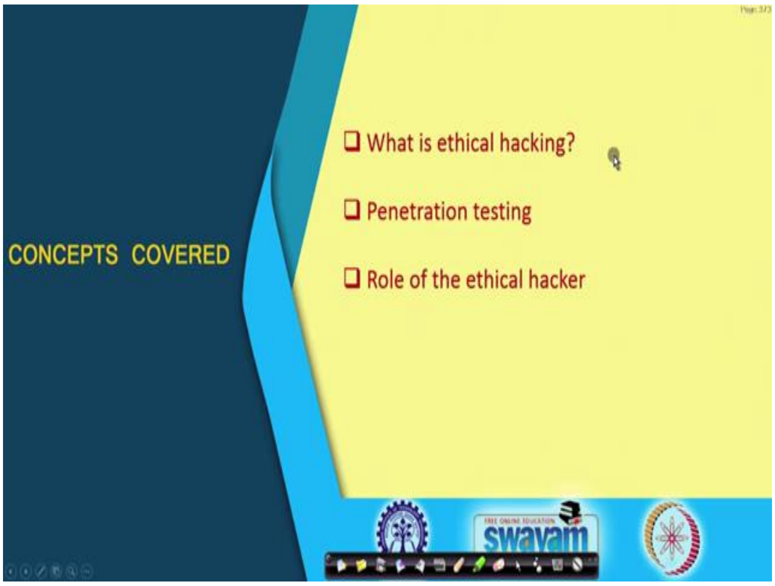
Ethical Hacking

Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 01
Introduction to Ethical Hacking

I would like to welcome you to this course on Ethical Hacking. This is the first lecture of this course. Now, in this lecture, I will try to give you a very overall idea about what ethical hacking exactly is, what are the scopes of an ethical hacker and towards the end, I shall give you some idea about the coverage of this course — what are the things we are expected to cover ok. So, the title of this lecture is Introduction to Ethical Hacking.

(Refer Slide Time: 00:51)



CONCEPTS COVERED

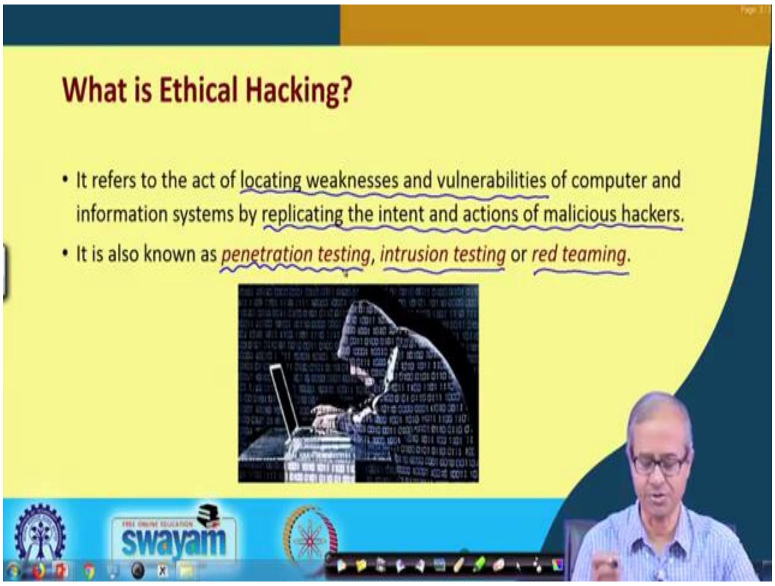
❑ What is ethical hacking?

❑ Penetration testing

❑ Role of the ethical hacker

Now, in this lecture as I told you, firstly we shall try to tell you what is ethical hacking? There is a related terminological penetration testing, we will also be discussing about that. And some of the roles of an ethical hacker, what an ethical hacker is expected to do and what he or she is not expected to do that we shall try to distinguish and discuss.

(Refer Slide Time: 01:18)



What is Ethical Hacking?

- It refers to the act of locating weaknesses and vulnerabilities of computer and information systems by replicating the intent and actions of malicious hackers.
- It is also known as *penetration testing*, *intrusion testing* or *red teaming*.

So, let us first start with the definition of ethical hacking. What exactly is ethical hacking? Well, we all have heard the term hacking and hacker essentially the term has been associated with something which is bad and malicious. Well, when we hear about somebody as a hacker, we are a little afraid and cautious ok. I mean as if the person is always trying to do some harm to somebody else to some other networks, try to steal something, trying to steal something from some IT infrastructure and so on and so forth.

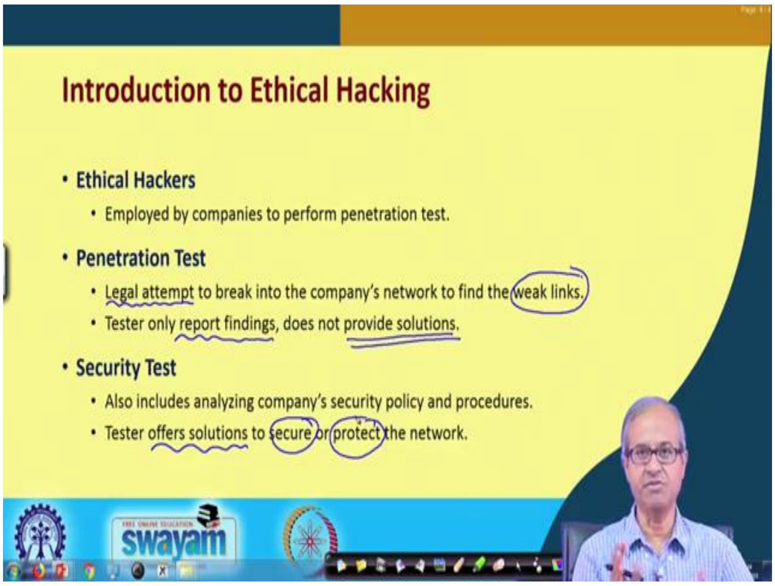
But ethical hacking is something different. Well, ethical hacking as per the definition if you just look at it, it essentially refers to locating the weaknesses and vulnerabilities. It means suppose you have a network, you have an organizational network, you have an IT, IT infrastructure, you have computers which contains some software, some data, lot of things are there. Now, you try a, I mean here you are trying to find out, whether your infrastructural network does have some weak points or vulnerabilities through which an actual hacker can break into your system, into your network.

So, this ethical hacking is the act of locating weaknesses and vulnerabilities in computers and information system in general, it covers everything, it covers networks, it cover databases, everything. But how this is done, this is done by mimicking the behaviour of a real hacker as if you are a hacker, you are trying to break into your own network, there you will get lot of information about what are the weak points in your own network. So, this term is important, by replicating the intent and actions of malicious hackers, whatever malicious hackers do in reality, you try to mimic that, you try to replicate that ok.

Your objective is to try and find out the vulnerabilities and weak points in your network. Well, you have a good intent, you try to identify the weaknesses and later on maybe the organization will be trying to plug out or stop those weaknesses, so that such attacks cannot occur or happen in the future ok. This ethical hacking is sometimes also referred to by some other names, penetration testing is a well-known terminology which is used — a phrase, intrusion testing, red teaming, these are also terminologies which are used to mean the same thing.

Well, you can understand penetration testing, the literal meaning of this phrase is, you are trying to penetrate into a system; you are trying to penetrate into a network, you are testing and find out whether or not you are able to penetrate. And if you are able to penetrate which are the points through which it is easier to penetrate, these are the objectives ok, all right.

(Refer Slide Time: 04:53)



Introduction to Ethical Hacking

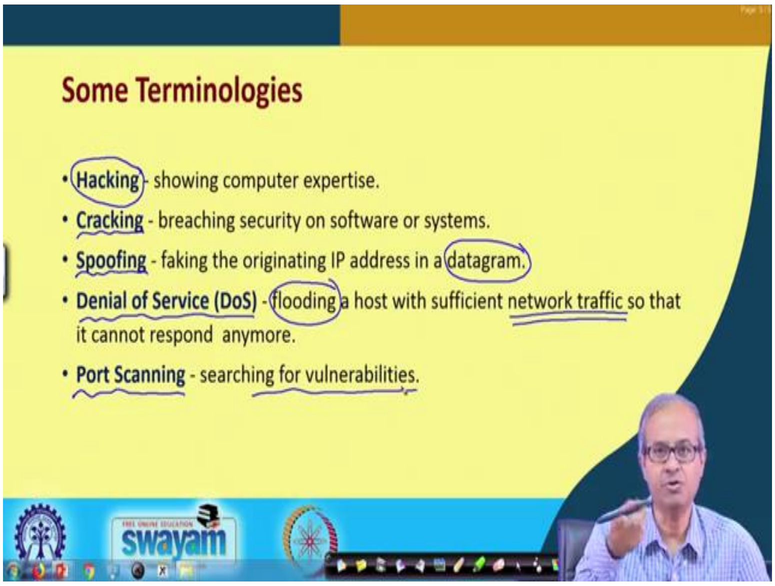
- Ethical Hackers
  - Employed by companies to perform penetration test.
- Penetration Test
  - Legal attempt to break into the company's network to find the weak links.
  - Tester only report findings, does not provide solutions.
- Security Test
  - Also includes analyzing company's security policy and procedures.
  - Tester offers solutions to secure or protect the network.

So, talking about ethical hacking, there are some terminology, let us see. Well ethical hackers are the persons who are actually carrying out ethical hacking. Now, they are not some unknown entities, they are some organization or persons who are actually hired by the company. The company is paying them some money to do a penetration testing on their own network and provide them with a list of vulnerabilities, so that they can take some action later on ok. So, these ethical hackers are employed by companies who typically carry out penetration testing or ethical hacking. Penetration testing, as I had said is an attempt to break into a network or a system or an infrastructure.

But the difference from malicious attempt is that this is a legal attempt. The company has permitted you to run the penetration testing on their own network for the purpose of finding the vulnerabilities. So, this is a legal attempt, you are trying to break in and you are trying to find out the weak links. Well, in penetration testing per se what the tester will do, tester will basically generate a report. The report will contain a detailed report; it will contain all the known vulnerabilities that have been detected in the network as a result of running the penetration testing process ok.

But normally they do not provide solutions. Well, you can also seek solutions for them, but everything comes with an extra or additional charge right. So, in contrast, security test is another terminology which is used, which includes penetration test plus this kind of suggestions to plug out the loopholes. So, this includes in addition analyzing the company security policies and offering solutions, because ultimately the company will try to secure or protect their network. Of course, there are issues, there may be some limited budget. So, within that budget whatever best is possible that have to be taken care of or incorporated. So, these are some decisions the company administration will have to take fine.

(Refer Slide Time: 07:41)



Some Terminologies

- Hacking - showing computer expertise.
- Cracking - breaching security on software or systems.
- Spoofing - faking the originating IP address in a datagram.
- Denial of Service (DoS) - flooding a host with sufficient network traffic so that it cannot respond anymore.
- Port Scanning - searching for vulnerabilities.

So, some of the terminologies that we normally use hacking, hacking broadly speaking, we use this term to refer to a process which involves some expertise. We expect the hackers to be expert in what they are doing. At times we also assume that hackers are more intelligent in the persons, than the persons who are trying to protect the network. This assumption is always safe to make that will make your network security better ok.

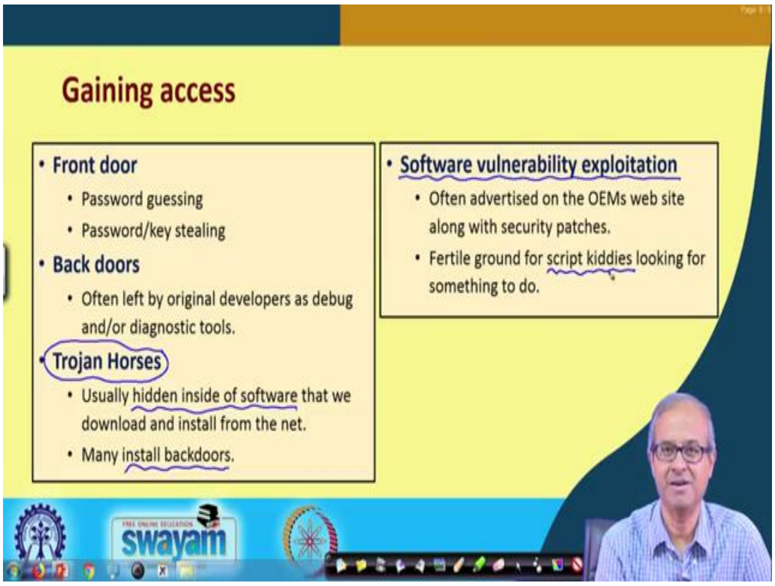
Cracking means breaching the security of a some kind of system, it can be software, it can be hardware, computers, networks whatever, this is called cracking, you are trying to crack a system. Spoofing is a kind of attack, where the person who is, who is attacking is trying to falsify his or her identity. Suppose, I am trying to enter the system, but I am not telling who I am, I am telling I am Mr. X, Mr. X is somebody else right. So, it is the process of faking the originating address in a packet, a packet that flows in a network is sometimes called a datagram ok. So, the address will not be my address, I will be changing the address to somebody else's address, so that the person who will be detecting that will believe that someone else is trying to do whatever is being done ok.

Denial of service is another very important kind of an attack which often plagues or affects systems or infrastructures. Well, here the idea is that one or a collection of computers or routers or whatever you can say, a collection of nodes in the network, they can flood a particular computer or host with enormous amount of network traffic. The idea is very simple, suppose I want to bring a particular server down, I will try to flood it with millions and millions of packets, junk packets, so that the server will spend all of its time filtering out those junk packets. So, whenever some legitimate requests are coming, valid packets are coming, they will find that the service time is exceedingly slow, exceedingly long, this is something which is called denial of service.

And port scanning is a terminology which you use very frequently, well ports in a computer system this we shall be discussing later. Ports indicate some entry points in the system which connects the incoming connections to some programs or processes running in the system. Say means in a computer system there can be multiple programs that are running, and these programs can be associated with something called a port number ok. Whenever you are trying to attack a system, normally the first step is to scan through some dummy packets ping, these are called ping packets and try to find out which of the port numbers in the system are active.

Suppose, you find out that there are four ports which are active then normally there is a well documented hacking guideline which tells you that for these four ports what are the known vulnerabilities and what are the best ways to attack or get entering those into the system through these ports. So, this port scanning is the process of identifying which are the active ports which are there and then searching for the corresponding vulnerabilities, so that you can exploit them ok. These are called exploits, once you identify the ports you try to find out an exploit through which you can get entry into the system, this is roughly the idea.

(Refer Slide Time: 12:29)



Gaining access

- Front door
  - Password guessing
  - Password/key stealing
- Back doors
  - Often left by original developers as debug and/or diagnostic tools.
- Trojan Horses
  - Usually hidden inside of software that we download and install from the net.
  - Many install backdoors.

- Software vulnerability exploitation
  - Often advertised on the OEMs web site along with security patches.
  - Fertile ground for script kiddies looking for something to do.

Now, talking about gaining access into the system, there are different ways in which you can gain access to a system. One is you are entering the system through the front door. So, the name is also given front door access. Normally, a system, normally I am talking about whenever you try to access the system you try to log in, you are validated with respect to some password or something similar to that.

So, passwords are the most common ways of gaining entry or access to a system in the present day scenario ok. So, the first attempt through that front door channel will be to guess valid password or try and steal some password. There are many methods that are used for this purpose. During this course you will be seeing some of the tools through which you can try and do this ok. This is the front door.

The second thing is a back door which normally a person coming is not able to see, but it is there. Those of you who know there is a back door, they can only enter through that back door. This is the basic idea. So, back doors are some you can say entry points to a system which had deliberately kept by the developers. Well, I am giving an example suppose I buy a router, a network router from some company, they give me some root password and access rights, I change the root password. So, I am quite happy that means, I have sole access to it, I have changed the password, I am safe.

But sometimes it may happen if something goes down, the company might automatically modify or configure, reconfigure the router through that back door. They will not even ask you at times. They will automatically enter the router through that backdoor entry, there will be some special password through which they can possibly enter and they can make some changes inside. Such back doors are known to exist in many systems, not only hardware systems also many of these software systems, software packages ok. Well, usually developers keep it as debugging or diagnostic tools, but sometimes these are also used for malicious purposes ok.

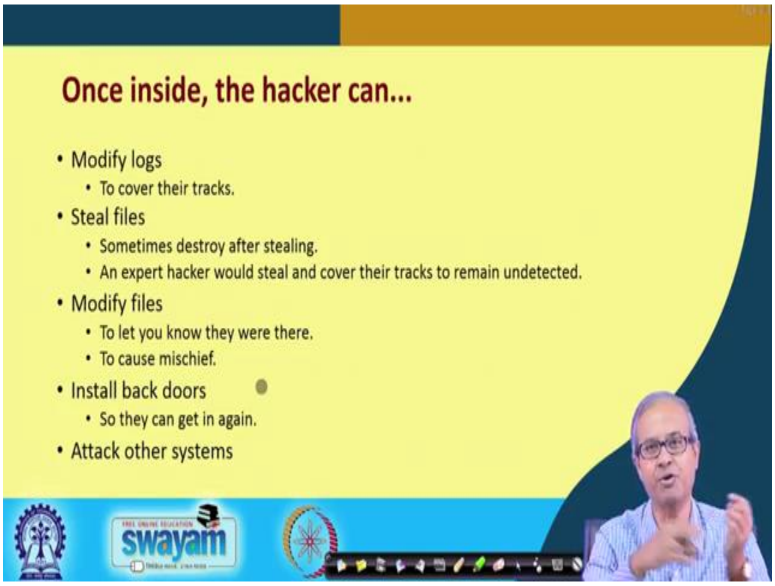
Then comes the Trojan horses. Now, if you remember the story of the Trojan horse where it is something which was hidden inside a horse, some warriors were hidden inside a horse. Suddenly some time one night, they just comes out and start creating havoc. Trojan horse is also in terms of a computer system something very similar. Here let us think of a software first. So, it is a software code that is hidden inside a larger software. Well, as a user you are not even aware that such a Trojan is there inside the software ok.

Now, what happens sometimes that Trojan software can start running and can do lot of malicious things in your system. For example, they can install some back doors through which other persons or other packets can gain entry into your system. Nowadays, you will also learn as part of the course later, Trojans can also exists in hardware. Whenever you built a chip, you fabricate a chip, without your knowledge, some additional circuitry can get fabricated which can allow unauthorized access or use of your chip, of your system during its actual runtime ok.

And lastly come software vulnerabilities exploitation. Well, when a software is developed by a company, that software is sold, with time some vulnerabilities might get detected. Normally, those vulnerabilities are published in the website of that company that well, these are the vulnerabilities please install this patch to stop or overcome that vulnerability. But everyone do not see that message and do not install the patch. But as a hacker if you go there and see that well these are the vulnerabilities in that software, you try to find out where all that software is installed and you try to break into those in using those vulnerable points ok.

And this kind of software vulnerabilities are typically used, you can say as a playground for the first time hackers. Sometimes they are called script kiddies. The hackers who are just learning how to hack and that is the best place means already in some website it is mentioned that these are the vulnerabilities, they just try to hack and see that whether they are able to do it or not all right.

(Refer Slide Time: 18:16)



Once inside, the hacker can...

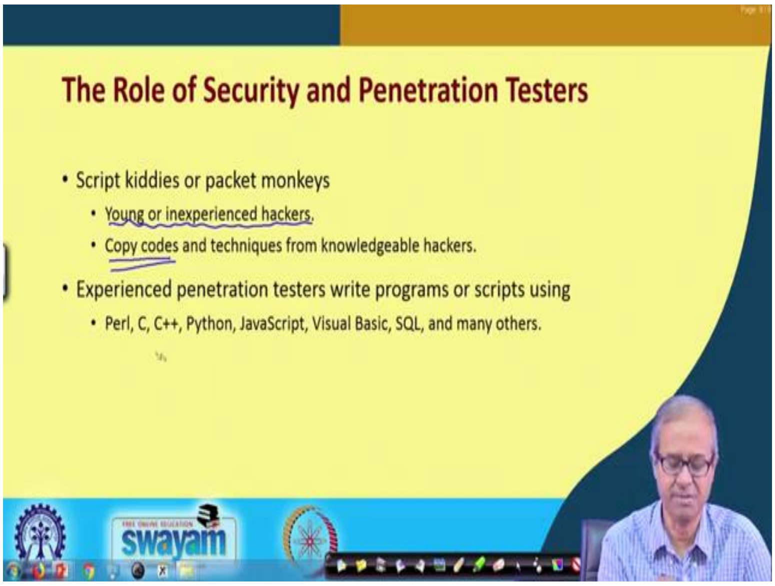
- Modify logs
  - To cover their tracks.
- Steal files
  - Sometimes destroy after stealing.
  - An expert hacker would steal and cover their tracks to remain undetected.
- Modify files
  - To let you know they were there.
  - To cause mischief.
- Install back doors
  - So they can get in again.
- Attack other systems

Now, once a hacker gains access inside a system, there can be a number of things that can be done. For example, every system usually has a log which monitors that who is logging into the system at what time, what commands they are running and so on and so forth. So, if the hacker gets into the system, the first thing he or she will possibly try to do is modify the log, so that their tracks are erased.

So, if the system administrator looks at the log later on, they will not understand that well an hacking actually happened or not. So, some entries in the log file can get deleted; can be deleted, some files may be stolen, sometimes after stealing the files, files can be destroyed also ok, some files might get modified, like you have heard of defacement of websites, some hackers break into a website and change the contents of the page to something malicious, so that people know that well we came here, we hacked your system, just to cause mischief well.

Installing backdoors is more dangerous. So, you will not understand what has happened, but someone has opened a back door through which anyone can enter into a system whenever they want ok. And from your system, some other systems can be attacked. Suppose in a network, there are 100 computers, someone gains entry into one of the systems, one of the computers; from there the other 99 computers can be attacked if they want to, right, ok.

(Refer Slide Time: 20:08)



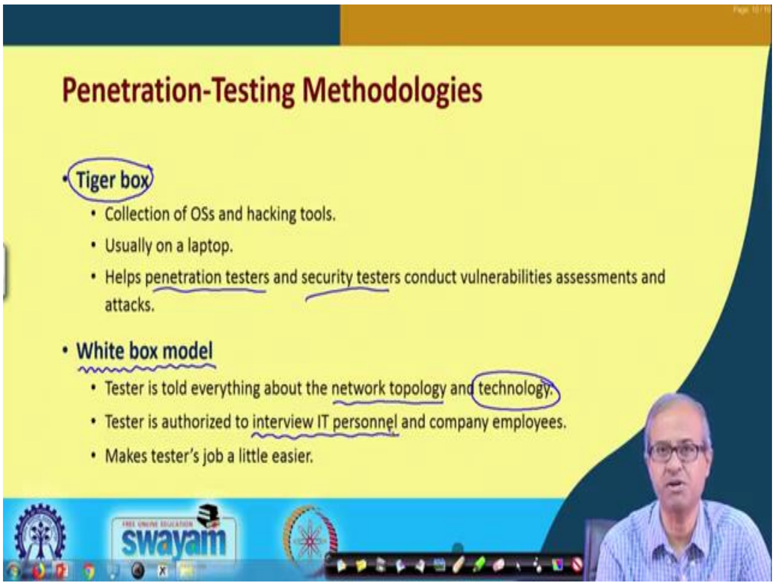
The Role of Security and Penetration Testers

- Script kiddies or packet monkeys
  - Young or inexperienced hackers.
  - Copy codes and techniques from knowledgeable hackers.
- Experienced penetration testers write programs or scripts using
  - Perl, C, C++, Python, JavaScript, Visual Basic, SQL, and many others.

Now, talking about the roles of the testers, who are carrying out the security testing and penetration testing. Well, I talked about script kiddies, the beginners who have just learned how to break into systems. They are typically young or inexperienced hackers. So, usually what they do, they look at some existing websites, lot of such hacking documentations are there, from there they typically copy codes, run them on the system and see that whether actually the attacks are happening as it has been published or discussed in those websites, right.

But experienced penetration testers they do not copy codes from such other places, they usually develop scripts, they use a set of tools and they run a set of scripts using which they run those tools in some specific ways to carry out specific things. And these tools or these scripts are typically written in different scripting language like Perl, Python, JavaScript, they can be written also in language like C, C++ and so on.

(Refer Slide Time: 21:30)



Penetration-Testing Methodologies

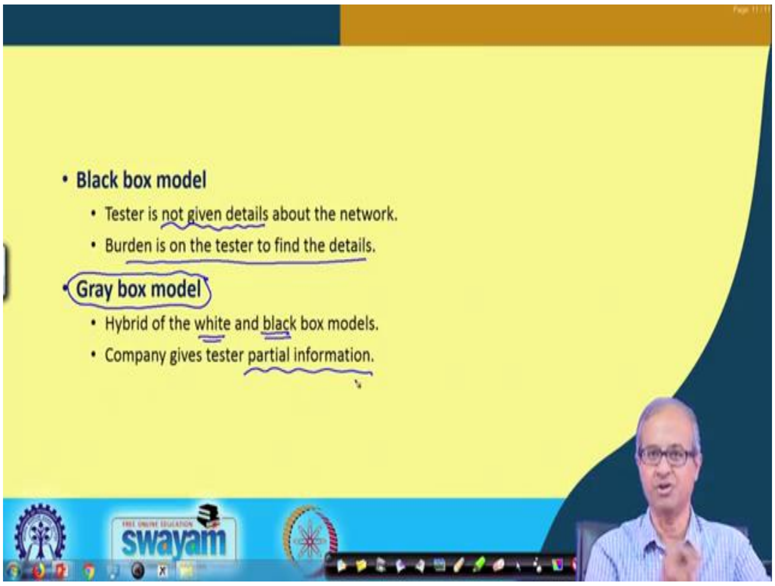
- Tiger box
  - Collection of OSs and hacking tools.
  - Usually on a laptop.
  - Helps penetration testers and security testers conduct vulnerabilities assessments and attacks.
- White box model
  - Tester is told everything about the network topology and technology.
  - Tester is authorized to interview IT personnel and company employees.
  - Makes tester's job a little easier.

Now, broadly the penetration testing methodologies if you think about, first thing is that the person who is doing penetration testing, he or she must have all the set of tools at his or her disposal. This is sometimes called a tiger box. Tiger box basically is a collection of operating systems and hacking tools which typically is installed in a portable system like a laptop, from there wherever the person wants to carry out penetration testing, he or she can run the correct tool from there and try to mount a virtual attack on that system, and see whether there are any vulnerabilities or not.

So, this kind of tools helps penetration testers and security tester to conduct vulnerability assessment and attacks. This tiger box contains a set of all useful tools that are required for that ok. Now, for doing this penetration testing, from the point of view of the tester, the best thing is white box model. Where the company on whose behalf you are doing the testing tells the tester everything about the network and the network infrastructure, they provide you with a circuit diagram with all the details ok, means about the network topology, what kind of new technologies are used in the network everything.

And also the tester if they require, whenever they require, they are authorized to interview the IT personnel. Many times it is required in a company, if you interview people, you will get to know a lot of things that how the information processing is carried out inside the company, what are the possible vulnerabilities that they feel there are ok. So, this white box model makes the testers job a lot easier, because all the information about the network whatever is available is made available or given to the tester ok.

(Refer Slide Time: 23:46)



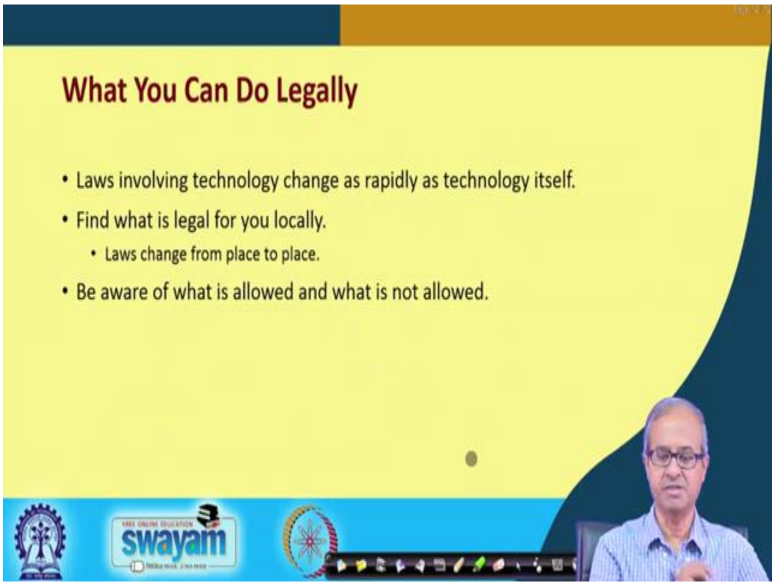
- Black box model
  - Tester is not given details about the network.
  - Burden is on the tester to find the details.
- Gray box model
  - Hybrid of the white and black box models.
  - Company gives tester partial information.

Now, the exact reverse is the black box model. Black box model says that tester is not given details about the network. So, it is not that the person who is asking the tester to test, is deliberately not giving, maybe the person is not competent enough and does not know the relevant information to be shared with the tester. So, tester will have to dig into the environment and find out whatever relevant information is required.

So, the burden is on the tester to find out all the details that may be required. In practice usually we have something in between, we do not have white box, we do not also have black box, we have something called the gray box model. What is grey box model? It is some kind of a hybrid of the white box and black box model. The company will provide the tester with partial information about the network and the other things.

Well, why partial? Because the company may be knowing the details of some of the subsystems, but for some other subsystem the details may not be available to them also. So, they cannot provide any detail for that ok. They have just bought it and installed it something like that. So, these are broadly the approaches.

(Refer Slide Time: 25:19)



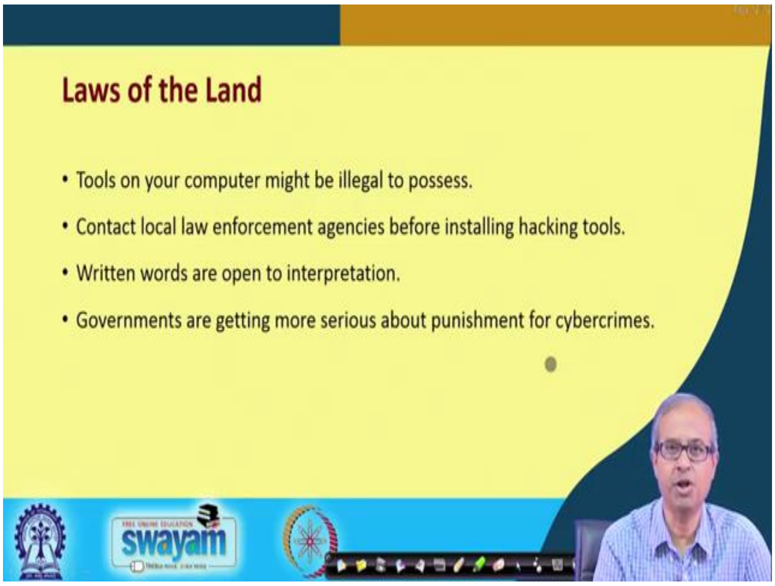
What You Can Do Legally

- Laws involving technology change as rapidly as technology itself.
- Find what is legal for you locally.
    - Laws change from place to place.
- Be aware of what is allowed and what is not allowed.

Now, there are some legal issues also. Well, it varies from country to country. Well, in our country it is not that rigid, there are some other countries where it is extremely rigid, that means you are not possibly allowed to install some kind of software on your computers. So, these laws that involve technologies, particularly IT, they are changing and developing very fast with time. It is very difficult to keep track of these changes, what is the latest law of the land ok.

Now, it is always good to know the exact set of rules that pertain in the place of your work, where you are working, what are the laws, what are the rules, so that you should be know what is allowed and what is not allowed, maybe you are using something or doing something in good faith, but possibly it is illegal in that state or that country ok, may be, you may be in trouble later on, all right.

(Refer Slide Time: 26:31)

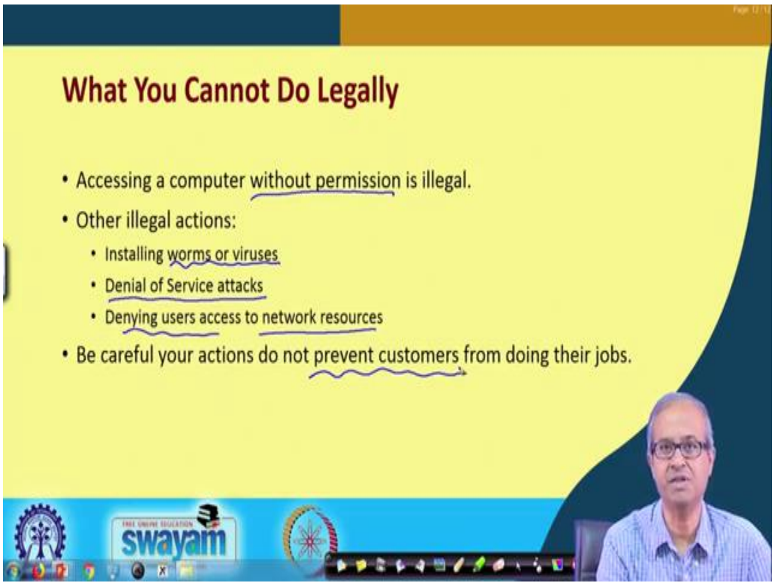


Laws of the Land

- Tools on your computer might be illegal to possess.
- Contact local law enforcement agencies before installing hacking tools.
- Written words are open to interpretation.
- Governments are getting more serious about punishment for cybercrimes.

So, the laws of the land are very important to know. Some of the tools you are using on your computer may be illegal in that country. So, you must be know about these things. The cyber crimes, punishment on cyber crime, these are becoming more and more crucial and severe with every passing day. So, these are a few things people should be extremely cautious about.

(Refer Slide Time: 26:57)



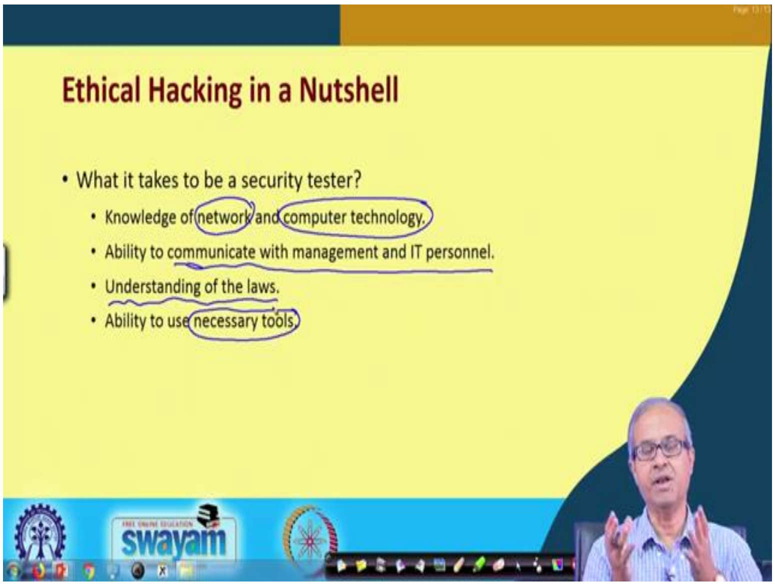
What You Cannot Do Legally

- Accessing a computer without permission is illegal.
- Other illegal actions:
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs.

But certain things are quite obvious that you should not do certain things legally that everyone understands that accessing a computer without permission is clear. So, it is my computer, why you are you accessing without my permission that is something illegal. Installing worms or viruses that is also supposed to be illegal, I have not installed worms and viruses, so I have also not asked you to install. So, why have you installed or injected these kind of worms or viruses in my computer ok. Denial of service attacks, well hackers do mount this kind of attacks, but these are illegal, some services or servers are installed to provide some service to customers.

So, if someone tries to deny those services that is something which is not permissible right. Then something similar to that denying users access to some networking resources, because you should be aware whatever you are doing maybe as part of ethical hacking, maybe as part of the work which company has asked you to do. Maybe you are doing something inside your, the network of the company, but you should be careful, you should not prevent the customers of that company from doing their job, this is very important ok. So, your action should not be disruptive in terms of their business.

(Refer Slide Time: 28:41)



Ethical Hacking in a Nutshell

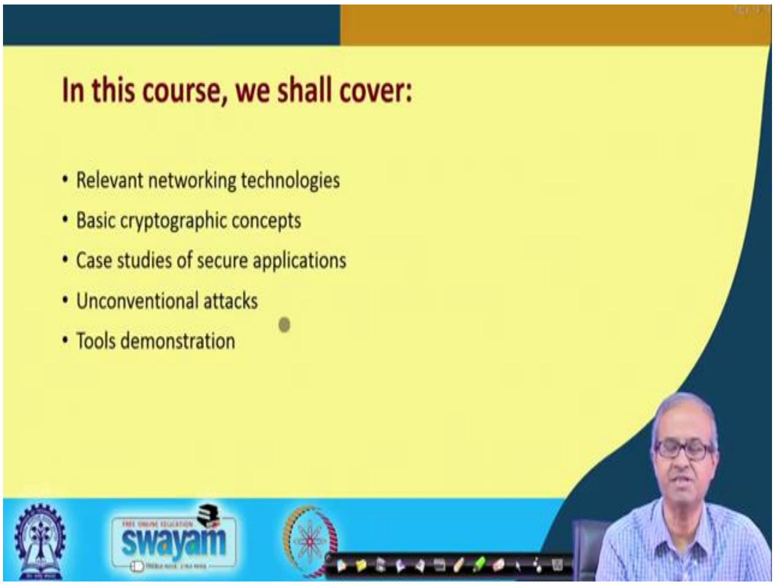
- What it takes to be a security tester?
  - Knowledge of network and computer technology.
  - Ability to communicate with management and IT personnel.
  - Understanding of the laws.
  - Ability to use necessary tools.

So, in a nutshell to summarize, this ethical hacking well if you are a security tester, so what are the things you need to know or you need to do? Well, the first thing clearly is, you should have a sound knowledge of networking and computer technology. So, you see as part of this course, we will devote a significant amount of time discussing or brushing up the relevant backgrounds of networking technology, because these are very important in actually understanding what you are doing, how are you doing and why are you doing.

And also you cannot do everything yourself on your own, you need to communicate with other people that art is also something to be mastered. You need to interact with other people. This quality is also very important.

And of course, I have mentioned the laws of the land are very important to understand and you should have the necessary tools at your disposal. Some of the tools may be freely available; some of the tools may have to be purchased, some you may develop on your own. So, you should have the entire set of tools at your disposal before you can qualify yourself to be a good network, you can say ethical hacker, penetration tester or a security tester ok, fine.

(Refer Slide Time: 30:22)



In this course, we shall cover:

- Relevant networking technologies
- Basic cryptographic concepts
- Case studies of secure applications
- Unconventional attacks
- Tools demonstration

Now, about this course very briefly speaking, very broadly speaking, we shall be covering relevant network technologies as I had said, understanding some basic networking concepts are very important to understand how these tools work. If you do not understand the networking concepts, we will not be able to use the tools at all ok.

Basic cryptographic concepts are required, because whenever you are trying to stop some of the weak points or vulnerabilities, often you will have to use some kind of cryptographic techniques or cryptographic solutions. So, you need to understand what are the things that are possible and what are not possible in terms of cryptography techniques ok.

Well, we shall look at some of the case studies of secure applications to understand how these cryptographic primitives are put into practice to develop secure applications. Then we shall be looking at unconventional attacks, some of the attacks which are hardware based attacks, which are very interesting and very recent and they are very unconventional. We shall be discussing about such kind of attacks. And a significant part of this course, we will concentrate on demonstrating various tools, how we can actually mount this kind of penetration testing and other kind of attacks on your system, on your network and so on and so forth ok.

So, with this I come to the end of this first lecture. And I would expect that the lectures that are yet to come would be very useful for you in understanding the broad subject of ethical hacking and motivate you in the subject to possibly become an ethical hacker in the future.

Thank you.