, not opening or viewing suspicious Internet material (even if it says it's from your best friend), and scanning your network for intruders. In the commercial world (where you'll probably end up working), all kinds of vendors sell all kinds of "solutions." Some vendors are better than others, but there is no replacement for a curious and smart security person.

There are several points to consider as a security professional that are rarely mentioned at security conventions, in magazines, in school, or any place besides hacking forums like DEFCON. The types of security shortfalls can be quite extensive so this lesson will focus on a few issues that are near and dear to our heart. Time, security vendors, egos versus profits versus hactivism, security experts, and changes to your environment are the top issues you should be aware of for defensive hacking.

Time will always be against you. Attackers don't usually have schedule or time cards to keep. A proper reconnaissance can take weeks, months, or even years to perform. Very few criminals want to get caught by law enforcement, so they will spend the time needed to ensure they are not exposed, identified, or captured. Careful planning is needed to pull off most attacks, which means attackers will invest the time needed to perform a safe



attack. Most other organizations do not have unlimited manpower, or the time needed, to plug all the holes in their network. These holes are prioritized based on risk assessments and are dealt with according to how important they are to that organization. This means your defense is limited to what that organization thinks is most critical to it. Attackers just want a way into your network- time is not an issue for them.

Everyone likes bright and shiny things. Marketing and sales folks know this even with security products. The problem is that security products rarely perform as advertised and often introduce more security issues, usually in areas you would least likely expect it. Operating systems are notorious for having major and minor security flaws that may or may not be fixed in your lifetime. Products are advertised to sound like they will fix every security problem you have, just like automobiles. Before you purchase anything, read the fine print, compare against similar vendors and know as much as you can about how that product will affect your network.

Our next issue is about motivation. Sane people don't attack others without some reason. The same holds true for network attacks. Attackers usually have one of two reasons for attacking their target. The first reason is for bragging rights. Egos are almost as critical as food is to some people. Criminals want to advertise their skills, so boasting to others about an attack is one major motivation factor. The second reason to be a criminal has to do with money: Why else would someone be a criminal if there wasn't some profit gain? The media likes to play this up by saying how many million dollars were taken during an attack when in reality it is usually difficult, if not impossible, to assess what was actually taken. Believe it or not but crime does pay as long as you don't get caught. Very few criminals are smarter than the law enforcement of the country they are attacking.

Next we have security experts. There are dozens of security experts out in the world and they get paid well for their advice. The problem is that they all have an opinion about the way things should be done. None of the opinions of these experts ever seem to line up with the opinions of other security experts. There is plenty of good advice out there, but there is also plenty of bad advice as well. Just because someone wrote a book about a topic doesn't make them an expert. Besides, in the area of digital technology, things change so fast that it is almost impossible to keep track of all the research, new techniques, legalities, or even the names of everything. Be careful of those who give advice and check your sources.

The last problem with security is the simple fact that everything changes. Attacks change daily, almost hourly. An example of this is malware, where one new engine comes out and within hours, there are several forks off that engine. Ransomware takes a bit longer to morph because a payment system has to set up to collect the ransom without being traced back to the criminals. If you try and keep up with all the changes, you will find yourself chasing your own tail. To fix this, focus on your assets. Your assets are the most important part of your job (besides being a good human being), so concentrate on protecting them.

Just understand that time will always favor the attacker, research any product you intend to introduce to your network, be careful of the advice you are given, and finally, protect your assets the best you can.




### **Game On: Bad Computer, No Cookie for You, Part 2**

Sweet G pointed to a small plainly wrapped postage box laying on Jace's bedroom floor next to a dirty sock and said, "The box must have fallen off your bed. I put it right there on the edge knowing you would want to see it when you came home the other day."

The teen picked up the package and did everything a bomb disposal expert would tell you not to do. First, she shook the box. Then she tossed the box into the air to see if anything fell out of it. Using a pair of scissors, she opened up the backside of the box. The





plain brown paper only had her address on it and a red stamp "DELIVER BY 10AM". There was no information about which delivery service brought the box. Both ladies detected a faint smell of expensive cologne from inside the box. They looked at each other without saying a word.

The curious teen pried open the cardboard exterior and removed the holding tape. She sat up straight as she pulled out each of the contents from the box. Inside was a Raspberry Pi 2 single board computer with several items attached to it. One of its four USB ports held a MultiBlue dongle. The other USB port had a long-range Alfa AWUS036NHA wireless adapter with a four-inch antenna bent over the top of the Raspberry Pi. The third USB port had a second WiFi dongle with a long antenna running underneath the computer.

The Raspberry Pi held a portable battery pack taped to the inside the box to keep it from sliding around. The USB to microUSB power cable connected the two together. The battery pack was a fairly nice Anker designed for 8,000mAh. Jace turned the box around to see what sort of media was running on the Raspberry Pi. To her surprise, the MicroSD card was still inside and the whole system seemed to be running.

Jace turned her phone's WiFi scanning tool on and it detected two new WiFi networks, one was an access point and the other was hidden. Her phone automatically tried to connect to the hidden network but Jace shut off her WiFi before it could finish the handshake. Her main computer was still turned off so Jace decided to take apart this contraption and see what it did and who sent it.

It bothered her that the box had a delivery time of 10AM, which meant it was supposed to be in the apartment while she was at school. It was just bad luck that her grandmother had forgotten to tell Jace about the package for a few days, but maybe the attacker knew about her dementia. The thought made her angry even if it was good reconnaissance on the attacker's part.

Jace notice a small breadboard attached to the General Purpose Input/Output (GPIO) header on the Raspberry Pi. She asked to borrow Sweet G's reading glasses. The breadboard contained a few transistors and a small voltage regulator. The wires on the board lead to the 5-volt input from the external power supply. Jace guessed that this was a trip wire mechanism that would cause the storage card to delete itself when the battery voltage got low. Jace bit her lower lip and yanked the power USB cable right out of the Anker power supply. That probably wasn't the best way to handle the situation, but Jace was pissed off that someone would send her an attack device like this.

She ejected the microSD card out of the Raspberry Pi and grabbed an old laptop from her closet. Not paying any attention to the dust on the lid, Jace pulled in the ten-year-old computer. She used this laptop on occasion so it had the tools she needed. Debian booted and Jace mounted the microSD card. "Kali," the two people in the room said at the same time. "Yup Sweet G, it looks like this thing is running a lean version of Kali Linux with several scripts during boot," Jace said. She was more interested in the scripts than the tools.

"Whoever set this thing up didn't bother to change the default password for Kali or the SSH keys, not that this matters because the logon was disabled for the scripts to work," Jace said. One of the first scripts on the storage card turned off the logon sequence and then looked to see if the proper WiFi adapters were installed and working. "Apt-get update" wasn't part of the boot sequence, which told Jace that this was the final build of the project. Whoever built this never expected to see it again.

The next couple of scripts checked for the location of certain tools and then queried the voltage regulator on the GPIO to see if the proper voltage was being supplied. Another script would trigger if the voltage dropped below 4.5 volts. Jace was very interested to see that this set of commands would cause the storage card to encrypt the data storage partition and then repartition that area. This set of commands would happen seven times. After the seventh time, the boot partition would be encrypted, rendering the storage card useless for evidence recovery.



Jace thought, "So this person was smart enough to put a boobytrap on the battery to wipe out the memory card, had enough money to use expensive equipment, but was stupid enough to leave the original Kali password. And then WiFi," she added as she looked at her grandmother. "It looks like they tried to gain access to my computer using WiFi but that didn't work because my WiFi adapter is disabled. I even removed the driver for it," she pondered.

"What about the other dongle," Sweet G pointed with her skinny finger.

"Other dongle," the teen looked at the third USB port and saw the MultiBlue device. If the attacker couldn't get in through WiFi and couldn't communicate using the other WiFi access point then they had to use another way; Bluetooth. Jace had set up her computer to use Linux without WiFi. "Whoever built this attack tool didn't know that but had to have a third option to take over my machine," she thought.

"Now let's see who this device is supposed to be talking with," Jace said. After several hours of research and pointing around, Jace was able to see exactly how the device was supposed to work. She also wanted to know if it had actually worked. The Raspberry Pi 2 had two WiFi dongles, one to brute force into her non-existent wireless one and the other dongle to act as an access point for the attacker to talk to. The MultiBlue dongle was added, which seems to be how the attacker managed to reboot her computer into Windows. Luckily, Jace didn't keep anything in Windows and her Linux drive was encrypted using VeraCrypt.

The battery on the device was supposed to have run out of power already except the WiFi card was set by default to shut off if no network was found after 30 minutes. This saved lots of power on the charger, which messed up the power calculations for the tripwire to wipe out the storage card. If the WiFi adapter had connected to a network, the battery would have been consumed enough to fail at around 5PM the day of the delivery.

If Jace had been a normal user, the attack would have worked on her. The problem was, who would go through all this just to get inside her computer?

**Game Over.**

## Getting the Help You Need

---

No, you don't have to admit that you are addicted to something, it's not that kind of help. In this profession you will need lots of information to help you along. When a new piece of malware comes out, you will turn to VirusTotal for in-depth information about that software. As new attacks happen, you'll need more than just Common Vulnerabilities and Exposures from <https://cve.mitre.org/> to provide details. The FBI does a fairly decent job of informing people about new scams but you will want more than just basic advice. So here you go!

---



## News & Opinion

---

Look in the following places to keep up on the security industry and community:

- Ars Technica – Risk Assessment
- CIO Security
- CSO Online
- Dark Reading
- Guardian Information Security Hub
- Homeland Security News Wire – Cybersecurity
- Infosecurity Magazine
- Naked Security
- SC Magazine
- SecureList
- SecurityWatch
- Threat Level
- ThreatPost

## Reddit

---

Here you'll find a whole boatload of opinion but also a lot of good techniques:

- [/r/blackhat](#) - Hackers on Steroids
- [/r/computerforensics](#) - IR Archaeologists
- [/r/crypto](#) - Cryptography news and discussion
- [/r/Cyberpunk](#) - High-Tech Low-Lifes
- [/r/HackBloc](#) - Hacktivism & Crypto-anarchy
- [/r/lockpicking](#) - Popular Hacker Hobby
- [/r/Malware](#) - Malware reports and information
- [/r/netsecstudents](#) - netsec for noobs students
- [/r/onions](#) - Things That Make You Cry
- [/r/privacy](#) - Orwell Was Right
- [/r/pwned](#) - "What Security?"
- [/r/REMath](#) - Math behind reverse engineering
- [/r/ReverseEngineering](#) - Binary Reversing
- [/r/rootkit](#) - Software and hardware rootkits
- [/r/securityCTF](#) - CTF new and write-ups
- [/r/SocialEngineering](#) - Free Candy
- [/r/sysadmin](#) - Overworked Crushed Souls
- [/r/vrd](#) - Vulnerability Research and Development
- [/r/xss](#) - Cross Site Scripting



## Blogs

---

Reading blogs is one of the best ways to keep up with the stuff that hasn't made it to the news yet:

IBM Security Intelligence Online Security Blog: <https://securityintelligence.com/>

ISECOM Academy: <https://www.isecomacademy.com/>

Schneier Security Blog: <https://www.schneier.com/>

Krebs on Security: <https://krebsonsecurity.com/>

## Useful Things

---

Here you'll find many of the knowledge tools you'll need to be successful:

UTPA Center of Excellence in STEM Education

CERIAS: Tools and Resources

CVE: Common Vulnerabilities and Exposures

Information Security Stack Exchange

Open Source Cybersecurity Playbook

OSSTMM: Open Source Security Methodology Manual

OVAL: Open Vulnerability and Assessment Language

Scholarship Opportunities

US-CERT

U.S. Department of Homeland Security – Cybersecurity

## Organizations

---

Join an organization because the best way to see far is to stand on the shoulders of giants:

ACM SIGSAC: Special Interest Group on Security, Audit and Control

CSA: Cloud Security Alliance

DC3: Defense Cyber Crime Center

HTCIA: High Technology Crime Investigation Association

ISECOM: Institute for Security and Open Methodologies

NICCS: National Initiative for Cybersecurity Careers and Studies

NSI: National Security Institute

NW3C: National White Collar Crime Center

## Other Resources

---

Because you'll need this:

Reverse Engineering Malware 101 and 102 - <https://securedorg.github.io/>



## Conclusion

---

Chess is a game played against two people with calculable odds and number of moves. When you first start to learn how to play chess, many people suggest you play against yourself as much as possible. This may be great advice, but our own consciousness causes us to favor one color (side) over the other. It is a bias built into our subconscious that few people can ever defeat or overcome. Cybersecurity is often thought of as a game. Many industry experts refer to this game as one between a cat and a mouse. The mouse is always one step ahead of the cat, using intellect and cunning over the cat's flexibility and prowess. Defensive hacking is not a game because the stakes are real. People's livelihoods are being taken away by criminals. Data is being hijacked or stolen for the sake of illegal profits.

In a very real sense, you are the guardian of millions or billions worth of assets. You need to know how to protect yourself against the real threat that is always evolving in the digital world. When attackers make a move, the security field comes up with a counter-move. The same tools that make great security tools also make great attack tools. The same goes for attacks tools. One of the biggest differences between the two sides has to do with ambition and resources. Attackers often have unlimited ambition, while security folks have ample resources (just used in the wrong locations). The key to this lesson is to learn which tools you have available to you, how they work, and what some attacks look like. You can't go hunting for snipes (or gurbles) if you've never seen one.

Some of the most successful attacks require very little money from the attacker, like password cracking or social engineering. Those same attacks require the security staff to pour resources into security education programs for the employees, create policies to ensure staff are using appropriate information safeguarding, and audit all accounts to ensure nobody is using poor two-factor authentication or moving data from places it should not go. This level of protection requires constant work on your part. You can automate some of that work using tools like QRadar, Wireshark and Nmap, but the attacker has the advantage since they can execute any of those attacks at the local coffee shop or in your company gift shop.

It is up to you to know how the attacks work and how your tools affect the network. There is plenty of work to be done in this area. We hope you enjoyed this lesson and maybe even learned something.

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.**