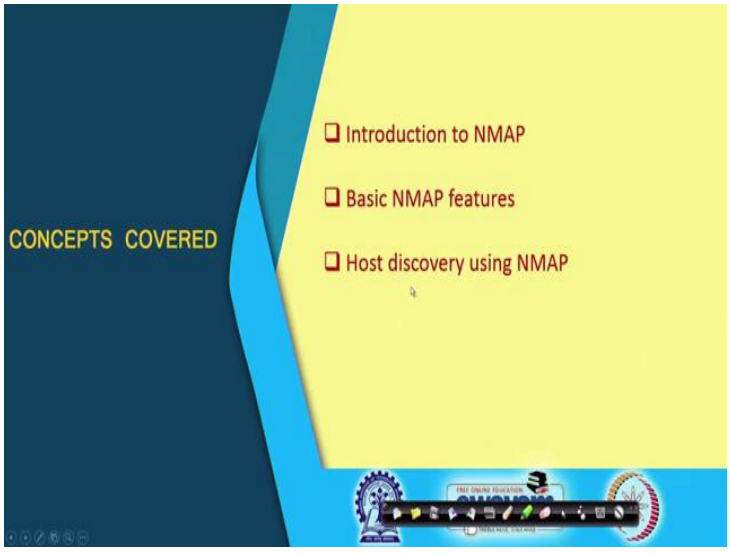
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 56
The NMAP Tool : A Relook (Part - I)

The NMAP tool as you have seen is a very important tool, which is available to the ethical hacker or hacker whatever you say. The tool can be used for a variety of purposes with respect to network discovery, host discovery, OS discovery and so on so forth. So, you have already seen some demonstrations on NMAP; but what we shall be doing over the next three lectures?

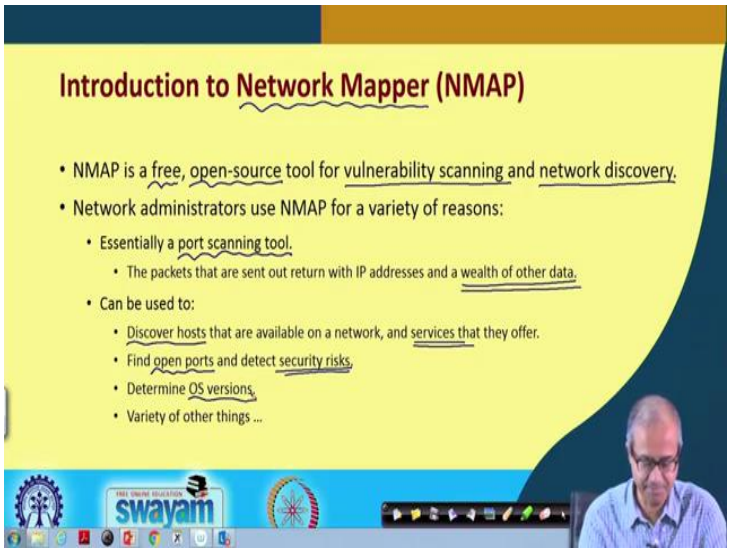
We shall be talking more formally about the NMAP tool, the different commands and some explanations about how some of those commands work ok.

(Refer Slide Time: 01:03)



In this first lecture of the series “The NMAP Tool : A Relook” here we shall be mainly talking about, firstly, what NMAP is, what are the basic features, and in particular we shall be looking at the some of the more commonly used commands which relate to host discovery ok.

(Refer Slide Time: 01:20)



So, let us start with this; first talking about the NMAP tool; NMAP is the short form for the Network Mapper. So, it helps an individual or a person to create the map of a network. Now, what do you mean by map of a network? You see map in a atlas what does it contain? It contains all the geographical detail; it contains not only information about the cities and the towns, but also it contains information about the roads, rivers, hills and other things.

Similarly, when you are doing network mapping, you are gathering a lot of information about the network to know about what are the hosts which are there; which are the host which are active; what are the ports which are currently open and so on and so forth. This is what network mapping is all about. And the good thing about NMAP is that it is freely available; it is open source. So, actually you can have the access to the source code also and you can make modifications if you want.

And this is very widely used particularly for vulnerability scanning and also for network discovery or network mapping ok. Now, basically the NMAP is a something called a port scanning tool; you look into the ports at the transport layer level and find out what ports are open. Now, let us very briefly try to tell about what do you mean by saying that a port is open. Let us say I have a computer system which is running a lot of, a number of services at the TCP or UDP layer level. Let us say some services are at, let us take some examples Telnet, FTP, mail, SMTP, HTTP and so on.

So, what does the services mean? They mean that there is a server program already running in the background, which is listening to a particular port number. For example, for Telnet it will be listening over port number 23; for HTTP it will typically be listening over port number 80 and so on.

So, whenever there is a request coming over that particular port number, the request will be forwarded to that particular server program. This is what you mean by a port is open; that means, the corresponding server program is currently active, running and is listening for some incoming request on that port. But, if the server is shut down, we are not running the server; we say that the machine is up but that particular port is closed ok.

So, basically NMAP is a port scanning tool; the packets are sent out to different hosts in the network and you can gather a wealth of information about the network, about the hosts based on what you get ok. We shall see some of these. This NMAP tool can be used firstly, to discover hosts, what are the hosts, their IP addresses or other things whatever, they are active on the network. And what kind of services they offer; services mean as I had said that port number; the servers that are running on those ports ok.

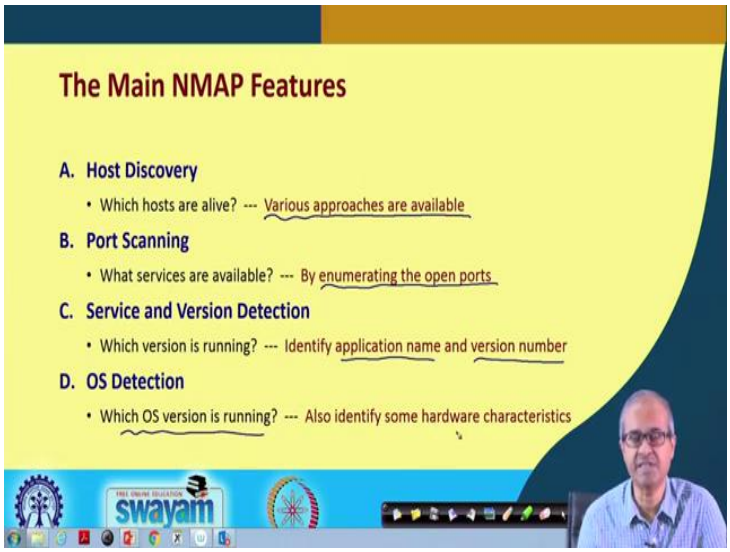
Related, find open ports; some of the ports if they are left open, there are known vulnerabilities or security risks; that means, there are well publicized exploits, you can run those exploits to break into the system through those open ports. So, if you have a list of open ports then you can also know what are the security risks involved. You can know about the operating system versions and various other things ok.

(Refer Slide Time: 05:25)

This NMAP tool was first developed in the year 1997 by a gentleman called Gordon Lyon. And there is a website **nmap.org** where lot of information and resources are available on NMAP. There are very good tutorials available on NMAP there, where we can get the details of the all the commands, their meaning and lot of examples. Since 1997 several NMAP versions have released, have been released. So, in general when you, when after installing NMAP on a machine, when you want to run it, here I am showing that how to run it on a command prompt. There are GUI versions also available; you can run through a GUI.

The command is **nmap**, then there are a number of optional things; you can specify what kind of scan you are trying to do; there can be various options you can specify. And you can tell which host or which network you are trying to scan; you can also, so, broadly there are three things you specify what is the type of scan, what are the options that you want to exercise for scanning and what are the hosts or networks that you want to include in this scan ok.

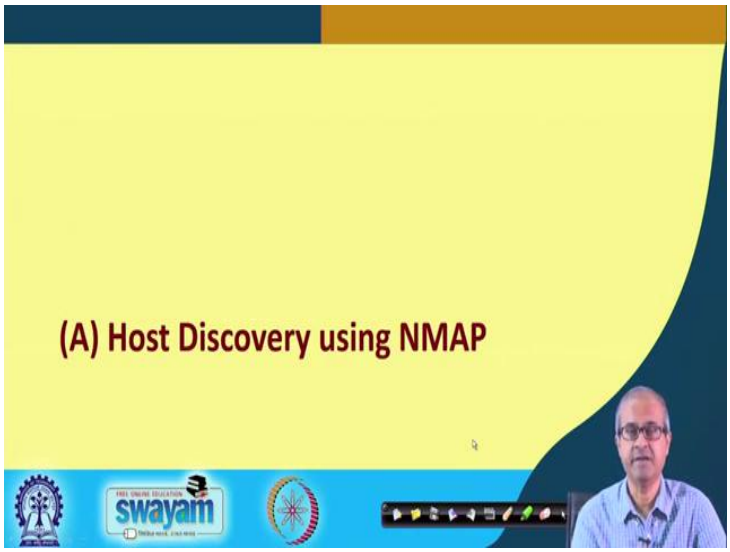
(Refer Slide Time: 06:47)



Talking about the features that NMAP provides, broadly speaking there are four features you can say. First is of course, the first and foremost host discovery. Here you are trying to find out which hosts on a network are currently alive. Here again various ways you can do; there are various approaches; some of them we shall be discussing. Next comes port scanning; after you have detected which hosts are up and running; they are alive; you try to find out what are the services which are currently running on that on those hosts; that means, which are the port numbers; which are open?

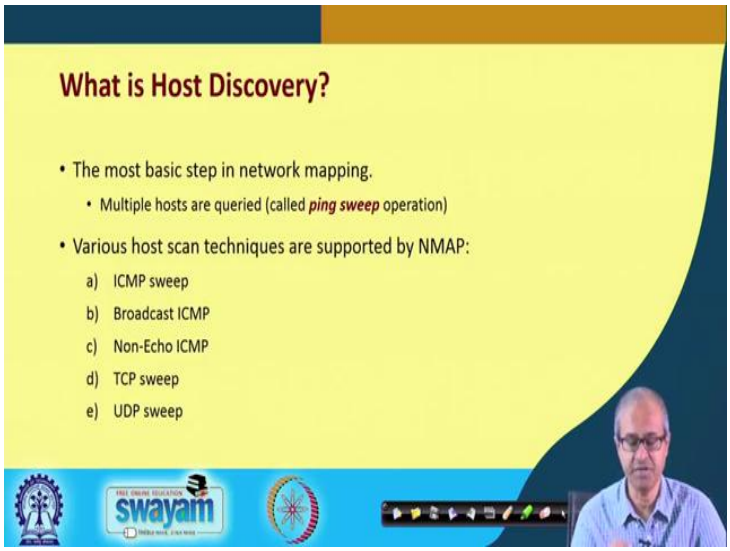
So, you can enumerate the open ports and you can find out the services; because open port means the services are running ok. Then you can look at a number of service and version types; you can detect them that which version is running; you can specify application name and also their version numbers. Like for example, if there is a web server running, you can also get information about which version of the web server is running on a particular machine and finally, operating system detection. So, you can get information about which OS version is running on a particular host or a machine. And it can also identify some other characteristics at the same time fine.

(Refer Slide Time: 08:21)



So, we look at specifically in this lecture about the host discovery features that are supported by NMAP.

(Refer Slide Time: 08:29)

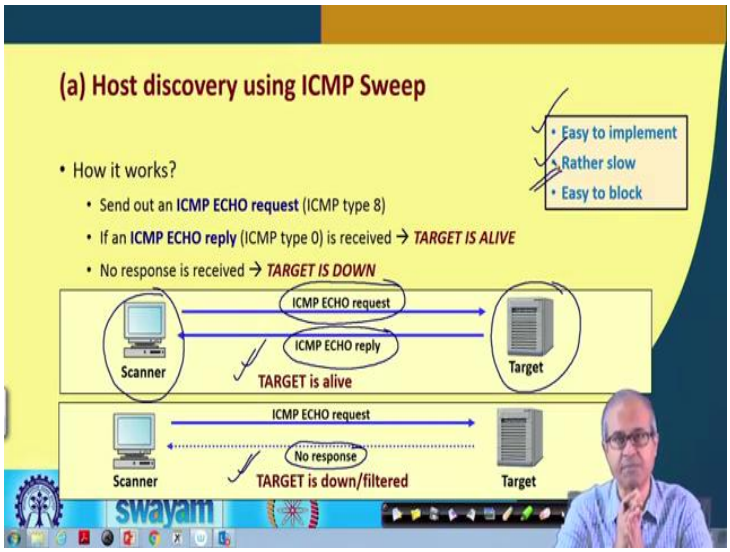


So, let us look at it; first let us try to understand what do you mean by host discovery? Host discovery means to detect which are the hosts that are currently active in a network. And this is the first and foremost step that you need for any hacking attempt; whether it is ethical hacking or non ethical hacking; whatever, you do; the first step is host discovery. You must understand, what are the hosts that are currently active in a

network? Now for this purpose you have to query; send some query packets to multiple hosts; sometimes generically we call it as ping sweep operation.

But this may not be always be the ping command you are sending; but sometimes you call it as ping sweep; as if you are pinging the different hosts to find out which of them are alive. There are various kinds of techniques that are available under NMAP through which you can try and discover a host; these are listed here ICMP sweep, broadcast ICMP, non-echo ICMP, TCP sweep and UDP sweep. We shall be explaining these methods briefly in subsequent slides.

(Refer Slide Time: 09:43)



So, we start with ICMP sweep; let us understand what this ICMP sweep means. You know that ICMP is a protocol which is running in a network; this ICMP requests and responses can be used to find out whether a host is alive or not. There is something called ICMP echo request packet; in an ICMP packet there are many request types; this ICMP echo request corresponds to type 8. So, in the type field of the packet the number 8 is stored ok.

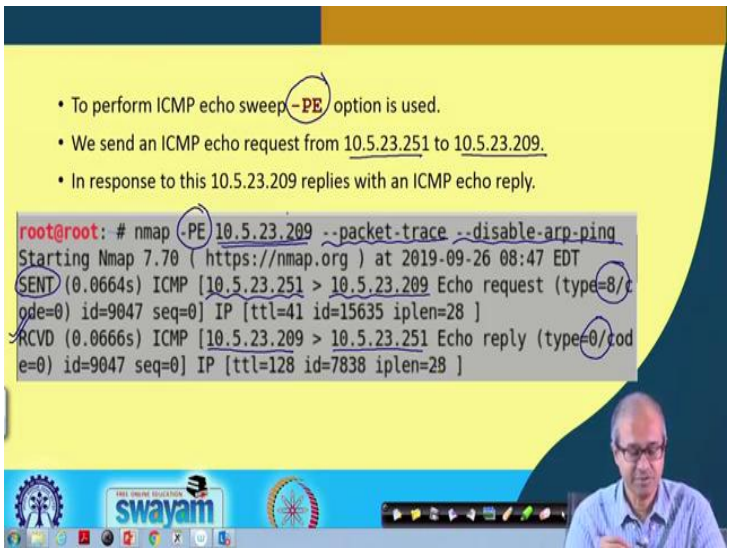
So, the thing is that the host that you try to discover, you sent an IP echo request packet to that host; what the host will do? The host will possibly be sending back an ICMP echo replay like packet is active if it is alive and this echo replay packet is of type zero; these are all ICMP packet types. So, if you receive the echo replay packet, then your

conclusion is the target is alive; but if you do not see that the targets, that the response is coming, no response is obtained, then you conclude that the target is down.

Now pictorially I am trying to depict it here; suppose you are here; you are trying to scan a particular target host out here. So, you sent an IP, ICMP echo request packet; the target if it is open running, it will send back an echo reply packet; your conclusion is target is alive. But, if you find that there is no response from the other side, then you conclude that the target is either down or there is a firewall or router which is filtering you requests; there are firewalls you can which can filter this kind of ICMP echo request packets.

So, it is either it is down or it is filtered. Now the good thing about the ICMP sweep host discovery is that this is easy to implement; but because you have to sent individual packets to all the hosts this is slow; if there is 1000 hosts, you will have to send 1000 packets and it is relatively easy to block. Firewall or router you can configure it easily to block this kind of packets so that you cannot mount this kind of approach or host discovery.

(Refer Slide Time: 12:18)



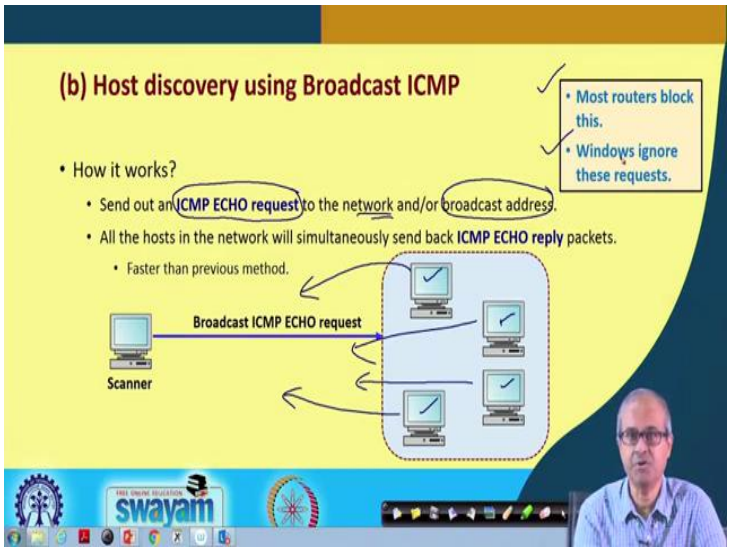
So, here we have an example; to carry out this ICMP echo sweep you will have to use "**-PE"** option with your NMAP command. In this example you see, we have given **nmap -PE**, then we specify the IP address of the host ok. And we specify some options packet-

trace, disable-arp-ping. Packet trace means, we want to get some details about the packets going and coming.

So, the details are printed and disable-arp-ping is, arp-ping is also one of the methods for discovering hosts. And of course, arp-ping you can use only inside a LAN; across LANs you cannot use it. So, sometimes we usually disable arp-ping by giving a command like this. So, you see what happens; it sends a packet; this is an ICMP packet; you see; this is a type 8. So, it is going from this host; it is going, suppose you are, I mean your IP address is 10.5. 23.251; you are sending the packet to the, this target 209.

So, from this you are sending it to this. So, this is your machine. So, id, sequence number, the IP packet, time to live, id, the length of the packet all these things are printed; because you have given this packet trace option. And you can also see the received packet; there is a packet which is coming back; from the target machine it is coming back to my machine. And reply packet as I had said, is of type 0; type 0 is printed and also ids, the time to live, id, IP length etc. So, if you see that responses coming back, then you can conclude that your, the particular IP you are trying to query, discover is up ok.

(Refer Slide Time: 14:34)



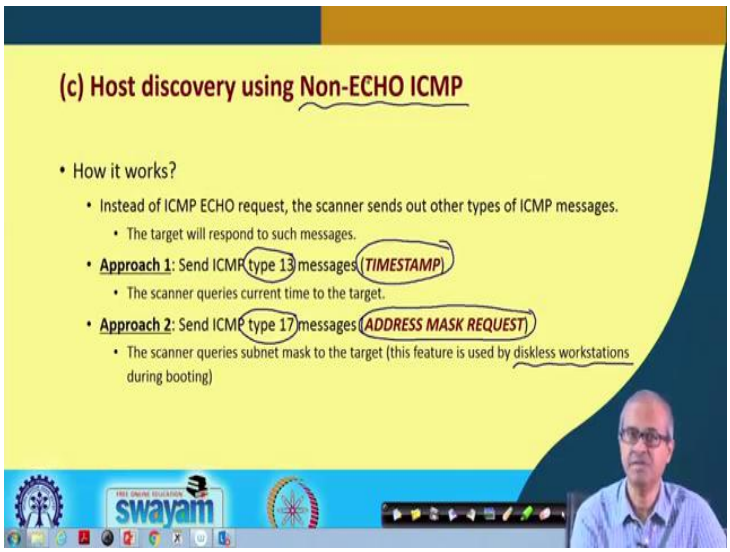
So, there is a faster method available; you can also use this using the same kind of commands; the idea is as follows. Here you are trying to use broadcast ICMP features; what is broadcast ICMP? Well, here also you are sending an ICMP echo request packet;

but you send it not to a particular host, but to a broadcast address or a network address; what will happen? That this scanner; that means, you are sitting here; that whatever echo request packet you are sending, that will be going to all the machines at the same time; it will be a broadcast.

And when this kind of echo request packet reaches all the machines, what will happen? All these machines will be responding back. So, this scanner will be receiving all the responses at once. So, you will be getting information about all the hosts all together. So, this method is faster; but the problem is that most of the routers, they block this kind of requests. Most routers will block this; also Windows, if you are running Windows operating system on the target machine, Windows usually ignore requests which are coming with the broadcast address.

So, responses will not be sent. So, this method all though theoretically looks good, but many a time it does not work; because the machine or the router will block this kind of broadcast request packets. Because they might indicate that some kind of attack is going on and this system administrator might have disabled those options ok.

(Refer Slide Time: 16:30)

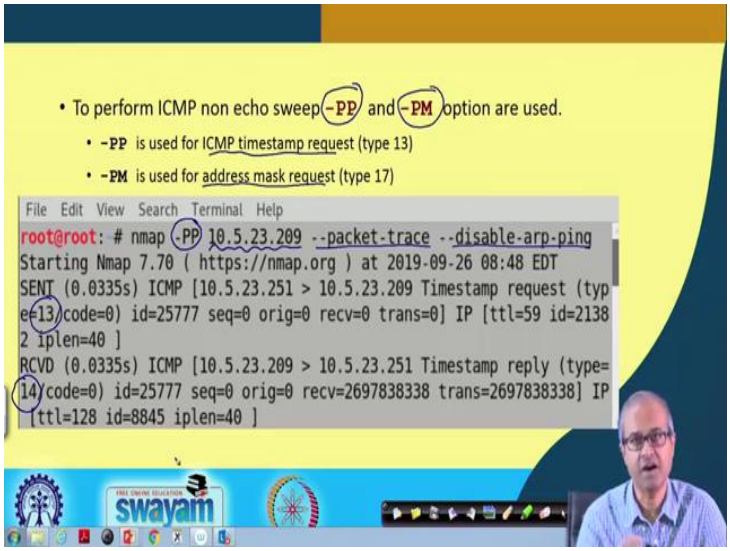


So, instead of sending echo kind of packets, there is another way you can proceed; you can send something, some kind of non-echo ICMP packets which are not echo request and echo replay, other types. Well, two types of such packets you can send; one is called timestamp packet; other is called an address mask request packet. Timestamp packet has

type 13; address mask request is of type 17. The idea is that both this requests when you send it to a host, the host will respond back for the first case with timestamp information and for the second case with some information about the subnet mask.

The second one, this address mask request is typically used by diskless workstations which does not have an IP address or subnet mask allocated to it. So, it will be sending a query to a server whenever it boots up; it will be getting subnet mask from there and from there it will start the network services ok. So, there are broadly two approaches; timestamp or address mask request using which you can mount this kind of non-echo ICMP requests to discover a host.

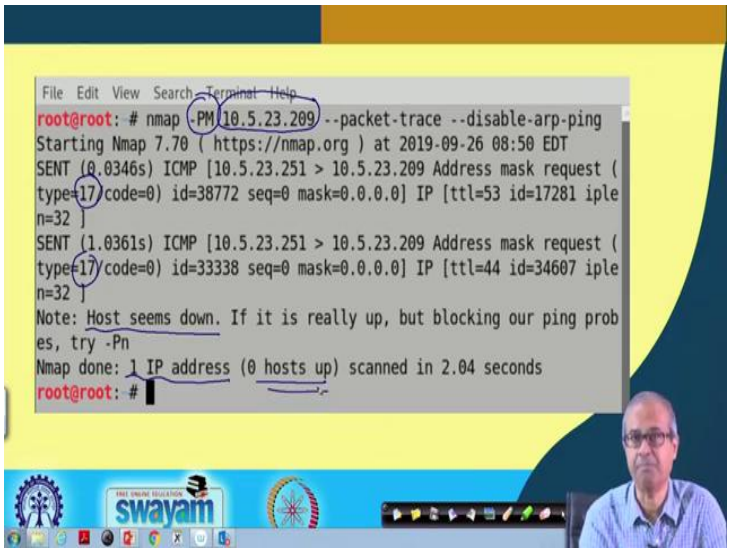
(Refer Slide Time: 17:55)



So, let us see how you can do it. There are two options you can use "**-PP**" or "**-PM**"; "**-PP**" is stands for ICMP timestamp and "**-PM**" stands for this address mask request that I have said. So, here an example is shown with the "**-PP**" option; here we are running **nmap**; we are trying to query this particular host; IP address is specified. Well, again we are trying to trace the packet and we are disabling arp-ping ok.

So, this is not an IPMP echo, I have mean the ICMP echo request packet. So, you can see, here type 13 is specified. So, it is timestamp request packet and the responds which is coming back; responses will always be of, this is type 14. So, in response to type 13 the response comes back of type 14. So, this kind of response it comes; you conclude that the host is up and running.

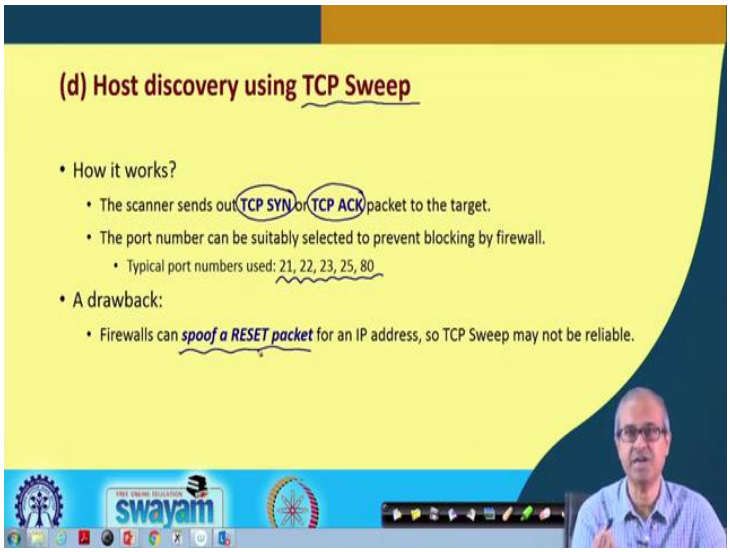
(Refer Slide Time: 19:09)



Similarly, for the address mask request you can give this kind of "**-PM"** option. The rest looks same; let us say, we are querying this particular host, packet trace, disable-arp-ping same kind of options. So, here again you see, here you are sending an ICMP packet whose type is 17; 17 means address mask request ok. And well you are sending another request. So, multiple requests are being sent; two requests are being sent, because response was not obtained; if there is no response, it will do some kind of a time out and it will try again.

So, the final conclusion is host seems down; no response is obtained ok. Well, the host may not, may or may not be actually down; may be some filter is filtering out the request; that is also possible. So, you have to try different kinds of host discovery options; sometimes to bypass the firewall or router if they are trying to prevent this kind of host discovery ok. So, it says that one IP address scanned, zero hosts up alright.

(Refer Slide Time: 20:31)

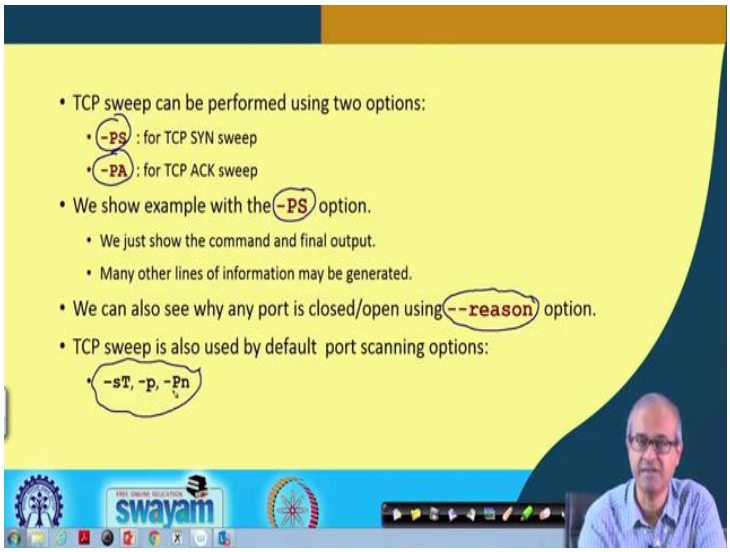


So, there are other methods also; there is a method that uses TCP sweep. The idea is very simple; this scanner, that means, the person is trying to discover will be sending out **TCP SYN** or TCP acknowledge packet. That means, a TCP packet with the **SYN** flag set to 1 or the **ACK** flag set to 1. So, if such a packet is send to a server, it may mean that someone is trying to establish a connection. So, the server will usually send back response packet to try and complete that connection.

Usually when this connection request is send, some of the popular port numbers are used; because normally these port numbers are open on most machines; 21, 22 are for FTP; 23 is for telnet; 25 is for SMTP and 80 is for HTTP ok. But drawback is that firewalls can again block this kind of ping; that means, it can change the IP address spoof or reset packet for an IP address. For some particular IP address if you send a connection request the firewall can reset the connection; because I can set my firewall in such a way that I will not allow any incoming request to some particular hosts.

So, for some cases such a request can be terminated by sending back a connection reset packet. So, that you will not know whether that particular host was up or not; it is the router or the firewall which is sending you back the reset packet ok.

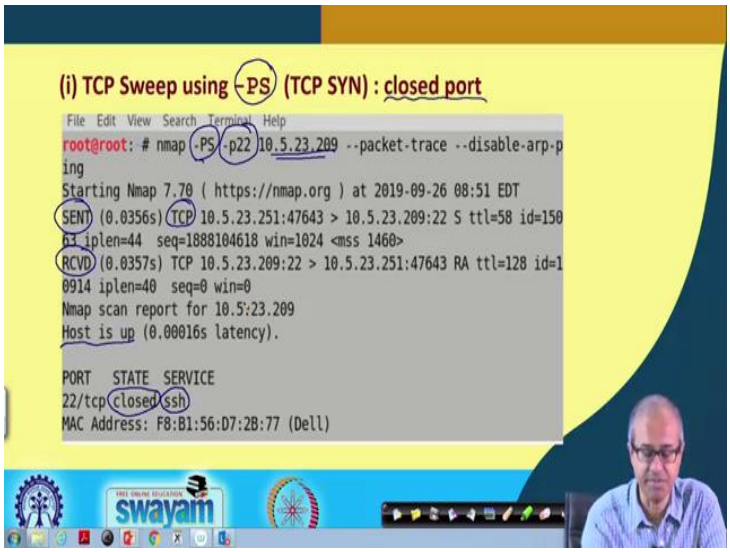
(Refer Slide Time: 22:22)



So, for TCP sweep there are two different options, you can use ok, "**-PS**" or "**-PA**"; "**-PS**" is used for TCP SYN; it will be sending a TCP SYN packet; "**-PA**" will be sending a TCP acknowledgement packet. Well, we show some examples with the "**-PS**" option; "**-PA**" will be very similar ok. So, there is another thing to point out. So, when you give these commands, you can also specify an option "**- -reason"**.

This option will give you some kind of justification that why some conclusion it is in drawn that a port is open or closed. So, reason will give you some justification that why this is happening. Now, TCP sweep is not used only for "**-PS**" and "**-PA**"; there are other options also like **-sT**, **-p**, **-Pn**; here also this TCP sweep kind of host discovery option is used.

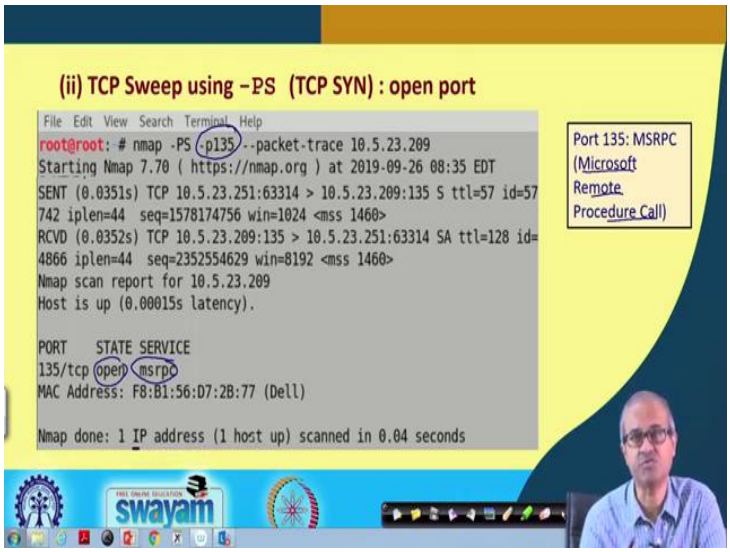
(Refer Slide Time: 23:37)



So, let us see some examples here; here we are using "**-PS**", TCP SYN where the particular port that we are querying is actually closed; let us see. So, we are running **nmap** with "**-PS**"; we are specifying port number 22; **-p 22**, this option specifies that we are trying to look at whether port 22 is open or not and then we specify the IP address. So, you see some packet is send; this is a TCP packet; we just send of type TCP and some response is coming back right.

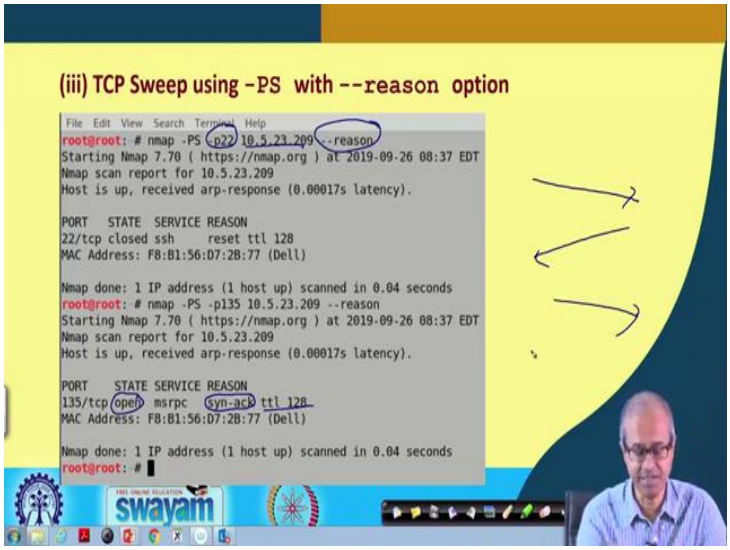
And this response is specifies that this particular thing is closed; this port number 22 actually stands for secured shell, **ssh**. So, for **ssh** the port number is actually closed right. So, by looking at the different headers in the file you can conclude that ok. The host is up; the responses coming back; but that port number is closed; that means, when you are sending a connection request, it is not sending you back the request for the acknowledgment; rather it is trying to reset the connection. So, by looking at the flags you can conclude that.

(Refer Slide Time: 25:09)



Similarly, for an open port, if it is an open port, let us say here we are trying to query port number 135 which is Microsoft remote procedure call, that service. So, similarly, you sent a packet, receive a packet and you can see that the port is open; the service name is **msrpc**. So, one IP address, one host up you can see these things ok.

(Refer Slide Time: 25:38)

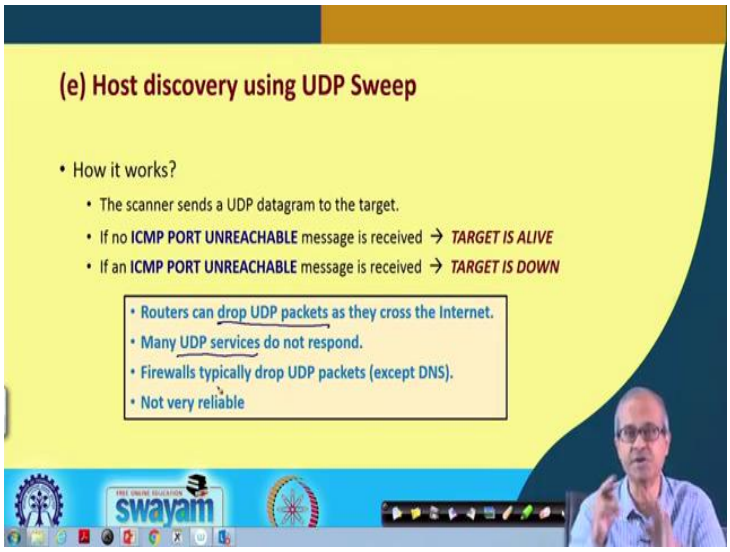


So, there another example I am giving with this reason option. So, here we are giving this reason option; we are scanning a host with port number 22. Well, for this particular

machine the port number 22 was open; this state is open; final conclusion it is open. And the reason is we have received the syn-ack with the time to live 128.

So, the reason is also mentioned; why you are concluding this; that means, after sending the ACK signal, you recall in TCP there is a three way handshake; you send a SYN; you get back a SYN-ACK. So, the other side is up; that is why you conclude that the host is up.

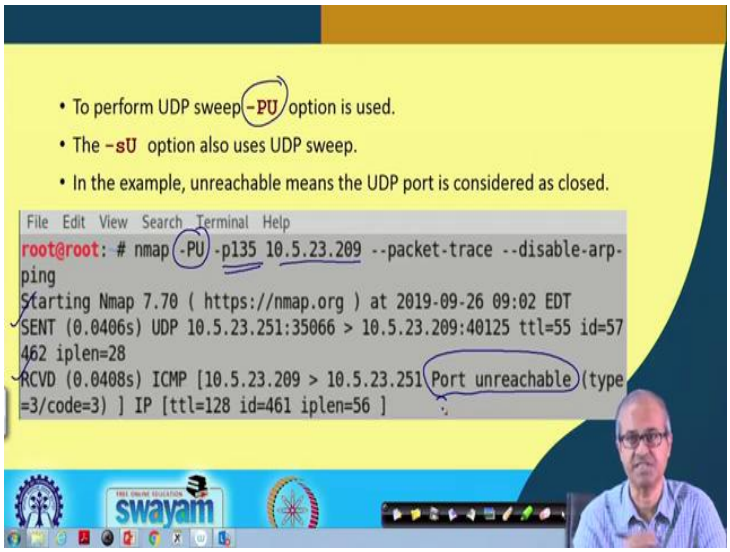
(Refer Slide Time: 26:31)



You can carry out this kind of host discovery also using UDP sweep. UDP sweep is simple; you simply send a UDP datagram to a target. So, whenever a UDP packet is send, the target host will be responding back with an ICMP port unreachable message; either it is received or it is not received. If no such message is received, then you say that the target is alive; but if the target is not alive, then such a packet will come back to you; then you say that the target is down.

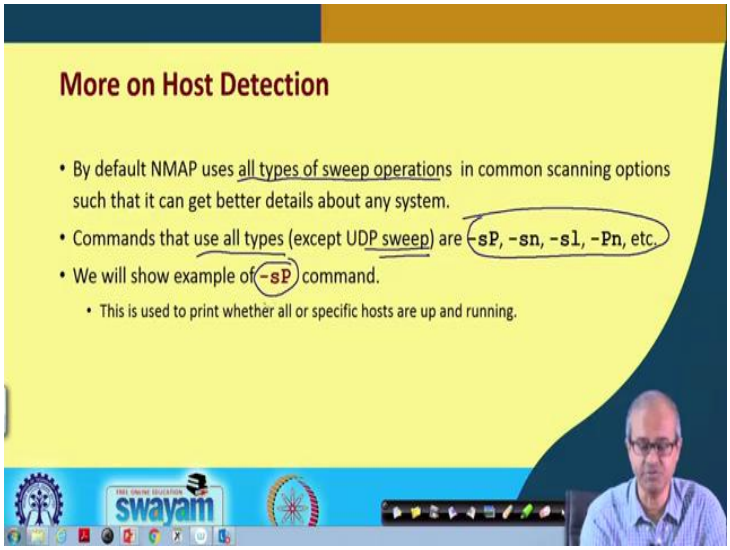
But the problem is that this is again not reliable; because many routers can drop UDP packets when they cross a network boundaries, from one network to another. And, many UDP services are there which do not respond to this kind of ICMP port unreachable messages. So, this is not a very reliable way to discover a host. And, similarly firewall drops UDP packets; because UDP packets are meant to be used inside a network only, not outside the network; so, this is not reliable.

(Refer Slide Time: 27:47)



So, here I am showing you one example using the "**-PU**" option. So, use **PU** you are querying a port number 135 with a particular IP address. You see, you are sending something; you are getting back something, port unreachable message. So, you can say that your, that particular port, UDP port number on the host is down; it is not reachable.

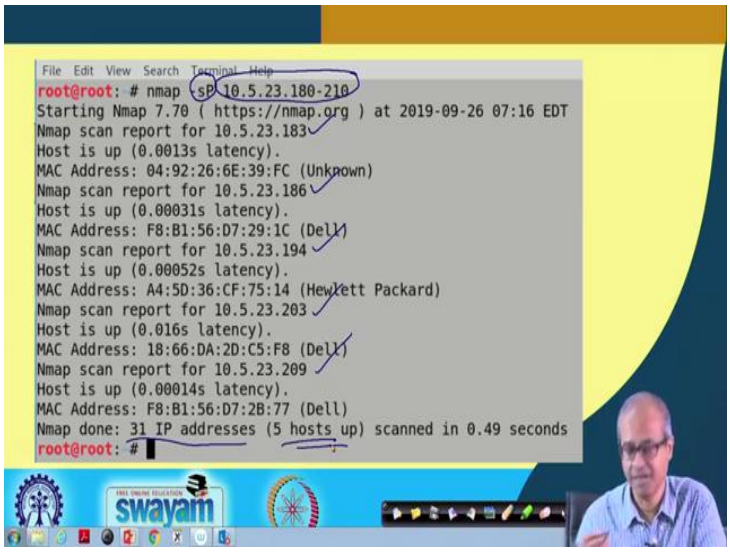
(Refer Slide Time: 28:18)



There are few other things on host detection; the thing is that by default, if you, if you just an NMAP without any flags, it will use all types of sweep operations that are available; it will try to use that, the common types. And, there are some commands like -

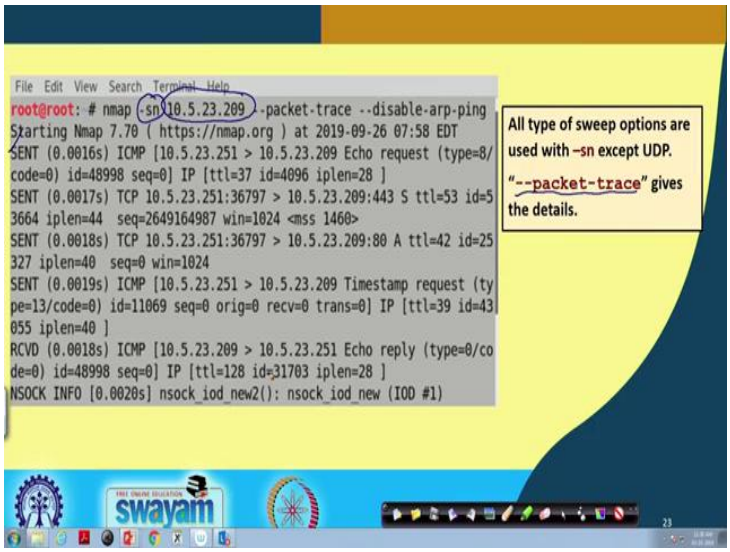
sP, -sn, -sl, -Pn, they use all types of sweep operation except UDP sweep; because UDP sweep is not very reliable as I told you. So, we shall be showing you some examples of one of these "**-sP**"; "**-sP**" is used to print whether some host is up and running.

(Refer Slide Time: 29:06)



So, here you see this example; here we are using this "**-sP**" with a particular hosts; in fact is a range of a IP addresses 10.5.23.180-210; that means, the last byte can be anything from 180 up to 210. So, a block of IP addresses we are scanning. So, you can see that it is generating reports from first several IP addresses from where response has been obtained. So, all of these may not be up; but whatever IP addresses which are up, you get those information. So, out of those 31 IP addresses, 5 hosts are up ok; you can get this kind of information.

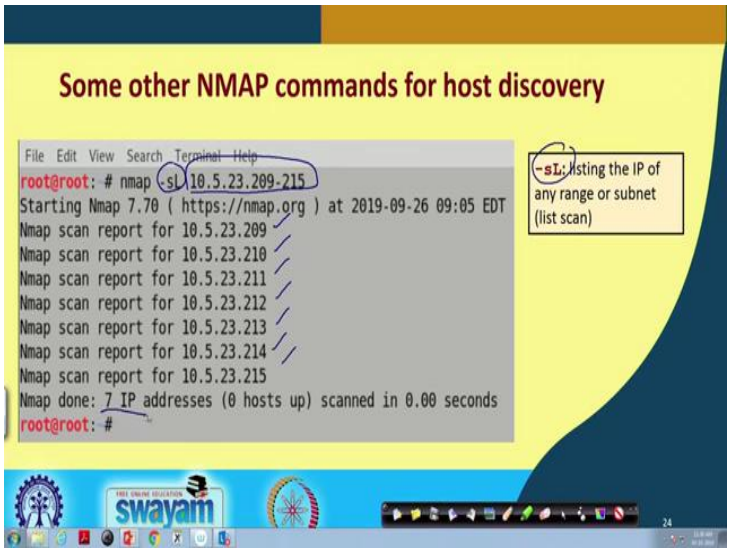
(Refer Slide Time: 29:54)



Similarly, another example, here we are using "**- -packet-trace**" option to get the details. So, here you see, here we are coding one particular host with the "**-sn**" option. Here we are sending the query and we are receiving the query. So, here all the details are obtained; what kind of TCP packet is obtained from which machine to which machine, which port number all those details you can analyze ok.

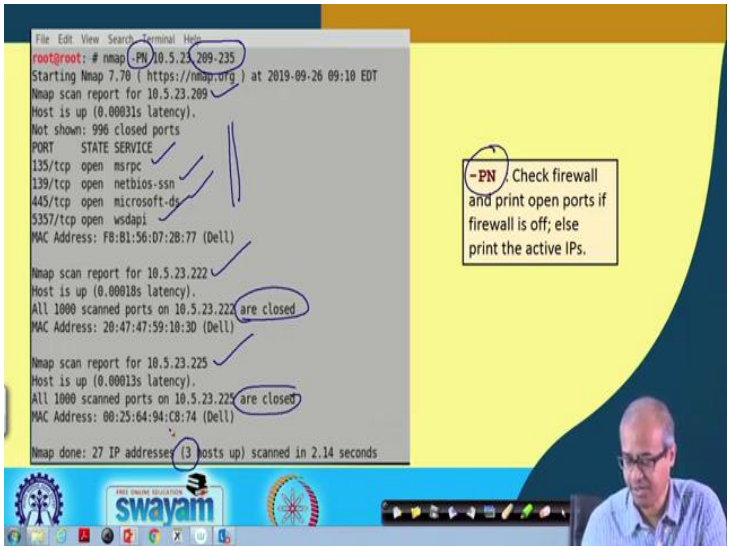
So, if you want to analyze all the details of the packets, I am not going into details; but you can see this. So, from here you can conclude what is actually this status of the connection or status of the host.

(Refer Slide Time: 30:41)



Some other NMAP commands are also there for host discovery; like "**-sL**" you can use; "**-sL**" like here when you specify a range of IP addresses again 209 to 215, it will just scan all those hosts and give you the final verdict. 7 IP addresses, 0 hosts are up; none of them are up; like this you can get.

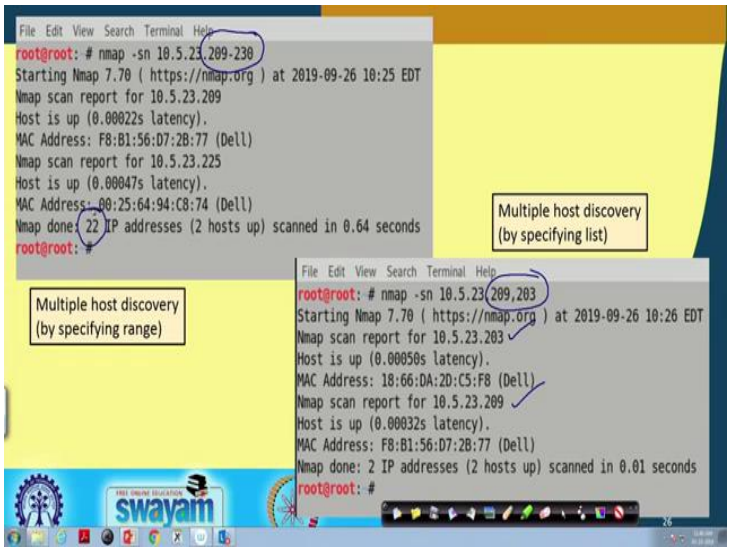
(Refer Slide Time: 31:11)



There is another example with the "**-PN**" option; you are using "**-PN**". So, here again you are using a range of IP addresses. So, you can see here you can get the details that whichever services are up for a particular; this was the IP address; these are the services

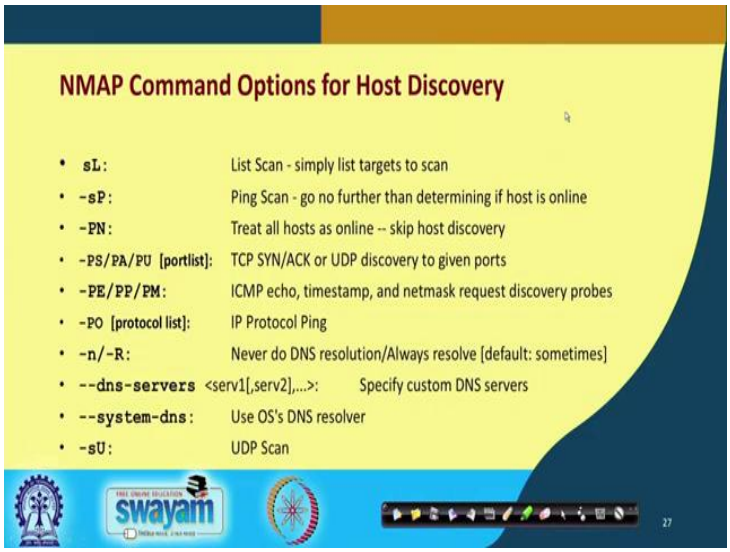
which are up on these port numbers ok. Then for some other IP address host is up; all 1000 scanned ports are closed; none of the ports are open. Say for another IP address you scan all these; they are, they are all closed. So, whenever there are some ports open, those information will be listed. So, out of twenty seven IP addresses three of them are only up.

(Refer Slide Time: 32:06)



Here I am showing multiple host discovery by specifying a range. Here we specify a range; you can specify range or you can specify a list; like you can specify a "**,**" also, **209, 203** which means **10.5.23.209** and also **10.5.23.203**. So, you can see, it is scanning both these machines; but when you specify a range, then all these 22 IP addresses will be scanned. So, these are the different ways you can specify IP addresses during scan.

(Refer Slide Time: 32:45)



These are some of the NMAP command options for host discovery; I am not going into the detail, **-sL, -sP, -PN**. So, if you look into the manual or the tutorials, you will get all details of these commands. So, a brief explanation is also shown on the right ok; these are the different commands which are which are available ok.

So, with this we come to the end of this lecture where we have tried to tell you some of the basics about NMAP. And, we also showed in particular how hosts discovery can be carried out, the different methods. And, exactly what is done; what is the mechanism behind this kind of, this kind of sweep options. So, and also we showed some examples with screenshots; actually how this sweep operations can be actually carried out. So, in the next lecture, we shall be continuing with our discussion with some other options with NMAP.

Thank you.