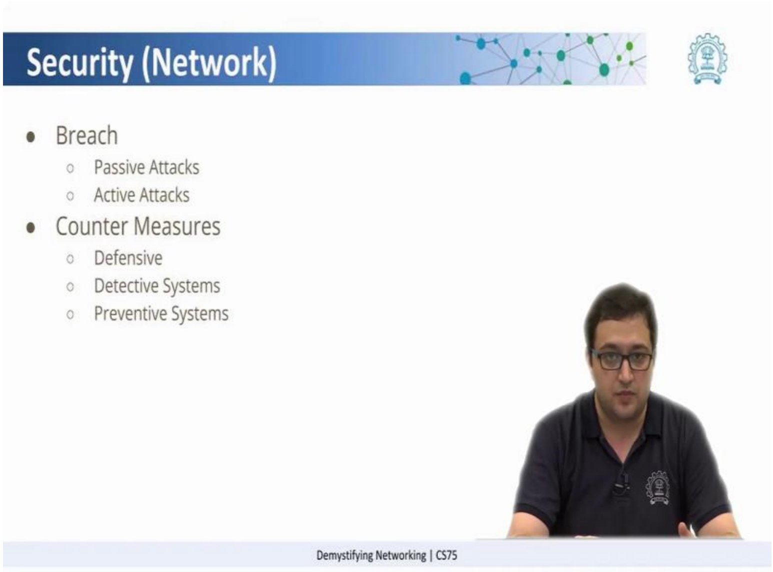
Demystifying networking
Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 79
Network Breach and Countermeasures

Now, the next important point in network that we should look at is the Breaches.

(Refer Slide Time: 00:05)



Security (Network)

- Breach
  - Passive Attacks
  - Active Attacks
- Counter Measures
  - Defensive
  - Detective Systems
  - Preventive Systems

Demystifying Networking | CS75

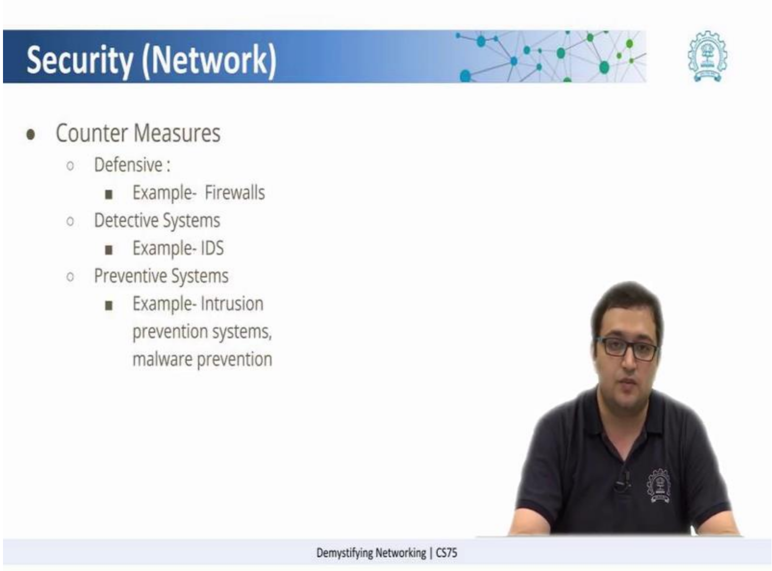
As we talked previously that it is important to be aware. So, we should be knowing that what are the kind of attacks that can happen on a network. So, there are basically two types of attacks, we will not be going into the depth of each, but let us talk at the broad level. So, the two types are active and passive attacks. So, a passive attack is something which happens before an active attack usually.

So, a passive attack, the objective of a passive attack is to come to know how the network looks like or what are the kind of systems that are available or say what is the operating system that you are operating right now on the systems.

So, from the information that is collected from a passive attack, they are able to determine on which systems they could do an active attack. What does an active attack mean? So, now, they can be sending some say information some scripts or certain codes to that particular system, that can say take advantage of a vulnerability and gain access to that system without proper authentication and authorization and once you have access to that system.

So, once you are in the network, it becomes easier for you to penetrate into the other networks, where you can take advantage of the network policy and the user policy. So, for example, if we were able to breach say a network with the user policy of a network admin, you could access almost each and every part of company's network through that policy account.

(Refer Slide Time: 01:35)



Security (Network)

- Counter Measures
  - Defensive :
    - Example- Firewalls
  - Detective Systems
    - Example- IDS
  - Preventive Systems
    - Example- Intrusion prevention systems, malware prevention

Demystifying Networking | CS75

What are the current type of countermeasures that can be put in place to take care of such breaches? So, there are three types of countermeasures one is called the defensive countermeasure. So, let us look at your house in this case, let us discuss these three types looking at a house. So, the gate that you have in front of your house is a defensive measure which restrains people from coming in. But say someone has been able to open the gate or breach the gate and get into the house, then say you have put a security camera there. Now the camera is able to detect a person there and maybe send you an alert, so that is what we called a detective system.

Now if you have another system which based on the detector system the security camera here, is able to say lock your doors and lock your windows, so, that becomes a preventive system.

So, similarly in security what we have is, we have defensive systems like firewalls that basically block ports that are not in use or certain type of information say certain applications like for example, in a lot of places you have certain applications that are not allowed to be used, some social networking websites for example; so, those are defensive measures that you have.

Then we have detected systems, these systems do not block communication or do not, but they keep watch on what kind of communication is happening and if they come to know that this communication has been tampered with or say somebody is trying to send some malicious code into the network, they can alert the network administrators about it. Now if there is a preventive system, that system can actually come in and say disconnect that communication from happening so that it can prevent certain things from going wrong on the network.

Now some examples of preventing systems are intrusion prevention systems and these days intrusion prevention systems are also aware available as something called malware assessment systems. Now what these do is, they check real time communications for signatures of malwares and viruses and if they feel that this particular communication or this particular network or say host is sending information which looks like a malware, they can block that host or say that network from communicating with our network.