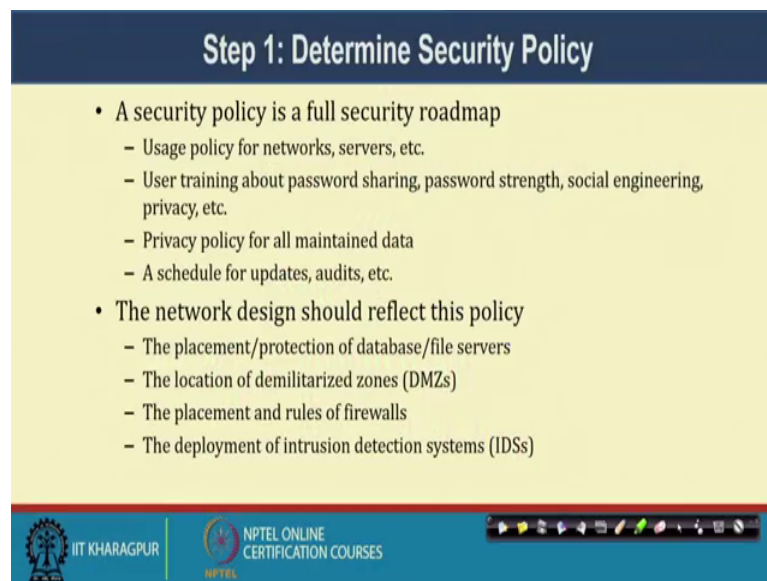


**Computer Networks and Internet Protocol**  
**Prof. Soumya Kanti Ghosh**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture – 59**  
**Network Security – II**



Hello. So, we will be continue our discussion on Computer Networks and Internet. Actually we are discussing on Network Security in the last lecture; we will be continuing our discussion on network security. So, what we are in the last lecture we are discussing on some of the aspects of network security like determining network security policies, implementing the security policies and there rest of the things are step by step what are the things will be there.

(Refer Slide Time: 00:49)



**Step 1: Determine Security Policy**

- A security policy is a full security roadmap
  - Usage policy for networks, servers, etc.
  - User training about password sharing, password strength, social engineering, privacy, etc.
  - Privacy policy for all maintained data
  - A schedule for updates, audits, etc.
- The network design should reflect this policy
  - The placement/protection of database/file servers
  - The location of demilitarized zones (DMZs)
  - The placement and rules of firewalls
  - The deployment of intrusion detection systems (IDSs)


 IIT KHARAGPUR |  NPTEL ONLINE CERTIFICATION COURSES

So, actually we have seen that how to this thing that what are the issues related to determining the network security policies.

(Refer Slide Time: 00:57)

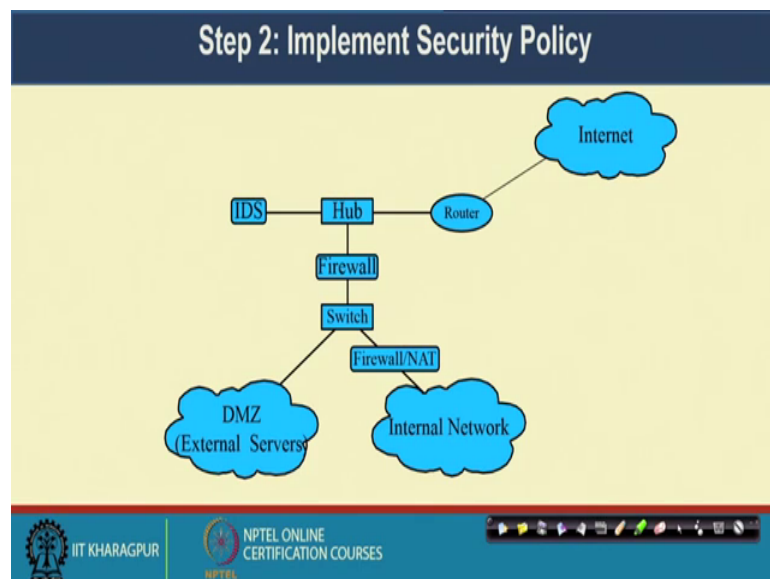
### Step 2: Implement Security Policy

- Implementing a security policy includes:
  - Installing and configuring firewalls
    - *iptables* is a common free firewall configuration for Linux
    - Rules for incoming packets should be created
      - These rules should drop packets by default
    - Rules for outgoing packets *may* be created
      - This depends on your security policy
  - Installing and configuring IDSes
    - *snort* is a free and upgradeable IDS for several platforms
    - Most IDSs send alerts to log files regularly
    - Serious events can trigger paging, E-Mail, telephone



And, also we have seen the issues related to implementation of the security policies, right

(Refer Slide Time: 01:03)



And, today we will look at the other aspects. So, if you look at the implementation of the security policies. So, we require other than our standard devices we require some more stock right like one is that IDS intrusion detection system. And, there is a concept of firewall like firewalling the thing and there is another thing called firewall or NAT will come to those aspects and this is my internet network.

So, what I am trying to do? I am trying to do an internet network secure from the rest of the world or so to say the internet, right. So, what I am having a router to connect to the internet and there are some of the devices which need to be external to be needed to be put some place where it will be accessed by the external world. So, that is the concept of demilitarized zone or DMZ zone where the external server which need to be accessed like for example, web server or some other servers we need to be accessed they are in the DMZ zone. So, there is a switch which connects this DMZ zone through the firewall to a some sort of a hub to router and this hub as the whatever the packets comes in the hub it is in the same broadcast and collision domain.

This idea is basically try to look at the intrusion detection system. So, it has protocols it has a logic to look at that to detect the interface or it has a database of knowledge base that how to detect. And, this firewall is basically to prevent to the thing from the external world. Now, IDS cannot be inside firewall right then it cannot know that what is going on inter the things right. And so, there that is DMZ zone if you see there are two category or two firewalls one is which basically makes a isolated DMZ zone.

So, this network is protected through this firewall whereas, this firewall protect this the systems in the DMZ zone and create a space where this type of systems can be there whereas this is a more exposed things where we want to know that what are the different type of net attack etcetera going on.

(Refer Slide Time: 03:25)

**Step 2: Implement Security Policy**

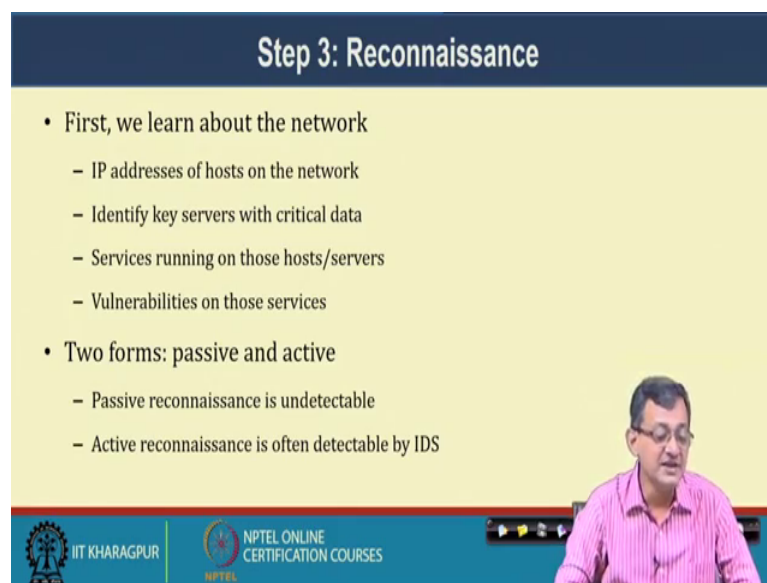
- Firewall
  - Applies filtering rules to packets passing through it
  - Comes in three major types:
    - Packet filter – Filters by destination IP, port or protocol
    - Stateful – Records information about ongoing TCP sessions, and ensures out-of-session packets are discarded
    - Application proxy – Acts as a proxy for a specific application, and scans all layers for malicious data
- Intrusion Detection System (IDS)
  - Scans the incoming messages, and creates alerts when suspected scans are in progress
- Honeypot/honeynet (e.g. honeyd)
  - Simulates a decoy host (or network) with services

The slide features a blue header with the title 'Step 2: Implement Security Policy'. The main content is on a light yellow background with a list of security measures. A small video inset in the bottom right shows a man in a pink shirt. The footer contains logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES.

So, implementing security policies one is the firewall is one of the major aspects other is the intrusion detection system or IDS and also there is a concept of honeypot or honeynet, right. So, it is something which are which attracts as the name suggest attracts this attackers to attack on the things.

By that it the signatures of the attacks are learned which may update the knowledge base of the IDS or something IDS detection systems and other things. So, that is important to have those type of things in large installation which are think. Now, there can be a network of this honeypots and to share the information and it can be across different organisations also. So, that there is a other information. So, simulates a decoy host or network with services which are exposed to the attack where the attack signatures are learned.

(Refer Slide Time: 04:21)



**Step 3: Reconnaissance**

- First, we learn about the network
  - IP addresses of hosts on the network
  - Identify key servers with critical data
  - Services running on those hosts/servers
  - Vulnerabilities on those services
- Two forms: passive and active
  - Passive reconnaissance is undetectable
  - Active reconnaissance is often detectable by IDS

The slide includes a video inset of a man in a pink shirt speaking. At the bottom, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES.

The next step is to learn about the network. I need to know that what the networks IP address of the host on the network, key servers on the critical data, services running on those host and server, vulnerabilities on those server. So, two form, one maybe a passive or active. Passive thing is that undetectable as I will say and active are by active attack on the things or which can be detectable by the intrusion detection system.

(Refer Slide Time: 04:57)

**Step 4: Vulnerability Scanning**

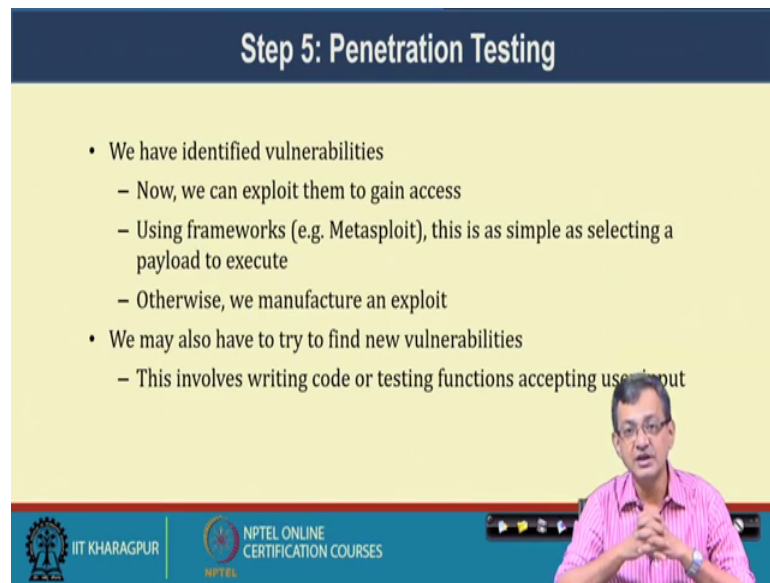
- We now have a list of hosts and services
  - We can now target these services for attacks
- Many scanners will detect vulnerabilities (e.g. nessus)
  - These scanners produce a risk report
- Other scanners will allow you to exploit them (e.g. metasploit)
  - These scanners find ways in, and allow you to choose the payload to use (e.g. obtain a root shell, download a package)
  - The payload is the code that runs once inside
- The best scanners are updateable
  - For new vulnerabilities, install/write new plug-ins
  - e.g. Nessus Attack Scripting Language (NASL)

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, another aspect what we want to look at the network that is the vulnerability scanning next step is the. So, I want to scan that how vulnerable I am. What are the vulnerabilities inside the thing? So, list of host and services that and many scanners will detect vulnerabilities like there is a scanner called nessus, other scanner will allow you to exploit them right. So, there is a metasploit source cannot exploit. So, if the vulnerability is there how to exploit them. Like I say there is a vulnerability in the user level login case, right. So, that is exploited to generate a higher level access right to the things. So, this is a one is that one the attack happens then you detect and learn other is that I can do a self scanning of the things.

That what are the different vulnerabilities viz a viz with my exploit database and try to find out what sort of vulnerabilities are there. So, there are scanners which are updatable that is for few vulnerabilities install write new plug INS. So, nessus attack scripting language and there are several language is there. So, that is means scanning the vulnerabilities.

(Refer Slide Time: 06:13)



**Step 5: Penetration Testing**

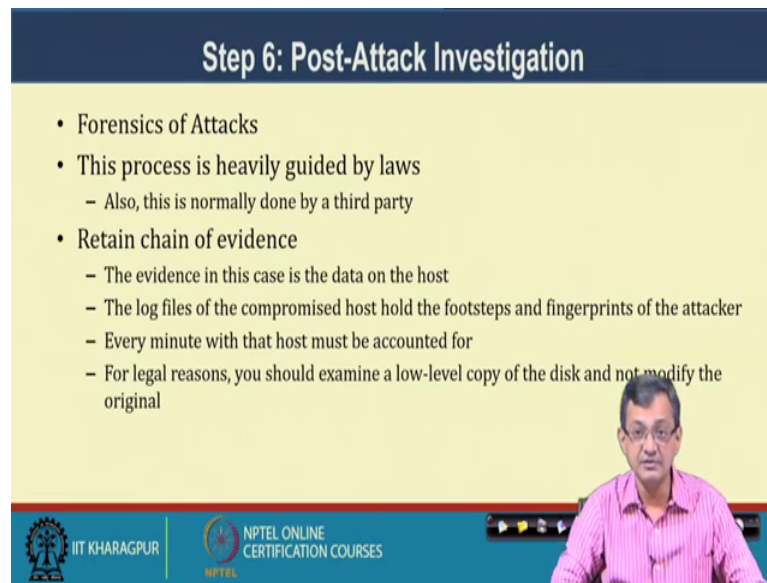
- We have identified vulnerabilities
  - Now, we can exploit them to gain access
  - Using frameworks (e.g. Metasploit), this is as simple as selecting a payload to execute
  - Otherwise, we manufacture an exploit
- We may also have to try to find new vulnerabilities
  - This involves writing code or testing functions accepting user input

The slide includes a video inset of a man in a pink shirt speaking. At the bottom, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES.

So, if I have the vulnerabilities whether I can do some sort of a penetration testing like I want to do some sort of a what we say known lethal attack on my system and see that how much I can penetrate and type of things or some sort of a ethical hacking on the systems right identify the vulnerabilities once the vulnerability identify we can exploit them to gain access using a framework like metasploit is a simple as selecting a payload to execute otherwise we manufacture a exploit or we generate an exploit and type of thing. So, there are different exploit for which there is no per se prevention on the things. So, these are these are what we say this zero day exploit type of things.

So, there are with there are so to say quote unquote costly exploits. So, that things are there, but once we learn then we go on patching. So, we may have also try to find out new vulnerabilities, the symbols writing, code testing function etcetera. So, these are this is a separate activity of the security group of a organisation to look at that what are the different well known vulnerabilities and type of things do a sec self exploitation of my network or ethical hacking on my network, find out that what are the possible attacks which are possible in to the systems and then try to recommend or find out what are the mechanisms will help in the detecting a in preventing those, right. So, these are the different aspects of this exploits vulnerability scanning and what we say penetration testing.

(Refer Slide Time: 07:45)



**Step 6: Post-Attack Investigation**

- Forensics of Attacks
- This process is heavily guided by laws
  - Also, this is normally done by a third party
- Retain chain of evidence
  - The evidence in this case is the data on the host
  - The log files of the compromised host hold the footsteps and fingerprints of the attacker
  - Every minute with that host must be accounted for
  - For legal reasons, you should examine a low-level copy of the disk and not modify the original

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

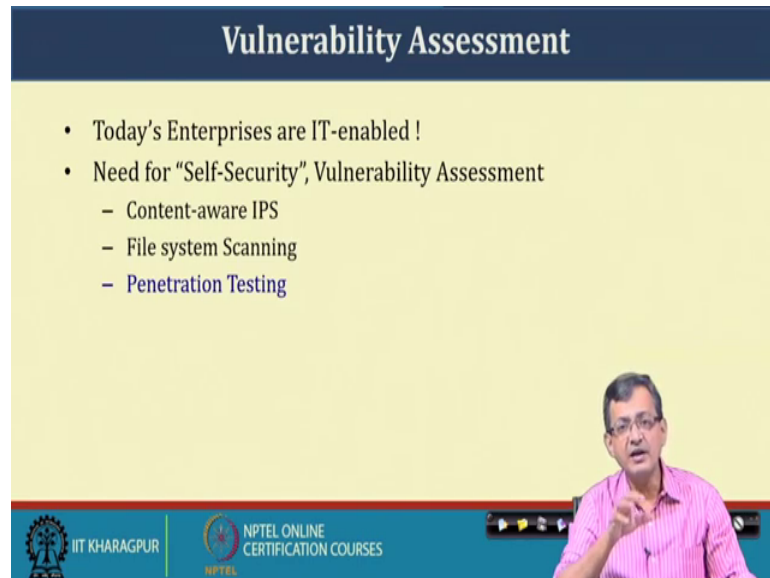
Now finally, we have the post attack investigation. So, forensic of the attack so, like if there is a attack then we have to investigate and do the some forensic or post mortem of the attacks, right. This process is heavily guided by law like what we have to do and what are allowed etcetera and there can be different guidelines from the organisation to organisations like the type of things which is true for academic organisation may not be true for a banking or financial organisation.

So, retain chain of evidences. This evidence is the case in this case is the data on the host. So, that is a what are the different evidences log files of the compromised host to hold the footprint or the fingerprints of that attacker to find out that how that attacker came. Every minute with that host must be accounted for. For legal reason you should also examine a low level copy of the disk and not modify the original thing, right. So, type of things that for legal later on some litigation etcetera we need to do specially commercial organisation, organisation giving services to other organisation and type of things.

So, in some cases your data is in some other place and type of things and need to be handled appropriately. So, what we see these type of steps are not a onetime things, it has to be executed on a routine basis because the system is evaluating or having different state at different point of time. There are different updates applications attacks and type

of scenarios are changing both the system scenarios are changing on the other side these attack scenarios are changing, right.

(Refer Slide Time: 09:33)



**Vulnerability Assessment**

- Today's Enterprises are IT-enabled !
- Need for "Self-Security", Vulnerability Assessment
  - Content-aware IPS
  - File system Scanning
  - Penetration Testing

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, vulnerability assessment of any network is very important, right that I need to a priori know that how vulnerable I am, right. So, though it say something which is difficult to say that I fully charged, but never the less there should be always a way of or always looking at the vulnerabilities. So, today's enterprise are fully or mostly IT enabled, right. So, any enterprise any organisation any even academic institution or any government federal organisations are all IT enabled, right or heavily dependent on IT infrastructure where the networking plays a major role in making things connected. So, need for self security that is vulnerability assessment is a order of the day, right.

You need to do vulnerability assessment. So, there are content aware intrusion protection system. So, it is content aware IPS file system scanning penetration testing. So, these are the different aspects which we need to be looked into.



(Refer Slide Time: 10:53)

**Penetration Testing**  
(Tiger team attack / Red team attack)

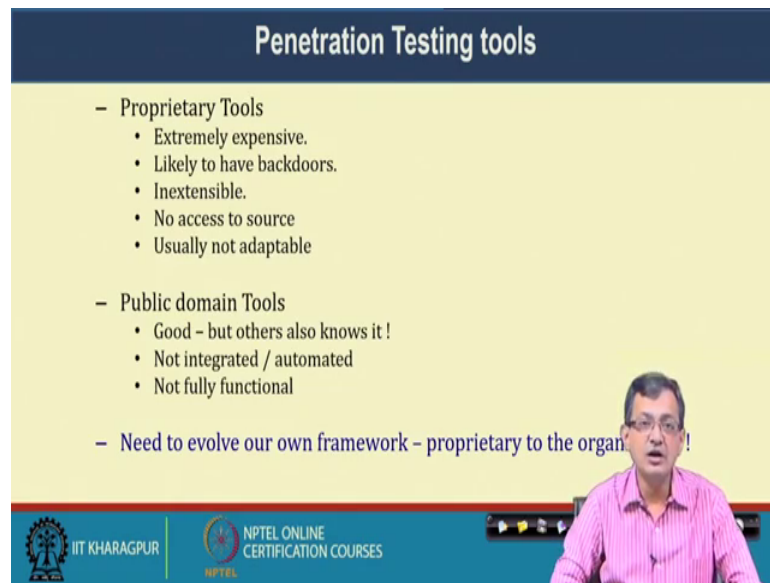
- Test for evaluating the strengths of all security controls on the computer system
- Goal : Violate the site security policy
- NOT a replacement for careful design and implementation with structured testing
- Methodology for testing the system *in toto* - once it is in place
- Examines procedural and operational controls as well as technological control

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, this penetration testing sometimes also called the tiger team attack or red team attack that test for evaluating the strength of all security controls on the computer systems. Goal, violate the site security policies. So, the I have a security policy a mechanism to implement those policies then I what I want to know that whether I can basically compromise this policy and attack this the system, right. So, not a replacement for careful design and implementation with structured testing. So, it is independent of what the best practices you are having. So, it is a careful design implementation structure testing in spite of that whether there is a loop hole or not need to be looked into.

So, methodology for testing the system in toto right once it is in so, system in place. So, the system is in place I have a mechanism to testing that whether the system is working faithfully or not. Examine procedural operational control as well as technological control, alright. So, it tries to look at procedural operation control and as well as the technological control in the things.

(Refer Slide Time: 12:05)



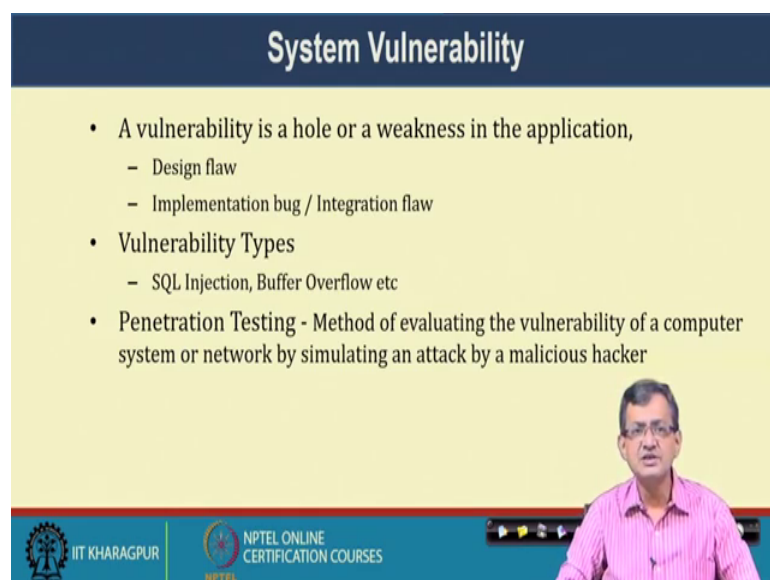
### Penetration Testing tools

- Proprietary Tools
  - Extremely expensive.
  - Likely to have backdoors.
  - Inextensible.
  - No access to source
  - Usually not adaptable
- Public domain Tools
  - Good - but others also knows it !
  - Not integrated / automated
  - Not fully functional
- Need to evolve our own framework - proprietary to the organ!

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, there are different tools some are proprietary tool which are pretty costly public domain tools, but good, but others also knows that you are doing like this and there are integration problem and issues like that. Need to evolve on one favour proprietary to the organisations etcetera that maybe a need, but is not may not be always followable never the less there are price productor always there.

(Refer Slide Time: 12:27)



### System Vulnerability

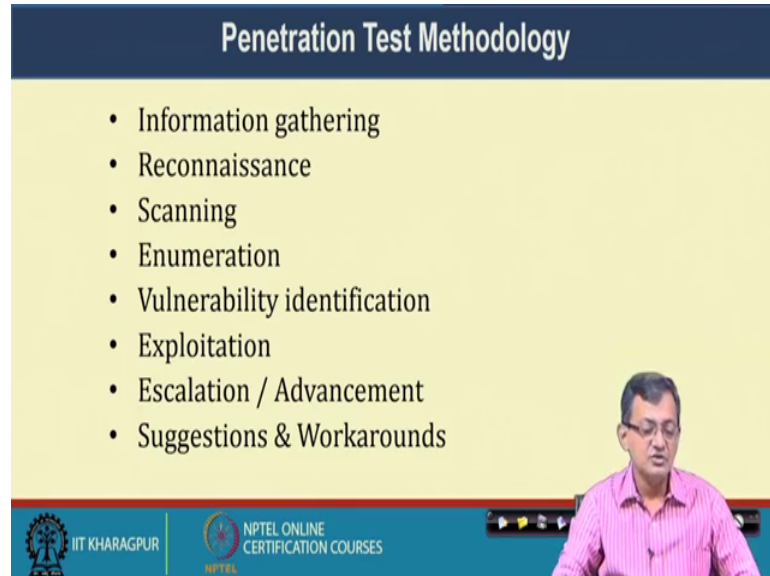
- A vulnerability is a hole or a weakness in the application,
  - Design flaw
  - Implementation bug / Integration flaw
- Vulnerability Types
  - SQL Injection, Buffer Overflow etc
- Penetration Testing - Method of evaluating the vulnerability of a computer system or network by simulating an attack by a malicious hacker

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, system vulnerability is in a hole or weakness in the application design flow implementation vulnerability type can be different SQL injection, buffer overflow.

Penetration testing - method of evaluating vulnerabilities of a computer system on network by simulating the attack of the malicious hacker.

(Refer Slide Time: 12:47)



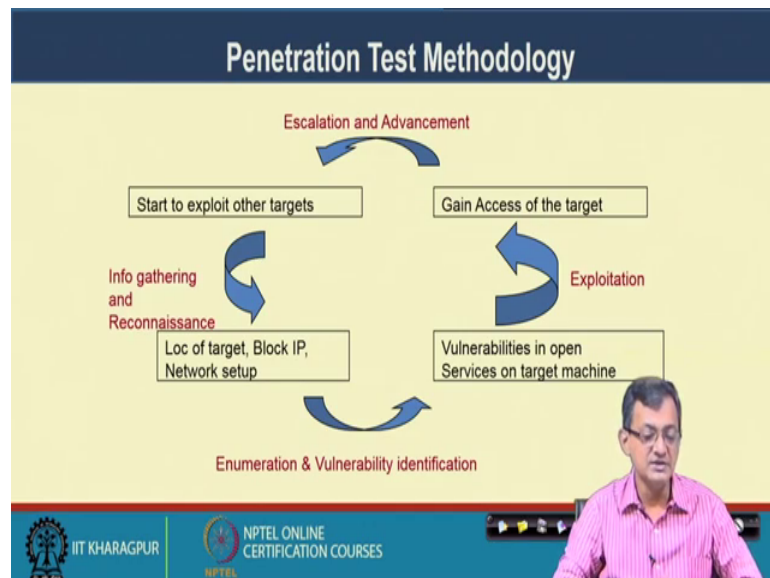
The slide titled "Penetration Test Methodology" lists the following steps:

- Information gathering
- Reconnaissance
- Scanning
- Enumeration
- Vulnerability identification
- Exploitation
- Escalation / Advancement
- Suggestions & Workarounds

The slide also features the IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES logos at the bottom left, and a small video inset of a speaker on the right.

So, methods again it falls in that same line we are not again discussing.

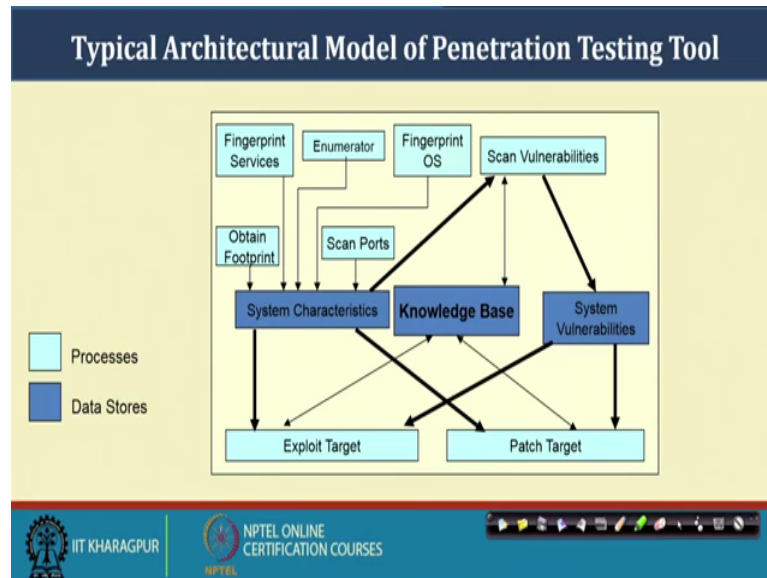
(Refer Slide Time: 12:53)



So, if you if you look at the penetration testing things. So, location of the target, block IP, network setup, vulnerability is in open services. So, enumeration vulnerability identification then whether we can exploit from the using the exploit database gain access of the system. Escalation and advancement stage to exploit the other targets

information gathering and reconnaissance so, to look into this whole loop. So, this is the way it goes on that you first learn about the system, get the footprint of the different devices and type of things then accordingly whether they are exploitable consulting the exploit database then try to escalate and advancement and then again information gathering and so and so forth, it goes in a loop.

(Refer Slide Time: 13:45)



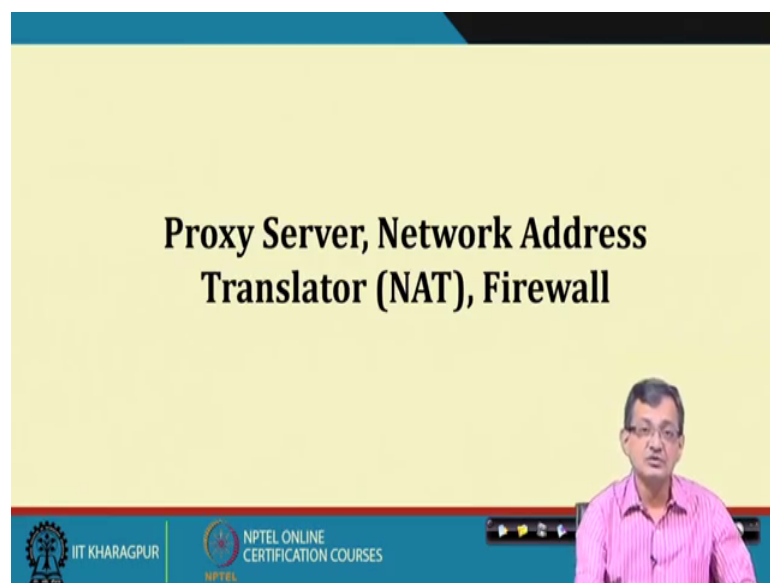
Or if you look at the typical architectural model of a penetration testing tool, so, there is a system characteristic knowledge base and system vulnerabilities right. So, these are the things. So, obtain footprint fingerprint services enumerator. So, that is fingerprint OS scan reports. So, it is a these are the things which go to find out the system characteristics. So, this from these the scan vulnerability is to find out what are the vulnerabilities consulting the knowledge base whether the system vulnerabilities then exploit targets can be there, right. On the other hand this thing can be used to patch the target also. So, some of the processes some of the data stores where things are there.

So, it is a not that very straightforward process the requires lot of expertise on the system level or wage level it also need good exploit database which and which are up to good and up updated exploit database which allows you to this exploit the system, but everything done in a quote unquote ethical manner that is non destructive manner. So, that the system is not goes off rather try to find out that what are the different

vulnerabilities and other things so that the patchwork can be or appropriate patches can be deployed.

So, with these mechanisms we will try to look at now that different system level things like as if you just recollect this one. So, there are different type of things right, one is your router, firewall or NAT there is IDS and type of things. So, we try to see that the what are the different properties whether something can help us in achieving better security features.

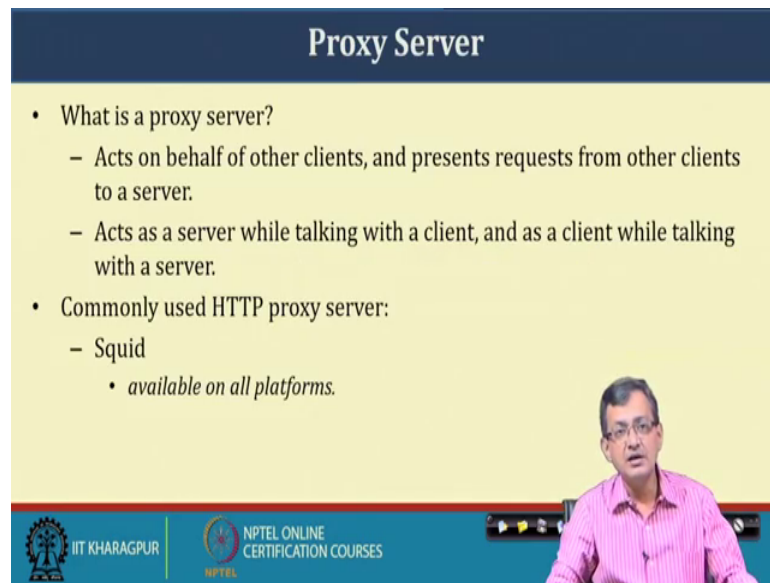
(Refer Slide Time: 15:49)



So, some of the things like proxy server, network address translator, firewall are some of the features or the things. To be very to be on at the beginning so, say that these are the things which are not primarily some not all the things are primarily meant for the security etcetera. So, they have other purposes also, but also can be looked into as a security measure.

As these are nowadays common for at all the network and it has some of the property to isolate the incoming or expose the or can handle the exposing of the internal host to the external things. So, this can be utilized only concern. some of the things has been already discussed in our in your in this lecture series also. But for the say sake of generality and to continue our discussion we are looking into some aspects again with the first; that means, we say so, that it is easy to correlate with the what we are discussing.

(Refer Slide Time: 16:31)



**Proxy Server**

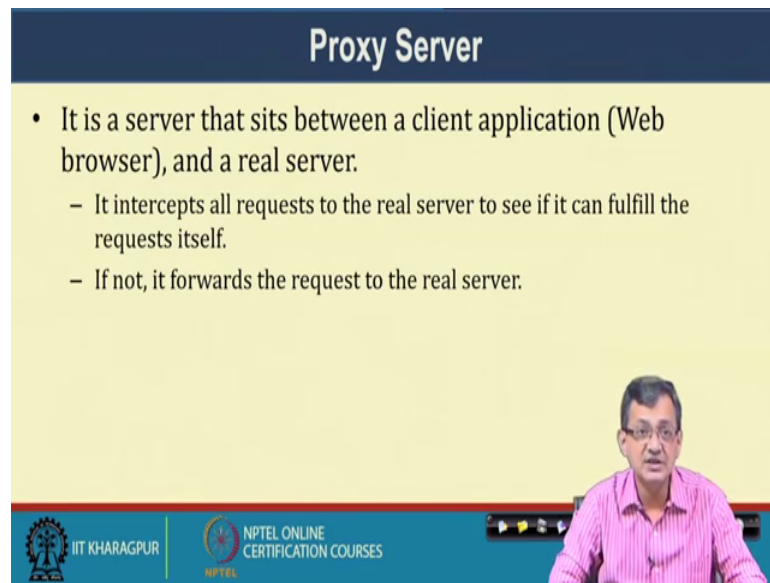
- What is a proxy server?
  - Acts on behalf of other clients, and presents requests from other clients to a server.
  - Acts as a server while talking with a client, and as a client while talking with a server.
- Commonly used HTTP proxy server:
  - Squid
    - *available on all platforms.*

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, what is a proxy or proxy server? Acts on behalf of other clients and presents requests from the other clients to the server, right. So, proxy is as the name suggest proxy is for the other clients, right. Acts as a server while talking to a client and acts as a client while talking to the server. So, it is a intermediate system with this proxying for the other.

So, the primary need maybe I like IIT Kharagpur we may be private IP block which are not routable. So, somebody is proxying for me and type of things or actually proxy can have much higher labels like or different type of aspects of the things even do content based filtering etcetera and type of and allows to do some of the things like caching and like caching and giving a better accessibility and type of things. So, commonly used HTTP for this squid, mostly available in most of the systems.

(Refer Slide Time: 17:57)



**Proxy Server**

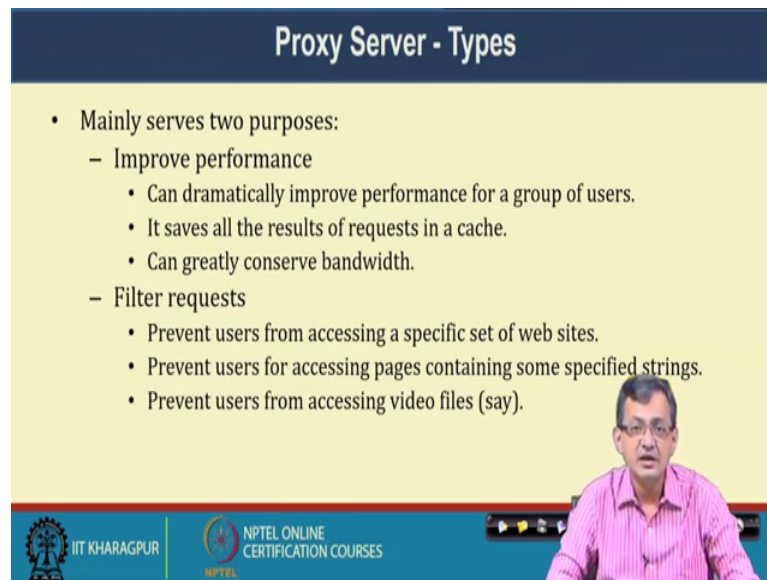
- It is a server that sits between a client application (Web browser), and a real server.
  - It intercepts all requests to the real server to see if it can fulfill the requests itself.
  - If not, it forwards the request to the real server.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Proxy server it is a server that sits between the client application for example, web browser and a real server. So, I am accessing something like for typically for IIT Kharagpur, if I want to access say any external surface IIT Bombay page, IIT Bhuvaneshwar page or IIT something or some any other page say some networking or I triple E standard page. So, what I am doing I am sending a request as I am generating from the IP a particular private IP even not that we have a proxy server which it hits the proxy takes that observe that IP and the port and in turn send a request on behalf for me, right. How the things maintained I have a IP and port proxy has a IP and port and this and the protocol this proof and this particular tuple is unique for our connections, right.

So, even if I have two browser say Mozilla or something, two instances do the same page if the things, but they have a different port right going out the thing. So, it intercepts it a it intercepts all requests to the real server to see if the full fill the request itself if not it forward the request to the real server, right. So, what happened that as it is accessing the things it is also caching the content, somebody requesting it may check there where is fulfilling the request or not.

(Refer Slide Time: 19:29)



The slide is titled "Proxy Server - Types" in a dark blue header. The main content is on a light yellow background and lists two main purposes for proxy servers:

- Mainly serves two purposes:
  - Improve performance
    - Can dramatically improve performance for a group of users.
    - It saves all the results of requests in a cache.
    - Can greatly conserve bandwidth.
  - Filter requests
    - Prevent users from accessing a specific set of web sites.
    - Prevent users for accessing pages containing some specified strings.
    - Prevent users from accessing video files (say).

In the bottom right corner of the slide, there is a small video inset showing a man in a pink shirt speaking. At the bottom of the slide, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES.

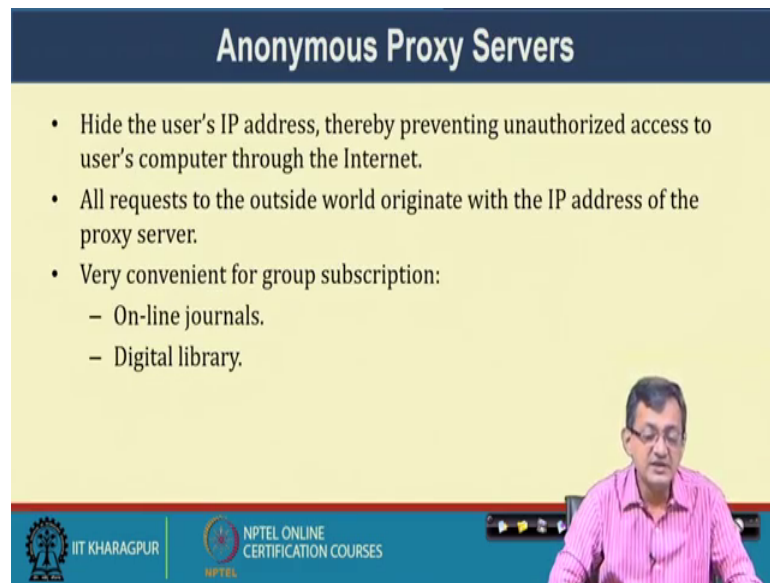
So, there are many servers this two types of servers this works up improve the primary to improve performance can dramatically improve performance for a group of users. It saves all the results of request in a cache can generally conserve bandwidth. So, I have a thing which is of replying the proxy in turn replying if the already it is in cache there is filter request that is another types is there or if instead of type I should say that basic purpose of the proxy server. So, it is not the proxy server types it is rather purposes of the proxy server.

One is that input performance because it is send on the cache another it has a property of filter request right when a request comes checking it that the weather request can be send or not there filter the request, in turn it gives a some sort of a security feature. Like prevent users from accessing a specific set of website IIT Kharagpur, the organisation think that these set of website cannot be accessed by the inside by means it is own users, so, it can prevent. Prevent user from accessing pages containing some specified things even the higher level proxy where the content can be seen where which can prevent user from specified pages which having a string.

Prevent user from accessing video files for example, the type of things, right and it also have apart from that the caching effect that we have discussed that to give you things. So, these are different mechanisms what we can do with this proxy things.






(Refer Slide Time: 21:19)



### Anonymous Proxy Servers

- Hide the user's IP address, thereby preventing unauthorized access to user's computer through the Internet.
- All requests to the outside world originate with the IP address of the proxy server.
- Very convenient for group subscription:
  - On-line journals.
  - Digital library.

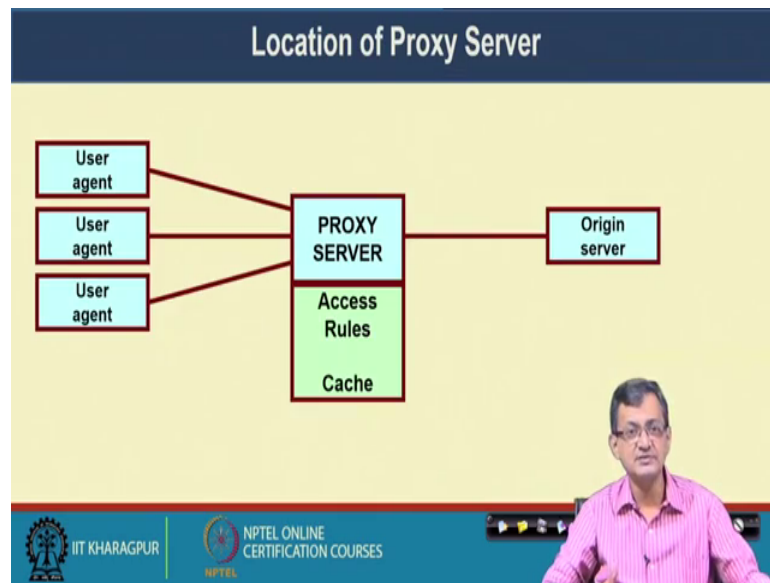


 IIT KHARAGPUR |  NPTEL ONLINE CERTIFICATION COURSES

There is a concept of anonymous proxy hide the users IP thereby preventing unauthorised access to the user's computer to the internet. So, it is anonymous proxy hides the user IP, right and all request to the outside world original with the IP address of the proxy server, right. So, what are the external IP address of the proxy server the original outers original this it basically the hides the users IP right. So, all request of the outside world originate with the IP address. So, the IP address of the proxy becomes the IP address which is gone to the external server.

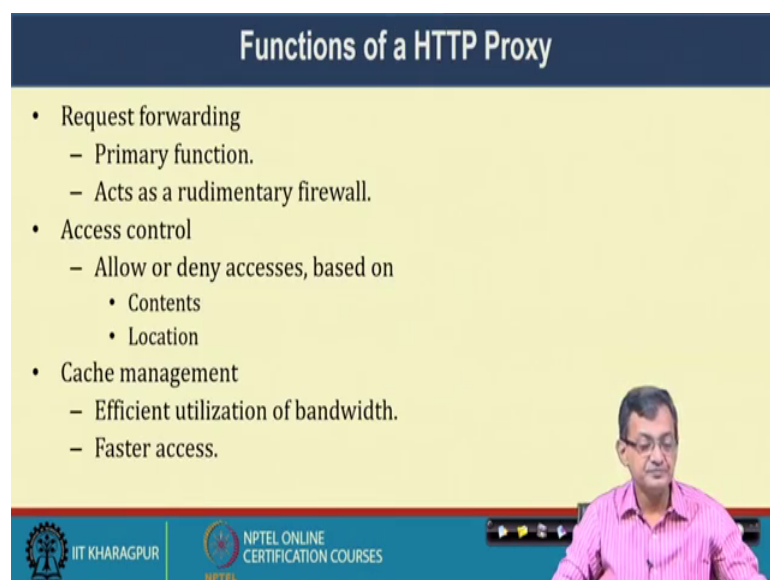
It is sometimes very convenient like online subscription of channel like IIT Kharagpur have online subscription of various journals I EEE, AICE, (Refer Time: 22:05) and type of things, right I do not know the exact list immediately with me. But, what happened that instead of while accessing it gives the proxy IP for the access of authentication to access the journal. Whoever has going using this proxy will be able to authenticate the get a access to this general things then digital libraries these are the things which we are which we are benefited here at sitting at IIT Kharagpur and that must be doing we must be doing in several other organizations.

(Refer Slide Time: 22:33)



So, where the it is located. So, somewhere in between right one side that original server where it accessing all these user agents are is request come to this proxy server. It has a access control list or access rules that by which the proxy that particular page can be requested and all the cache if it is already there, it will reply from the catch. So, that is the basic bottom line of the proxy server.

(Refer Slide Time: 23:01)



So, function of HTTP proxy request forwarding primary function acts as a rudimentary fire wall of taking care of that which can be filter. Access control allow or deny access is

based on contents and locations, right. It can do if it is if the proxy is able to look at up to the content at a higher level then you can it look at the it can open up the packet at the application layer or the message itself and check that what whether there is a any access control restriction based on content or based on the location. Cache management utilised efficient utilisation of the bandwidth for first hour access that is the cache management.

(Refer Slide Time: 23:55)

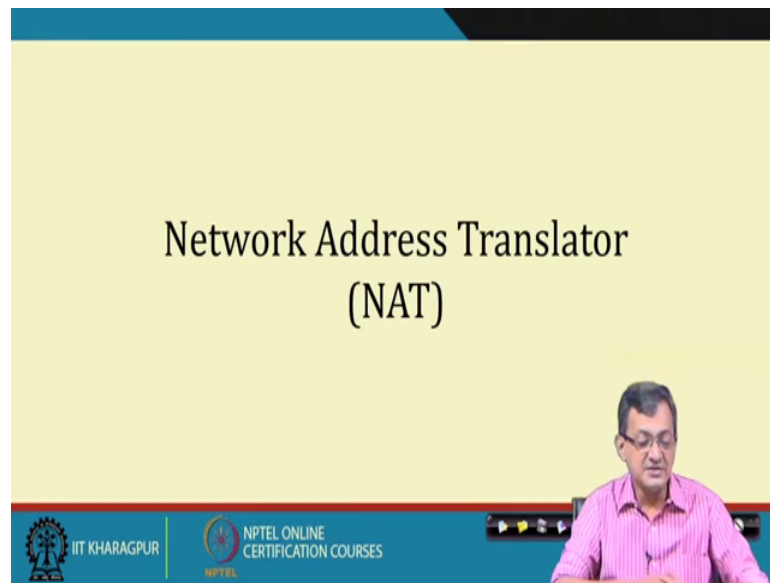
**Functions of a HTTP Proxy**

- Request forwarding
  - Primary function.
  - Acts as a rudimentary firewall.
- Access control
  - Allow or deny accesses, based on
    - Contents
    - Location
- Cache management
  - Efficient utilization of bandwidth.
  - Faster access.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

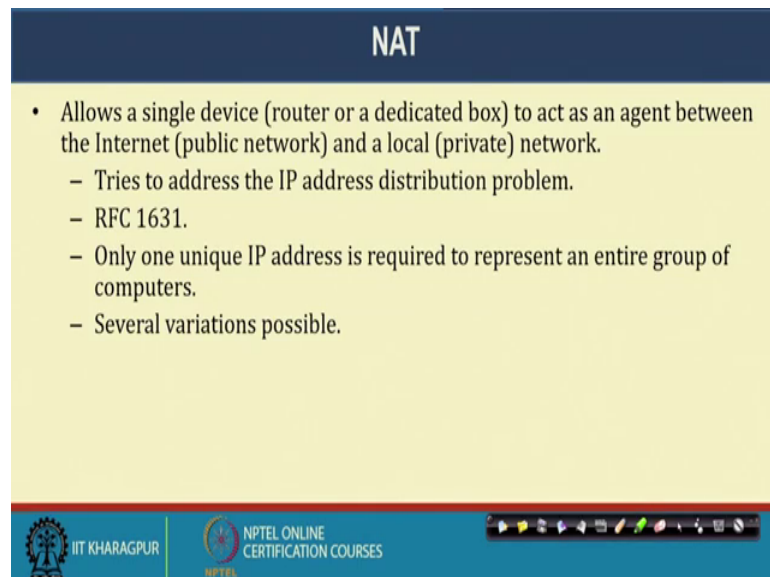
So, this is broadly the how a proxy works, but it though we are primarily looking at the HTTP proxy there can be other type of proxy also, right. So, it is proxying for other services and type of things.

(Refer Slide Time: 24:13)



The next is network address translator. Now, this has been I believe this has been already has been discussed during the in this course specially, when we discussed about the IP and type of things. But, I thought that it may be good to have a quick review of the things to look at the things.

(Refer Slide Time: 24:31)

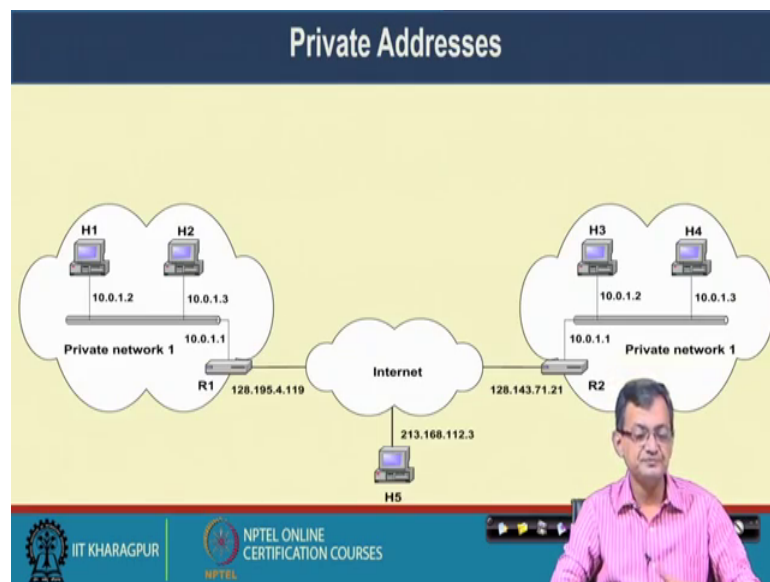


The as the name suggest allows a single device router or dedicator box to access agent between the internet, public network and the local or the private network. So, the it allows it is sort of a single box and it basically map the one IP set to another IP set, right

for that matter IP and proxy to port to another IP an port, so that it can a seamless connection.

So, tries to address the IP address distribution problem so that that you know that to of the IP address like IIT Kharagpur is running on a private IP blocks like that several organisation writing on their private reverse these are non routable. So, this network at this translate a change this IP to a valid IP which is routable and go on and remember that who has connected to this for the particular IP. So, that when the requested come from the client IP plus port and also with the IP port and things goes on. Several variants of this network address translators are possible.

(Refer Slide Time: 25:35)



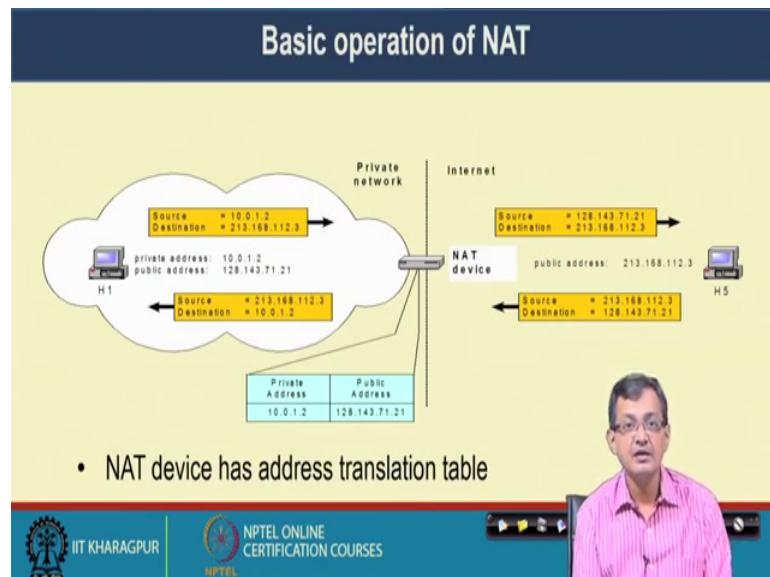
So, this private address space like these are on the LAN see this is a private IP space, this is also private IP space. Incidentally they are using same IP blocks and, but so, if it is on the in a routable scenario this could have been IP class and it would have been gone for a spin. But, here what we are doing from there is there is something which translate this IP to a valid IP is goes on and if it is going there it also take a IP translate the IP and get that equivalent or the translated IP to access the private IP of the other network.

So, this will be this there is some again small type of there should have been private IP network 1 private IP network 2, so, that it access. So, the H 1 accessing H 3. So, 10 dot time series dot 1 dot 2 are mapped to this IP, this carries over this IP again remap to H 3

means to this particular IP address right. So, though both are 10 dot time series dot 1 dot 2, but there are different IP blocks.

Now, so, while communicating across the network. So, these are NATed or translated to this particular IP which is a routable and cross there and this also IP of this interface and goes into the thing. Now, multiple things like H 1, H 3, H 2 can simultaneously do because of their having that mapping with the port number. So, it is it is mapped appropriately at the by the NATer. So, when the request comes back it knows that where to be delivered.

(Refer Slide Time: 27:23)



Now, basic operation of the net as we are discussing. So, this source IP, destination IP goes on. So, it is the mapping goes on and it goes on into the system. So, this is private IP, public IP NATing is being done out here, right. So, it comes with a 10 dot 0 dot 1 dot 2 this one and goes out with a 128 143 721. While it is coming up looking at this public IP stuff it map it to that particular IP like here 10 dot 1 dot. So, it comes with 128 143 721. So, it was having a mapping of this and goes on doing this. So, it is a mapping.

(Refer Slide Time: 28:07)

Source Computer	Source IP address	Source port number	NAT IP address	NAT port number
A	10.5.17.112	500	203.11.16.5	1
B	10.5.17.85	75	203.11.16.5	2
C	10.23.10.5	2480	203.11.16.5	3
D	10.22.5.118	1120	203.11.16.5	4

So, IP device had address translation table so or ATT like typically this is address translated table source is computer A, source IP this one, source destination NATing IP is this one at port number 1. So, it is NATed and this stable is maintained and so that it can basically this differ where from the request came and who will get the thing.

(Refer Slide Time: 28:27)

- Maximum number of concurrent translations:
  - Mainly determined by the size of the memory to store the ATT.
  - Typical entry in the ATT takes about 160 bits.
  - Memory size of 8 Mbyte will support about  $8 \times 1024 \times 1024 \times 8 / 160 = 4,19,000$  concurrent translations.

So, capability of NATing maximum number of concurrent translator is a one thing, like it can concurrently do typically mainly determined by the size of the memory to store typically determine ATT takes over 160 entry of a 160 bits. So, memory size 8 bit we

will support around so much concurrent connection which say pretty high for any organisation.

(Refer Slide Time: 28:51)

### Main uses of NAT

- Pooling of IP addresses
- Supporting migration between network service providers
- IP masquerading
- Load balancing of servers

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Main uses pooling of IP address supporting migration from network service providers. So, when IIT, Kharagpur today change the IP it does not have to change the internal IP block. So, it is a private IP and still there and IP masquerading is another challenge, load balancing of the server is definitely need of the our.

(Refer Slide Time: 29:15)

### Concerns about NAT

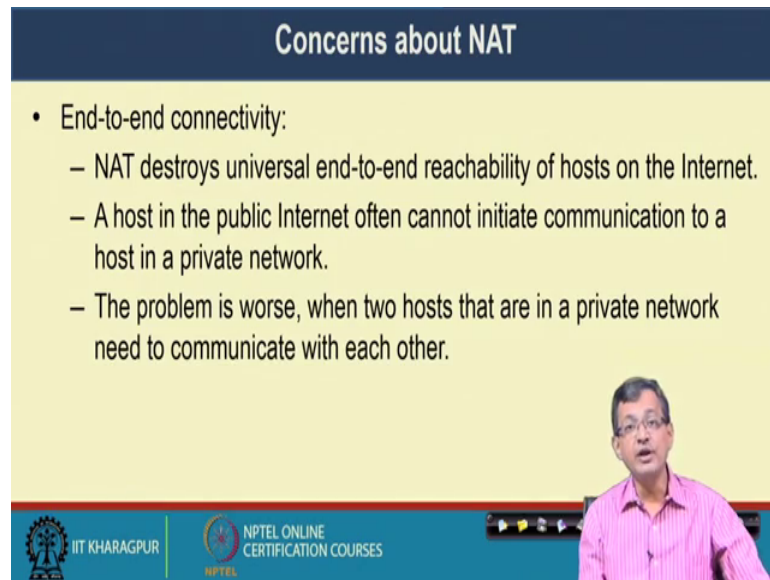
- Performance:
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum.
  - Modifying port number requires that NAT boxes recalculate TCP checksum.
- Fragmentation
  - Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES



There are some of the concern performance as there is a one hub, there is a performance issue. Fragmentation care must be taken to datagram for fragmented before reaching the device. It is not design for different IP address different port number etcetera. So, that the fragmentation is a challenge.

(Refer Slide Time: 29:33)



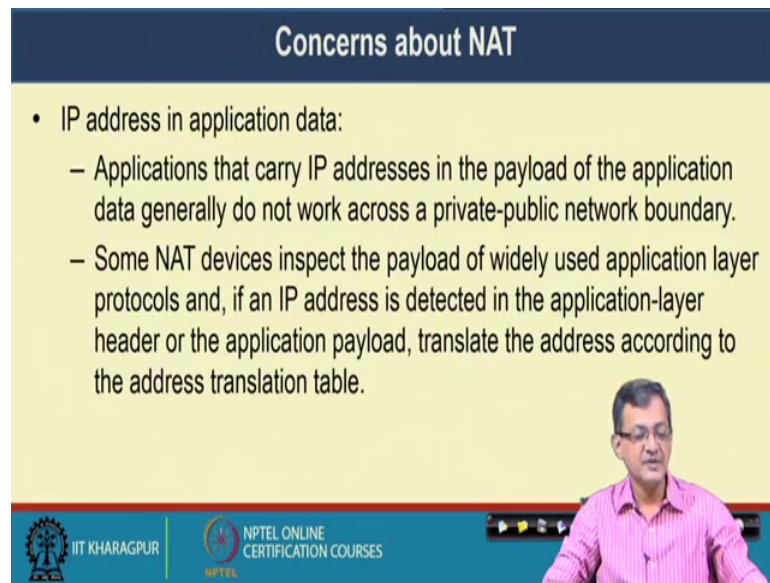
**Concerns about NAT**

- End-to-end connectivity:
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.

The slide includes a video inset of a man in a pink shirt speaking. At the bottom, there are logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES.

End-to-end connectivity is destroyed by the thing, right. So, you have a another hub into the things. So, NAT destroys the universal end-to-end reachability of the hosts in the internet a host in the public internet often cannot initiate communication to the host in the private internet. The problem is worse. So, in the two hosts are in the private internet need the communication with each other. So, there are two hubs as we have seen right here the NATer at the other end.

(Refer Slide Time: 29:57)



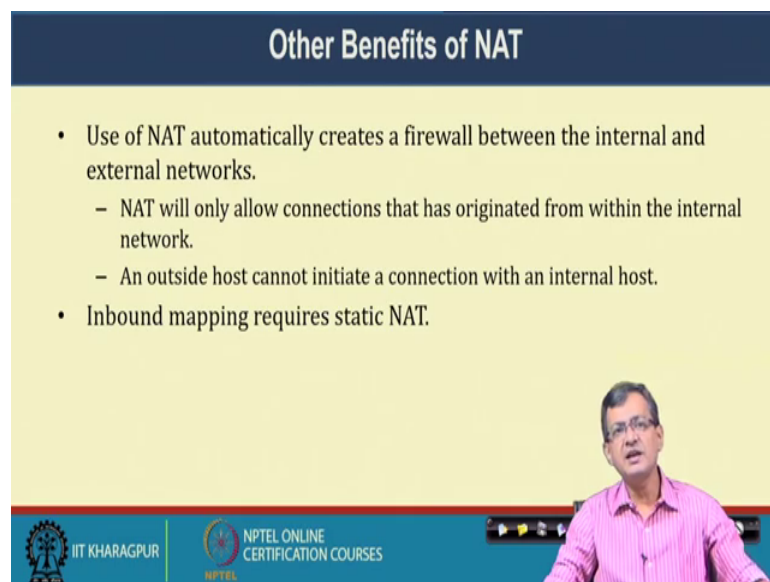
### Concerns about NAT

- IP address in application data:
  - Applications that carry IP addresses in the payload of the application data generally do not work across a private-public network boundary.
  - Some NAT devices inspect the payload of widely used application layer protocols and, if an IP address is detected in the application-layer header or the application payload, translate the address according to the address translation table.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, IP address in application if it is there. So, that if the application carries the IP address this NATer is destroyed application to carry IP address in the payload of the application generally do not work well with this public private NATing thing.

(Refer Slide Time: 30:13)



### Other Benefits of NAT

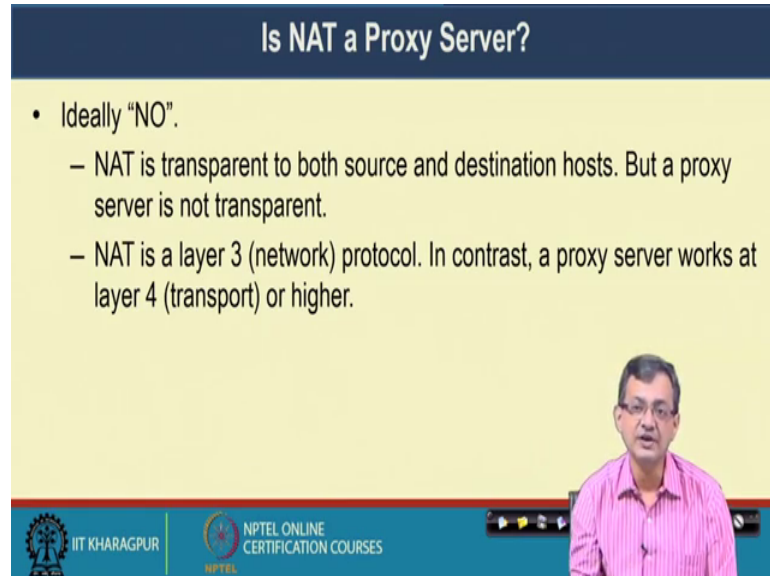
- Use of NAT automatically creates a firewall between the internal and external networks.
  - NAT will only allow connections that has originated from within the internal network.
  - An outside host cannot initiate a connection with an internal host.
- Inbound mapping requires static NAT.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

And, there are several other benefits use of NAT automatically creates a firewall between the internal. So, it is a security benefit. So, this IPs and never exposed NAT will allow only the connection that are originated from within the internal to NAT you can device that method on this that approach an outside host cannot initiate a connection with the

internal host right directly. So, inbound mapping required say static NATing. So, if you want to this IP to think we require static NATing.

(Refer Slide Time: 30:43)



The slide is titled "Is NAT a Proxy Server?" and contains the following text:

- Ideally "NO".
  - NAT is transparent to both source and destination hosts. But a proxy server is not transparent.
  - NAT is a layer 3 (network) protocol. In contrast, a proxy server works at layer 4 (transport) or higher.

The slide also features a video inset of a man in a pink shirt and a footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES.

So, finally, is NATing a proxy server? No, ideally no. NAT is transparent to both the source and destination host, but proxy is not always transparent to the things, right. You know that where the proxy server NAT is primarily a layer 3 device it is a network at this protocol though we have a port number, but it is a primary NAT 3 NATing IP addresses, right. So, in contrast proxy is primarily layer 4 or layer 4 plus device. So, it is more at the other end of the things, right.

So, with this let us conclude our discussion today. Finally, we will like to see at on the security network security part that what are the different aspects with respect to the different layers of the TCP IP or OSI layer and some aspects of firewall and so and so forth.

Thank you.