Cybersecurity Module 1: Think Like a Hacker, Defend Like a Ninja (50 min) - Peter Holliday

Cybersecurity Introduction (0:00-5:26)

You've got to start thinking like your enemy and you start thinking like, “Well, how are they gonna get into my network?” And I will take you through a few of those things and then I'll look at defending like a ninja--well, defending like a ninja the Cisco way.

So I'll take you through some of the Cisco things that we do. Should point out that no one company is ever going to be perfect when it comes to private security, so at least at Cisco, we look primarily at the network. That's our main area of the defense. You really need to be across all elements of this spect--from, you know, end-user protection all the way down to the network and physical security as well as your policy and plans to have a complete security architecture for what you're going to do--what you're gonna do on your networks.

So cyber is more than just the internet. A lot of people think, I'm talking about cyber, so I'm talking about what I do when I bring up a browser. Cyber is really anything where you have some sort of electronic information. And that could actually be what we term as "at rest." So if you got a computer that's in a sensitive computer that you got a lot attached to a network, that's actually part of cyberspace, and it's part of what's classified as a cyber--piece of a cyber puzzle, because you need to protect it.

Even though it's not connected to a network, it could still be infiltrated, as we'll show in a couple of the great examples over the next month of some of the issues. And this includes things like, particularly, these days, we'll be going from what we call the nonkinetic to the kinetic world, so where we go from-- to a digital space into--into physical space, and the SCADA networks are a great example of this.

So if I had a computer malware that was able to take control of a process control system such as a power bridge or, let's say, a nuclear enrichment facility, then I'm now crossing the barrier from an electronic system, from a digital world into a physical world. And this probably the most scariest part of cyber security as we go forward is that we're now seeing these sorts of infiltrations into networks.

In my defense lecture that's coming up on February 13th, I'll actually look at one of the greatest recent--one of the greatest recent break-ins, which is the STUXNET and Duqu malwares, which are just fantastic case studies of how to write really good malware that's very hard to detect, because it crosses that boundary of electronic into the physical realm. So if cyber's everything that
contains electrical information-- electronic information, then cyberspace is really, then, all forms of activity that happen with that sort of information. Okay, so that includes all our networks, and that includes the internet, includes private networks, and also networks that are disconnected. So therefore it follows that cyber security is protection of this cyberspace. And what we're talking about today is really just a few basic elements of that cyber security.

When you choose to start, say, your first training in cyber security, you'll definitely come across what we call the CIA triad, which is confidentiality, integrity, and availability. That's--that's probably a very well-known triad, and certainly you'll come across it in the Cisco courses on security. It also includes, though, the exploitation of cyberspace so you need to be very proactive in cyber security. It's no good just being-- sitting back as a network security expert just watching the logs. You need to be very proactive on how you actually protect your network and how you can install these countermeasures on the network to sort of intervene with the adversaries actually getting on to your network in the first place.

So who are we up against? There's no real single definition for what a hacker is and who--what sort of profile would be behind a hacker. You'd never see one walking down the street or a person walking down the street and know that they're a hacker. And this is the real hard thing about when we get into cyber crime, and we'll have a great lecture about cyber crime in the next month, but unlike real criminals, hackers love the anonymity that the internet gives them so they can hide behind anything. They can hide behind a name; hide behind these pseudonyms that they use on the net. But what we find with the activists, such a groups like LulzSec and Anonymous, not even the whole group know who each other--real identity of the other members of the group. They work together for a particular time, but their identity is largely-- largely kept private, so very hard to track people down.

**Cyber Adversaries (05:26-11:19)**

**State-sponsored cyber operations**
The threat spectrum of our cyber adversaries really goes from top to bottom here. So the biggest threat and the number one threat, really, is from state-sponsored cyber operations. Now, these will include governments and large corporations who actively--actively pursue their competition, whether that be another nation, whether that be another corporation as part of that nation, to really illicit confidential information and use that information.

Probably a weird-- the greatest threat to most of corporations around the world at the moment in terms of state-sponsored cyber operations is really China. China is leading the way in this particular area at the moment. In fact, one of the greatest breaches that has been documented in the last three months was the U.S. Department of Commerce. Their network was so infiltrated by Chinese that one of their printers actually started printing a Chinese print job. So the hackers
had actually--were so blasé about the infiltration that they sent a print job to the wrong printer, which was a printer in the U.S. Department of Commerce. So it's common-- it's a common thought amongst security professionals that if you are doing business with China, it's pretty well assured that your network is either under attack or it's already been infiltrated by the Chinese government.

They want to know what you're doing. They want to know the inside information. And they're not the only ones. There are many countries that practice cyber operations to better their own companies, to better their own positions in the world, so... China's just leading the way. There are many other people that do that--many other countries that do that.

**Ideological and political extremism (hacktivism)**
Probably the most frightening ones are the next group, which are the activists. These are the ideologues who-- with nothing better to do would like to attack various sites for a particular reason.

Now, we're seeing that recently in the last week with the U.S. SOPA legislation going through Congress how the group Anonymous attacked, you know, FBI and many government sites, brought them down, and are able to do that really quite easily and quickly. So we see a lot of these sort of activisms--activism groups sort of popping up now.

In the case study I'm gonna use today in this presentation is actually--looks at one of these activist groups, the Anonymous group, and what they've done and how they actually operate.

**Criminal organizations for profit**
Then we have the profit-motivated groups, and we've got a lecture later in the month on criminal-motivated cyber threat. But really these are the ones who want to get money out of you, and they use a number of different threat-makers to get into your system, so whether they just break in and get information or they put malware on individual devices, use your computer in an attack against somebody else-- a lot of different things there.

**Individual hackers for personal gain**
And then we have the last level, which is now personal gain, the people who do something just to say, "Look what I can do." With cyber security or information security 30 years ago when I got started, the last group is probably the most prevalent in this field. People were hacking just to show other people what they could do.

The other top three groups really weren't on the scene, and they've really grown in the last 30 years. Particularly since everyone's now connected to the internet, it's much easier to get a threat vector and to infiltrate different systems that are connected to the net, and people are connecting a lot more information, a lot more systems to the internet and are not doing it in a secure way and they're allowing a lot of these security holes to appear.
We can actually define what we call threat economy where we have, on the left, people who actually develop the threats, develop these sort of worms, spyware, malware. Then we see the middle men, the people who are able to sell those wares to other people and produce, a lot of times, that sort of--that capability and then hit the end user.

So there's a different number of end values that they're after, but, really, they--you follow the money, you find out where these sort of things are all happening.

So here's a good example. In Russia, there's a botnet site--there's a number of botnet sites--that you can--if you wanted to become an overnight master criminal, you just go to that site, you hire a botnet, get them to install your malware on as many nodes as you can afford to pay for, and then you are allowed to sit back and enjoy the revenue coming in.

So these sorts of things are real, and a lot of these are quite frightening, because they're hard to stop and wouldn't take long on the net to find a number of these people who are selling 10,000-plus botnets to do the work of a criminal for you.

**Steps to Hacking (11:20-43:44):**

So let's get on to thinking like a hacker. So really if we're looking at the top--the top three threats, so we're looking at our state-sponsored and our criminal organizations and largely our ideologues, the thing with these hackers--they only want to be able to get into a system and then get out, and the best hackers is one that is not actually discovered.

So if you can infiltrate a system, do what you want to do, extract the information you want, and then leave and cover your tracks, that's what we call sort of the perfect hack, if that's what you wanted to do.

There's a lot of other less sophisticated attacks that we're seeing, particularly in the criminal world, where they go and hire a botnet and essentially hire--hold for ransom a company to take in their website.

Recently I was involved with Cisco. We had a company here in Australia which was at--had exactly that. So they had a ransom that was sent to them. A botnet was launched from Estonia at that corporation. Very effective. And there's not a lot you can do about these things, 'cause you've got to--these botnets come from all around the world, so it's very hard to just put simple blocks on file or things like that.

These things occur from multiple sources around the globe. But luckily, in this case, all the botnet came out of the Eastern Bloc and so they were able to block that traffic. But this is a very, very common criminal activity when they can hire
botnets and hold people for ransom. The first step in thinking like a hacker is reconnaissance.

Reconnaissance (12:55): Gathering information
Now, hackers are very patient, and they're very clever people. So what they will do, before they go into a site, they will get as much information as they can that they think they can use against you. And surprisingly enough, a lot of businesses and a lot of corporations publish far too much information on their own corporate websites. This includes email addresses and usernames and things like that-- things that you can probably use to gain access to the system.

Also, one other popular one is social engineering, so meeting people and using the weakest link in a security chain which is the person to gain information that probably wouldn't be easily obtained through any other means. We should say that social engineering has turned a new face, so if we--we're seeing now that sites like Facebook and those sort of sites are just a goldmine for the criminal hackers who spy on Facebook and look for information that you have accidentally put up on the--put up there. But they can use that information against you. So I would warn anybody who uses Facebook to making sure that information you put up there is kept fairly innocuous and can't be used against you.

So Google hacking is also a good one, and I've just got a quick demonstration of that right now. So I'll pull up a search page on my browser, and what I'm doing is, I'm actually using Google to do the work for me. So I'm a hacker, and what I want to do is look for sites where perhaps there had been a naive or lazy programmer and they haven't really-- they might have left a password file or people list file out that one of the web crawlers has picked up.

Just use Google, see if there's a people list file, and sure enough, there's a-- there's a password that's being picked up by Google. I can then look at that, go and have a look, grab a password file, and then see if I can break the passwords using some sort of hash-- hash collision technique, rank by title, that sort of thing.

We'll get on to passwords a bit later. But I'm using Google to do all that sort of reconnaissance for me so I can go and find these sites. Google hacking is a very common tool used by the hackers. I just showed you a very simple one.

But what about this one? This is an actual real Google search, and it's one that's recommended by a couple of the hack sites in Russia. So what I'm asking for here-- I'm saying to Google, "I want you to find me all of the documents that have some sort of"-- So these are the doc, PDF files, et cetera, that have confidential in the actual document itself. Things like budgets, those sorts of things. I could extend this. Interesting--if you run this, you see there's so many hits, it's just unbelievable. I haven't run this on this slide. I'll leave that for some homework for you to have a go at.
So if you put this in your Google search engine, you'll find so many different PDF files and confidential salary writings with people's names and all these sorts of things, so it just makes it a hell of a lot easier for a hacker to find out about the sites and this sort of information.

I put this up as an example of a very good social engineering exercise that this--a guy called Jim Stickley. He's a professional social engineer. He sells these services to companies just to prove that social engineering allows him so much access to sites. And this guy--and he's-- They posed as firemen, went into a bank, and claimed to do a fire safety survey of the bank. So they're let into the bank. They were shown all the systems. While he was going around, he got away, attached keyboard loggers; they wrote down--as you know, people put passwords on post-it notes on their screens; they were able to take down passwords, usernames.

They left the bank and came back and were able to show the bank how much information they were able to steal just from a simple social engineering activity. So if you're working in a very sensitive field-- and we see this all the time in our mining industry, particularly in Australia, where you're overseas and you're approached or tried to be picked up by somebody or someone starts a conversation, just be aware that they may not who they seem they are-- they seem to be. And it's very easy to use social engineering to get additional information about a particular company or the target they're after. And then we go to scanning and enumeration.

**Scanning and Enumeration (18:10): Identification and exploitation of vulnerabilities**

This is really sort of old-school. This is where we are trying to work out, well, okay, I've identified my target. Now I want to see what’s open, what ports I can get into, what sort of vulnerabilities have they got at the network level to get into this particular system?

Now, luckily, we have very good security devices now that pick up a lot of these. So we got firewalls and Intrusion Detective and Prevention Systems will light up like a Christmas tree if somebody's doing full port scans on a particular system. But what if I had a piece of malware that I was able to get on the inside of the firewall? What if someone had, through sort of drive-by attack, I was able to put a bit of malware on somebody inside the system where the IDS is not normally placed?

So the IDS is normally placed toward the edge of the network for people coming in, but if I'm already inside, we'll get a nice bit of malware, and I can then start looking for vulnerabilities on the network that generally aren't picked up by any IDS, IPS, or firewall. I'm on a trusted system. And what they do-- the hacking techniques here is that rather than use, you know, the old, "Oh, I'll just scan all
the computers on this network "and leave a great big crash if anybody's listening to this sort of ping sweep." I'm very patient.

So I've got a bit of malware. Rather than scan all my devices in the next minute, what I'll do is just to scan one device every five minutes. I've got a lot of time. I don't care. These things aren't picked up by any IDS. It's very innocuous and so low level it won't trip any threshold. So I'll just check a host every couple of minutes, and I won't be using ICMP. What I'm gonna use is one of the other flags in the TCP. So ICMP's an easy one to pick up.

But if you go to the diagram here with the three-way handshake of TCP, the SYN, SYNACK hack, which is very common for guys doing networking on the call. Denial of Service attacks, what they--will employ what they call Half Open SYN attacks, that'll do a SYN-- the host will do a SYNACK, but they won't ACK, so the port's left open.

The theory behind that is if I do enough of these, the Half Open SYN attacks, I'm here, so he's allowing that thing to go by, and they won't be able to answer any other networks. Very simple and very effective attack. But it's also very picked up quite easily even by host-based IDSs and host-based firewalls. What we see hackers doing is playing around with these TCP flags and the TCP headers.

They're not actually using SYN and ACK. They'll use something like the SYN flag or a Push flag, and they won't let the others-- might set the other flags, because I can just use a FIN flag and I can still use that to see if a port is open on a particular system. I won't get any response. That tells me that it's open. If I get someone that comes back and says it's reset, then I know that that port's closed.

So I can use what they call stealth mode to actually look around the network and find other ports. So I've got a bit of malware on the inside. Then I use these sort of stealth mode attacks to work out, well, what's open, what's available, those sorts of things. And these things are really picked up by your internal security devices.

Okay, so while your external armor and all that is-- your firewall placed at the edge are picking these up. So if I'm on the outside trying to break in with a brute-force attack, I'm gonna be picked up by your firewall and your IDS. But if I'm on the inside, it's a different story. We're gonna look at scanning and enumeration from the web side of things.

So we've looked at the networking side or looking at what ports are open and what hosts might be allowing other vulnerabilities. The biggest vulnerability by far is the end user on a web browser. So hackers will look at what websites and application vulnerabilities I can find just simply by the web, and really, the two outstanding hacks that we're seeing-- two attacks called SQL injection and cross-site scripting.
At the moment, these make up about 30% of all attacks on the end user's device, and they completely bypass your firewall and IDS. I mean, people say, "Well, I've got an IDS and an IPS. It's gonna pick up an SQL injection attack." It's fairly difficult to do that, because they're after your signatures-- after your--based on a signature-based security method. It should look for specific signatures, and with SQL injection, it's very, very easy to change the signature and use different signatures to do the same thing. And the attack signature database is always catching up to where--what's happening at the user space here.

So what would those attacks be? The most, I guess, frightening for a security professional is the zero-day. Zero-day just simply means this is an unpatched vulnerability in a bit of web code or a bit of software and operating system. And why it's so frightening is because we just don't know-- it doesn't-- we don't know it exists until somebody tells us it's there.

I mean, you look at an application like Windows XP and Windows 7, millions of lines of code with thousands of libraries, and you can guarantee there are still an untapped number of zero-day faults in the operating system. In the browser, in things like Adobe-- Adobe Acrobat, Adobe Flash-- all these things have holes in them that we don't even know about. And they're probably the most scariest things that are around at the moment.

The best defense against this sort of attacking is, we have some really great web applications, email application firewalls. So these are things--I've got my networking firewalls, but I also need some sort of application firewall to guard against. And these will remove 90% of the SQL injections. They say that no product is perfect for this, and you can always get around something, and the hacker is always one step ahead. Endpoint protection is very important, and also, primarily, user education. Just warning the user that these sorts of things can happen and when to be-- when to show caution when they're going to a particular website.

I just want to show you-- this is the--sort of a breakdown of other-- other threats that people-- of the--one of the website monitors are picking up at the moment. As you can see, SQL injection and cross-site scripting make up the majority, but there are just so many others--other attacks, other threats that are happening on the web. And this is a bit worrying. There--got 19% of unknowns, so these things are coming in. We don't know there's a signature. We don't know what to call them. We don't know what they are. But they're--there's just a large number of threats, so we're definitely not on top of this by any stretch of the imagination.

I want to take you through a quick SQL Injection demonstration here, because wherever I go, when people ask, what does it mean, SQL injection? It sounds very technical, but it actually isn't. It's actually probably one of the easiest hacks around, and it's just unbelievable. It's still--possible to do this today. And it all centers around the fact that people writing back in database applications don't do any parameter filtering when they take the--when they take the filter off the
website, when they take the parameters from the website. So they just feed it straight back into an SQL query.

So in this particular demo, what I'm doing is looking for a page that I know is gonna do some sort of SQL query like this. I'm--I want to break into a page that, it's just doing a simple selecting all from users where username is John and password is whatever, and these are two variables that are being passed through the host from the website.

So let's say I've come to a company login page, and I used my reconnaissance to work out, well, I definitely know there's a user called John, and I want to break into this page. And I can use--I can use a password that I've guessed through brute-force if I want and try and get into their passage, but that's really hard. That takes a long time to do that, and I generally get sick of that sort of thing. You could probably write your own bot to do it, but the easier way to do it is to do something like this. At the end of the guy's name, I add a few more things to his username field here, so... I don't have to put any password in it at all, and magically, I can log in as John. And the reason why that works is because what I've done is; I've kind of finished off the SQL statement and made it true in all cases for when user is John.

I don't really care about the password. That's just allowed me to log in as that person because the website developer of that site has not done any parameter filtering whatsoever and just placed that directly into an SQL call. Now, these are really, really dangerous, because if you find a site or if a hacker finds a site that's got a weakness or a vulnerability within an SQL back-end database, they can do anything they want. They can drop tables. They can add tables. They can get a list of a table. They can look at other tables, fire up the whole database structure, and that's generally what--what--the most attacks we're seeing today. Anonymous, their favorite attack is this SQL injection.

**Gaining Access (28:48): Cracking passwords, root kits, privilege escalation**

So once we're in, we've gained access to the system through some poor user who--or some poor programming, what we want to do now is hack some passwords, and I want--I want to look at a couple of hashes, because we're probably all aware, computer systems, when they store passwords, they generally store them as a hash, and the most popular one around in the past has been a hash called MD5.

The old versions of XP and early versions of NT used an NTLM label, which is actually an MD4 type of hash, which is even less secure. And unfortunately, Cisco routers still use MD5 in its hash for its passwords as well. If you do service password encryption, it'll show that as an MD5 hash. MD5 is largely broken in the fact there's no security agency in the world now that recommends using MD5 for anything. They recommend SHA-2 as a minimum for any hashing algorithms, and I'll show you why very soon. We'll just take a quick look at passwords and why they're so important, okay?
Module 1: Think Like a Hacker, Defend Like a Ninja

So a couple of years ago, there was a website called RockYou. And through an SQL injection flaw in their database, a hacker was able to get in and pull nearly the entire user database of 32 million users. And not only was the application developer who wrote the site bad with his parameter checking, he was also bad with storing the information.

So all the passwords were actually stored in SQL, so he gained access to all 32 million accounts and their passwords in SQL. And it's not like he decided to publish that and show how wrong, how bad the RockYou site was-- you know, that they didn't actually use that against the people who actually registered, because what we're finding is that generally people use the same password for a number of sites, and the hacker here, luckily, he decided just to out the RockYou website and show them how bad they were, and they were able to bring it down. And hopefully people changed their passwords who were on that site.

But interestingly, the top 10 passwords that they noticed from those 32 million were these. And I don't want to hold up all of you today on the--on WebEx, but I guarantee there are a number of you who are listening in who probably use one of these passwords already. And you probably use these passwords more than once, so you probably use it for your Twitter account, perhaps, and your Facebook account and maybe some other account-- your email account. And--which opens up this issue that if someone breaks your password once, they will use it again. They will try and use it in other places, so it's a good idea to not have the same password, particularly for one of your social media sites, unless you want to have them owned by somebody else.

A hacker will use these default, use this knowledge that they have about these default usernames and passwords-- the top ten users and start with those when they're trying to break into an account. This default username/password, this first point here, actually applies to things like Linksys access points or Cisco routers when you first buy one. They have a default password, so Linksys is "admin" and "admin." Cisco routers used to be Cisco, Cisco login. Same for every other consumer electric device that has network access.

Again, we find, there will be default usernames and passwords. And, unfortunately, most people don't change them. So if you're driving down the road and you find an access point that's open, chances are, that will also be using a default username and password to get into that access point. So it's a very important security lesson to change those default passwords, 'cause they're the first things people look for.

Other methods for cracking passwords. Unfortunately for us, our computing power is doubling every year, and the hackers have found really great ways of hacking into our hash passwords. What we've--what we're doing, how we're extending GPUs, our graphics processing units-- so all these fantastic 3-D
Module 1: Think Like a Hacker, Defend Like a Ninja

graphics cards that we’re using these days to play these games are also turning out to be very good number crunchers for breaking into passwords.

So what we’re seeing is that, like here, I've got a single GTX NVIDIA card. It can take less than five days to crack a password using a 69-character key stroke. The GPU is increasing again, so they're like a normal CPU. So they--they double in processing power almost every year as well.

So as an example, this is why MD5 is a bad choice for password hashing. A GTX 295 card will break-- can break almost 1.2 billion passwords or can brute-force attack at 1.4 billion passwords a second, which is a frightening number. What does that mean? Well, it also means that we can join these things together in a distributed hash attack, so just take down this number here. Go on salting an MD5 password. Those of you who don’t know what salting means, you'll have to enroll in the CCNA Security course or the CC entry course in security and they'll teach you all about it.

But it's a more secure way of doing MD5s. So I can--I can break, say, 1 million hashes per second with a salted MD5, or with a standard MD5, I've got 2.5 million hashes per second I can do with these sort of distributed hashes. And this is--like I said, these are all the cards. The latest generation can double this again, and next year, you can double it again. Like I said before, MD5 is basically insecure. If you're using any form of hashing algorithms in your system, you'll be better off using a SHA-based-- SHA-2 based system.

So what does this all mean? It all comes down to what we call password entropy. Now, entropy is a term we use that specifies the amount of randomness in a password, so if I'm just using-- and it comes from Shannon's information theory. It's basically locked to the available character space. So if I'm just using a character full of digits-- so from zero to nine-- it works out that there's an entropy there of about 3.32 bits a character. So if I'm gonna make a character password, so I've just used 12345678, like all the people on... It's gonna take less than a second to crack that password using--even if it was hashed and salted MD5 using that-- those distributed password hashing cracking methods.

So even if I moved up to start using lowercase letters only in my password, it's still gonna take 58 seconds to break that password. That's why it's important. You see people or sites you go to continually ask for you to have eight-digit character passwords which have upper and lowercase, a digit, and a special character, because as you can see, it’s an exponential-- it makes an exponential difference in cracking these passwords, so if I've got a full 94-character prompt or word prompt, an eight-character password salted MD5 at a million hashes per second, it's gonna take 200 years to break that password, theoretically.

So that's why it's always worthwhile to use those sorts of-- lots of traits in your password. If you've got a really simple password, it doesn't take very long to break. If you're not using a salted MD5, you're just using a straight MD5 or you're
on an older XP or NT system, if you're just using an NTLM type hash, then multiple that-- divide that by 2,500. So your eight-digit password here would be broken in under an hour instead of six years. So that's the sort of quantum-- exponential lift you're seeing in this password breaking, and this is how they're getting better year after year.

But one point, and this is made well by of the "XKCD" guys who writes these cartoons, it's--it's not necessarily the complexity-- a short complex password that's hard for you to remember. In general, a longer password would also be very, very secure.

So if you've got a passphrase that you can easily remember, you can get away with using upper and lowercase letters and be far more secure than somebody using-- a password using all these letters, 'cause it's very hard-- something that's very hard for you to remember but easy to break. That's the point he's making in the cartoon. So if you've got a passphrase, they're actually much harder to break in the hashing with MD5.

So I want you to take you through a quick case study here. And one of these here is HBGary Federal. This was last year. HBGary Federal is a security firm. And they were trying to drum up business for their company with the Intelligence community in the U.S. And the CEO was doing some research, and he believed that he could uncover the identities of the Anonymous group just by using his sort of method of looking at Facebook and looking at associations in Facebook. So he was doing some Facebook trolling through social engineering around Facebook, and he reckoned he could uncover the identities of the Anonymous group. He couldn't. It was a total fallacy. But he made the claim, and he made it publicly. And unfortunately, it upset a number of the Anonymous groups.

A good point here to take away is that if you come out publicly against a hacking group, you better be sure that you can withstand their assault on your website. This firm was an actual security firm, but it turned out that their website was horribly insecure. They had very-- a lot of vulnerabilities in their--in their content management systems, which allowed Anonymous to access via a simple SQL injection, and they were able to pull off all the employee usernames and passwords. Basically in the same method that I just gave a demo on before, they were able to break in and pull down the whole user database. They were using an earlier version of MySQL, which used a not-so-very-good password hashing algorithm, and they were able to break the password quite easily.

So then they had the whole site, the whole employees, and the passwords quickly cracked. From what they cracked, they were able to pull out the Chief Operating Officer's password, and they discovered that he reused in other accounts, like his Twitter and LinkedIn accounts, so they hijacked those, took them over.
They also found that the company server was also-- used the same password, so the COO used the same password for a number of places. They were able to break in and delete files, shut down computers, delete backups, things like that-- just wreaked general mayhem. Remember, this is a security firm. This is a firm that advertises itself as being a leader in network security-- a leader in endpoint security, at least, anyway.

Once they had the CEO's password, they also decided to have a look around with that, and they discovered that he used the same password for his Google apps account for the company. So they were able to get into that. They were able to grab all the emails-- 60,000 emails from the company, and they published them online.

So imagine if you were a security company and suddenly, all the emails that you thought were confidential between them were suddenly published online. So they started to lose face a bit by this attack. But in the end, the co-founder-- So HBGary Federal has a parent company called HBGary. The co-founder's email account was also compromised, and the parent company's website was also defaced.

Now, it was probably the worst time, because they were trying to restructure the company and sell it. They had a number of buyers for the HBGary Federal at the time, but all of them all walked, and so HBGary Federal no longer exists, and it doesn't exist anymore because Anonymous, that activist hacking group, decided to askew the company, and they basically brought it to its knees and destroyed it. So HBGary Federal no longer exists.

You can still find the HBGary website. They make no mention of this attack, which is--funnily enough, but there's plenty of it written on Wikipedia and whatnot, and you can have a look at it for yourselves. I encourage you to have a look at how not to do-- how not to threaten the Anonymous activist group in public. It's a very good case study for that.

**Defend Like a Ninja Using Cisco's Approach (43:44):**

**Trust**

So how do we defend, then? Now that you see--and, again, I've only scratched the surface on what hackers are capable of and what they can do. But now we're looking at, well, how do I defend against a hacker? And from the Cisco point of view, you have--we have a sort of a mind-set where we look at trust, visibility, and resilience, where the idea is that we need to be able to trust the network and the end users that are attached to that network, we need full visibility of what's happening so we can prevent detection-- any attack, and we need resilience. We need to respond to it. We need to be able to recover. We need a plan B if our whole network has gone down. We need some sort of continuity of operations.
So this is the sort of thing that you'll be entering into as you progress along your training in the Cisco networking academies and things like that. This is their sort of approach to this. So it's really about the who, what, where, when, and why about these hackers. So with my trust, I really want to know who's on my network and what devices on my network. So I'm using things like my identity and access control. I'm using things like identity-based network security, and these sort of things with that new technologies like TrustSec and those sorts of things we can do. It discerns between a user who is, say-- a user at the desktop and somebody who is VPNing in from, say, a wireless hotspot at the local cafe or local McDonald's.

And I want to be able to give those two types of modes of access to my networks a different access, so I want to be able to say, well, if you're at your desktop, I want to be able to give you better access than someone who's, say, VPNing from a public network. And those sorts of things are absolutely possible to do these days with things like TrustSec.

And we also look at-- we must do physical security and audit and compliance checking on our network. It's no good to us just building it, working, and then say, "That's it." It's always good practice to have a physical security checklist, make sure that your servers are secure, make sure your equipment is secure, and have it regularly audited and be compliant to whatever standards you have in your particular country or region.

**Visibility**

But then we look at the visibility options. So we want to know what threats are present and where they are and how do we take action, so this is where we're looking at continuous monitoring of the network. It's very hard to monitor everything.

There are a lot of things. There are a lot of signatures that give false positives, and we have to make sure that we can look at what will work and what doesn't work in your particular area. You need to know what data is leaving your network. Data extraction is a very key problem these days, particularly through the email system, so knowing what information is being sent out and having some sort of email file to make sure that sensitive information is not leaving the company accidentally or on purpose.

Looking at what malware and advanced phishing threats for the defenses you might have as well in the visibility. So then we look at how do we avoid disruption? And how do we mitigate the risk? How do we get back to trust our network? And that's on our resilience side of the hat.

**Resilience**

So looking at our continuity of operations, incident handling, and how do we mop up after an attack? Always good to document the process and procedures that you have. And after you've had an attack or if you sense an intrusion in your
system, it's always good to document or write it up so you can learn from those mistakes and so--so you don't go down and that same thing happens to you again.

So in terms of Cisco, we have quite a broad-- quite a broad set of technologies and products that cover these areas of trust, visibility, and resilience. And as you sort of progress your training from new entry-level security right up to professional and expert level security, you'll come across all these sort of devices. So even in your network-- associate level, you will come across a lot of the VPN and access control devices and learn how to use them and learn how to put them in a network and where to put them in a network.

So it's a great series of qualifications to go through, from entry to associate to professional to expert, if you want to pursue that. And it all starts with the first step, so I encourage everybody, if you haven't already started, to go to the Learning Network, Cisco.com, and have a look at all the courses that we have in the Security stream and see which ones you'll find interesting and which ones you can follow.

And I certainly started my career a long time ago with CCNA, so it's a very good qualification to start with and to work on. It's very easy these days to take a course and--online or through a provider and pass that qualification and move on. And that's really my presentation for the day, so thanks very much. Please fill out your feedback forms and join me on Facebook if you have any questions. Thanks very much.