Information Security - IV

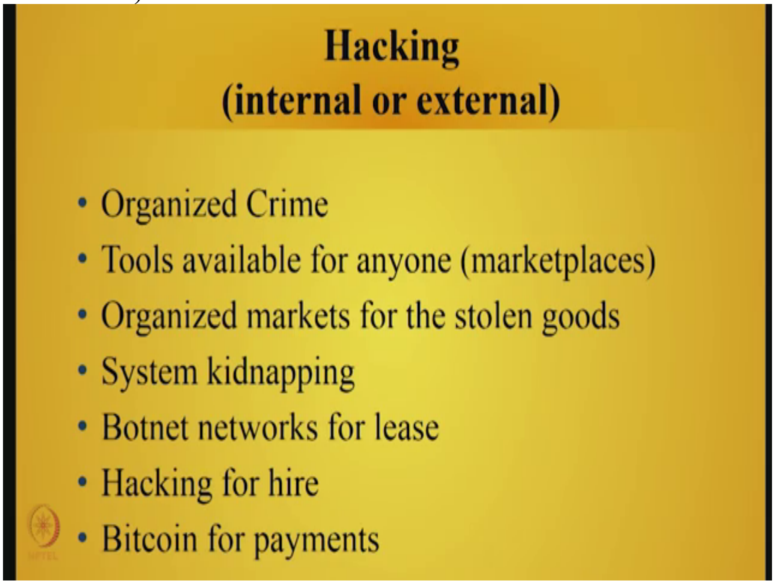
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 10
Network Security And Forensics
(Protecting computers connected through the Internet)
Part 1

Welcome to this module on network security and forensics. Until now you would have heard about the issues with respect to O S forensics and O S security. Now all this things would have been and introductory session would also got a review about what had happened in the previous I S 1 I S 2 and I S 3. What we will do now is, we will provide you a very brief introduction into this area of network security and forensics.

We will be elaborating on many of these aspects in the forthcoming classes, after we complete the O S security. Therefore this is just an introductory session on what all the areas will be covering on network security and forensics. We all know that hacking either internal external is a crime.

(Refer Slide Time: 01:07)



Hacking
(internal or external)

- Organized Crime
- Tools available for anyone (marketplaces)
- Organized markets for the stolen goods
- System kidnapping
- Botnet networks for lease
- Hacking for hire
- Bitcoin for payments

There are of course; certain course on ethical hacking, and the idea behind this course is that we have to put our self in the feet of an hacker and think if one person, if a person is a hacker, how is it going to work on hacking a machine. Therefore there is, you have a lot of courses on ethical hacking, and we know that there are lots of tools available in the market for doing ethical hacking. You should be aware that many of the hackers or less than 15 years of age, and this hacking is actually organised crime. The reason why people hack is, they will be able to catch hold of sensitive data ok, and one if you are a media person, you want to increase your TRP rating by getting this kind of sensitive data. If you are a criminal, then you want to get make money out of the sensitive data and everyone knows the data is very sensitive, because there are issues of privacy and secrecy etcetera.

Now, with every data going digital, it is inevitable that we have to protect our data as much as possible. So, the work of a network administrator today is not only taking care of a computer network and ensuring security of the organisation from external hacking or attacks , but also the configuration of networks etcetera. Now we will see that if you do not configure a machine or a network properly, then you give rise to whole security loopholes, whereby by a hacker can take over your network or your machine.

Now this kind of hacking is similar to organised markets for stolen goods. For example, I get some data and there are people who are waiting to consume this data; say probably to get fame or probably to get money or probably to increase their TRP rating, if it is a news channel.

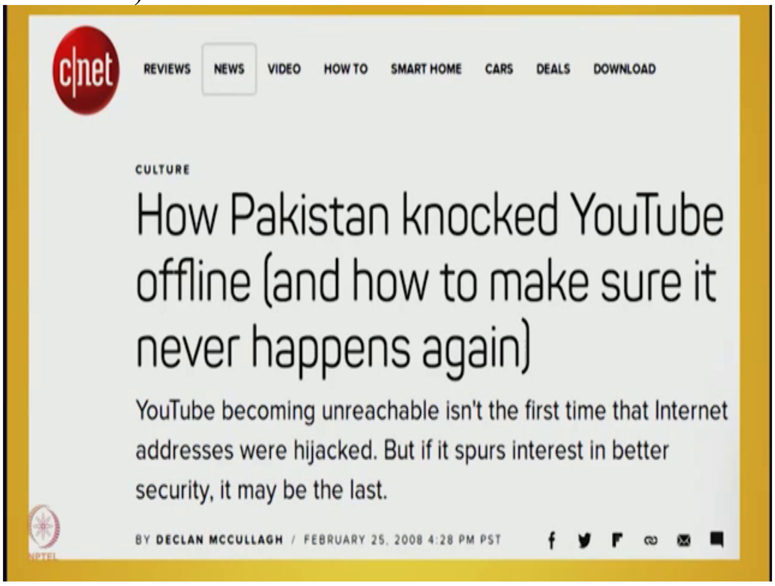
Now, that is one way. The other way is that, they might do some sort of a system kidnapping. The idea is they will be monitoring your activities and they will be stealing personal data or they even you will take over your system. In fact, in many of the ransom wares, what people will do is, that they take over your system and then encrypt your disk and then send you email that, unless you actually pay me some money, we will not give you the decryption key, because of which you will not be able to look into your data.

Now in order to avoid any trace of money transfer being taken what they usually do is, they will ask for bit coin for payments. I hope you are aware of meaning of such things. And what are the simplest ways to take care of this, is not to click on links for which I mean out of curiosity. You know many times you get some emails where you say you click this link, you gets this much money etcetera.

Now, as long as you are not greedy and go on clicking that link, many of these kind of attacks can be prevented , then there is one bunch of groups which actually does higher hackers; say for example, I have a company and there is a competitor for me. Now I want to get internal marketing details of that company ok.

So, what do I do? I go and legally hacker, I mean a higher hacker and he does the job for me and he gets me all the data, and using which I can gain market share or anything and many of these payments usually happen why are bit coins, let us not think about hacking alone, because of this very famous incident ok.

(Refer Slide Time: 05:04)



CULTURE

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.

BY DECLAN MCCULLAGH / FEBRUARY 25, 2008 4:28 PM PST

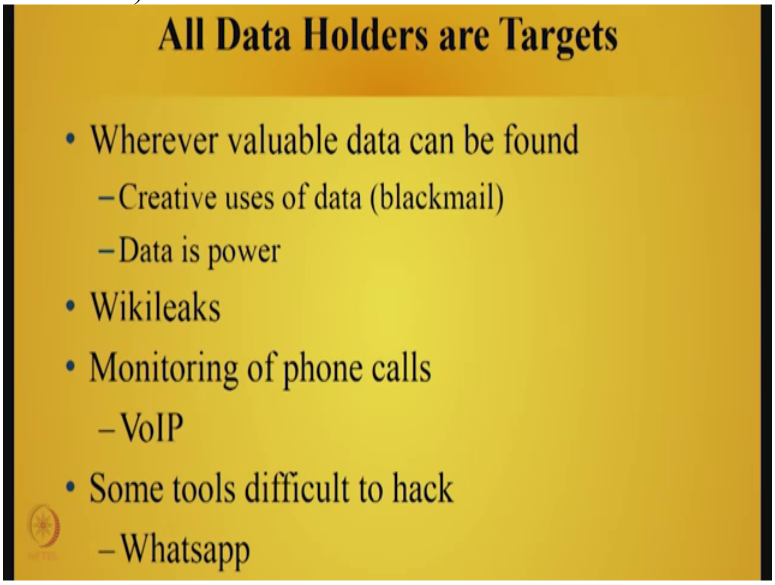
So, it so, happened in 2008 that Pakistan wanted to black block YouTube, know what happened was, this system administrator actually wrongly cannot keep configure the network, and because of which any YouTube traffic was not. I mean out of Pakistan or in of inside Pakistan and all this traffic was sent to something known as a black hole, and actually YouTube was different for such a long time. I think those around 2 hours if it got distracted.

Now, the point here is that, it is not who is blocking, you have to know that the internet is so vulnerable that even a very minimal mis-configuration can lead you to the loss of availability of the internet, and if you remember a loss of availability can be, it can be translated to, to something tangible like money for a company.

For example, you assume that Amazon dot com does not have itself available for 2 or 3 hours. Imagine the amount of loss that would happen to this company ok, if it loses internet connectivity for 2 or 3 hours from its not only true with Amazon dot com, its true for other internet based companies also.

For example, Uber so, these companies have to have the network 24 plus 7, and there should not be any downtime at all and that is one of the very stringent requirements and a minimal miss configuration can lead to this which tell you, how you are doing a tightrope walk with this networks and internet etcetera. Then who does the hackers target ok.

(Refer Slide Time: 06:45)



All Data Holders are Targets

- Wherever valuable data can be found
  - Creative uses of data (blackmail)
  - Data is power
- Wikileaks
- Monitoring of phone calls
  - VoIP
- Some tools difficult to hack
  - Whatsapp

So, one of the you all know that in this age of knowledge economy data is power and that is why you have lot of course; like data science, data mining etcetera. So, wherever a data, valuable data is found people will hack it ok, and the other point is that you could use the data for even doing an illegal or unauthorised activities.

One of the other points is that, see all these, many of these governments work in secrecy and secrets is needed in any governance ok, and sometimes if the data can get hacked ok. So, whatever happened in Wiki leaks for example, I mean some of the personal conversations are converse, all the conversations between some top level presidents ok.

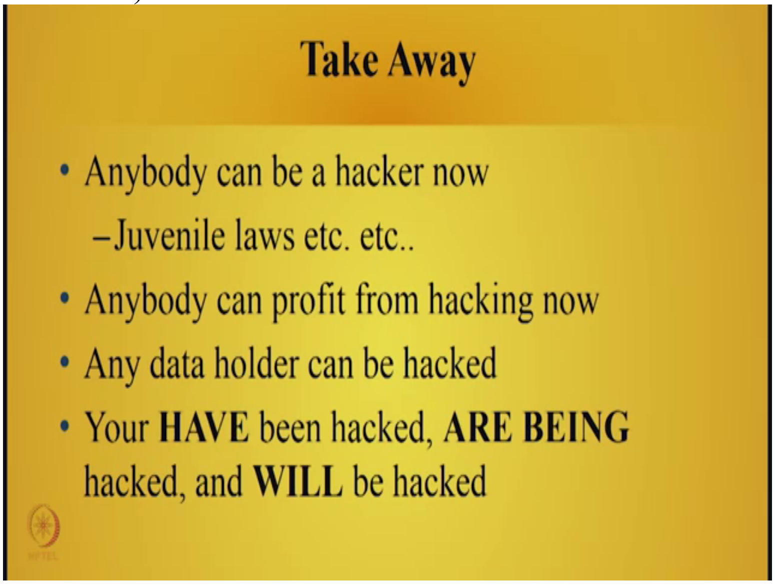
These were let out by Wiki leaks and it created a huge amount of sensation and even you can bring down governments.

So, you need to be careful that data is very precious and it has to be protected as much as you are protecting your money, monitoring of phone calls ok, both for legal and illegal activities ok, and if you look at this, all I mean if I am going to talk to someone over phone ok, this called as phone tapping ok, and this is made very easy with voice over IP ok, because in many a time voice over IP data is not encrypted. Of course, there are certain protocol encrypted voice over IP data.

Now, there are certain tools very difficult to hack. For example, Whatsapp and that is why many of the countries also prevent our people from using Whatsapp ok, because it is very difficult to see Whatsapp is a personal one to one communication. If that happens it does not leave any trace, until someone picks up the phone and then get the data, because it would be a very short communication also, whereas if you are going to use something like S M S, these data can be recorded.

So, some tools are very difficult to hack; like Whatsapp. So, because of this anyone who is a data, might be a target of these hackers, know the whole idea behind the network security and forensics. There is also some kind of legal stuff that is involved.

(Refer Slide Time: 09:06)



Take Away

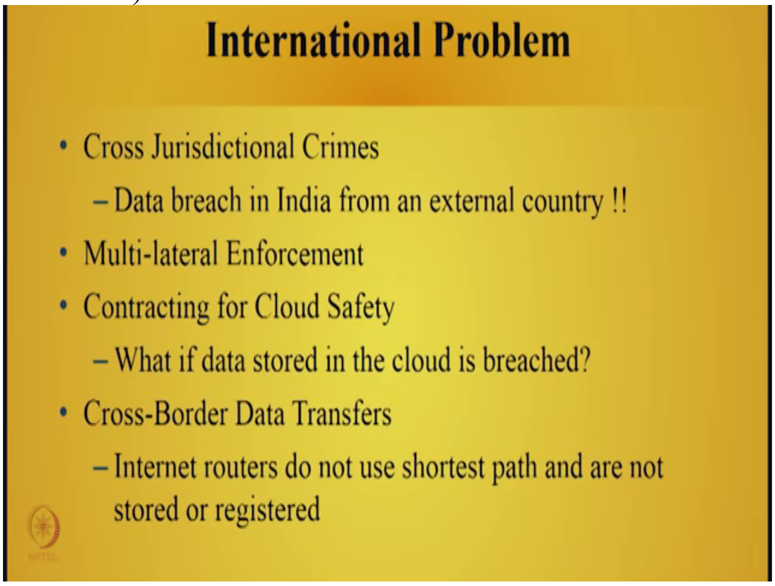
- Anybody can be a hacker now
  - –Juvenile laws etc. etc..
- Anybody can profit from hacking now
- Any data holder can be hacked
- Your **HAVE** been hacked, **ARE BEING** hacked, and **WILL** be hacked

For example, anybody can be a hacker now and so in India, especially you have this kind of Juvenile law which are much different from laws that are applied to the adults ok. And if for example, a 10 year old persons by chance hacks some companies at work. Now how are you going to actually punish him ok, what kind of laws are you going to use. So, this is another aspect that we need. Think about and today anybody can profit from hacking server; example I am able to hack a movie booking site, let us assume ok, where I am able to book tickets with zero money ok, and these are, there have been cases such things are happened ok.

So, now, just for fun ok, I might book for 10 tickets and then go and watch the movie with no trace of who did all this, and that will be a data for lost for the theatres ok. So, you know any who data holder can be hacked and we should be prepared for if some kind of hacking happened. How are you going to get out of the string. Remember it is like getting affected in health; first let us try to do lot of preventive care, if you are with prevention and you are able to your, like vaccination, then well and good; otherwise if you get affected then you have to protect yourself from getting effected again. So, that is going to be the agenda ok.

So, the forensics, the idea is that, one you can find out with forensic whether anyone is trying to hack you ok. Two, if someone hacks you know what is it that, the person attacker has used to hack you. So, that is this second way in which forensic can be used and let us be aware that, I mean even though we talk about personal data and all that, once you go into the web and once you log into to websites; like Facebook, twitter no longer is your data personal. I mean you can, anyone can just find out what your nature is and what your interest is by using twitter and Facebook data anyway.

(Refer Slide Time: 11:08)



International Problem

- Cross Jurisdictional Crimes
  - Data breach in India from an external country !!
- Multi-lateral Enforcement
- Contracting for Cloud Safety
  - What if data stored in the cloud is breached?
- Cross-Border Data Transfers
  - Internet routers do not use shortest path and are not stored or registered

So, you need to be careful about this problem of security, net security, network security if you. How is this network security problem different from the other problems that you are facing, like say a O S hacking. What are the things is, network security is cross jurisdictional crimes ok. For example, you could have a data breach in India that arises from another country.

For example, your external country or enemy country, you would have heard of a lot of websites being defaced by people hackers from other countries, and actually there is a kind of war that is going on. If hackers from another country deface some of the website then hackers from India do it to that country.

So, this kind of stuff is going on in the internet for quite a long time. I mean if you do it with guns and bullet us you call it as a war, but here you can call it as a cyber war which is, the cyber war is a actually going on between many of the countries I mean and some of this is just for fun anyway, but if it is illegal to do this anyway.

Now, the other thing is if there is a problem ok, if I even if I do cyber forensics, then you are supposed to have multilateral enforcement. For example, security is not just about securing your network, it is also, physical security is also a part of security. I mean you let anyone in inside your campus and then say that my network has been hacked, even though I might have lot of physical system in network security in your infrastructure ok.

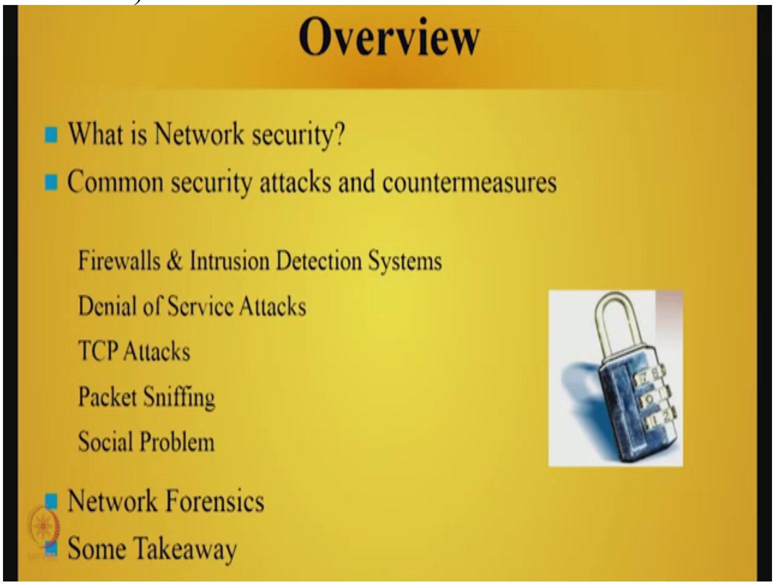
The other aspects is that what happens if I store my data in the cloud ok, and that data is breach, whom are you going to hold responsible. I mean is it, because you should not as to store the data in the cloud or there is cloud service provider did not provide you the effort or the network which was back. So, that they were able to hack it etcetera. So, a lot of issues that will come in, the other thing is that about the cross border data transfers ok.

So, what things about internet routers you be aware, is that they do not use the shortest path to transfer data from one location to another location, because a protocol like B G P is actually policy based, which means it runs based on certain policies that are governed by, means some latest say a transaction or some kind of agreement between service providers ok.

So, for example, if I find out that my BSNL link is much more cheaper than the other link from Airtel, then I would normally like to route lot of my data through BSNL rather than Airtel, because I save on certain amount if a router BSNL something like that is used ok. So, that is known as policy based routing; that is you visit on certain policies and not on the network architecture and you also use network, but this is so B G P as such policy based routing, and because of which the data need not take the shortest path, even though shortest path is one of the criteria that is used by B G P ok, and due to this you are not given an assurance that data will go from one location to another location to the specific path.

Of course, there is lot of research work that is done, being on source based routing and etcetera where you tell which part your take it etcetera , but then the idea is that, because if you know which path you are going to take, you can at least secure the path and if you do not know which path you are going to take, what will you secure ok. So, this is actually a problem with architecture as well as, and what is network security and forensics, is actually an international problem ok.

(Refer Slide Time: 15:00)



Overview

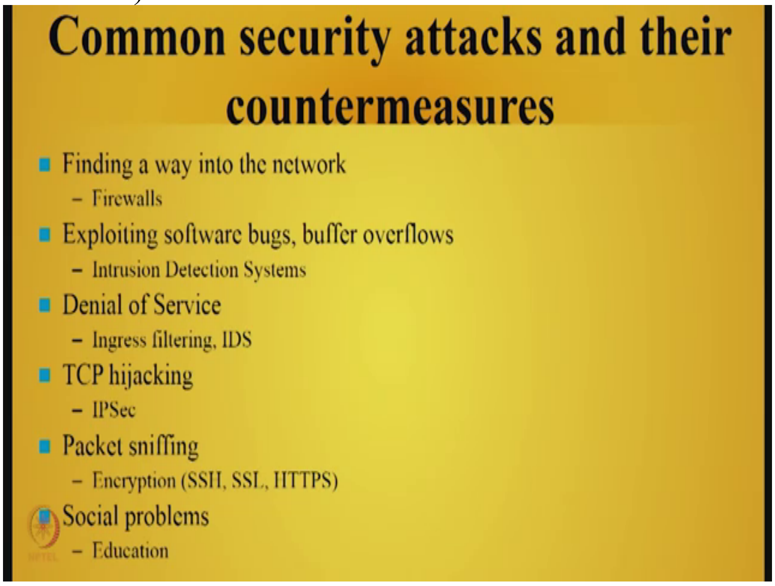
- What is Network security?
- Common security attacks and countermeasures

  Firewalls & Intrusion Detection Systems
  Denial of Service Attacks
  TCP Attacks
  Packet Sniffing
  Social Problem
- Network Forensics
- Some Takeaway

So, what do you do in the next few sessions is, that the few sessions this is over the course is that, we will talk about network security at one point and then will also talk about that all the security attacks and countermeasures; like firewalls intrusion, detection etcetera. In fact, the course will also tell you what is the forensic value of each one of these devices and for example, if I use a firewall or intrusion detection system, they can provide much more information than something else ok, and will be touching about these aspects, will also look at network forensic.

We will give an introduction about how to analyse data; for example, how to get the data, how to upload data, how to analyse it. We are not going to look at very data intensive or computer intensive technique, will be talking to a given you sort of introduction, after which you can take it from there and will also give you some kind of takeaways from the whole course and that will be happen at the end of the course.

(Refer Slide Time: 16:03)



Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

So, what we will do is. We will now in the next module take a look at what are the common security attacks and their counter measures, and we will discuss each one of these devices very briefly. So, that this act as an introduction to you, when we go and look at the forensic value of these devices. For example, if you firewalls actually protect, if someone is trying to find a way into the network; that means, want enter your network ok, then you actually use firewalls to stop them and what you do is that, you only allowed those traffic in which you are interested and you filter away all this traffic if you are not interested.

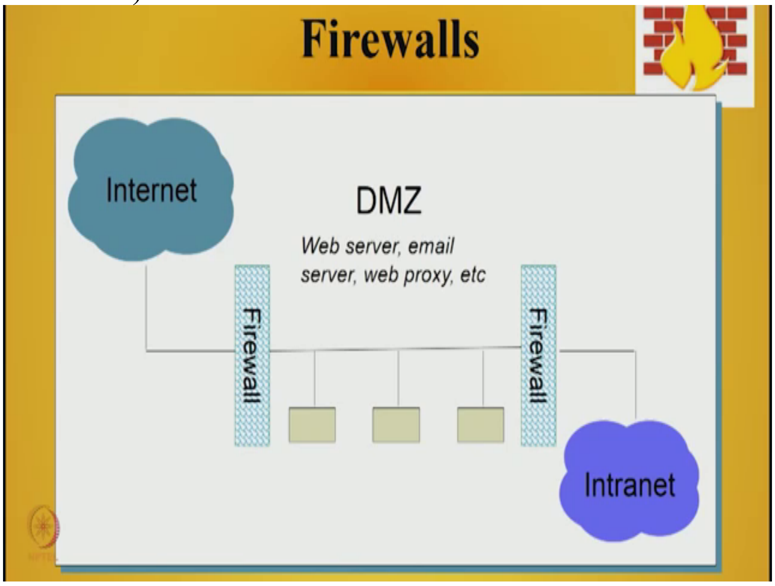
The second point, kind of security attacks is exploiting software bugs and buffer overflows and for this, the intrusion detection system prevention system ids for IP's can be used to ensure that ok, many of these ransom wares and other things like that can be filtered out at the entry stage itself, because we, once the data entrance a computer and spread then it is like a virus ok, is better you prevent something from happening rather than after something and you try to check a everyone another disk have been affected etcetera. The third one is denial of service and denial of service is ensuring that you do not have 100 percent availability for your mission ok. That can be prevented by using ingress filtering or intrusion detection system.

Then there is this hijacking of session, T G P session that can be hijacked ok. For example, when two users are communicating with each other then you can actually go inside and then participate or change the data packets, eaves drop, they call it as eaves dropping and change the data packet etcetera ok. So, that you can prevent by using I P sic, where you can either, you can have a encrypted security payload or you can have a authentication header which is encrypted etcetera. Ok then you can look at packet sniffing and that can be prevented by using encryption ok, you can also look at social problems.

It is also very important I mean someone would like to act as a friend to you and he is going right end, and trying to get data out of you and that can be done by continuing education, I mean there is known as the social engineering attack ok, and this social engineering attacks is similar to someone becoming friends with you or; for example, I mean this is very important see you meaning of you try to enter a password while travelling in a train or something ok.

Someone could peep from your back and then find out what your password is for the website and use it. So, you have to be very careful when you are doing, when you are moving in a social group and then avoid these kind of think; otherwise some people will like will come to you and act as if they are very concerned about your problems and then guilt try to extract information about of you, all this things can happen. So, this is known as a social engineering attack, and the only way to prevent social engineering is to educate people that kind of attacks can happen.

(Refer Slide Time: 19:11)



Firewalls

We will very briefly look at each of these devices that are used for providing network security. In the due course when I go into the details of the network forensic subjects, we will look at what is the forensic value that these kinds of devices provide. For example, a firewall can provide you lot of details about who is trying to intrude into the system. So, in that way we will be collecting logs from each of these devices, and then trying to identify how attacker is trying to attack a network. What is in general, many network applications and protocols have security problems at a fixed over time.

If you want a similarity in automobile industry, even though it is not about security , you would see that many of the automobile companies after one and half years of releasing a product, come back and say that look we have a mall function in one of these devices; for example, an airbag. So, therefore, come to our shop and please replace your head back.

Similarly what happens is that many network applications and protocols, when people start using, hackers can to those applications and protocols, and the people who want to prevent this kind of hacking, provide lot of patches to ensure that people do not have the system, Os it is a kind of a tug of war, who is going to win we really do not know, and usually it is a the hackers movie ok.

Now, the problem is that say let us say that people keep on releasing patches quite often and everyone has to fix this package; say for example, windows patch, everyone has to fix windows patch and all the mission, suppose your organisation has ten thousand missions. Now it should be practically impossible that all the people would patch, and even if they patch at the same time look at the amount of data, to download the data from the website and then install it in their machine and for that they have to have administrator privileges etcetera.

Sometimes what happens is in order to ensure that other, in order to not to solve the or pass on the problem to the end people, you could have certain devices such as firewalls ok, where the network administrator can limit access to certain websites or devices that these people make. Say for example, if you keep your net, if you are if you keep your computer open, anyone can hack into the networks.

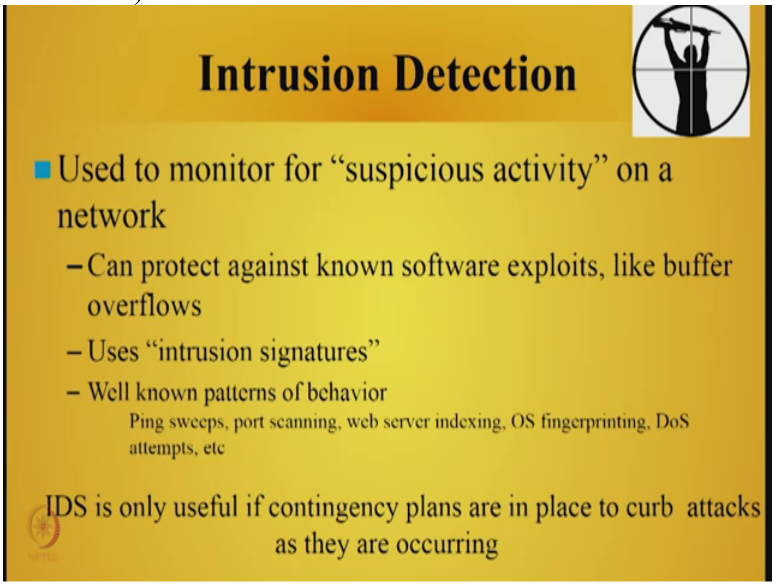
So, what I can do is, I can put some kind of restrictions that you cannot go to this kind of sites, you cannot browse these kind of sites etcetera, and you will not be let some kind of a traffic for example, a (Refer Time: 22:08) set happens and your network, your computer may be directly affected, but I can have some device in front of your computer will prevent the this kind of the attack, that is exactly what a system like firewall does.

But you should also be have a that firewall should be kept updated by the administrator, and firewall is like a castle with the drawbridge. So, you can be the hardware or software. So, only if a person enters through the firewall they will be able to access your network. Now your firewall should be strong anyway, because a firewall is the first level of defence that any organisation does, it should also have capability one, it should be very powerful box ok.

Two it should be able to give you lot of data, if a hacking or any attack happens ok. So, the last come from firewall can be extremely useful for forensics. Now you usually what does a firewall do, you will have something known as an external firewall and an internal firewall. So, this is the external firewall which actually prevents attacks from the internet, and this is the internal firewall which actually tries to prevent attack into your come, into your local organisation network, and will be in between these two, you will have something known as a dream militarized zone, while have a server e mail server web proxy etcetera.

So, what is device do you, suppose I want access the internet, what you do is, if you do not directly access that you come by this firewall and access these devices, and these devices will provide a path to access the internet. We will talk about web proxies in details in the forthcoming network forensic expressions ok. Now the idea is that, you feel happy that this will not get hacked ok. So, that is why they are placed between two firewalls to prevent the internal hacker from doing some damage to this or an external hacker from doing some damage to this.

(Refer Slide Time: 24:09)



Intrusion Detection

- Used to monitor for "suspicious activity" on a network
  - Can protect against known software exploits, like buffer overflows
  - Uses "intrusion signatures"
  - Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc

IDS is only useful if contingency plans are in place to curb attacks as they are occurring

The next is the intrusion detection, this is usually kind of live monitoring device which looks at suspicious activity on your network ok. And the idea behind this you know that a lot of software exploits that are released, then like buffer overflows extract this. This intrusion detection system can actually look out for those kind of signatures ok, which they call it as the intrusion signature, and then they can actually go ahead and ensure that this system is protected.

The idea is that this kind of signatures my arise over a period of time. Suppose I come to normal if this web server that have an, these a virus it has a certain signature, signature is generally a pattern that you detect out of the software. Usually a signature is identified for example, if someone does port scanning ok.

The signature is that the port numbers might get incremented one by one. So, X plus 1 X plus 1 X plus 1. If you see the port numbers increasing, then you have an idea that someone is trying to do a port scan ok. So, in order to do that you can do a random number generation which can generate all the random number with equal probability, in that way you can overcome this n plus one n plus one kind of a pattern based behaviour.

So, essentially, as I told you this will kind of a tug of war, where if the hacker finds out that we are having intrusion detection system is can detect, that port scanning is happening, even go ahead and change the hacking algorithm. Again you have to come up looking at the distributions of the port in which someone is accessing you, they will be able to identify that this guy is a hacker etcetera. So, this is a kind of tug of war as I told you who is smarter than the other ok.

Similarly, you can do some kind of o s fingerprinting. For example, I will try to find out, I think Vasan will be talking about this, when I scan a machine I will try to find out what kind of operating system that machine is using. So, if I find out that, its a windows operating system then I will try to work on software, which will help me hack the windows operating system.

So, this kind of O S finger printing helps me identify or help me in writing code which is specific to that particular O S and exploited it. Similarly denial of service attacks etcetera. So, ideas only useful if contingency plans are emplaced the curve attack as their occurring, it is an all about live system.

Thank you very much.