BE A HACKER!!!

-To protect yourself

-By Team Nikist

Ch-1 how protected do you feel?

Ch-2 Difference between hacking and cracking in a computer.

Ch-3- Information Security

Ch-4-Hacking vs. Ethical Hacking

Ch-5-Fundamentals of Information Security

Ch-6-Speak like a Hacker.

Ch-7-Zero-Day attack

Ch-8 The Technology Triangle

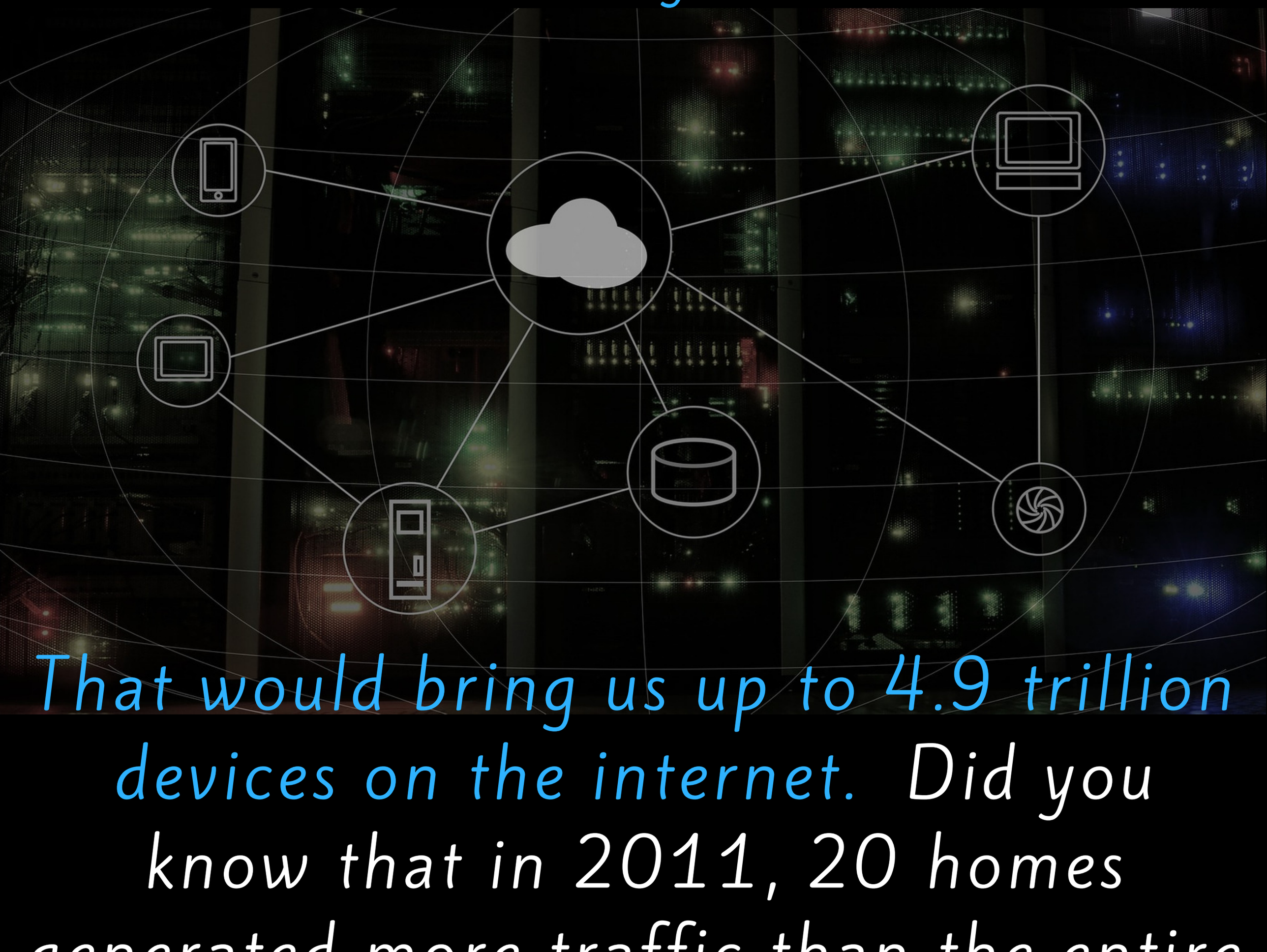
Ch-9 Shrink-wrap Code Attacks

Ch-10 CEH Certification Program

Ch-1

how protected do you feel?

Did you know that in 1984 there were only a thousand devices on the internet as a whole? In 1992, there were 1 million devices, in 2015 a billion. And today there are 1.4 trillion devices on the internet(2018), by 2020 it's supposed to increase by 30%.



That would bring us up to 4.9 trillion devices on the internet. Did you know that in 2011, 20 homes generated more traffic than the entire internet of 2008? And if you think that's amazing, 90% of the world's data has been created in just the past 2 years.

Now here's the scary part, more than 600,000 Facebook accounts are compromised every single day, and 1 in 10 social networking users actually admit to falling victims to some type of phishing scam or fake link that's posted on the social networking platforms.

Fifty-nine percent of the ex-employees, this is kind of a scary one too, 59% *of ex-employees who leave the company admit to stealing company data when they leave their jobs.* *So I ask you again, how protected do you feel? Well, that's what we're going to show you.*

Many of you want to become an ethical hacker, right?? But did you know what actually Ethical Hacking is? *So in this chapter we are going to talk about actual meaning of Ethical Hacking.*

When we talk about a hacker, people think of a guy sitting wearing a hood with a laptop and hacking someone's account right? That is what people imagine but that's not the case. The problem is people actually don't know the meaning of hacking, the actual meaning of hacking.

The term Ethical Hacking is composed of two words, you have ethical and you have hacking. But hacking is not only related to computers. If you use anything without the owner permission, that's hacking.

But in this ebook, we are talking about a Hacking which means indexing the weakness in the computer system or network or cracking the system to gain access.

And nowadays people want to learn how to hack Facebook accounts but they do not know how to secure their own Facebook account.

People want to learn to hack because our Hollywood and Bollywood movies make it so cool.

But we just want to say "Learn hacking to protect yourself and other self too".

Because the cybercrime victims per year are over 566 million victims. Let's break that down. That equals out to be 1.5 million victims per day or 18 victims per second. Now the cost of cybercrime includes not only the effects to businesses, but also to hundreds of millions of people globally.

Over 657 million identities will be exposed, and a majority of those will end up being stolen. In fact, of that, 40 million were from the United States, 54 million from Turkey, 20 million from Korea. This isn't just a single country issue, this is a global issue, and the cost of cybercrime will continue to increase as businesses move more of their functions to an online presence and as more companies and customers around the world get connected.

And again this is not limited to just a single or just a couple of industries. Some of the most heavily hit industries for data breaches, you can see, are healthcare and businesses, well, well beyond banking and government and education. And a lot of times people look at that and they go, well I would think that banking would be a bigger hit. Well, not really.

Think about the information I can gather from healthcare, tons of identity information, social security numbers, income. Businesses are going to be your customer base. Businesses also include the loss of intellectual property. This is a big issue. We've got major countries that are stealing intellectual properties from other countries, and they'll continue to do that so long as the acquiring countries improve their ability to make use of this information and to manufacture competing goods.

One of our biggest issues is how it's controlled. Governments have got to get serious about somehow controlling this environment. I'm not saying government control, but prosecution. I mean think about this one. If you come home and somebody has broken into your front door, who do you call? Police, local police.

They come out; they help you out, right? If somebody steals your credit card, okay granted you may contact your credit card company and say, hey there's a weird charge on my card and they refund that, but who goes after that person? How do you go after somebody in a completely different country? So I've got to ask you the question, how protected do you feel?

Ch-2

Difference between hacking and cracking in a computer.

Now you all know about what is hacking but did you know there is one more term called cracking. Basically both hacking and cracking are 2 ways of getting access. Hacking is when something is under attack by software that has been designed to a Bypass, Disable, Break etc in order to gain access

Cracking is when users, passwords and keys are detected with dictionary, brute force and hybrid attacks in order to gain access to the target using existing user data.In simple term,Cracking is when someone illegally breaks into something, and also includes the creation of malicious software with the intent on releasing it into the internet.

Most of the stuff you see on TV like Credit card numbers being stolen and such is the work of hackers. It can be argued that you are a hacker because you power up your computer. You are, after all, manipulating the power button to cause electricity to flow to your computer. When you move a mouse or type something it can also be considered hacking. Most hackers are out to obtain knowledge.

That is what we do. We find security breaches and learn how to fix them, we figure out ways to make things perform better. When a computer is hacked, the only way you will know is if you monitor your system and catch them in the act, or if they tell you, because a hacker leaves no traces that he was there, and leaves the system exactly as he found it.

Ch-3

Information Security

So we're going to start to introduce to you some new concepts, new phrases, new ideas that you need to become familiar with. To that point, there's a famous quote by Sun Tzu who wrote The Art of War, and in it he said, "If you know the enemy and know yourself, you need not fear the results of a hundred battles. If you know yourself, but not the enemy, for each victory gained you will also suffer defeat.

If you know neither the enemy nor yourself, you will succumb in every battle." And this is so true when it comes to protecting ourselves for security or --- and hacking. If you don't understand what the hacker can do to you, you will never be ahead of the game. So now it's time for you to start thinking like a hacker. You need to think like the hacker so that you understand what's coming at you, how they're coming at you, which will result in how to protect yourself.

We'll also take a look at some new terminology that you may or may not be familiar with, we're going to introduce some new concepts and new terms, and hopefully make sure that they are clear to you. Then we re going to talk to you about the technology triangle. This is a concept that everybody in the IT industry has to face, and the dilemma that we have with it.

Ch-4

Hacking vs. Ethical Hacking

Hacking is defined as basically taking an object, it could be a computer, operating system, hardware, a person, we call that social engineering, but we take those objects and we are able to make them do something that they were not necessarily designed to do.

Giving you an example, back in the day I had an Xbox, and with lot of games, and I got really tired of having to deal with different CDs all the time so I went --- this was a pretty in-depth hack, I had to actually purchase this special chip, and I had to solder it into my Xbox, and I had to download some software.

And what it did for me is it allowed me to put in a bigger size hard drive, I think I put like a 500 GB in, and then I was able to rip my game CDs and store them on the hard drive and actually play them from the hard drive. It actually launched a different OS than the Xbox OS.

And I still kind of do the same thing today, whenever I buy an Android phone or any type of Android tablet, I'm a big Android guy, the first thing I do is I go through and root it so that I can actually use the hardware to my advantage. Now I would consider that ethical hacking.

Some people might have questioned that, I know a lot of manufacturers have tried to stop people from doing it. Recent court cases have come out and said you know what? Basically the consumer has purchased the product, they can do whatever they want with it.

I can tear apart an Xbox if I want to tear it apart. I can smash it into pieces if I want to. So I should be able to make modifications if I want to. And until someone starts giving me a free phone, or a free Xbox, I'm going to continue to do those things. But when it comes to the major difference between hacking and ethical hacking, you have to find out first of all if what you're doing in any way breaks any type of cyber laws, or commits an internet crime.

There are tons of laws out there, not just in the United States, but worldwide. Each country has its own cyber laws. The concept here or the thing you've got to be tricky is that many times when you do a hack or when a hacker attacks you, he's actually in violation of two counts of that law.

And the reason behind is because first of all you can use a computer in the commencement of a crime, and then if you're attacking a computer, that target, getting into the information or getting into that machine without permission is also a separate crime. So there's a double whammy there for the user if they get caught.

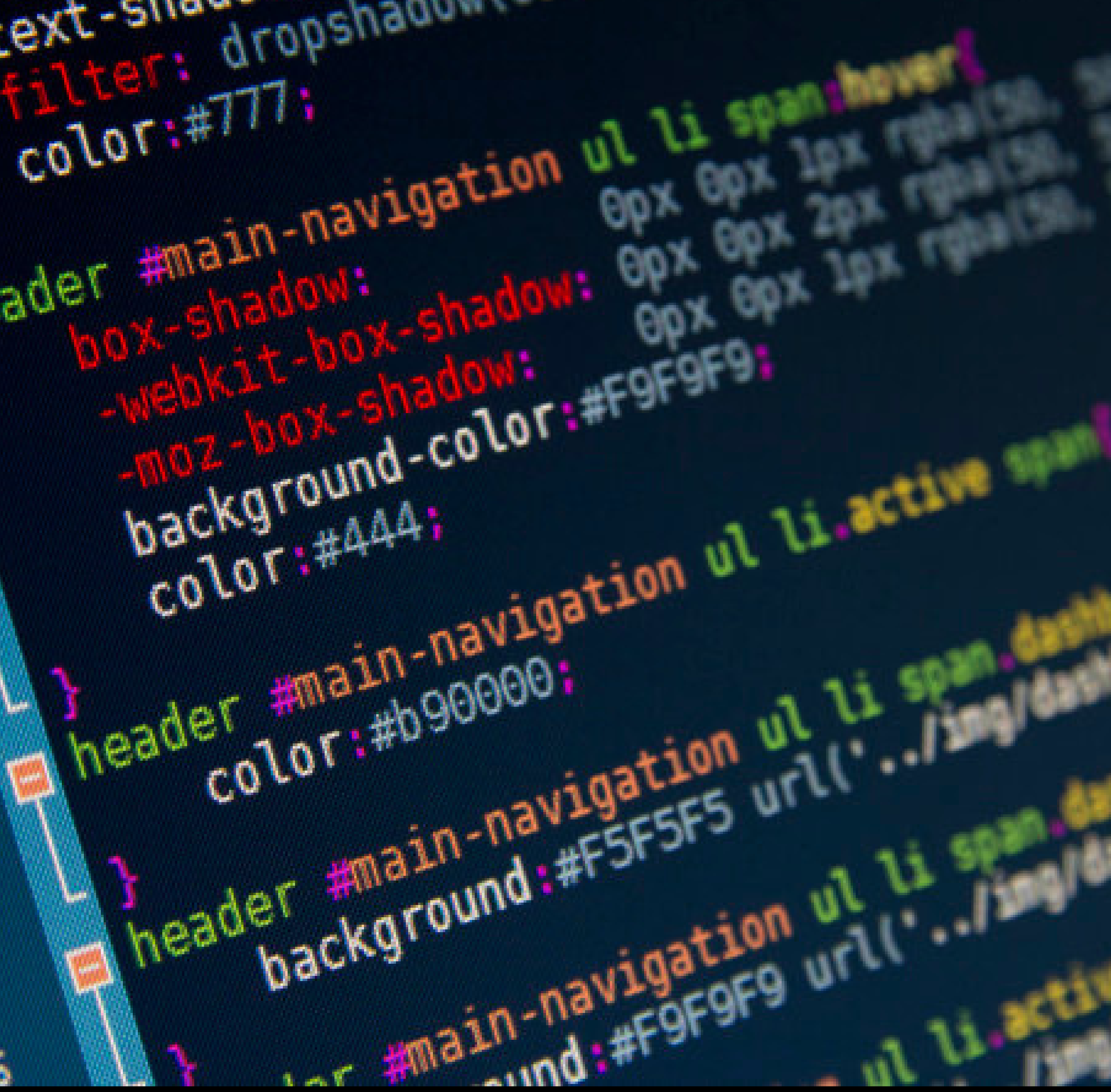
So you want to ask yourself is the thing I'm about to do, let's say that you learn something really fun and interesting during these modules, you learn how to go through and do an SQL injection, well if you try to do that SQL injection against somebody's network that you don't have permission to; you're going to be in trouble. So that would be hacking.

Ethical hacking, I'm going to use these same skill sets and try to do an SQL injection attack against my SQL server and see if that works or doesn't work, or maybe I hire somebody to come in to do a pentest, or penetration test, which is just going through and pretending like they're a hacker trying to get in, I've given them permission; therefore I'm ethical at that point

We also have to be concerned about intellectual property. If your goal is to take intellectual property or modify intellectual property; again you're going to be in trouble. This is the big thing that we're trying to protect nowadays, and so a lot of ethical hackers are going to go through and see what information is exposed

And believe it or not, information gets exposed.I don't care what you have out there deployed, something can be exposed. So if you were to take a look at ethical hacking, it's basically the process of going through and testing

and checking a network infrastructure for any type of possible loopholes or vulnerabilities, and we'll talk about vulnerabilities here in just a second.



Ch-5

Fundamentals of Information Security

@nikist_

Let's take a look at the fundamentals of information security. Now we need to make sure that we understand why we're securing things down. Typically we're going to start off with authenticity, meaning when Himanshu logs in and he tries to gain access to a resource, we want to make sure that that's actually Himanshu.

Or if I'm trying to gain access to my bank, the bank wants to make sure that it is actually me trying to get into my account information. We refer to that as authenticity. The next one is making sure that we support the integrity of the data, meaning that we trust the source of where that data is stored.

So again if I'm trying to get into my checking account, I want to make sure I'm actually on my bank's website, right, and that I'm getting into the data and the data there that represents my account is valid.

Next, we want to look at availability. Now when it comes to availability typically in the IT world we think of high availability or for example redundant power supplies or I'm going to have a RAID of some type for my hard drives to protect those. Or I may have a cluster of servers combined together so if one fails another server picks up to where it left off.

That's not really the availability we're talking about here. When it comes to information security we need to make sure that people can get to their data and they're not being denied access to that data. One of the biggest hacks out there right now that we hear about all the time is something called a Denial of Service attack, or DOS.

A DOS is designed to refuse availability for users to gain access to resources. So, if I was someone, a malicious hacker, that I wanted to go out and cause some grief for PayPal, me doing a denial of service attack against PayPal is going to stop them from being able to continue doing business with their users, so we're denying availability, which costs companies thousands and millions of dollars.

Another thing we may want to take a look at here when it comes to information security is confidentiality.

Some of the biggest headlines today in security evolve around companies whose databases get hacked and their customer information gets revealed or gets exposed.

Ch-6

Speak like a Hacker.

@nikist_

Okay now it's time to speak like a hacker. That was my hacker slang coming in. Did you like that? These are some of the terms, that's what we want to teach you here, some of the terms that you should be aware of. Some of them you may be aware of, some of them you may never have heard of before, we're going to make sure that you understand them. The first one is referred to as an exploit.

Maybe they've got a card key access into a door. Well if I just simply tailgate somebody, that's an exploit that I could implement or I could take advantage of. So an exploit is just simply a way of breaching the security of some type of system through some type of vulnerability.

And we'll talk about vulnerabilities here in just a second, that's another term I want you to become familiar with. But first I want to talk about the hack value. That's not something that when you're sick and you hack up, nah, that was gross. The hack value is a value that a hacker associates to a system.

Let's say that I go through and I scan your network and in it I discover that you've got, I don't know, 10 Window 7 machines, you've got a Windows 2003 server, you've got a Windows 2012 server, you've got a Linux box, and you've got a couple of Macs out there too.

Now I'm going to go through as a hacker and associate a hack value, meaning which machines are going to be more advantageous for me to go after, not that I can't get into all of them, it's always a matter of time. We'll talk about that one a little bit later on too. Time is our worst enemy when it comes to hacking, or protecting ourselves from hacking.

I always love it when I'd have relatives say, yeah I went off and bought a Mac because I don't have to worry about anti-virus. And I'm like, oh man, yeah that's it, don't give yourself any type of protection, just assume. And the truth behind that whole concept, that whole marketing from Apple is brilliant by the way, but when you think about it, at the time Apple had less than 10% of the market share. Now pretend like you're a hacker for a second.

Do you really want to go after only 10% of the systems out there? Or if you're trying to create a piece of malware, do you only want to infect 10% of the systems out there? This is why Windows typically gets a really bad rap for itself, is because of the fact that they own so much of the market share they are a primary target. So I'm going to go through and I'm going to look at your machines and say, okay, a Linux box? Not impossible, but it may be more difficult.

I'm going to maybe focus more on these Windows 7 machines, but you know what, even easier, older technology, you've got a Windows server 2003 system sitting out there, it may not be patched, or it may not have a hotfix installed, which leads me into vulnerabilities.

Vulnerabilities are a weakness in the design or a weakness in the implementation of a system, whether again it's a, I shouldn't just say a system, I've got to come up with a good word for this one, but it's for either operating systems, hardware, applications, anything that's dealing with the IT environment, it may have a vulnerability. There are vulnerabilities on routers.

There are vulnerabilities on Adobe Acrobat. There are vulnerabilities for webcams. I mean they're everywhere. A target of evaluation, now what we mean by this term is some type of system, an application, a device, a component, a person, that the hacker has identified as a device that requires a security evaluation.

This actually, going through and listing your targets of evaluations, helps an evaluator understand all the functionality, all the vulnerabilities, all the technology that's involved in that apparatus, or that, again it can be from system to users, so we need to go through and evaluate those

Ch-7

Zero-Day attack

@nikist_

Now a zero-day attack is very similar, well this is probably the most common or known term that we use in the hacking world. A zero-day attack is an attack that a hacker can issue against a target where there's been no patch or fix deployed.

So a zero-day attack could, it doesn't necessarily have to be 0 days or just today, if Microsoft figures out 3 months from now that there's a vulnerability through one of their operating systems, until they come out with a patch, any attack that's thrown at that machine or that particular target is referred to as a zero-day attack.

So again a zero-day attack is just simply something that hasn't been fixed, either from the developer or could be lack of training if it's a user. And finally, we have something called daisy-chaining. Daisy-chaining is, well let me explain it to you, sometimes it's a little bit easier to understand if I explain it.

Daisy-chaining is, let's say that I come into your network and I scan your network and I see that you've got these Window 7 machines out there, you've got some servers out there, I'm going to try to compromise one of your desktop machines, and I'm going to take Himanshu down at the Mail Department, his mailroom.

Do we even have mailrooms anymore? Email rooms? No, we'll go with Marketing. So we're going to go through and exploit his machine, I'm going to pon his machine really, really bad so that I'm in total control of it.

Then I'm going to use his machine to attack your servers, and I'm going to clean my tracks when it comes to making sure on his desktop machine that you can't tell I was on his machine. I really don't care that you can see that Himanshu's machine was on your server, because guess what's going to happen?

An inexperienced IT person is going to look at the server, look at the logs, and go, oh, Himanshu's machines is attacking me. And then they run down to Himanshu's machine, and they're like what are you doing Himanshu? And he says I don't know what you're talking about.

An inexperienced IT person is going to look at the server, look at the logs, and go, oh, Himanshu's machines is attacking me. And then they run down to Himanshu's machine, and they're like what are you doing Himanshu? And he says I don't know what you're talking about.

Ch-8

The Technology Triangle.

@nikist_

Okay, the technology triangle, it's mysterious. I would say as mysterious as the Bermuda Triangle, just not as big. No, the technology triangle is a concept that everybody that's involved with technology, whether it's an IT guy or a software developer or a hardware developer.

It doesn't matter, we have to deal with these concepts, one of them being usability, or we often think of it as the GUI environment versus functionality, which would be our features, versus security, which would be restrictions.

Now the dilemma that we have is we have to come up with a good balance between these, because as we move, say for example, from usability we lose security and functionality. And the same thing is if I move towards security, I'm going to lose functionality and usability, and yeah you can see where I'm going to go with this one, it's finding this balance.

And some operating systems balance more towards, and applications, balance more towards one area than the others. Great example this is, back in, back in the day of Windows server 2000 they deployed the operating system

And some operating systems balance more towards, and applications, balance more towards one area than the others. A great example this is, back in, back in the day of Windows server 2000 they deployed the operating system

when you deployed it,
it automatically
installed IIS, which is a
web server
environment, and the
web server
environment had every
feature turned on and
it was holier than
Swiss cheese, and
believe me it's quite
holy.

Not a religious reference. Anyway, we lost security functionality because Microsoft was trying to be nice, to set this server up for you, because the internet was brand new and everybody wanted a piece of it, right?

They then came out, actually right around Windows Vista they came out with something that was really annoying to most IT guys, it was referred to as the UAC, or the annoying pop-up, that every time you wanted to try to do something it would pop-up and say, are you sure you want to do this?

Now from the perspective of the administrator, it was really annoying because we were like, yes, I want to do this, but from the perspective of the end-user it would say in order for you to do this you had to provide a username and password

So as we move heavier towards security we lose usability and functionality. In fact, as we move closer to security we end up with an operating system like Linux. Yeah I know I'm going to hear on that one. I'm not slamming Linux.

Linux is, is secure. It's not that all secure, there are plenty of vulnerabilities out there for you, but if it was as friendly as Windows, maybe it would have a little bit more footprint in the IT world. So that's the dilemma that we have.

Here's another one for you, usability. So you go off to, I don't know, your local technical retail store and you purchase a brand-new Linksys router, and you come home and the instructions say, plug it in, turn it on, and push this button, and you're done. Okay, very, very usable.

Very, very nice to set up, yet what's the password? How difficult is that password? And when we get to passwords trust me, you're going to hear me get up on a soapbox and lecture you about passwords. The security goes right out the window when we have that type of usability.

Ch-9

Shrink-wrap Code Attacks.

@nikist_

Shrink-wrap Code Attacks; now the concept behind this particular type of attack is not necessarily... well, what it is it's the attacker taking advantage of, in some cases, and I'm not saying all developers are lazy, but a lazy developer can take shortcuts, and what they will do is they will go out and find code.

They don't want to have to rewrite the code to show an installation display. You know the little file scrolling across or flying across or maybe a progress bar. They don't want to have to recreate that.

So instead, they either purchase that particular part of the code or in some cases, it's free. They might find it as a software repository out there or a developer repository that people are sharing their different code.

Well if they reuse that code over and over in their application or maybe through multiple applications and there is a flaw in that code that creates a vulnerability, now all of a sudden, I've got multiple points that I can hit.

So, what I always tell developers is that if they plan on reusing code over and over, that they may or may not, matter of fact; think about this one, if I really wanted to create some problems or create a lot of targets that I can go after, how about if I create a piece of code that everybody's going to really want.

So maybe I tweak an existing one and maybe put in a little, inject some of my own little special code and give it away for free and everybody goes, "Wow, this is so cool. "It's free," and they don't look, they don't review the scripts or they don't review the code itself.

The other issue that we have is that many times, operating systems, as well as applications, come with built-in scripts, and these scripts again are designed to make things easier for the user, for the end user, or in your case the IT guy, but because you're not aware of these particular scripts, and me as attacker, I've done my vulnerability research, I can utilize my knowledge in the fact that there are built-in scripts to take advantage of your system.

Now, a really simplistic version of this would be for example, macros in Microsoft Word, and this used to be a really big issue back in the day. You could download a Word document and I could have a macro or an Excel document and I'd have a macro built into it. When you opened it up, it executed.

Most of the antivirus products today will actually protect you from those types of attacks, as well as now, Microsoft Office doesn't allow you to run a code or a macro without your knowledge.

Ch-10

CEH Certification Program

I love movies, I love finding quotes, I love trivia about movies, and one of my favorite quotes, I know you're going to be shocked, it doesn't really come from an action film. You would think something like, I'll be back, would be one of my favorite quotes, but it's not.

It's from a film starring Tom Hanks and Geena Davis. I'll give you a little trivia and see if you can figure out what that is, 1990s. It was called A League of Their Own, and in it Tom Hanks delivers one of the best lines I've ever heard. Geena Davis *gets really tired or really difficult.*

There's a relationship thing going on with her sister, her husband is coming back from the war, and she's leaving the team, and Tom Hanks and her have this big argument. And in the middle of the argument, he says why are you quitting? And she says I'm quitting because it got too hard. And here comes the line.

An inexperienced IT person is going to look at the server, look at the logs, and go, oh, Himanshu's machines is attacking me. And then they run down to Himanshu's machine, and they're like what are you doing Himanshu? And he says I don't know what you're talking about.

He says, "If it wasn't "hard", everyone would do it... "Hard" is what makes "it" great." Now I'm not going to pull any punches here folks. The CEH exam is not that easy, and it's not designed to be that easy, but once you take the exam you're going to have to keep up on that certification, so in this module we're going to go through and talk about this whole CEH (CERTIFIED ETHICAL HACKER) certification program.

Okay, the technology triangle, it's mysterious. I would say as mysterious as the Bermuda Triangle, just not as big. No, the technology triangle is a concept that everybody that's involved with technology, whether it's an IT guy or a software developer or a hardware developer.

We'll go through and talk about what the certification brings you. We'll also take a look at how to maintain your certification. This is not a one shot pony here. You're going to have to, that's the wrong acronym, but you get the idea. You're going to have to maintain this certification. You don't just take the exam once and go oh, I'm done.And then we'll go through and take a look at what's expected of you.

So first, what does certification bring you? A lot of times we take an exam, we get a certification, and we get that certificate, and we put it on our wall for about the first year, and then it ends up on our dartboard or becomes a doorstop

Well, when it comes to certification with CEH, you need to understand that this certification actually brings to you an internationally recognized certification. This is one that's known throughout the entire IT industry.

It is in fact an industry standard so much so that the CEH certification actually meets the Department of Defense directive 8570.1, which basically is a directive that it came out and said anybody that deals in the IT side of things when it comes to government it has to have some type of certification, CEH being one of those.

As far as benefiting your resume is concerned, CEH will actually help make you stand out as someone who understands how a hacker thinks. The most recent survey in 2015 showed that a certified ethical hacker, their salary range is anywhere from $25,000 up to $111,0000 per year.

And obviously with everything that's been going on in this world, as far as hacking and technology is concerned, this certification is in high demand just because the aspect that it again is teaching you to be more proactive than reactive to what's happening.

So by ending this ebook I just to say if you want to learn complete ethical hacking for free then there is a website called

"www.cybrary.it"

go to this website and start learning.

I hope this ebook gives you some know about hacking ...