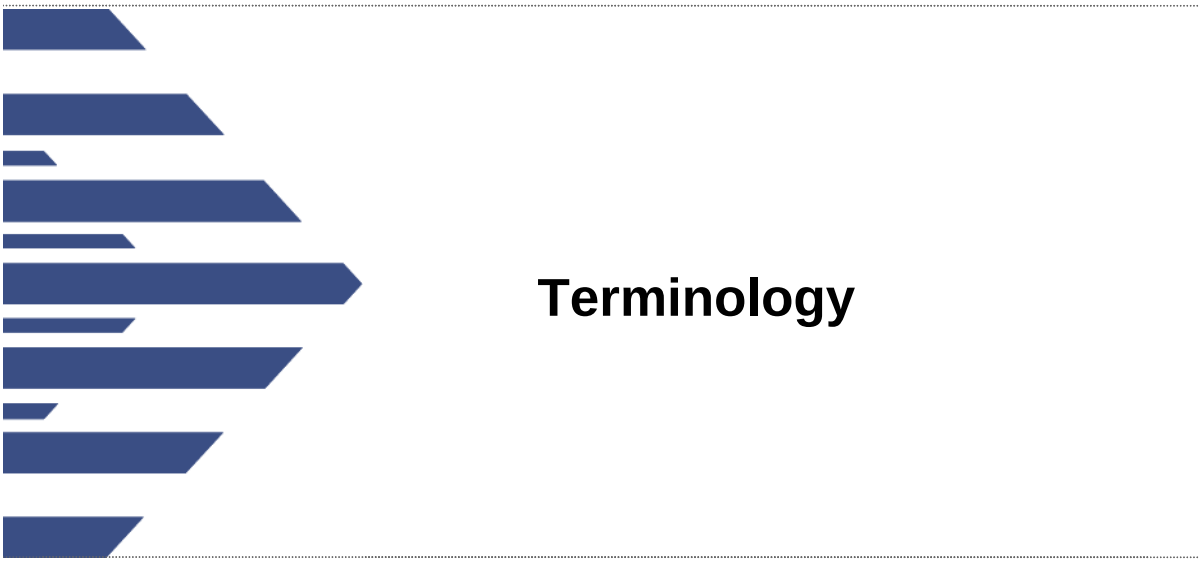
Ethical Hacking Terminology

Table of Contents



**014 So we have a bunch of terms that we need to go through.

Terminology -1

Threat	An entity or action that has the capacity to exploit a vulnerability
Vulnerability	A bug or glitch in software, operating systems, or firmware that can be exploited, leading to a system compromise
Risk	The probability of a threat exploiting a vulnerability.
Attack	The action of a threat exploiting a vulnerability on a system or network
Target (of Evaluation)	A system, program, or network that is the subject of a security analysis or attack

**015 We'll just kind of start listing various things out here. What is a threat? A threat would be me.

A threat would be my compatriot over here. Somebody who is going to- or an actor who is going to do something to you. What is a vulnerability? A vulnerability is something that I can take advantage of. It's a flaw in a software program. It's a misconfiguration. It's something wrong with your systems that I can take advantage of. A risk. A risk is probably those of you who have had risk management or risk assessment backgrounds, you might disagree with this definition but the risk here is the probability of a threat and vulnerability

being exploited. An attack, this is the actual action of exploiting a vulnerability. And then a target is what I'm actually going against, a system, an application, something like that.

What happens when all of these come together? What do I have? A breach? Okay. I have a problem. Might be a breach, might be somebody exfiltrating information. It might be a denial of service attack, I have a problem. If you take away any one of these, what do I have? Let's say I have a threat, a vulnerability and a risk and I have an attack but I have no target. What happens?

Student: Still there's a problem.

Chris Evans: Could be a problem. But if I'm missing any one of these what I'm getting at is if I have all of them together, I have a problem and it's a very interesting talk at Black Hat or DEF CON. If I have two out of the five or four out of the five, I have a little interesting idea and maybe a side discussion at Black Hat or DEF CON. Generally it's not a big deal. You might have a problem but without all five of these it's not definite. If you have all five of these, you really have a problem.

Terminology -2

Exploit	A procedure or code that takes advantage of a vulnerability in software, an operating system, or firmware
Remote Exploit	An exploit that executes over a network, without physical access to the target system
Local Exploit	An exploit that executes directly on a target system due to previous access to the target system

**016 A couple other issues here or definitions of exploit, what do we mean by exploit? This is a procedure or code that takes advantage of a vulnerability so your actor or your threat which we define before will have an exploit that they will run against a target. There are two types of exploits that are out there, the general categories of them are a remote exploit meaning this is a piece of code that I can again sit in a hotel room halfway across the world and affect directly that system right there. A local exploit is something that I have to actually have access to the system already to be able to run that so I can't run these local exploits from around the world unless I've got some other method to access that system. So remember remote

exploits are things that make very big news. These are usually things that are rated as critical vulnerability when it comes to patching. There are things that you can fire off at a system. As long as it's connected to the Internet and it might work. Local exploit you have to be sitting on that box already in order to run it. That means either physically on the box or maybe you've got some other malware that you put on there in order to take advantage of it.

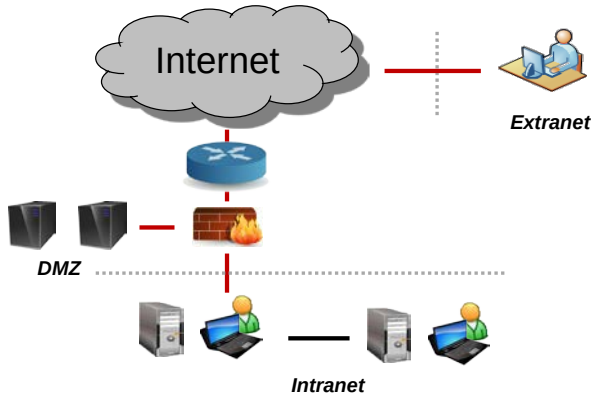
Defense in Depth

Defense in Depth

Using multiple security controls to protect an asset

- The idea is if one security control fails, another will hopefully stop the attack.

Example: A screening router, a network firewall, a network IDS, and a host-based firewall



CERT | Software Engineering Institute | Carnegie Mellon 17

**017 You'll see a lot a term called "defense in depth". This is the idea that you've got multiple systems, multiple controls security controls in place to prevent various types of attacks. The thinking is

that if you have one black box and nothing else around it and that's what you call network security, if the attacker gets by that black box there's nothing else to stop them. And so defense in depth is this notion of having multiple controls, multiple steps, multiple hurdles that the attacker has to go through in order to do what they want to do.

Let's talk really quickly about motivation levels of hackers. If let's say Laurie has a system that's got really good defense in depth and it's protected by two fire walls and has a host-based intrusion detection system on it but there's really good critical information stored on that and then has a system that has critical information on it but it's only protected by let's say network address translation or something like that. No firewall, no intrusion detection system. Me as the hacker, who do you think I'm going to go after. They both have the same information on them. One is very heavily defended and guarded, one is not. Which one am I going to go after? The weaker one, right? Because me as a hacker I am inherently lazy and why would I go through all of the speed bumps and the hurdles that she's put in place if I can get the same information by getting into the system very easily? The general hacking mindset is unless you are an advanced persistent threat and that term has been overused and under-misunderstood for a while but unless you're a very well-resourced attacker and very persistent in what you do, generally hackers are lazy folks. They're out there to make a name for themselves. They're out there to do what they need to do as quickly as possible and then go on to the next bright shiny object. And so what

you'll see is that the defense in depth strategies work because not because they're the silver bullet of network security but because they are a deterrence factor. It's so much work to get through all these layers of defense that I'm not even going to bother with it. I'm not going to do it. I'm just going to go after the easier target. And that's the point behind implementing a defense in depth strategy.

Confidentiality, Integrity and Availability

Confidentiality, Integrity, and Availability

Core security principles that ensure layers of defense against disclosure, alteration, and denial or the DAD triad

Confidentiality

Ensuring information is only available to those authorized to have access to the information

Integrity

Describes the wholeness and completeness of the information without any alteration except by authorized sources

Availability

The ability to use the information or resource when it is needed

CERT | Software Engineering Institute | Carnegie Mellon 18

**018 Confidentiality, integrity, and availability, you see this a lot within the network security world because everybody kind of latches onto this and go says we have to provide confidentiality. We have to provide integrity, we have to provide

availability. Well confidentiality is nothing more than making sure that information is only available to those who are authorized or who have access to see it. Integrity is protection of that information and make sure that it's not modified except by people who are supposed to modify it. And availability is making sure that that information is accessible when it's needed. So how would you go about ensuring confidentiality of something? What are some strategies that you can do to provide confidentiality? I'm willing to bet you use one or two of them every day? What would you do? If I said "This email message has to remain confidential," what would you do to protect it?

Student: Encrypt it.

Chris Evans: Encrypt it, yep, use your PKI or CAT card or something to encrypt that message. What else could you do with it?

Student: Provide an authentication to see it?

Chris Evans: Authentication or authorization methods to actually see it, right. You could also delete it but that would kind of impact the availability of it. What about integrity? What could you do to make sure that that message isn't changed by people who aren't supposed to change it?

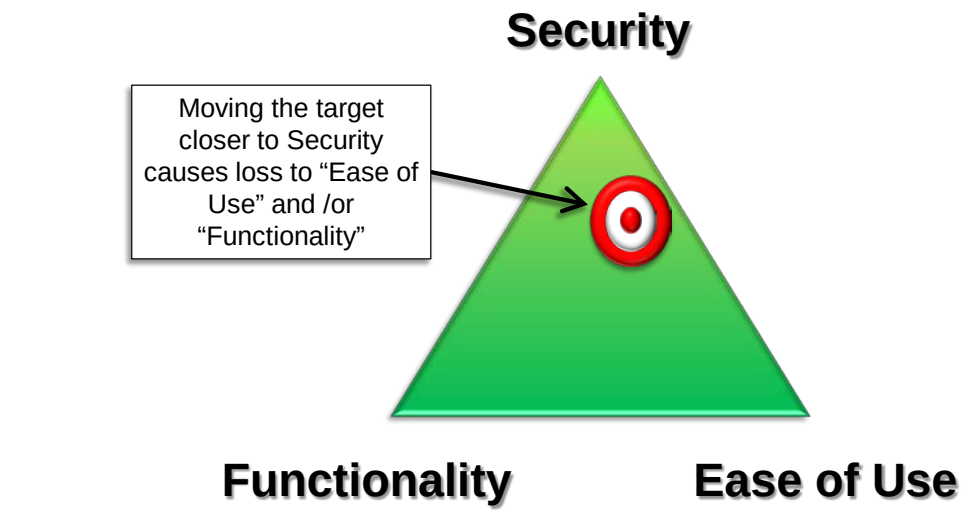
Student: Provide a checksum?

Chris Evans: Checksum or hashing algorithms, yep, signatures, digital signatures. What about availability? How would you provide availability of email or more accurately the email system itself?

Student: Redundancy.

Chris Evans: Redundancy right, so you have encryption, hashing, and redundancy. Those are the three primary methods that you go about accomplishing all this. So what is your job as an ethical hacker? Circumvent encryption, get around, find ways to break hashing algorithms or hashing schemes that have been put in place. Or for availability how do you defeat redundancy? Find the single points of failure and go after those. Again, so if your organization subscribes to this model that you need to provide: confidentiality, integrity and availability, your job now as an ethical hacker is to go through and find ways of defeating these protection measures that you've put in place.

The "Ease of Use" Triangle



**019 There's a constant battle between network security and convenience. Nine times out of ten what wins?

Student: Ease of use.

Chris Evans: Ease of use or convenience, right? Because we're not willing to impact the end user experience for draconian security measures. And so what you'll see is that generally if you have functionality and ease of use over here security, if you start putting in more ease of use, generally you're getting rid of security or you're reducing the effectiveness of security measures or maybe reducing functionality. So again, as you're going through your ethical hacking routine and

you're coming up with recommendations, understand that your recommendations are going to have to balance these three things. Because if you come in and say you've got to have this security measure, you've got to have this control, no more single sign on. Everybody can't go browse MSNBC or something like that. We're shutting off all Internet access on the network because we're getting hacked through the internet. That generally is not going to work. You will probably get laughed right out of your, or screamed at, right out of your out brief. So understand that as you go through ethical hacking and you're finding these problems, you have to recommend solutions to those problems and they have to balance these three areas because without that they're going to end up draconian security or no security at all with ease of use. So that's one of the challenges you'll have to do is balance that.

Types of Hackers – Black Hats

Use their skills for malicious and illegal purposes

- **Script Kiddies** – Individuals who download and use scripts/exploit tools with no real understanding of the concepts being employed in causing an effect.
- **Hacktivists** – The non-violent use of illegal or legally ambiguous digital tools in pursuit of political ends.
- **Business/For Profit** – Hackers who use their skills to earn a profit from selling the capabilities of their exploits or rent the use of hosts under their control.
- **Crackers** – Reference for hackers who use their skills for malicious purposes..

**020 There are various types of hackers out there: black hats, gray hats, white hats. What would you define a black hat hacker as? Clearly somebody who has malicious intent, right? They're there to break into the system. They're there to do it for profit, all of the things that we kind of mentioned before. They're there to do this maliciously. There are a couple of different kinds of black hat hackers, script kiddies which are the person who goes out and downloads something off the Internet because it's cool and they plug in an IP address and click a button and say it says "Start Attack." They don't know what's going on behind the scenes. They don't know what that tool is doing. They're just kind of hopping on the hacking

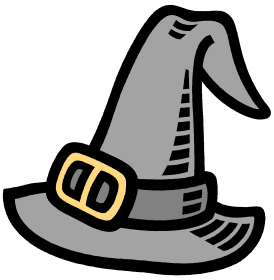
bandwagon and having a good time with it. Hacktivisits, these are folks who usually have some type of political message or statement that they want to make. Look at everything that the Anonymous and [Inaudible] security groups have been doing over the last two or three years. This is predominantly hacktivism. They're there to make a statement. They're not doing it primarily for profit. They're doing it for a statement to make some kind of get their message out.

There are cyber criminals out there who do this as a business and do this for a profit. It's amazing. You can take a look at YouTube for hackers for hire and you'll see videos out there of people who are basically putting themselves up and say look, I'll hack for money. You send me a task and a check for 500 dollars. As soon as the check clears I'll go out and do this task for you. You can actually find ads out there for these hackers for hire. And then there's another term up here, "crackers". The idea that these are folks who are hackers but using their skills for malicious purposes. There's a lot of confusion about what is a cracker, what is a hacker? Generally these are the definitions that are used. If you stick with these this is making sure that everybody is on the same page with regard to terms.

Types of Hackers – Gray Hats

Use their skills for both offensive and defensive purposes that are not illegal or malicious and have approval to operate

- **Penetration Testers –** Take a holistic look at an organization in identifying vulnerabilities to a network and systems.
- **Red Teams –** Team of experts acting as an adversary (hacker) to penetrate an organization just as a Black Hat would do but with the intention of stressing and/or training the organizations security programs and processes.



**021 Grey hat hackers, a little bit different category here. These are people who are using offensive skills for defensive purposes. What does it sound like? What type of hacker would be doing offensive stuff for defensive purposes? What's the primary role of an ethical hacker? Doing bad stuff for good purposes right? So if you were going to look at where does ethical hacking fit into am I a white hat, am I a grey hat, am I a black hat, it's probably more squarely fit in here with grey hat hackers.

And so you've got pen testers and red teams. Those of you who are within the Department of Defense community are probably very familiar with the idea of a

red team contrasted to a pen tester.
So a pen testers comes in and they take a really kind of broad look at your network and go look, here are the things that we can take advantage of to access the network, access information, these are the holes that you need to fix. Vulnerability assessment or vulnerability testers are there to find all the possible holes in the network. Pen testers only look at specific ones or give them access to meet their objectives. Red teams kind of apply all of that. When you're using a red team the notion is that you want somebody to be able to provide a stimulus or replicate some type of threat and so you kind of see that to a little extent with pen testers. Maybe they'll do social engineering. Maybe they'll do some type of exploit, zero-day exploits against you, but it's not really guided by any set criteria or any type of motivation. Red teams are motivated by threats and so what they'll do is they'll go out and they'll research various threat entities and various actors and then they'll apply that in an exercise environment or as part of the pen test or something like that. Red teamers are informed by threats, whereas a pen test may just be general threats.

Types of Hackers – White Hats

Use their skills for defensive purposes

- **System Administrators –** Those individuals tasked with the management and security of an organization's network infrastructure and systems.

**022 White hats are there to use their skills for defensive purposes. These are system administrators. So people who are pushing patches, configuring their systems, generally doing things from a defensive standpoint, that's how they define white hat hacking.

Hacktivism

The act of hacking for a cause

Hacktivism has received the most attention during conflicts between nation-states such as:

- Estonia
- Georgia

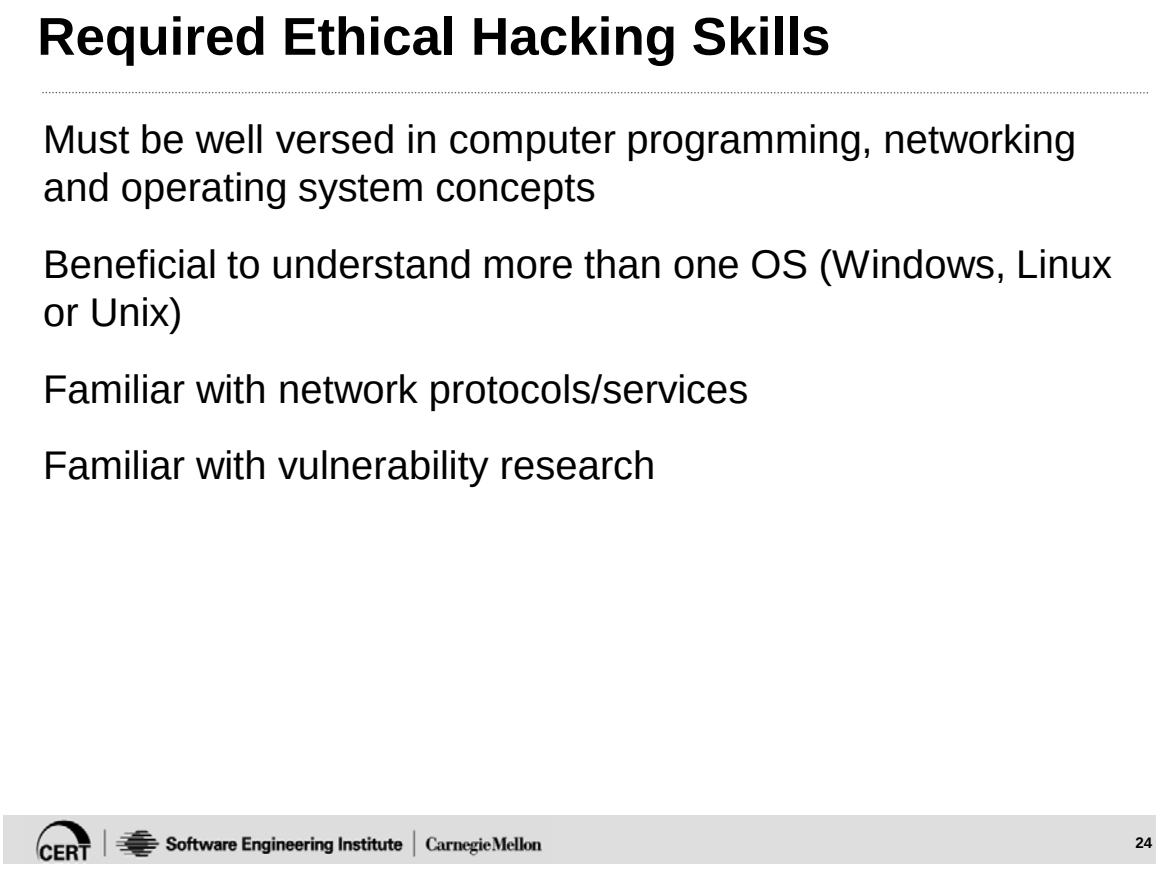
More recently, the group Anonymous epitomizes hacktivism.

Can take the shape of any person or organization defacing, hacking or DoS'ing another organization's websites, systems or networks due to a difference in beliefs, policies, and/or actions.

**023 Hacktivism we talked a little bit about this earlier but it's the idea that you're hacking for a cause. Look at groups like Anonymous, [Inaudible] these folks are out there to make a political statement or some other type of message they want to get out. You look at what happened between in Astonia and Georgia. This is the case where people were just hopping on the bandwagon, right? There was this concept of a tool called a low-orbit ion cannon and basically it was a script that you could go out and you could download, there would be a big red button that said "attack", you'd push the button and your computer basically starts sending packets to whatever the people and program, the tool, whatever IP

address they had designated in there. And so you had thousands of people downloading this tool and jumping on the denial of service bandwagon in both Astonia and Georgia. And certainly more recently groups like Anonymous are making political statements here. They types of attacks they do range anywhere from embarrassment, you know, hacking into email accounts and publishing people's personal information all the way up to denial of service attacks and website defacements.

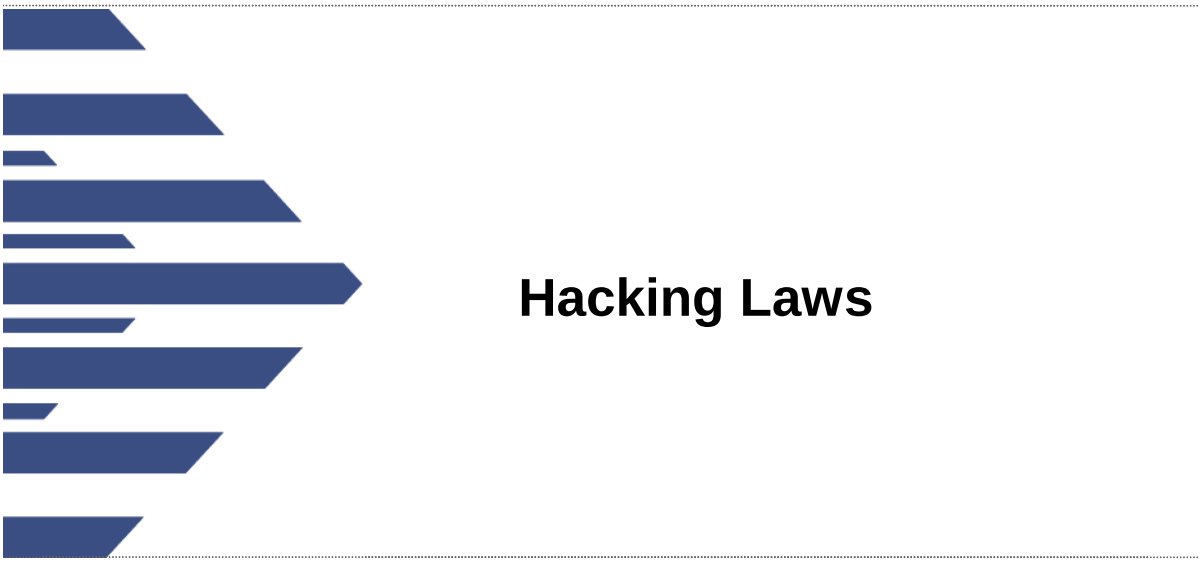
Required Ethical Hacking Skills



**024 If there's a certain skillset you need as an ethical hacker this is probably it. You should be well versed in computer programming or network and operating

systems at the conceptual level. I will tell you that the best ethical hackers out there are usually system administrators who understand how their systems work and how things can be taken advantage of, and probably computer programmers. Those of you who program let's just take Windows for example. If you're familiar with a windows API, you have a very good understanding of how Windows can be taken advantage of just because Windows API is how Windows is built, you understand the internal components of it. Turn your mindset away from using this to accomplish some task and look at it from the standpoint of how can I exploit this? That's what makes a really good ethical hacker. It's beneficial to understand more than one operating system, but usually what you'll find it's good to specialize and so you'll see teams of ethical hackers get together to do pen tests and you'll have a Windows guy, you'll have a Linux guy, you'll have a router guy and so you've got general coverage across everything you might find as a- or come across as a pen test.

It does help to be familiar with network protocols and services because as an ethical hacker you're going to want to find those, figure out what they are and take advantage of them. And it does help to be familiar with vulnerability research. Again you want to be more than just, you know the definition of an ethical hacker is not I download tools and run them. It's I either build my own tools or download tools to understand how they work and apply them in some type of defensive manner.



**025 We'll talk really quickly about hacking laws. This was actually removed from the ethical hacker objectives.

Hacking Laws

U.S. Code Title 18

Federal Information Security Management Act (FISMA)

Privacy Act

SPY ACT

U.S. Patriot Act

International Laws

The laws and policies in place continue to change and effect the nature of the function performed by CEH personnel. It is your responsibility to stay informed as changes occur both in the United States and abroad.

CERT | Software Engineering Institute | Carnegie Mellon 26

**026 But the reason this is here is because it's important for you to understand the various laws that might apply to you if you're doing various types of hacking. Give me one good reason why you would want to be aware of thesevarious laws?

Student: To protect our self [inaudible].

Chris Evans: Okay, Why else? The monkey does not want to end up in jail. The monkey does not want to go to the federal pen. Believe me, I don't either and so with any of these laws if you understand them you're going to protect yourself, you're going to protect your organization, you're going to keep yourself out of jail maybe.

There are various ones up here. We'll kind of go through each of them really quickly.

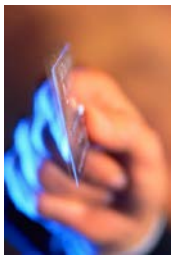
18 U.S.C. 1029

18 U.S.C. § 1029

Fraud and related activity in connection with access devices

Applies to any persons who knowingly and with intent to defraud, produce, use, or traffic in one or more counterfeit access devices

Example: Stealing a person's credit card number using an illegal credit card scanner, creating a counterfeit card, then using the card for illegal purchases.



**027 U.S. code 1029, this covers people using malicious use of access devices meaning PINs, passwords. This law says I can't go and steal Val's personal password to her bank account and use it. Okay well that may seem like common sense but there actually is a law that says you can't do that.

18 U.S.C. § 1030

Fraud and related activity in connection with computers

Applies to any persons who knowingly accesses a computer **without authorization, exceeds authorized access, and obtains information** contained in:

- financial record of a financial institution
- any department or agency of the United States
- a protected computer if the behavior involves an interstate or foreign communication

Intentionally causing the transmission of information, code, command, or a program resulting in, **intentional damage without authorization**, to a protected computer.

**028 U.S. code 1030, this governs actually using systems or hacking into systems without authorization. Again there's that key word "authorization". Who authorizes you to do this type of activity? If you had to get authorization to hack into this system here, where would that authorization come from?

Student: From the owner.

Student: Of the system.

Chris Evans: From the owner of the system, right. That could be some type of designated approval authority or some type of certification and authorization official, whoever the owner of this system

is. Let's talk about that really briefly. There's a system owner. There's usually a data owner, and then there's the guy who owns the hardware itself. Who is the real owner? Which one would you want to make sure you had authorization from?

Student: All of them?

Chris Evans: All of them? Again, that's your get out of jail free card, right if you have authorization from all of them. So it might be fine that you've got access to this system. The system owner said yes, you can access this, but if there's data on there that doesn't belong to the system owner and you go in and access that data, and you didn't tell that guy who owns that information that you were going to do that, you're now in trouble. So usually that's pretty rare that you'll have multiple competing people with ownership of that particular system but always make sure that if you're in a big environment doing some type of ethical hacking, pen tester or something like that, you've got authorization from everybody who is concerned about this or he has some type of stake in this system. So 1030 kind of stipulates that you can't go out and hack into systems. Again, that's kind of obvious but here it is, here's the actual code behind it.

FISMA

Federal Information Security Management Act of 2002

Requires federal agencies to develop, document, and implement agency-wide information security programs

FISMA requirements include

- Periodic risk assessments
- Information security plans for networks
- Security awareness training
- Periodic test and evaluation of information security effectiveness

CERT | Software Engineering Institute | Carnegie Mellon 29

**029 There is FISMA the Federal Information Security Management Act which if you're in the U.S. federal government, you're probably very well aware of it and what the requirements are for it. Generally the U.S. government said we're not too good at this cyber security thing. We need to get better at it and all these individual information systems out there and this was ten years ago when information systems were kind of like the wild west of a hundred years ago in the western U.S. but the idea was FISMA kind of came down with the idea that you've got to do risk assessments. That you've got to look at your systems and actually do something to protect them. It's not sufficient just to have the system sitting

here, you have to protect it. So you have to have an information security plan, you have to do some type of security awareness training, and you also have to test or evaluate the effectiveness of the controls that you put in place, meaning that you have to go out and do vulnerability assessments, you've got to do penetration tests, you've got to do continuous monitoring on your systems and make sure that everything is still effective.

Privacy Act of 1974, U.S.C. 552

Privacy Act of 1974, U.S.C. 552

Established a code of fair information practice that governed the collection, maintenance, use, and dissemination of personally identifiable information (PII)

Requires that agencies provide the public notice of their systems of records by publication in the Federal Register.

Prohibites disclosure of information from a system of records, unless pursuant to one of the twelve statutory exceptions

**030 The Privacy Act of 1974, again if you're in Department of Defense you see this on every little form that you've got to put your name and social security number on. But the idea was that the government wanted

to protect from people just harvesting personal information for identity theft purposes, and so now you've got Privacy Act which prevents disclosure of information from a system of records so it's usually personally identifiable information: name, address, phone number, social security number, that sort of thing so anything that collects that type of information and stores it and process it is usually subject to Privacy Act laws. So if you are an ethical hacker and you break into a system and see that it's a database full of names and Social Security numbers and home addresses as an ethical hacker, what would you do?

Student: Warn someone.

Chris Evans: You know what? That deserves a squeeze the monkey. That actually is exactly what you're supposed to do and fortunately he'll shut up. Report it, absolutely. If you are out on a pen test and you come across something that is just kind of floors you as a security professional, you don't raise the flag and go "Look what I found! Look what I found!" And go run off to the security message boards or the blogs and go "Look what happened, look what I got." Nope, it's your responsibility as an ethical hacker to go report it and say whoever hired me to do this or my organization "Look, we found a database full of personal information and I was able to get into it which means somebody else is able to do the exact same thing as well and we need to protect that." As an unethical hacker what would you do with that information?

Student: Expose it.

Chris Evans: Expose it.

Student: Sell it.

Chris Evans: Sell it. Yep, I can make two dollars and fifty cents per identity on the black market with that. Sixty-thousand people? Yeah, I'm set for the next year. That's a vacation in Hawaii, not that I'd do that; that's unethical hacking. But all of that is governed by Privacy Act.

SPY ACT (2007)

SPY ACT (2007)

Securely **P**rotect **Y**ourself **A**gainst **C**yber **T**respass

Makes it illegal to collect personal information without user's consent

Deemed "unfair or deceptive acts"

- Taking unsolicited control of a system
- Collecting Personally Identifiable Information (PII)
- Tricking an owner or authorized user to divulge PII
- Using malware (key logger) to gain PII

CERT | Software Engineering Institute | Carnegie Mellon 31

**031 Spy Act the securely protect yourself against cyber trespass kind of improves on Privacy Act stuff. It means I can't collect information on you without your consent so if you give me I have to ask you can I get your name, email address

and phone number? And usually I'll tell you what I'm going to do with that if I have some type of ethics. And it's designed, this law was designed to prevent deceptive acts, meaning people tricking you out of your information and then doing bad things with it.

USA PATRIOT Act of 2001

USA PATRIOT Act of 2001

Uniting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism

Created in response to the Sep 11 terrorist attacks

Drastically increases the government's ability to monitor, intercept, and maintain information gathered from numerous communications methods (phone, email, financial records)

CERT | Software Engineering Institute | Carnegie Mellon 32

**032 The Patriot Act, uniting and strengthening America to provide appropriate tools to intercept and obstruct terrorism. I really don't know how they come up with these acronyms and these names. I think there's a data base somewhere, they put in a word and push a button and out comes a list of potential words or statements behind it. But this came out right after September 11th and it really

gave the government power to go through and look at communications, emails, phone calls for anti-terrorism measures.

International Cyber Crime Laws

International Cyber Crime Laws

Data and systems are often located in other countries.

Data or communications may travel through other countries.

Therefore, it is important to understand the pertinent countries' cyber crime laws.

Examples

- Cyber Crime Law in Mexico: Section 30-45-5: Unauthorized computer use
- Cyber Crime Law in India: The Information Technology Act, 2000

CERT | Software Engineering Institute | Carnegie Mellon 33

**033 International cyber-crime laws. There's just a little bit of information on this but generally the U.S. has cyber laws. Generally other countries will have cyber laws as well. If you are an ethical hacker working only in the U.S. you don't necessarily have to worry about this. If you're doing international or you're transiting international gateways on the way to a U.S. target, maybe you're doing a U.S. military base overseas or something like that, you're probably going through non-U.S. transit points on the way to get there at least over the network

depends on what you're doing. But be aware that there are international cyber laws and they do govern how people using systems in that country what they are and what they are not allowed to do. There are some countries that are more stringent than the U.S. There are a lot of countries that are less stringent than the U.S. As an unethical hacker, if I wanted to cover my tracks and make sure that I made it next to impossible for somebody to find and more importantly prosecute me what would I do? I would find the various countries out there that have less than stellar cybercrime laws or maybe nonexistent cybercrime laws and I would use them as jumping points for my attacks. And so what you'll see is that with corporate espionage or national security espionage and that sort of thing there are usually multiple hot points that these attacks go through. It only takes three hops through different jurisdictions to make it next to impossible to prosecute. Why is that?

Student: Because of how long it takes to subpoena for the information.

Chris Evans: Bingo, yep. So if I jump through country X, country Y, country Z before ending up on Andy's computer here, if Andy does some type of forensics he's going to backtrack it to country X or country Z, whichever one. And then he's got to go from there to the next country and from there to the next country keeping in mind that there are different jurisdictions involved, there are different law enforcement involved, there are different collection subpoena requirements involved. It's all it takes is three hops. Now what's even more

disconcerting is there are reports out there that say one of the countries that's used most often for these types of attacks, anyone want to guess?

Student: China.

Chris Evans: Surprisingly no.

Student: Really?

Student: Russia?

Chris Evans: That's one of the big ones but not the biggest. The United States. Whoops. And the reason for that is because there are usually two things involved here. One it's propagation of computers so my grandmother has one, my aunt and uncle have one everybody in my family has one and they're not all computer savvy so it's on all the time and so we have broadband access. Makes it a great always on, always available system that nobody monitors but also because of various cyber laws the Patriot Act aside, it makes U.S. citizens are generally protected against cyber monitoring or any type of activity without some type of warrant or subpoena so it makes it very easy for somebody to bounce through one of these systems because there's no monitoring, there's no response, there's nothing going on to that system. And so you'll find that the United States is actually the biggest jump off point for these types of attacks just because the attackers are taking advantage of our own laws against us. And the fact that everybody has broadband Internet and everything is on all the time so it's kind of convenient.

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.